Security

Cloud Insights

NetApp
April 16, 2024

Table of Contents

Security

Cloud Insights Security

Product and customer data security is of utmost importance at NetApp. Cloud Insights follows security best practices throughout the release life cycle to make sure customer information and data is secured in the best possible way.

Security Overview

Physical security

The Cloud Insights production infrastructure is hosted in Amazon Web Services (AWS). Physical and environmental security-related controls for Cloud Insights production servers, which include buildings as well as locks or keys used on doors, are managed by AWS. As per AWS: “Physical access is controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff utilize multi-factor authentication mechanisms to access data center floors.”

Cloud Insights follows the best practices of the Shared Responsibility model described by AWS.

Product security

Cloud Insights follows a development lifecycle in line with Agile principles, thus allowing us to address any security-oriented software defects more rapidly, compared to longer release cycle development methodologies. Using continuous integration methodologies, we are able to rapidly respond to both functional and security changes. The change management procedures and policies define when and how changes occur and help to maintain the stability of the production environment. Any impactful changes are formally communicated, coordinated, properly reviewed, and approved prior to their release into the production environment.

Network security

Network access to resources in the Cloud Insights environment is controlled by host-based firewalls. Each resource (such as a load balancer or virtual machine instance) has a host-based firewall that restricts inbound traffic to only the ports needed for that resource to perform its function.

Cloud Insights uses various mechanisms including intrusion detection services to monitor the production environment for security anomalies.

Risk Assessment

Cloud Insights team follows a formalized Risk Assessment process to provide a systematic, repeatable way to identify and assess the risks so that they can be appropriately managed through a Risk Treatment Plan.

Data protection

The Cloud Insights production environment is set up in a highly redundant infrastructure utilizing multiple availability zones for all services and components. Along with utilizing a highly available and redundant compute infrastructure, critical data is backed up at regular intervals and restores are periodically tested. Formal backup policies and procedures minimize the impact of interruptions of business activities and protects business processes against the effects of failures of information systems or disasters and ensures their timely and adequate resumption.

Authentication and access management

All customer access to Cloud Insights is done via browser UI interactions over https. Authentication is accomplished via the 3rd party service, Auth0. NetApp has centralized on this as the authentication layer for all Cloud Data services.

Cloud Insights follows industry best practices including “Least Privilege” and “Role-based access control” around logical access to the Cloud Insights production environment. Access is controlled on a strict need basis and is only granted for select authorized personnel using multi-factor authentication mechanisms.

Collection and protection of customer data

All customer data is encrypted in transit across public networks and encrypted at rest. Cloud Insights utilizes encryption at various points in the system to protect customer data using technologies that includes Transport Layer Security (TLS) and the industry-standard AES-256 algorithm.

Customer deprovisioning

Email notifications are sent out at various intervals to inform the customer their subscription is expiring. Once the subscription has expired, the UI is restricted and a grace period begins for data collection. The customer is then notified via email. Trial subscriptions have a 14-day grace period and paid subscription accounts have a 28-day grace period. After the grace period has expired, the customer is notified via email that the account will be deleted in 2 days. A paid customer can also request directly to be off the service.

Expired tenants and all associated customer data are deleted by the Cloud Insights Operations (SRE) team at the end of the grace period or upon confirmation of a customer’s request to terminate their account. In either case, the SRE team runs an API call to delete the account. The API call deletes the tenant instance and all customer data. Customer deletion is verified by calling the same API and verifying that the customer tenant status is “DELETED.”

Security incident management

Cloud Insights is integrated with NetApp’s Product Security Incident Response Team (PSIRT) process to find, assess, and resolve known vulnerabilities. PSIRT intakes vulnerability information from multiple channels including customer reports, internal engineering, and widely recognized sources such as the CVE database.

If an issue is detected by the Cloud Insights engineering team, the team will initiate the PSIRT process, assess, and potentially remediate the issue.

It is also possible that a Cloud Insights customer or researcher may identify a security issue with the Cloud Insights product and report the issue to Technical Support or directly to NetApp’s incident response team. In these cases, the Cloud Insights team will initiate the PSIRT process, assess, and potentially remediate the issue.

Vulnerability and Penetration testing

Cloud Insights follows industry best practices and performs regular vulnerability and penetration testing using internal and external security professionals and companies.

Security awareness training

All Cloud Insights personnel undergo security training, developed for individual roles, to make sure each employee is equipped to handle the specific security-oriented challenges of their roles.

Compliance

Cloud Insights performs independent third-party Audit and validations from external Licensed CPA firm of its security, processes, and services, including completion of the SOC 2 Audit.

NetApp Security Advisories

You can view NetApp's available security advisories here.

Information and Region

NetApp takes the security of customer information very seriously. Here is how and where Cloud Insights stores your information.

What information does Cloud Insights store?

Cloud Insights stores the following information:

- Performance data

  Performance data is time-series data providing information about the performance of the monitored device/source. This includes, for example, the number of IOs delivered by a storage system, the throughput of a FibreChannel port, the number of pages delivered by a web server, the response time of a database, and more.

- Inventory data

  Inventory data consists of metadata describing the monitored device/source and how it is configured. This includes, for example, hardware and software versions installed, disks and LUNs in a storage system, CPU cores, RAM and disks of a virtual machine, the tablespaces of a database, the number and type of ports on a SAN switch, directory/file names (if Storage Workload Security is enabled), etc.

- Configuration data

  This summarizes customer-provided configuration data used to manage customer inventory and operations, e.g. hostnames or IP addresses of the monitored devices, polling intervals, timeout values, etc.

- Secrets

  Secrets consist of the credentials used by the Cloud Insights Acquisition Unit to access customer devices and services. These credentials are encrypted using strong asymmetric encryption, and the private keys are stored only on the Acquisition Units and never leave the customer environment. Even privileged Cloud Insights SREs are unable to access customer secrets in plain-text due to this design.

- Functional Data

  This is data generated as a result of NetApp providing the Cloud Data Service, which informs NetApp in the development, deployment, operations, maintenance, and securing of the Cloud Data Service. Functional Data does not contain Customer Information or Personal Information.

- User Access data

  Authentication and access information that allows NetApp Cloud Central to communicate with regional Cloud Insights sites, including data related to user Authorization.

- Storage Workload Security User Directory Data

  In cases where the Workload Security functionality is enabled AND the customer chooses to enable the User Directory collector, the system will store user display names, corporate email addresses, and other information collected from Active Directory.

User Directory data refers to user directory information collected by the Workload Security User Directory data collector, not to data about the users of Cloud Insights/Workload Security themselves.

No explicit personal data is collected from infrastructure and services resources. Collected information consists of performance metrics, configuration information and infrastructure metadata only, much like many vendor phone-homes, including NetApp auto-support and ActiveIQ. However, depending on a customer's naming conventions, data for shares, volumes, VMs, qtrees, applications, etc. may contain personally identifiable information.

If Workload Security is enabled, the system additionally looks at file and directory names on SMB or other shares, which may contain personally identifiable information. Where customers enable the Workload Security User Directory Collector (which essentially maps Windows SIDs to usernames through Active Directory), the display name, corporate email address and any additional attributes selected will be collected and stored by Cloud Insights.

Additionally, access logs to Cloud Insights are maintained and contain users' IP and email addresses used to log into the service.

Where is my information stored?

Cloud Insights stores information according to the region in which your environment is created.

The following information is stored in the host region:

- Telemetry and asset/object information, including counters and performance metrics
- Acquisition Unit information
- Functional data
- Audit information on user activities inside Cloud Insights
- Workload Security Active Directory information
- Workload Security Audit information

The following information resides in the United States, regardless of the region hosting your Cloud Insights environment:

- Environment site (sometimes called "tenant") information such as site/account owner.
- Information that allows NetApp Cloud Central to communicate with regional Cloud Insights sites, including anything to do with user Authorization.
- Information related to the relation between the Cloud Insights user and the tenant.

Host Regions

Host regions include:

- US: us-east-1
- EMEA: eu-central-1
- APAC: ap-southeast-2

More Information

You can read more about NetApp's privacy and security at the following links:

- Trust Center
- Cross-Border Data Transfers
- Binding Corporate Rules
- Responding to Third-Party Data Requests
- NetApp Privacy Principles

SecurityAdmin Tool

Cloud Insights Includes security features that allow your environment to operate with enhanced security. The features include improvements to encryption, password hashing, and the ability to change internal user passwords as well as key pairs that encrypt and decrypt passwords.

To protect sensitive data, NetApp recommends you change the default keys and the *Acquisition* user password after an installation or upgrade.

Data source encrypted passwords are stored in Cloud Insights, which uses a a public key to encrypt passwords when a user enters them in a data collector configuration page. Cloud Insights does not have the private keys required to decrypt the data collector passwords; only Acquisition Units (AUs) have the data collector private key required to decrypt data collector passwords.

Upgrade and installation considerations

When your Insight system contains non-default security configurations (i.e. you have rekeyed passwords), you must back up your security configurations. Installing new software, or in some cases upgrading software, reverts your system to a default security configuration. When your system reverts to the default configuration, you must restore the non-default configuration in order for the system to operate correctly.

Managing security on the acquisition unit

The SecurityAdmin tool allows you to manage security options for Cloud Insights, and is run on the acquisition unit system. Security management includes managing keys and passwords, saving and restoring security configurations you create or restoring configurations to the default settings.

Before you begin

- You must have admin privileges on the AU system in order to install the Acquisition Unit software (which includes the SecurityAdmin tool).
- If you have non-admin users who will subsequently need to access the SecurityAdmin tool, they must be added to the *cisys* group. The *cisys* group is created during AU installation.

After AU install, the SecurityAdmin tool is found on the acquisition unit system at either of these locations:

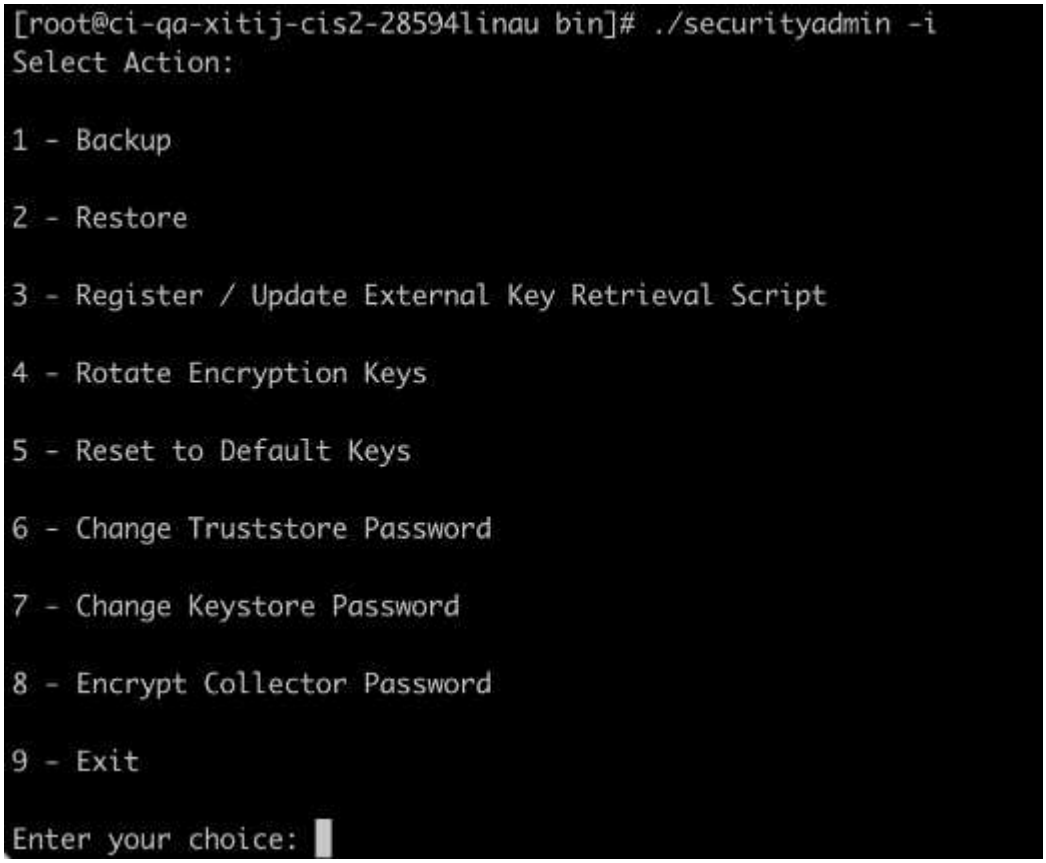
```
Windows - C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat
Linux - /bin/oci-securityadmin.sh
```

Using the SecurityAdmin Tool

Start the SecurityAdmin tool in interactive mode (-i).

> It is recommended to use the SecurityAdmin tool in interactive mode, to avoid passing secrets on the command line, which can be captured in logs.

The following options are displayed:



1. **Backup**

   Creates a backup zip file of the vault containing all passwords and keys and places the file in a location specified by the user, or in the following default locations:

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

   It is recommended that vault backups be kept secure, as they include sensitive information.

2. **Restore**

   Restores the zip backup of the vault that was created. Once restored, all passwords and keys are reverted to values existing at the time of the backup creation.

   Restore can be used to synchronize passwords and keys on multiple servers, for example using these steps: 1) Change encryption keys on the AU. 2) Create a backup of the vault. 3) Restore the vault backup to each of the AUs.

3. **Register / Update External Key Retrieval Script**

   Use an external script to register or change the AU encryption keys used to encrypt or decrypt device passwords.

   When you change encryption keys, you should back up your new security configuration so that you can restore it after an upgrade or installation.

   Note this option is only available on Linux.

   When using your own key retrieval script with the SecurityAdmin tool, keep the following in mind:

   - The current supported Algorithm is RSA with minimum 2048 bits.
   - The script must return the private and public keys in plain text. The script must not return encrypted private and public keys.
   - The script should return raw, encoded contents (PEM format only).
   - The external script must have *execute* permissions.

4. **Rotate Encryption Keys**

   Rotate your encryption keys (un-registers current keys and registers new keys). To use a key from an external key management system, you must specify the public key id and private key id.

1. **Reset to Default Keys**

   Resets acquisition user password and acquisition user encryption keys to default values, Default values are those provided during installation.

2. **Change Truststore Password**

   Change the password of the truststore.

3. **Change Keystore Password**

   Change the password of the keystore.

4. **Encrypt Collector Password**

   Encrypt data collector password.

5. **Exit**

   Exit the SecurityAdmin tool.

Chose the option you want to configure and follow the prompts.

Specifying a user to run the tool

If you are in a controlled, security-conscious environment, you may not have the *cisys* group but may still want specific users to run the SecurityAdmin tool.

You can achieve this by manually installing the AU software and specifying the user/group for whom you want access.

- Using the API, download the CI Installer to the AU system and unzip it.
  - You will need a one-time authorization token. See the API Swagger documentation (*Admin > API Access* and select the *API Documentation* link) and find the *GET /au/oneTimeToken* API section.
  - Once you have the token, use the *GET /au/installers/{platform}/{version}* API to download the installer file. You will need to provide platform (Linux or Windows) as well as installer version.
- Copy the downloaded installer file to the AU system and unzip it.
- Navigate to the folder containing the files, and run the installer as root, specifying the user and group:

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

If the specified user and/or group do not exist, they will be created. The user will have access to the SecurityAdmin tool.

Updating or Removing Proxy

The SecurityAdmin tool can be used to set or remove proxy information for the Acquisition Unit by running the tool with the *-pr* parameter:

```
[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 Cloud 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.)
```

For example, to remove the proxy, run this command:

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

You must restart the Acquisition Unit after running the command.

To update a proxy, the command is

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

External Key Retrieval

If you provide a UNIX shell script, it can be executed by the acquisition unit to retrieve the **private key** and the **public key** from your key management system.

To retrieve the key, Cloud Insights will execute the script, passing in two parameters: *key id* and *key type*. *Key id* can be used to identify the key in your key management system. *Key type* is either "public" or "private". When the key type is "public", the script must return the public key. When the key type is "private", the private key must be returned.

To send the key back to the acquisition unit, the script must print the key to standard output. The script must print *only* the key to standard output; no other text must be printed to standard output. Once the requested key is printed to the standard output, the script must exit with an exit code of 0; any other return code is considered an error.

The script must be registered with the acquisition unit using the SecurityAdmin tool, which will execute the script along with the acquisition unit. The script must have *read* and *execute* permission for the root and "cisys" user. If the shell script is modified after registering, the modified shell script must be re-registered with the acquisition unit.

input parameter: key id	Key identifier used to identify the key in the customers key management system.
input parameter: key type	public or private.
output	The requested key must be printed to the standard output. 2048 bit RSA key is currently supported. Keys must be encoded and printed in the following format - private key format - PEM, DER-encoded PKCS8 PrivateKeyInfo RFC 5958 public key format - PEM, DER-encoded X.509 SubjectPublicKeyInfo RFC 5280
exit code	Exit code of zero for success. All other exit values are considered failure.
script permissions	Script must have read and execute permission for the root and "cisys" user.
logs	Script executions are logged. Logs can be found in - /var/log/netapp/cloudinsights/securityadmin/securityadmin.log /var/log/netapp/cloudinsights/acq/acq.log

Encrypting a Password for use in API

Option 8 allows you to encrypt a password, which you can then pass to a data collector via API.

Start the SecurityAdmin tool in interactive mode and select option 8: *Encrypt Password*.

```
securityadmin.sh -i
```

You are prompted to enter the password you want to encrypt. Note that the characters you type are not shown on screen. Re-enter the password when prompted.

Alternatively, if you will use the command in a script, on a command line use *securityadmin.sh* with the "-enc" parameter, passing in your unencrypted password:

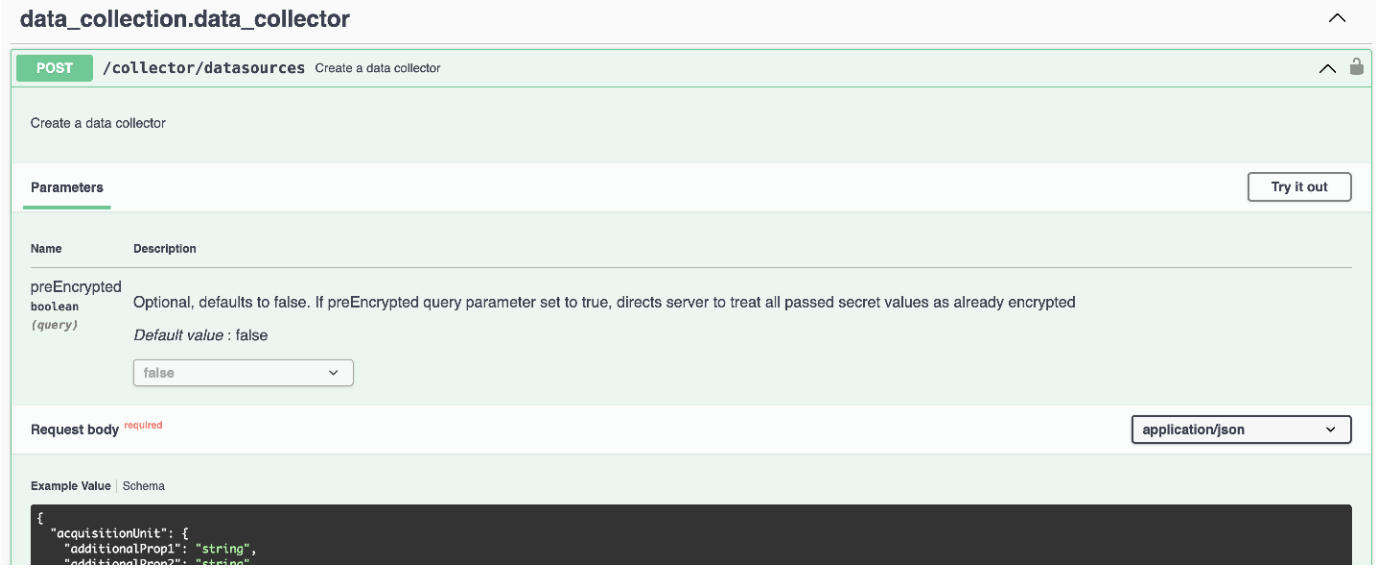
```
securityadmin -enc mypassword
```

```
[root@ci-eng-srivardh-learn bin]# securityadmin.sh -enc mypassword

Please copy paste the encrypted password below:

ciYJAMpdEncBsfc2PiXVBTappugSscDq3XF7Pw7/r5fOOJL0mbSel6QA/umLrr8PzBnjcJUHHRwrgf3jFio/2H3GftnqIxSs7ATKiQw5011uvxYiGftkzYaH2BKYHjkIiD
M8BEZZhm7pmTKWWpvAxhJbtjBrwUK2llM1GrnvaFlVVeydvsUMiggOenyJ/wxiko4gddif1Yq6rmia4yzvuYNw6Ppp5k/Pwy+0Hu0voRT+gca1ks8OjQToAAO6WSHZfp71
mMokM3Oaf43iV7eJZuMQ5RSq1cjBtYVnTWjp0Rn0g2kBCDf0PpWVrS6EKzh0HKQRRWpBZnQJNPv1bqtP+OpUh5Yd29RGX5Q==
```

The encrypted password is displayed on screen. Copy the entire string including any leading or trailing symbols.

```
[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==
```

To send the encrypted password to a data collector, you can use the Data Collection API. The swagger for this API can be found at **Admin > API Access** and click the "API Documentation" link. Select the "Data Collection" API type. Under the *data_collection.data_collector* heading, choose the */collector/datasources* POST API for this example.



If you set the *preEncrypted* option to *True*, any password you pass through the API command will be treated as **already encrypted**; the API will not re-encrypt the password(s). When building your API, simply paste the previously-encrypted password in the appropriate location.

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"
  }
}
```

Copyright information

Trademark information