Product Security

Enterprise applications

NetApp
April 25, 2024

Table of Contents

Product Security

ONTAP tools for VMware vSphere

Software engineering with ONTAP Tools for VMware vSphere employs the following secure development activities:

- **Threat modeling.** The purpose of threat modelling is to discover security flaws in a feature, component, or product early in the software development life cycle. A threat model is a structured representation of all the information that affects the security of an application. In essence, it is a view of the application and its environment through the lens of security.
- **Dynamic Application Security Testing (DAST).** This technology is designed to detect vulnerable conditions on applications in their running state. DAST tests the exposed HTTP and HTML interfaces of web-enable applications.
- **Third-party code currency.** As part of software development with open-source software (OSS), you must address security vulnerabilities that might be associated with any OSS incorporated into your product. This is a continuing effort because a new OSS version might have a newly discovered vulnerability reported at any time.
- **Vulnerability scanning.** The purpose of vulnerability scanning is to detect common and known security vulnerabilities in NetApp products before they are released to customers.
- **Penetration testing.** Penetration testing is the process of evaluating a system, web application, or network to find security vulnerabilities that could be exploited by an attacker. Penetration tests (pen tests) at NetApp are conducted by a group of approved and trusted third-party companies. Their testing scope includes the launching of attacks against an application or software similar to hostile intruders or hackers using sophisticated exploitation methods or tools.

Product security features

ONTAP tools for VMware vSphere includes the following security features in each release.

- **Login banner.** SSH is disabled by default and only allows one-time logins if enabled from the VM console. The following login banner is shown after the user enters a username in the login prompt:

  WARNING: Unauthorized access to this system is forbidden and will be prosecuted by law. By accessing this system, you agree that your actions may be monitored if unauthorized usage is suspected.

  After the user completes login through the SSH channel, the following text is displayed:

```
Linux vsc1 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

- **Role-based access control (RBAC).** Two kinds of RBAC controls are associated with ONTAP tools:
  - Native vCenter Server privileges

    - vCenter plug-in specific privileges. For details, see this link.
- **Encrypted communications channels.** All external communication happens over HTTPS using version 1.2 of TLS.
- **Minimal port exposure.** Only the necessary ports are open on the firewall.

  The following table describes the open port details.

TCP v4/v6 port #	Direction	Function
8143	inbound	HTTPS connections for REST API
8043	inbound	HTTPS connections
9060	inbound	HTTPS connections Used for SOAP over https connections This port must be opened to allow a client to connect to the ONTAP tools API server.
22	inbound	SSH (Disabled by default)
9080	inbound	HTTPS connections - VP and SRA - Internal connections from loopback only
9083	inbound	HTTPS connections - VP and SRA Used for SOAP over https connections
1162	inbound	VP SNMP trap packets
1527	internal only	Derby database port, only between this computer and itself, external connections not accepted — Internal connections only
443	bi-directional	Used for connections to ONTAP clusters

- **Support for certificate authority (CA) signed certificates.** ONTAP tools for VMware vSphere supports CA signed certificates. See this kb article for more information.
- **Audit logging.** Support bundles can be downloaded and are extremely detailed. ONTAP tools logs all user login and logout activity in a separate log file. VASA API calls are logged in a dedicated VASA audit log (local cxf.log).
- **Password policies.** The following password policies are followed:
    - Passwords are not logged in any log files.
    - Passwords are not communicated in plain text.
    - Passwords are configured during the installation process itself.
    - Password history is a configurable parameter.
    - Minimum password age is set to 24 hours.

- Auto complete for the password fields are disabled.
- ONTAP tools encrypts all stored credential information using SHA256 hashing.

SnapCenter Plug-in VMware vSphere

NetApp SnapCenter Plug-in for VMware vSphere software engineering uses the following secure development activities:

- **Threat modeling.** The purpose of threat modelling is to discover security flaws in a feature, component, or product early in the software development life cycle. A threat model is a structured representation of all the information that affects the security of an application. In essence, it is a view of the application and its environment through the lens of security.
- **Dynamic application security testing (DAST).** Technologies that are designed to detect vulnerable conditions on applications in their running state. DAST tests the exposed HTTP and HTML interfaces of web-enable applications.
- **Third-party code currency.** As part of developing software and using open-source software (OSS), it is important to address security vulnerabilities that might be associated with OSS that has been incorporated into your product. This is a continuous effort as the version of the OSS component may have a newly discovered vulnerability reported at any time.
- **Vulnerability scanning.** The purpose of vulnerability scanning is to detect common and known security vulnerabilities in NetApp products before they are released to customers.
- **Penetration testing.** Penetration testing is the process of evaluating a system, web application or network to find security vulnerabilities that could be exploited by an attacker. Penetration tests (pen tests) at NetApp are conducted by a group of approved and trusted third-party companies. Their testing scope includes the launching of attacks against an application or software like hostile intruders or hackers using sophisticated exploitation methods or tools.
- **Product Security Incident Response activity.** Security vulnerabilities are discovered both internally and externally to the company and can pose a serious risk to NetApp's reputation if they are not addressed in a timely manner. To facilitate this process, a Product Security Incident Response Team (PSIRT) reports and tracks the vulnerabilities.

Product security features

NetApp SnapCenter Plug-in for VMware vSphere includes the following security features in each release:

- **Restricted shell access.** SSH is disabled by default, and one-time logins are only allowed if they are enabled from the VM console.
- **Access warning in login banner.** The following login banner is shown after the user enters a user name in the login prompt:

  WARNING: Unauthorized access to this system is forbidden and will be prosecuted by law. By accessing this system, you agree that your actions may be monitored if unauthorized usage is suspected.

  After the user completes login through the SSH channel, the following output displays:

```
Linux vsc1 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

- **Role-based access control (RBAC).** Two kinds of RBAC controls are associated with ONTAP tools:
  - Native vCenter Server privileges.
  - VMware vCenter plug-in specific privileges. For more information, see Role-Based Access Control (RBAC).
- **Encrypted communications channels.** All external communication happens over HTTPS by using TLS.
- **Minimal port exposure.** Only the necessary ports are open on the firewall.

The following table provides the open port details.

TCP v4/v6 port number	Function
8144	HTTPS connections for REST API
8080	HTTPS connections for OVA GUI
22	SSH (disabled by default)
3306	MySQL (internal connections only; external connections disabled by default)
443	Nginx (data protection services)

- **Support for Certificate Authority (CA) signed certificates.** SnapCenter Plug-in for VMware vSphere supports the feature of CA signed certificates. See How to create and/or import an SSL certificate to SnapCenter Plug-in for VMware vSphere (SCV).
- **Password policies.** The following password policies are in effect:
  - Passwords are not logged in any log files.
  - Passwords are not communicated in plain text.
  - Passwords are configured during the installation process itself.
  - All credential information is stored using SHA256 hashing.
- **Base operating system image.** The product ships with Debian Base OS for OVA with restricted access and shell access disabled. This reduces the attack footprint. Every SnapCenter release base operating system is updated with latest security patches available for maximum security coverage.

NetApp develops software features and security patches with regards to SnapCenter Plug-in for VMware vSphere appliance and then releases them to customers as a bundled software platform. Because these appliances include specific Linux sub-operating system dependencies as well as our proprietary software, NetApp recommends that you do not make changes to the sub-operating system because this has a high potential to affect the NetApp appliance. This could affect the ability of NetApp to support the appliance. NetApp recommends testing and deploying our latest code version for appliances because they are released to patch any security-related issues.

Copyright information

Trademark information