安全性

Data Infrastructure Insights

NetApp
January 17, 2025

目录

安全性

数据基础架构洞察力安全性

产品和客户数据安全性在 NetApp 至关重要。Data Infrastructure Insight在整个发布生命周期遵循安全最佳实践、以确保以尽可能最佳的方式保护客户信息和数据。

安全性概述

物理安全性

Data Infrastructure Insight生产基础架构托管在Amazon Web Services (AWS)中。Data Infrastructure Insight生产服务器(包括建筑物以及门上使用的锁或钥匙)的物理和环境安全相关控制由AWS管理。根据 AWS： " 物理访问由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外围和构建入口点进行控制。授权人员可利用多因素身份验证机制访问数据中心楼层。 "

Data Infrastructure Insight遵循"共同责任模式"AWS所述的最佳实践。

产品安全性

与发布周期较长的开发方法相比、Data Infrastructure Insight遵循敏捷原则、遵循开发生命周期、因此可以更快地解决任何以安全为导向的软件缺陷。通过采用持续集成方法，我们可以快速响应功能和安全方面的变化。变更管理过程和策略用于定义何时以及如何发生变更，并有助于保持生产环境的稳定性。在将任何有影响的变更发布到生产环境之前，系统会正式传达，协调，适当审核和批准这些变更。

网络安全

在Data Infrastructure Insight环境中、对资源的网络访问由基于主机的防火墙控制。每个资源（例如负载平衡器或虚拟机实例）都有一个基于主机的防火墙，该防火墙仅限制入站流量，使其仅限于该资源执行其功能所需的端口。

Data Infrastructure Insight使用各种机制(包括入侵检测服务)监控生产环境中的安全异常。

风险评估

数据基础架构洞察力团队遵循正式的风险评估流程、提供一种系统、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管理。

数据保护

Data Infrastructure Insight生产环境是在高度冗余的基础架构中设置的、该基础架构会对所有服务和组件使用多个可用性分区。除了利用高可用性和冗余计算基础架构之外，还会定期备份关键数据，并定期测试恢复情况。正式的备份策略和程序可最大限度地减少业务活动中断的影响，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，充分地恢复这些策略和程序。

身份验证和访问管理

所有客户对Data Infrastructure Insight的访问均通过https上的浏览器UI交互完成。身份验证通过第三方服务 Auth0 完成。NetApp 已将此作为所有云数据服务的身份验证层进行了集中处理。

Data Infrastructure Insight遵循行业最佳实践、包括围绕对Data Infrastructure Insight生产环境的逻辑访问的"最低权限"和"基于角色的访问控制"。访问权限严格按照需要进行控制，并且仅允许使用多因素身份验证机制的特定授权人员进行访问。

收集和保护客户数据

所有客户数据都会在公有网络之间传输时进行加密，并在空闲时进行加密。Data Infrastructure Insight利用系统中各个点的加密功能、使用包括传输层安全(Transport Layer Security、TLS)和行业标准AES-256算法在内的技术来保护客户数据。

客户取消配置

电子邮件通知会以不同的时间间隔发送，以通知客户其订阅即将到期。订阅过期后， UI 将受到限制，并开始为数据收集提供宽限期。然后，系统会通过电子邮件通知客户。试用订阅享有 14 天的宽限期，付费订阅帐户享有 28 天的宽限期。宽限期到期后，系统会通过电子邮件通知客户帐户将在 2 天后被删除。付费客户也可以直接请求停止服务。

宽限期结束时、或者在确认客户终止其帐户的请求后、Data Infrastructure Insight Operations (SRE)团队会删除过期的租户和所有关联的客户数据。无论哪种情况， SRE 团队都会运行 API 调用来删除帐户。API 调用将删除租户实例和所有客户数据。通过调用同一 API 并验证客户租户状态是否为 " 已删除 " ，可以验证客户删除情况。

安全意外事件管理

数据基础架构洞察力与NetApp的产品安全事件响应团队(Product Security Incident Response Team、PFIRT)流程相集成、可发现、评估和解决已知漏洞。PSIRT 可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源。

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

数据基础架构洞察客户或研究人员也可能发现数据基础架构洞察产品存在安全问题、并将此问题报告给技术支持或直接报告给NetApp的意外事件响应团队。在这些情况下、数据基础架构洞察力团队将启动PTIRT流程、评估并可能修复问题。

漏洞和渗透测试

Data Infrastructure Insight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 Insight人员都要接受针对个人角色制定的安全培训、以确保每位员工都有能力应对其角色中特定的安全挑战。

合规性

Data Infrastructure Insight对外部特许会计师事务所的安全性、流程和服务执行独立的第三方审计和验证、包括完成SOC 2审计。

NetApp安全通报

您可以查看NetApp提供的安全建议"此处"。

信息和区域

NetApp 非常重视客户信息的安全性。下面介绍了Data Infrastructure Insight如何以及如何存储您的信息。

Data Infrastructure Insight存储哪些信息？

Data Infrastructure Insight可存储以下信息：

- 性能数据

  性能数据是指提供有关受监控设备 / 源性能的信息的时间序列数据。例如，这包括存储系统提供的 IOS 数量， FibreChannel 端口的吞吐量， Web 服务器提供的页面数量，数据库的响应时间等。

- 清单数据

  清单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/文件名称(如果启用了存储工作负载安全性)等

- 配置数据

  此表汇总了客户提供的用于管理客户清单和操作的配置数据，例如受监控设备的主机名或 IP 地址，轮询间隔，超时值等

- 机密

  机密信息由数据基础架构洞察力采集单元访问客户设备和服务所使用的凭据组成。这些凭据使用强非对称加密进行加密、私钥仅存储在采集单元上、绝不会离开客户环境。由于这种设计、即使是有权限的Data Infrastructure Insight SRE也无法以纯文本格式访问客户机密。

- 功能数据

  这是由于 NetApp 提供云数据服务而生成的数据，该服务在云数据服务的开发，部署，操作，维护和安全方面向 NetApp 提供信息。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 BlueXP 与区域数据基础架构洞察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。

- 存储工作负载安全性用户目录数据

  如果启用了工作负载安全性功能、并且客户选择启用用户目录收集器、则系统将存储用户显示名称、公司电子邮件地址以及从Active Directory收集的其他信息。

  用户目录数据是指由工作负载安全性用户目录数据收集器收集的用户目录信息、而不是有关数据基础架构洞察力/工作负载安全性用户本身的数据。

- 不从基础架构和服务资源收集任何明确的个人数据 * 。收集的信息仅包含性能指标，配置信息和基础架构元数据，与许多供应商的电话住宅非常相似，包括 NetApp 自动支持和 ActiveIQ 。但是，根据客户的命名约定

，共享，卷， VM ， qtree 的数据， 应用程序等可能包含个人身份信息。

如果启用了工作负载安全性、则系统还会查看SMB或其他共享上的文件和目录名称、这些共享可能包含个人身份信息。如果客户启用了工作负载安全性用户目录收集器(实际上是通过Active Directory将Windows SID映射到用户名)、则Data Infrastructure Insight将收集并存储显示名称、公司电子邮件地址以及所选的任何其他属性。

此外、还会维护对Data Infrastructure Insight的访问日志、其中包含用于登录到服务的用户IP和电子邮件地址。

我的信息存储在哪里?

Data Infrastructure Insight根据创建环境的区域存储信息。

以下信息存储在主机区域：

- 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
- 在Data Infrastructure Insides.中审核有关用户活动的信息
- 工作负载安全性Active Directory信息
- 工作负载安全审核信息

无论您的Data Infrastructure Insight环境位于哪个地区、以下信息都驻留在美国：

- 环境站点（有时称为 " 租户 " ）信息，例如站点 / 帐户所有者。
- 允许NetApp BlueXP 与区域数据基础架构洞察站点进行通信的信息、包括与用户授权相关的任何信息。
- 与Data Infrastructure Insight用户和租户之间的关系相关的信息。

主机区域

主机区域包括：

- 美国：美国东部 1
- 欧洲，中东和非洲： EU-central-1.
- 亚太地区： AP-东南部 2

更多信息

有关 NetApp 隐私和安全的更多信息，请访问以下链接：

- "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"

securityadmin工具

Data Infrastructure Insight提供了多种安全功能、使您的环境能够以增强的安全性运行。这些功能包括对加密、密码哈希以及更改内部用户密码以及用于加密和解密密码的密钥对的功能进行了改进。

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 Insight中、当用户在数据收集器配置页面中输入密码时、Data Infrastructure Insight会使用公共密钥对密码进行加密。Data Infrastructure Insight没有解密数据收集器密码所需的私钥；只有采集单元(A课)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

如果您的Insight系统包含非默认安全配置(即您已重新设置密码密钥)、则必须备份安全配置。安装新软件或在某些情况下升级软件会将系统还原为默认安全配置。当您的系统还原到默认配置时、您必须还原非默认配置、系统才能正常运行。

管理采集单元上的安全性

通过SecurityAdmin工具、您可以管理Data Infrastructure Insight的安全选项、此工具可在采集单元系统上运行。安全管理包括管理密钥和密码、保存和还原您创建的安全配置或将配置还原为默认设置。

开始之前

- 要安装采集单元软件(包括SecurityAdmin工具)、您必须在AU系统上拥有管理员权限。
- 如果您的非管理员用户随后需要访问SecurityAdmin工具、则必须将其添加到_cisys_组中。_cisys_组是在AU安装期间创建的。

安装AU后、SecurityAdmin工具位于采集单元系统的以下任一位置：

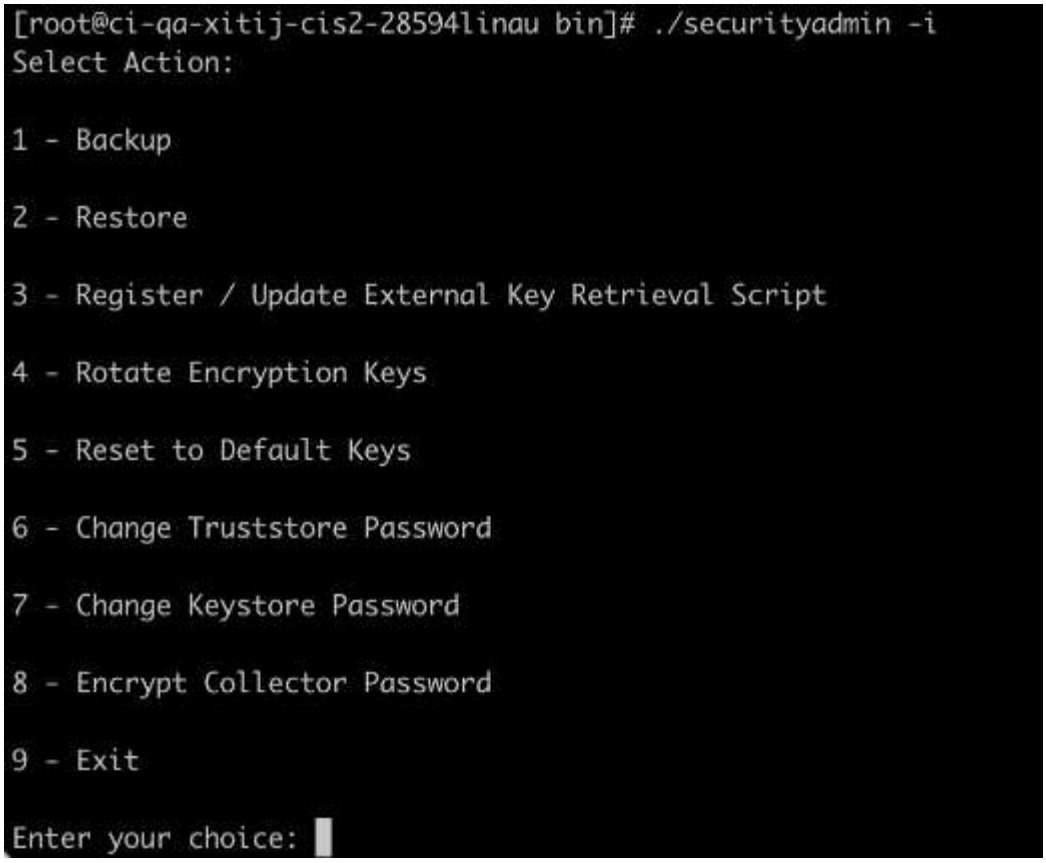
```
Windows - C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat
Linux - /bin/oci-securityadmin.sh
```

使用SecurityAdmin工具

以交互模式(-I)启动SecurityAdmin工具。

建议在交互模式下使用SecurityAdmin工具、以避免在命令行上传递可在日志中捕获的机密。

此时将显示以下选项：



1. * 备份 *

   为包含所有密码和密钥的存储创建一个备份zip文件、并将该文件放置在用户指定的位置或以下默认位置：

   ```
   Windows - C:\Program Files\SANscreen\backup\vault
   Linux - /var/log/netapp/oci/backup/vault
   ```

   建议确保存储备份的安全、因为它们包含敏感信息。

2. * 还原 *

   还原已创建的存储的zip备份。还原后、所有密码和密钥将还原为创建备份时的现有值。

   还原可用于同步多个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)创建存储的备份。3)将存储备份还原到每个AUP。

3. 注册/更新外部密钥索引脚本

   使用外部脚本注册或更改用于对设备密码进行加密或解密的AU加密密钥。

   更改加密密钥时、您应备份新的安全配置、以便在升级或安装后还原它。

   注意：此选项仅在Linux上可用。

   在将您自己的密钥检索脚本与SecurityAdmin工具结合使用时、请记住以下几点：

- 当前支持的算法为RSA、最小值为2048位。
- 该脚本必须以纯文本格式返回私钥和公共密钥。该脚本不能返回加密的私钥和公共密钥。
- 该脚本应返回原始编码内容(仅限PEM格式)。
- 外部脚本必须具有_execute_权限。

4. 旋转加密密钥

   轮换加密密钥(取消注册当前密钥并注册新密钥)。要使用外部密钥管理系统中的密钥、必须指定公共密钥ID和专用密钥ID。

5. 重置为默认密钥

   将采集用户密码和采集用户加密密钥重置为默认值、默认值是在安装期间提供的值。

6. 更改信任存储库密码

   更改信任存储库的密码。

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. * 退出 *

   退出SecurityAdmin工具。

选择要配置的选项、然后按照提示进行操作。

指定要运行该工具的用户

如果您处于安全意识强的受控环境中、则可能没有_cisys_组、但可能仍希望特定用户运行SecurityAdmin工具。

为此、您可以手动安装AU软件并指定要访问的用户/组。

- 使用API将CI安装程序下载到AU系统并进行解压缩。
  - 您需要一次性授权令牌。请参见API Swagger文档(_Admin > API Access_并选择_API Documentation_链接)、然后找到_get /au/oneTimeToken _ API部分。
  - 获得令牌后、请使用_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系统并解压缩。
- 导航到包含这些文件的文件夹、然后以root用户身份运行安装程序、并指定用户和组：

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

如果指定的用户和/或组不存在、则会创建这些用户和/或组。用户将有权访问SecurityAdmin工具。

正在更新或删除代理

SecurityAdmin工具可用于设置或删除采集单元的代理信息、方法是运行具有—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
```

运行命令后、必须重新启动采集单元。

要更新代理、请使用命令

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

外部密钥已在进行中

如果您提供了UNIX shell脚本、则采集单元可以执行该脚本、以便从密钥管理系统中检索*专用密钥*和*公共密钥*。

要检索密钥、Data Infrastructure Insight将执行该脚本、并传递以下两个参数：*key id*_和_*key type*。*Key id*_可用于标识密钥管理系统中的密钥。_*Key type*"公共"或"私有"。如果密钥类型为"public"、则脚本必须返回公共密钥。如果密钥类型为"prival"、则必须返回专用密钥。

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。该脚本必须打印_only标准输出的关键字；不能在标准输出中打印任何其他文本。将请求的密钥打印到标准输出后、脚本必须退出并显示退出代码0；任何其他返回代码均视为错误。

必须使用SecurityAdmin工具向采集单元注册该脚本、该工具将与采集单元一起执行该脚本。该脚本必须对root用户和"cisys"用户具有_read_和_execute_权限。如果在注册后修改了shell脚本、则必须将修改后的shell脚本重新注册到采集单元中。

输入参数：密钥ID	用于在客户密钥管理系统中标识密钥的密钥标识符。
输入参数：密钥类型	公共或私有。
输出	必须将请求的密钥打印到标准输出中。目前支持2048位RSA密钥。密钥必须采用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。所有其他退出值均视为失败。
脚本权限	脚本必须对root用户和"cisys"用户具有读取和执行权限。
日志	记录脚本执行。日志位于：/var/log/acidsights NetApp /sociityadmin/securityadmin.log /var/log/acidsights NetApp /acQ/acq.log

加密要在**API**中使用的密码

选项8允许您对密码进行加密、然后可以通过API将密码传递给数据收集器。

以交互模式启动SecurityAdmin工具，然后选择选项8：加密 密码。

```
 securityadmin.sh -i
```
系统将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。

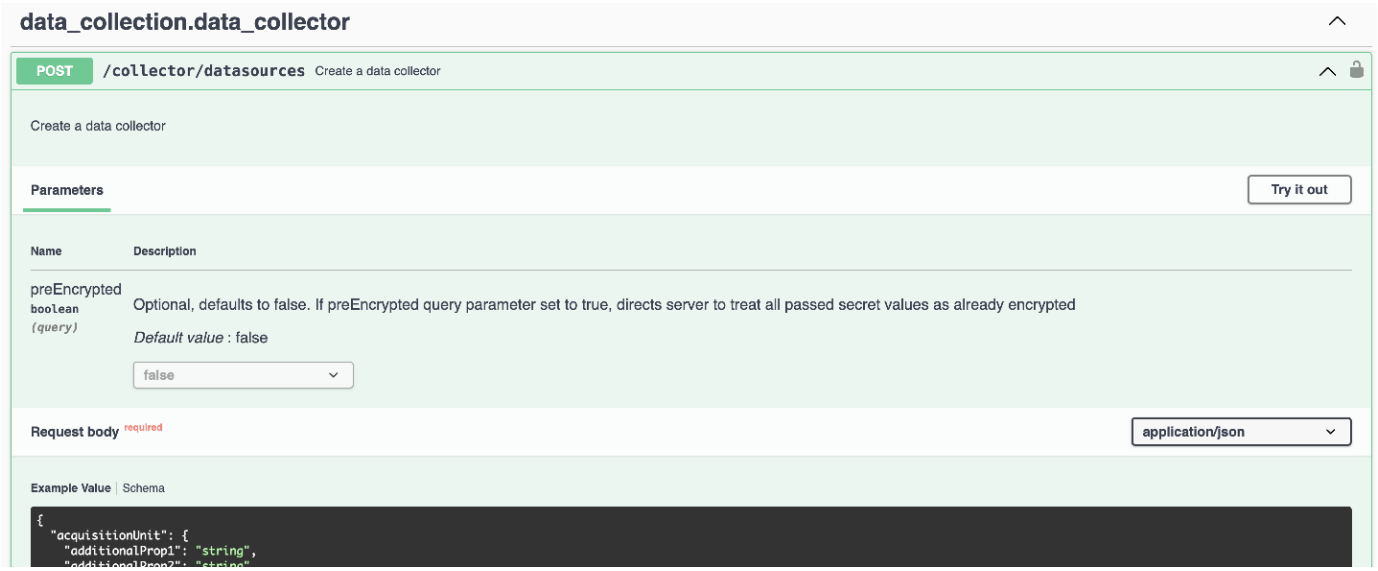
或者、如果您要在脚本中使用命令、请在命令行上使用_s术admin.sh_和"-enc"参数、传递未加密的密码：

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

加密密码将显示在屏幕上。复制整个字符串、包括任何前导或尾随符号。

```
[root@ci-eng-srivardh-learn bin]# securityadmin.sh -i
Select Action:

1 - Backup

2 - Restore

3 - Change Encryption Keys

4 - Reset to Default Keys

5 - Check for Default Encryption Keys

6 - Change Truststore Password

7 - Change Keystore Password

8 - Encrypt Password

9 - Exit

Enter your choice: 8
Please enter your password to encrypt:
Please confirm your password to encrypt:

Your Encrypted Password below

ciYJAMpdEncBsLQwF2gobbiERl4Jrwb7tLWOfYhu0dERGZZU3L+uWfcCXdNSXTWr6SFuumwsWVFib3h78vnM0s6vM7G/2klBd8gqJiQ+tS/lZkmJ6XKgTDcf3LGn8UqzQy
RnOv5jJBGip6nCysrt9dapsEiRVHrMJVr8btGYbb4Zoz62qudMfW9uQdm3qyzSKbIY0L0An89yDPC0kDkaXreyLfpjuOG5UmeZzlKGCT0aBTggri/JIYyyr4w2ZLnGOw21
LGm59vor7OGUOiKZYabLd+7LpsdCCBi1eF86BCj2RkxXOof891sHN+E7zTvZEofdGVWepc7b/HNah5XiXgVk1viCZ/WqkyQ==
```

要将加密密码发送到数据收集器、您可以使用数据收集API。此API的Swagger可在*Admin > API Access*中找到，然后单击"API Documentation"(API文档)链接。选择"数据收集"API类型。在_data_cCollection。data_Collector标题下、为本示例选择__/Collector /datsources_ POST API。



如果将_prePed_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不会重新加密此密码。构建API时、只需将先前加密的密码粘贴到相应位置即可。

https://<TENANT URL>/rest/v1/collector/datasources?preEncrypted=true


```
{
"name": "cdot-aaaaa",
  "config": {
    "dsTypeId": "93",
    "vendorModelId": "1",
    "packages": [
      {
        "id": "foundation",
        "displayName": "Inventory",
        "isMandatory": true,
        "attributes": {
          "RELEASESTATUS": "OFFICIAL",
          "enabled": true,
          "ip": "10.62.219.30",
          "user": "admin",
          "password":
"J8bepjwz9oNknfs6mcqbz3zuEThZQp1VyTk+1wE05gWwmmj1u0CB688nfOnB1xnlBVsAWyLmORxFAw
vcDCvGbTraqp/+nT0k94LO8Z7Q04I5KqhHfTvINGU54S4IVLWiMIFj8kSU4RhMvNNNq5Tarz0gJZhWR+
4RoNF+84R/uFFGwKeblrwfHxWZZMoW7pEJ2kzLFBtBzx2mUvRP0kn6AFbyS4+DM2YTPQkSk3W2Gzc
+nfPDDyH8Tq6AM5WsVCKqnZAa2ZlY1FxMkKT7iFt5oiYnl93ka7OrQlmM9QAyPoyw/JT0nXHDuf683uE
K32yn9CgxNGXy5NcNzRurdFNb5w=="
        }
      },
      {
        "id": "storageperformance",
        "displayName": "Array Performance",
        "isMandatory": false,
        "attributes": {
          "password": "this will not be encrypted on the server side"
        }
      }
    ]
  },
  "acquisitionUnit": {
    "id": "1"
  }
}
```