This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.
You can find the most up-to-date technical documentation on the VMware Web site at:

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com
# Contents

1. AppInsight Security  5

2. vFabric AppInsight Security Reference  7
   - Protecting Security-Relevant Configuration Files  7
   - Required Open Ports for AppInsight  10
   - vFabric AppInsight Log Files  11

Index  13
VMware vFabric AppInsight Security provides a concise reference to the security features of vFabric AppInsight.

- Configuration options and settings that have security implications.
- Resources that must be protected, such as security-relevant configuration files and passwords, and the recommended access controls for secure operation.
- Location of log files and their purpose.
- External interfaces, ports, and services that must be open or enabled for the correct operation of VMware AppInsight.

This information is intended for IT decision makers, architects, administrators, and others who must familiarize themselves with the security components of vFabric AppInsight.
When you are configuring a secure AppInsight environment, you can change settings and make adjustments in several areas to protect your systems.

- **Protecting Security-Relevant Configuration Files** on page 7
  You can make security changes in AppInsight server and code agent configuration files to control access to security operations. You can also upgrade the encryption algorithm.

- **Required Open Ports for AppInsight** on page 10
  You must have the following open ports for the AppInsight server virtual machine and the network probe.

- **vFabric AppInsight Log Files** on page 11
  AppInsight software creates log files that record the installation and operation of its components.

**Protecting Security-Relevant Configuration Files**

You can make security changes in AppInsight server and code agent configuration files to control access to security operations. You can also upgrade the encryption algorithm.

- **Upgrading Encryption Algorithms** on page 7
  It is good practice to use the strongest algorithms to protect your data. You can use this procedure to update the algorithms for the AppInsight server and network probe.

- **Changing Code Agent Security Settings** on page 8
  Use this procedure to make changes to security settings such as passwords and access control for security operations related to the code agent.

- **Changing AppInsight Security Settings** on page 9
  Use this procedure to make changes to security settings such as passwords and access control for security operations related to AppInsight.

**Upgrading Encryption Algorithms**

It is good practice to use the strongest algorithms to protect your data. You can use this procedure to update the algorithms for the AppInsight server and network probe.

You reference the algorithm in the AppInsight server and the network probe, then create a key in the server.
Procedure

1. In the console, open `conmanage.py`.
2. Type `stop_appinsight` to stop the AppInsight server, then `quit` to exit the configuration manager.
3. At the command prompt, type `cd /etc/openvpn` to open the Open VPN directory.
4. Open the appropriate configuration file.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vi server.conf</code></td>
<td>Open the AppInsight server configuration file.</td>
</tr>
<tr>
<td><code>vi client.conf</code></td>
<td>Open the network probe configuration file.</td>
</tr>
</tbody>
</table>

5. Add the following properties to the file.

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cipher</code></td>
<td>AES-128-CBC</td>
</tr>
<tr>
<td><code>auth</code></td>
<td>SHA512</td>
</tr>
</tbody>
</table>

6. In AppInsight server, locate `dh1024.pem` and change it to `dh2048.pem`.
   For example, `dh /usr/share/openvpn/easy-rsa/2.0/keys/dh1024.pem` changes to `dh /usr/share/openvpn/easy-rsa/2.0/keys/dh2048.pem`.

7. Save the file and exit.

8. In AppInsight server, register the key for the algorithm.
   a. Open `cd /usr/share/openvpn/easy-rsa/2.0`.
   b. Type `. vars`.
   c. Type `export KEY_SIZE=2048`.
   d. Type `.build-dh`.
   e. Verify that the key file `/usr/share/openvpn/easy-rsa/2.0/keys/dh2048.pem` is created.

9. Type `service openvpn restart` to restart the service.

10. Open `conmanage.py`.

11. Type `stop_appinsight` to stop the AppInsight server, then `quit` to exit the configuration manager.

Changing Code Agent Security Settings

Use this procedure to make changes to security settings such as passwords and access control for security operations related to the code agent.

You make changes in the `insight.properties` file.

Prerequisites

You must have application owner user privileges with read/write permissions for the file.
**Procedure**

1. Open the console and access the configuration directory.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unix/Linux</td>
<td><code>cd server install path/insight/conf</code></td>
</tr>
<tr>
<td>Windows</td>
<td><code>cd server install path\insight\conf</code></td>
</tr>
</tbody>
</table>

2. Change the owner.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unix/Linux</td>
<td><code>chown owner user[:group] insight.properties</code></td>
</tr>
<tr>
<td>Windows</td>
<td><code>icacls insight.properties /setowner owner user</code></td>
</tr>
</tbody>
</table>

3. For Linux or Unix users, type `chmod 600 insight.properties` to set owner-only permissions.

4. For Windows users, type `icacls insight.properties /inheritance:d` to revoke any inheritance permissions.

5. For Windows users, type `icacls insight.properties /remove:g user name` to revoke all permissions granted to another user with access to this file.

   You can type `icacls insight.properties` to view a list of all users who have permissions on this file.

**Changing AppInsight Security Settings**

Use this procedure to make changes to security settings such as passwords and access control for security operations related to AppInsight.

You make changes in the files listed in “AppInsight Virtual Appliance Files that Store Passwords,” on page 10.

**Prerequisites**

You must have application owner user privileges with read/write permissions for the file.

**Procedure**

1. Open the console and type `cd server install path/insight/file.name` to access the configuration directory.

2. Type `chown owner user[:group] file.name` to change the owner.

3. Type `chmod 600 file.name` to set owner-only permissions.

**Example: Changing Permissions in rabbitmq.config**

This example increases security by changing the owner and permissions in `rabbitmq.config`.

```
cd /etc/rabbitmq/rabbitmq.config
chown rabbitmq rabbitmq.config
chmod 600 rabbitmq.config
```
**AppInsight Virtual Appliance Files that Store Passwords**

Draft comment filepath: GUID-40CCA454-8499-4CFD-B6A4-D25B987F5EF1.xml

To maximize security, VMware recommends that the following owner and permission settings are applied.

**RabbitMQ**

Draft comment filepath: GUID-40CCA454-8499-4CFD-B6A4-D25B987F5EF1.xml

For RabbitMQ, change the following owner and permission settings.

**Table 2-1. RabbitMQ Files that Store Passwords in Clear Text**

<table>
<thead>
<tr>
<th>Filename</th>
<th>Required Owner</th>
<th>Required Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>/etc/rabbitmq/rabbitmq.config</td>
<td>rabbitmq</td>
<td>600</td>
</tr>
<tr>
<td>/opt/vmware/apm/conf/am-amqp-configuration.properties</td>
<td>root</td>
<td>600</td>
</tr>
<tr>
<td>/opt/vmware/appinsight/metric-store/conf/metric-inserter.properties</td>
<td>root</td>
<td>600</td>
</tr>
<tr>
<td>/var/setup-conductor/cfg/amqp.cxml</td>
<td>root</td>
<td>600</td>
</tr>
</tbody>
</table>

**Postgres**

Draft comment filepath: GUID-40CCA454-8499-4CFD-B6A4-D25B987F5EF1.xml

For Postgres, change the following owner and permission settings.

**Table 2-2. Postgres Files that Store Passwords in Clear Text**

<table>
<thead>
<tr>
<th>Filename</th>
<th>Required Owner</th>
<th>Required Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>/opt/vmware/apm/conf/am-db.properties</td>
<td>root</td>
<td>600</td>
</tr>
<tr>
<td>/opt/vmware/appinsight/metric-store/conf/metric-store-persister.properties</td>
<td>root</td>
<td>600</td>
</tr>
</tbody>
</table>

**Truststore**

Draft comment filepath: GUID-40CCA454-8499-4CFD-B6A4-D25B987F5EF1.xml

For Truststore, change the following owner and permission settings.

**Table 2-3. Truststore Files that Store Passwords in Clear Text**

<table>
<thead>
<tr>
<th>Filename</th>
<th>Required Owner</th>
<th>Required Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>/opt/vmware/apm/conf/am-common-ssl.properties</td>
<td>root</td>
<td>600</td>
</tr>
</tbody>
</table>

**Required Open Ports for AppInsight**

Draft comment filepath: GUID-850CD3B3-9E38-4765-95A1-0E6A9F22BE59.xml

You must have the following open ports for the AppInsight server virtual machine and the network probe.

**Table 2-4. Open Ports Requirement for AppInsight**

<table>
<thead>
<tr>
<th>Name</th>
<th>Port Number</th>
<th>Protocol</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS</td>
<td>53</td>
<td>UDP</td>
<td>DNS</td>
</tr>
<tr>
<td>NTP</td>
<td>123</td>
<td>UDP</td>
<td>Time Server</td>
</tr>
<tr>
<td>Open VPN</td>
<td>1194</td>
<td>UDP, TCP</td>
<td>Open VPN</td>
</tr>
<tr>
<td>HTTP</td>
<td>80</td>
<td>TCP</td>
<td>HTTP</td>
</tr>
</tbody>
</table>
Table 2-4. Open Ports Requirement for AppInsight (Continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Port Number</th>
<th>Protocol</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATM_TC_SERVER_SSL</td>
<td>8443</td>
<td>TCP</td>
<td>tcServer SSL Connector</td>
</tr>
<tr>
<td>RABBIT</td>
<td>5671</td>
<td>TCP</td>
<td>RabbitMQ</td>
</tr>
<tr>
<td>INSIGHT</td>
<td>21234</td>
<td>TCP</td>
<td>Code Agent</td>
</tr>
</tbody>
</table>

vFabric AppInsight Log Files

Draft comment filepath: GUID-2C7F0AAD-6A7D-4451-B974-8F71FF718B95.xml

AppInsight software creates log files that record the installation and operation of its components.

Note: AppInsight log files are intended for use by VMware Support.

Table 2-5. vFabric AppInsight Log Files

<table>
<thead>
<tr>
<th>AppInsight Component</th>
<th>File Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>AppInsight metrics server</td>
<td>/opt/vmware/appinsight/metric-store/metric-store-tcserver-instance/logs</td>
</tr>
<tr>
<td>AppInsight application server</td>
<td>/opt/vmware/apm/tcserver-instance/logs</td>
</tr>
<tr>
<td>Code Agent</td>
<td>/opt/vmware/apm/insight-dashboard/logs</td>
</tr>
<tr>
<td>RabbitMQ</td>
<td>/var/log/rabbitmq</td>
</tr>
<tr>
<td>Conductor</td>
<td>/var/conductor/log</td>
</tr>
</tbody>
</table>
Index

A
algorithms, updating 7
appinsight, security settings 9

C
change security settings 7
code agent, security settings 8
config files, protecting security 7

F
files that store clear text passwords 10

L
log files 11

O
open ports requirements 10

P
passwords
  Postgres 10
  RabbitMQ 10
  stored in clear text 10
  Truststore 10
  ports 10

S
security settings
  appinsight 9
  code agent 8