VMware AppDefense Getting Started

VMware AppDefense

vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

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

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

VMware AppDefense Getting Started

The *AppDefense Getting Started* provides information about how to sign up for VMware AppDefense™, install, and configure AppDefense to secure applications. You can also find instructions to integrate AppDefense with other solutions.

The information includes step-by-step configuration instructions, and suggested best practices.

Intended Audience

This information is intended for anyone who wants to sign up for AppDefense, install, configure, and integrate AppDefense. The information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and data center operations. This manual assumes familiarity with VMware vSphere ®, including VMware ESXi ™, vCenter Server, vSphere Client, and VMware Tools ™.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to http://www.vmware.com/support/pubs.

AppDefense Overview

1

AppDefense is a data center endpoint security product that protects applications running in a virtualized environment.

AppDefense monitors the application against the intended state, detect the deviation, and respond. It provides foundational elements of cloud workload protection, such as system integrity, application control, and memory monitoring.

AppDefense provides these features by leveraging the hypervisor to monitor the intended state of the application running in the guest at all levels (operating system kernel, process behavior, network connections). AppDefense does not look at a guest workload in isolation, instead it manages workloads as part of broader *Security Scope* which allows it to have a deeper understanding of interactive behavior in the data center, not just individual machine behavior.

AppDefense focuses on monitoring the applications against their intended state, what the applications are supposed to do, and automatically respond when the applications deviate from that intended state, indicating a threat. This feature maximizes Security Operations efficiency and effectiveness and streamlines the application security readiness review process. This authoritative understanding of the application's intended state is critical and AppDefense makes this process relatively simple. The key here is that AppDefense allows you to orchestrate ahead of time and automatically trigger the response when it detects a given threat.

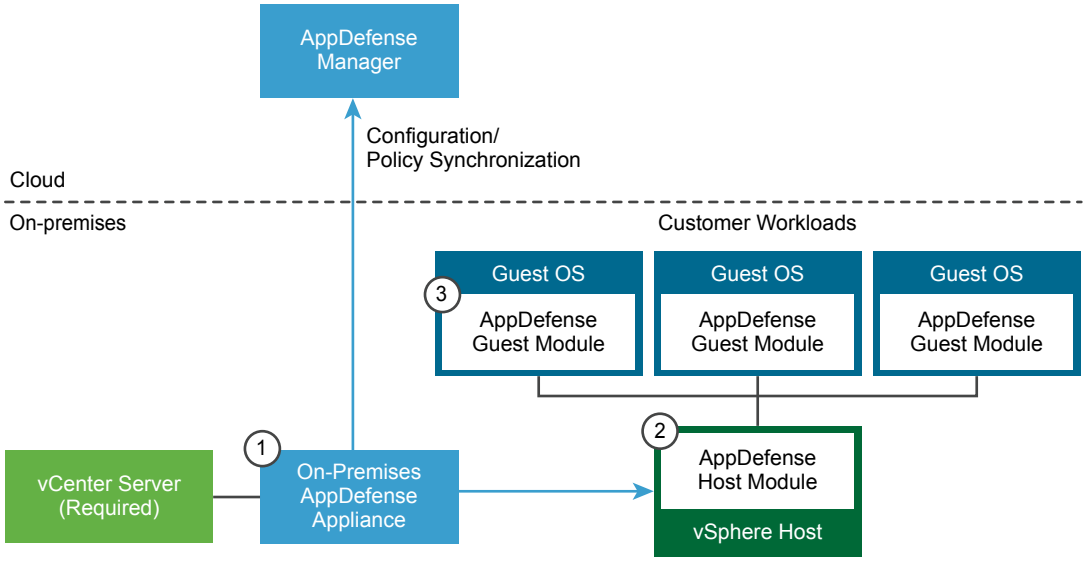
AppDefense uses vSphere and if installed NSX Data Center for vSphere, to act in response to a detected threat. For instance, you can take a snapshot of the compromised virtual machine for forensic analysis later using vSphere, then quarantine the virtual machine using NSX.

This chapter includes the following topics:

AppDefense Components

This section describes the architecture and primary components of the AppDefense platform.

AppDefense Service Architecture



AppDefense Manager

The AppDefense Manager console is a multi-tenant cloud service provided to define the intended behavior and protection rules of your applications in one place. You can monitor the enforcement of configuration, and security events and alarms from here.

AppDefense Appliance

AppDefense Appliance is an on-premises based control point for ingress and egress of data from and to the AppDefense Manager. It brokers connections to the VMware management components like vCenter Server and makes outbound connections to the AppDefense Manager.

AppDefense Modules

- The AppDefense Host Module is a standard VMware Integration Bundle (VIB) that is deployed on the ESXi host in order to support AppDefense. The Host Module enables VMs on that host to deploy and run AppDefense. For Windows environments, the Host Module also monitors and ensures the integrity of the Guest Module installed in the VM.
- The AppDefense Guest Module is also required on each VM, delivered with VMware Tools (Windows-only) or a one-click installation. The Guest Module collects guest context from the VM and communicates directly with the AppDefense Host Module.

vCenter Server

vCenter Server is used to gather inventory data on the customer's site. This inventory data is used for the security scope assignment, guest readiness (based on OS information), and guest to the host assignment. AppDefense can also use vCenter Server to perform remediation actions in response to security events, such as suspending a guest.

NSX Data Center for vSphere (Optional Component)

NSX can be optionally used as an extra, optional remediation channel for AppDefense. If any of the protection rules are violated, NSX can be used to automatically or manually quarantine the machines.

vRealize Automation (Optional Component)

vRealize Automation can be optionally used to capture the application context at provisioning time from the Application blueprint.

AppDefense Components at a Glance

AppDefense Components	Description
AppDefense Manager	No installation is required. You must sign up for a VMware AppDefense service.
AppDefense Appliance	Install AppDefense Appliance on-premises in the management cluster.
AppDefense Host Module	Host module is deployed at the ESXi host.
AppDefense Guest Module	Guest module is deployed at one or more hosts where your application workloads are running.

Key Concepts

The common AppDefense concepts that are used in the documentation and user interface.

Scope A Scope in AppDefense is the foundational component that establishes what the intended state and specific allowed behaviors of an application should be.

	A Security Scope defines the relevant configuration elements to protect an application and its constituent workloads. These configuration elements are like a *blueprint* or a *birth certificate* for the application. It contains a description, member workloads, rules, and behaviors.
Service	A service is a tier or a role within a scope. Typically, homegrown applications have three services (Application, Web, and Database), but scopes can include more than three services (file server, print server, compliance server, and so on).
Member	A member is a virtual machine (VM) within a service. Members (or VMs) in a service must have an identical operating system (means within a service, all the VMs must be homogeneous – either all Microsoft or all Linux).
Provisioning Events	AppDefense can tie into provisioning systems such as vRealize Automation or Puppet to define appropriate and allowed behaviors.
Behaviors	Behaviors are the ports, processes, or connections into and out of the application.
Discovery Mode	When you set up your scopes and services, AppDefense automatically enters into discovery mode. Discovery mode is when AppDefense creates a list of allowed behaviors to build a *blueprint* or a *birth certificate* of the natural state of the application. This mode helps AppDefense to understand how the application must function so that AppDefense can identify malicious or unintended behaviors. The orange color represents the VMs that are either in discovery mode or under protection.
Protected Mode	You can put your scope (application) into protected mode when AppDefense is learning no new behaviors, or you are comfortable with the number of behaviors it has learned. However, it is best practice to keep AppDefense in discovery mode for at least 14 days before moving to protected mode.

System Requirements

Before you install or upgrade AppDefense, consider your network configuration and resources. You can install one AppDefense Appliance per vCenter Server.

Table 1-1. Required Components

Product/Component	Description	Supported Version
VMwarevCenter Server	Used to manage the ESXi infrastructure.	6.5.x
VMware ESXi	Hypervisor where virtual infrastructure is spawned.	6.5a and above

Table 1-1. Required Components (Continued)

Product/Component	Description	Supported Version
VMware Tools	Guest Virtual Machine needs VMware tools installed.	
VMware NSX Data Center for vSphere (optional)	To leverage the network virtualization, integrate with NSX and use for remediation actions.	6.3 and above
VMware vRealize Automation (optional)	Provisioning system to manage a deployment of the application.	7.2
Puppet Enterprise (optional)	Provisioning systems that can help to define appropriate and allowed behavior.	
Windows Guest Operating System		■ Windows Server 2008 R2 x64 ■ Windows Server 2012 x64 ■ Windows Server 2012 R2 x64 ■ Windows Server 2016 x64 **Note** Windows guest operating system with Virtualization-based security (VBS) feature enabled is NOT supported.
Linux Guest Operating System		■ CentOS - 7.1,7.2,7.3, 7.4 (x86_64) ■ RHEL - 7.0, 7.3, 7.4 (x86_64) ■ Ubuntu - 14.04, 16.04 (x86_64) ■ SUSE - 11.4, 12.2, 12.3 (x86_64)
Supported Browsers		Internet Explorer 11 or Microsoft Edge, Google Chrome

Sign up for VMware AppDefense

2

You must verify that you satisfy the system requirements before signing up. Though AppDefense is delivered as a Software as a Service (SaaS) solution, it requires some on-premises components to be installed.

This chapter includes the following topics:

Sign up for VMware AppDefense Service

When you sign up for a VMware AppDefense service, or when someone invites you to join a service, you receive an email invitation containing a link that you can use to sign up.

You can request to sign up for VMware AppDefense at https://cloud.vmware.com/appdefense. You sign up forVMware AppDefense with your VMware ID or you can skip VMware ID and use your business ID.

VMware sets up your organization and user name within the AppDefense Manager. After the setup is done, you receive an invitation to join the AppDefense service.

Prerequisites

Procedure

1 Click the **Confirm my account** link in your invitation mail.

Note If you do not receive the invitation email, contact the VMware AppDefense support team at *appdefense_support@vmware.com*.

You are redirected to the AppDefense sign-in page.

If you are not redirected to the VMware AppDefense page, go to https://appdefense.vmware.com.

2 Log in to VMware AppDefense by entering the following parameters.

Parameter	Description
Select your region.	Select either **US** or **UK**. By default **US** region is selected.
Email	Enter email ID on which you received the invitation.

Parameter	Description
Password	Enter your own password.
Organization	Select your organization from the drop-down menu.

3 Click **Sign In**.

The **Dashboard** page of the AppDefense Manager appears as your default homepage.

What to do next

Configure AppDefense Appliance. For more information, refer to Deploying and Configuring the AppDefense Appliance.

Sign Out of AppDefense Service

Sign out of VMware AppDefense when you have completed your tasks.

Procedure

1 At the bottom of the left navigation pane, click the setting ( ) icon.

2 Click **Sign Out**.

You are logged out without disconnecting from the service.

Installing AppDefense

3

This topic describes the high-level tasks to track your installation progress.

Important Verify that your system requirements are satisfied.

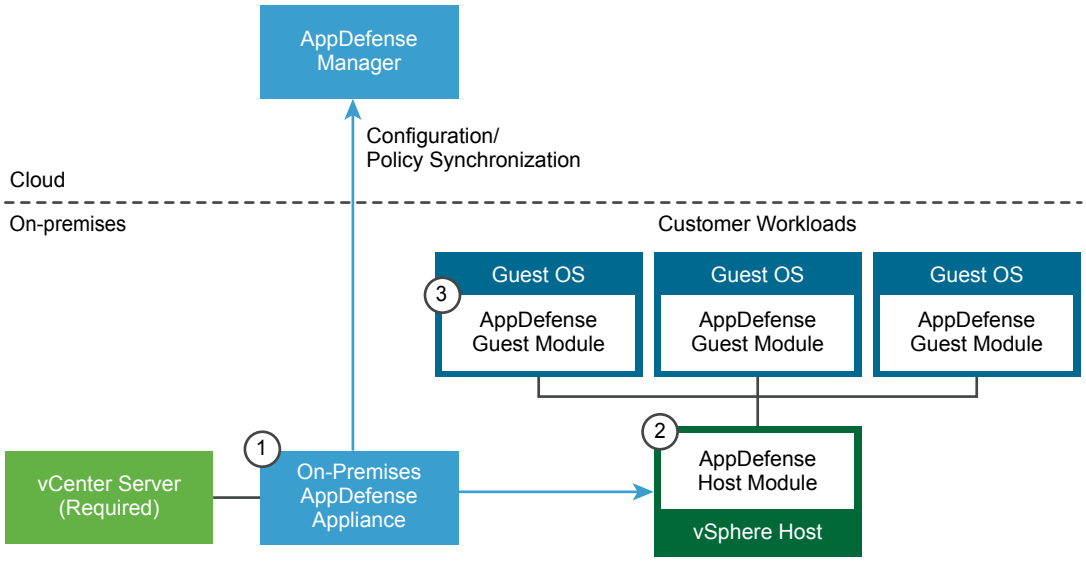


Table 3-1. AppDefense Components

Installation Steps	AppDefense Components	Task
System Requirements: Verify that versions for the following components are correct. ■ vCenter Server ■ ESXi Host ■ VMware Tools ■ Windows Guest Operating System ■ Linux Guest Operating System		System Requirements
Step 0: You must sign up for a VMware AppDefense service and can access AppDefense Manager. No installation is required.	AppDefense Manager	Sign up for VMware AppDefense Service

Table 3-1. AppDefense Components (Continued)

Installation Steps	AppDefense Components	Task
Step 1: Deploy and configure AppDefense Appliance on-premises in the vCenter Server.		
■ **Step 1A**: Deploy AppDefense Appliance in the vCenter Server.	vCenter Server	Deploy AppDefense Appliance in the vCenter Server
■ **Step 1B**: Provision the deployed AppDefense Appliance to get the appliance UUID and appliance API key.	AppDefense Manager	Provision the Deployed AppDefense Appliance
■ **Step 1C**: Configure the AppDefense Appliance.	AppDefense Appliance	Configure the AppDefense Appliance
Step 2: Install the AppDefense Host Module on the ESXi host.	AppDefense Host Module	Install the Host Module
Step 3: Install the AppDefense Guest Module on the hosts where your application workloads are running.	AppDefense Guest Module	Install the Guest Module

This chapter includes the following topics:

Deploying and Configuring the AppDefense Appliance

AppDefense Appliance pairs with vCenter Server. You must deploy one AppDefense Appliance per vCenter Server.

Make sure that you verify the setup requirements before deploying AppDefense Appliance.

You must first deploy the AppDefense Appliance at vCenter Server, then provision the deployed appliance, and then configure the provisioned appliance.

Environment Set Up

You must consider the following requirements before setting up your environment.

System Requirements

Verify that your system requirements are satisfied. Refer to System Requirements.

Set Up Requirements

- Put the appliance on a different host from the actual application VMs.

- Have a longer lease for the AppDefense Appliance IP address. Otherwise if there is change in an IP address, the host module might fail to connect. In such cases, you can configure the AppDefense Host Module from the **Inventory** page.
- Configure vCenter Server, vRealize Automation, NSX, AppDefense proxy appliance to run on a separate management cluster. The minimum number of hosts required in this cluster is ***one***. But for best results, run them across ***two*** hosts to balance the load.
- Configure a separate management network for communication within the management components and ESXi hosts.
- The AppDefense Appliance should communicate with the ESXi hosts on the management network. Refer to VMware vSphere networking best practices for details.
- The AppDefense proxy appliance requires a communication path with the AppDefense Manager. It is required that the proxy appliance can connect to AppDefense Manager over the Internet on port *443*. The requirement is only for the AppDefense Appliance to connect to the AppDefense Manager and does not require the AppDefense Appliance to be accessible over the Internet.

Deploy AppDefense Appliance in the vCenter Server

After you get access to AppDefense Manager, you must deploy the AppDefense Appliance on-premises in the management cluster.

Perform tasks in different systems as follows:

System	Task
AppDefense Manager	Get the AppDefense Appliance Open Virtualization Appliance (OVA) file.
vSphere Client	Install the AppDefense Appliance Open Virtual Appliance (OVA) file.

Prerequisites

You can access AppDefense Manager.

Procedure

1 Log in to the AppDefense Manager.

a At the bottom of the left navigation pane, click the setting () icon.

b Click **Downloads**, and then click the **Appliance** tab.

The appliance version is displayed with the latest appliance OVA file.

c You can either copy the download URL, or download the OVA file to your computer manually. To prevent any downgrade attack, download the Appliance OVA using an encrypted channel.

- To copy the download URL, right-click the download link and then click **Copy Link**.
- To download the AppDefense Appliance OVA file, click the **Download** link under the Download column.

Note If you have downloaded the OVA file manually, click the **Copy to Clipboard** icon and verify the OVA file with the SHA256 signature provided in the table.

2 Log in to the vSphere Web Client.

3 Right-click the host where you want to install the AppDefense Appliance, and then click **Deploy OVF Template**.

On the **Deploy OVF Template** page, configure the following values, and click **Next**.

Option	Description
Select Template	Paste the AppDefense Appliance URL, or click **Browse** to select the file on your computer.
(Optional) Select name and location	Change the name of the OVA file to **Appliance**.
(Optional) Select a resource	Verify if the selected host is the correct resource where you want to deploy the AppDefense Appliance.
Review details	Review the details. The Product must be **AppDefense Appliance VA** and Version must be **1.2.0.0**.
Accept license agreements	Click **Accept** to accept the VMware license agreements.
Select storage	Click **Accept** to accept the VMware license agreements.
Select networks	Select the network that has Internet access, and connectivity to vCenter Server and NSX Manager (If necessary).

Option	Description
Customize template	■ **Application**: ■ Type passwords for the *admin* and *root* user accounts and make sure that the password length is greater than eight characters. ■ **Networking Properties** : ■ If you want DHCP to be available while configuring the appliance, leave the configuration values empty. ■ If you want to configure the static IP address, ask your network administrator and add the following mandatory values: ■ Default Gateway, Domain Name Servers, Network 1 IP Address, Network 1 Netmask.
Ready to complete	Verify the details and click **Finish**. **Note** Even though the DHCP configuration is used, the **Review configuration data > Properties** section shows that the static IP configuration is used. Ignore data displayed under the **Properties** section.

The OVF begins to import and deploy. It can take up to 10 minutes, depending on public network download speed.

4 After the deployment is complete, go to the AppDefense Appliance virtual machine (VM), and power on the VM.

What to do next

Provision and configure the AppDefense Appliance.

Provision the Deployed AppDefense Appliance

After the AppDefense Appliance is deployed, you must provision the new appliance by registering your organization within the AppDefense Manager.

Prerequisites

- You can access AppDefense Manager.
- AppDefense Appliance is deployed.

Procedure

1 Log in to the AppDefense Manager.

2 At the bottom of the left navigation pane, click the setting ( ) icon.

3 Click **Appliances**, and then click **Provision New Appliance**.

The New Appliance window appears.

4 Create an appliance by entering the appliance name, and then click **Provision**.

The appliance name is an identifier and does not need to match the actual VM name within the vCenter Server, but the best practice is to match the names. For example, **Appliance**.

The **New Appliance Created** window appears.

5 The **New Appliance Created** window displays the URL for the manager in the region, UUID, and appliance API key. Keep this window open until the appliance configuration is done, or note down the information and preserve to be used in appliance configuration.

Following is the example of the information available in the **New Appliance Created** window:

```
mgr.endpoint.baseurl=https://appdefense.vmware.com/api/v1/
goldilocks.appliance.uuid=8xxxxxxx-xxxx-xxxx-xxxx-bxxxxexxxx8f
goldilocks.appliance.api-key=xxxxxxxxxxx.xxxxxxxxxxxxx.xxxxxxxxxx-xxxxxxxx-
xxxxxxxxxxxxxxxxxxxxxxxxxx_xxxxx
```

Important When you close the **New Appliance Created** window, there is no way to get back to the appliance API key. If you lose the appliance API key, contact the VMware AppDefense support team at *appdefense_support@vmware.com*.

6 (Optional) Click **OK** ONLY if you have saved the information.

What to do next

Configure the Appliance. After you configure the AppDefense Appliance, the Status column for the created appliance shows as **Active**.

Configure the AppDefense Appliance

After provisioning the deployed AppDefense Appliance, you must configure the appliance.

Perform tasks in different systems as follows:

System	Task
vSphere Client	Get the AppDefense Appliance virtual appliance (VA) GUI.
AppDefense Appliance virtual appliance	Configure an appliance.
AppDefense Manager	Verify the configured appliance.

Prerequisites

- Verify the AppDefense Appliance VM is powered-on.
- VMware Tools is installed on AppDefense Appliance VM.

Procedure

1 Log in to the vSphere Web Client.

2 Verify the AppDefense Appliance VM is powered-on. Open the VM console.

Note down the AppDefense Appliance IP address and default port is *5480*.

3 To start the appliance configuration, open a Web browser, and navigate to AppDefense Appliance GUI at `https://<appliance ip address>:5480`.

The AppDefense Appliance virtual appliance (VA) login page appears.

Note If you are not able to access the URL directly, refer to Configure AppDefense Appliance Manually.

4 Log in to the AppDefense Appliance virtual appliance.

Accept the self-signed certificate, and log in as admin credentials with the admin password that you added while deploying the AppDefense Appliance OVA file.

Make sure that you are in the **AppDefense > Status** tab, and the Service Status is displayed as **Not Configured**.

5 Click the **Configuration** tab, and configure the following values:

Option	Description
AppDefense Manager Configuration: **Required** Configuration	
Manager URL	Enter the appropriate URL based on your region. Following are the currently active regions with the URLs: ■ US region: https://appdefense.vmware.com/api/v1 ■ UK region: https://uk.appdefense.vmware.com/api/v1
Manager UUID	Enter the *goldilocks.appliance.uuid* obtained while Provision the Deployed AppDefense Appliance. For example, *goldilocks.appliance.uuid=xxxxxx1-axxx-4xxx-axxx-dxxxxxxxxxx5*.
Manager API Key	Enter the *goldilocks.appliance.api-key* obtained while Provision the Deployed AppDefense Appliance. For example, *goldilocks.appliance.api-key=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx*.
vCenter Configuration: **Required** Configuration	
vCenter Host Name	Enter the host name. Host name must exactly match with the Common Name from vCenter Server. For more information, refer to Find Common Name from vCenter SSL Certificate. The AppDefense Appliance must authenticate to vCenter Server via mutual TLS.
vCenter Username	Enter user name with administrative privileges for vCenter Server. For example: `administrator@vsphere.local`.
vCenter Password	Enter a password for the administrator user.
NSX Configuration: **Optional** Configuration. If you do not want to configure, leave the parameters empty. If you want to configure, enter information in all the parameters. **Note** NSX Data Center for vSphere must be up and running, while configuring the appliance connectivity.	

Option	Description
NSX Host Name	vCenter Server host name is required to exactly match Common Name from vCenter Server.
NSX Port	Enter a port number for NSX Data Center for vSphere.
NSX user name	Enter NSX administrator user name that has the Enterprise Administrator role.
NSX Password	Enter a password for the administrator user.
NSX Configured	Set to *true* to start connecting to NSX.
Puppet Configuration: **Optional** Configuration. If you do not want to configure, leave the parameters empty. If you want to configure, enter information in all the parameters.	
Puppet Master URL	Enter the authentication RBAC URL. For example: *https://{puppetMasterIP}:4433/rbac-api/v1/auth/token*.
Puppet Orchestrator URL	Enter the puppet orchestrator URL. For example: *https://{orchestratorIP}:8143/orchestrator/v1*.
Puppet DB URL	Enter the puppet database query URL. For example: *https://{DB IP}:8081/pdb/query/v4*.
Puppet Master Username	Enter user name for the Puppet Enterprise user account.
Puppet Master Password	Enter password for the Puppet Enterprise user account.
Puppet Configured	Set to *true* to start connecting to puppet.

6 Click **Save Settings**.

A vCenter Server thumbprint verification window appears.

7 Verify the thumbprint, and click **OK**.

The Service Status is displayed as **ACTIVE**.

8 Log in to the AppDefense Manager.

9 At the bottom of the left navigation pane, click the setting ( ) icon.

10 Click **Appliances**. The status of the new appliance that you provisioned are shown as Active.

The New Appliance window appears.

The AppDefense Appliance is configured.

What to do next

Set up AppDefense Guest Module andAppDefense Host Module.

Appliance logs are available at the */var/log/goldilocks* directory. For more information, refer to Collecting Logs Manually.

Find Common Name from vCenter SSL Certificate

You must obtain the Common Name from SSL certificate of the vCenter Server to proceed for AppDefense Appliance configuration.

Prerequisites

You are configuring AppDefense Appliance and must verify if the host name of the vCenter Server matches exactly with the Common Name.

Procedure

1. Open a Web browser, and enter the vSphere Client URL.

   Ignore the **Not Secure** warning and proceed.

   vCenter Server host name is case-sensitive, enter the same case in SSL certificate.
2. Click the **Secure** or **Not Secure** link, and click **Certificate**.

   A pop-up window appears.
3. Click **Details** and under the Issuer Name section, find the **Common Name**.

   For example: *vcenter65*. The vCenter Server host name must exactly match with this Common Name. If the vCenter Server is upgraded from an old version (for example, 5.5), Common Name might not be FQDN. In such cases, find the Issuer Name.

What to do next

Continue configuring AppDefense Appliance.

Configure AppDefense Appliance Manually

If you are not able to configure the AppDefense Appliance GUI, you can configure the appliance manually.

Prerequisites

Provisioned the deployed AppDefense Appliance.

Procedure

1. Log in to the vSphere Web Client.

   Verify the AppDefense Appliance VM is powered-on.
2. Go to the **Summary** tab, and note down the IP address of the AppDefense Appliance VM.
3. Open a terminal window and Secure Shell (SSH) into the appliance with *admin* user name and password.

   If prompted, type **yes**.
4. Go to the `cp /opt/vmware/goldilocks/etc/application.properties.sample` file.
5. Copy the sample configuration file (`application.properties.sample`), and save the file as `application.properties` at the same location, which is `/opt/vmware/goldilocks/etc/application.properties`.

6 Edit the configuration file with any terminal text editors like vim or nano as follows.

For example: `vi /opt/vmware/goldilocks/etc/application.properties`

Note Do not enter extra trailing spaces.

```
mgr.endpoint.baseurl= <copy-paste from the AppDefense Manager while Provision the Deployed AppDefense Appliance>
goldilocks.appliance.uuid=<copy-paste from the AppDefense Manager while Provision the Deployed AppDefense Appliance>
goldilocks.appliance.api-key=<copy-paste from the AppDefense Manager while Provision the Deployed AppDefense Appliance>
vc.ip.address=<vCenter FQDN or IP Address. See Note below>
vc.password=<Password of the vCenter Server user>
vc.username=<vCenter Server login user name. This user requires administrator's privileges>
```

Note For the *vc.ip.address* parameter, use the IP address of the vCenter Server. If the Common Name in the SSL certificate of the vCenter Server points to fully qualified domain name (FQDN), then use FQDN. If you have to use FQDN, make sure vCenter Server FQDN is resolvable by DNS. In case FQDN is not resolvable, add FQDN and IP address mapping for the vCenter Server in the `/etc/hosts` file on the AppDefense Appliance.

7 (Optional) If you want to configure NSX, enter the following details.

```
### NSX details - optional ###
nsx.enabled=true
nsx.address=<NSX FQDN - preferred, or IP address>
nsx.port=<NSX port>
nsx.username=<NSX login username>
nsx.password=<NSX login password>
```

8 Set the permission for the configuration file with an *admin* user as owner.

```
 sudo chown admin:wheel
/opt/vmware/goldilocks/etc/application.properties
```

9 Verify the status of current appliance process. Enter a password for the*root* user when prompted. If not changed, the password for the*root* user is same as the *admin* user.

```
 sudo systemctl status glx.service
$ sudo systemctl stop glx.service
```

10 Start the AppDefense Appliance service using the following command.

```
 sudo systemctl start glx.service
```

11 Verify that the AppDefense Appliance is running by verifying the status with the following command.

```
sudo systemctl status glx.service
```

If not changed, enter the same *admin* user password when prompted for the *sudo* command.

What to do next

Set up AppDefense Guest Module and AppDefense Host Module.

Installing the AppDefense Modules

You must set up the AppDefense Host Module on the ESXi host. You must set up the AppDefense Guest Module on one or more hosts where your application workloads are running.

You must verify that you have satisfied all the prerequisites before actual installation.

After installing the AppDefense Host Module on the ESXi host and AppDefense Guest Module on one or more hosts where your application workloads are running, you can start using AppDefense solution to monitor your application.

- Add the VMs that you want to monitor by AppDefense to a scope.
- Keep the VMs in the Discovery mode for at least two weeks.
- AppDefense package or operating system upgrades or restores must be done in the Discovery mode. Upgraded packages can change the application behavior that is not learned and can result into alarms.

Install the Host Module

You must set up the AppDefense Host Module on the ESXi host. Host module enables to enforce guest integrity and inspect the guest behavior.

Do not carry out these steps on the host which is running the vCenter Server or the AppDefense Appliance.

Prerequisites

- If you have an older version of the host module installed, then uninstall the older version before installing the new version.
- If the AppDefense Appliance has enabled the outbound filtering feature, then add the http://downloads.vmwaredrx.com website to the whitelist.

Procedure

1 Log in to the AppDefense Manager.

2 At the bottom of the left navigation pane, click the setting ( ) icon.

3 Click **Inventory**, and then click the **Hosts** tab.

4 Click the required ESXi host, and then click **Install/Update**.

Note If you do not have direct connectivity to the AppDefense Manager, then Install the Host Module Manually.

5 In the **Install/Update Host Module** window, select the required host version.

6 You can schedule the installation as **Immediate** or **Schedule** later by specifying hour and day.

7 To install the host module, click **Confirm**.

You can view the status of the installation as initiated, queued, or success with details. It takes few minutes to complete. Refresh the page after few minutes. You see that the action is completed successfully and AppDefense Host Module version appears.

8 Verify if the AppDefense Host Module is installed correctly.

a Log into the ESXi host.

b Use the `esxcli software lib list | grep glxhost` command to verify.

AppDefense Host Module is installed on the ESXi host.

What to do next

Install AppDefense Guest Module.

Install the Host Module Manually

If you do not have direct connectivity to the AppDefense Manager, then you can install the AppDefense Host Module manually. You can download the VIBs from AppDefense Manager, and then go to the ESXi host to install manually. When you install VIBs on the host, the VIB enables the host to enforce guest integrity and inspect the guest behavior.

Prerequisites

Configuration variables for the ESXi host are set.

Procedure

1 Log in to the AppDefense Manager.

2 At the bottom of the left navigation pane, click the setting () icon.

3 Click **Downloads**, and then click the **Host Module** tab.

4 Download the *zip* file containing the latest host module VIB to any location, and move the *zip* file to the ESXi host.

5 Log into the ESXi host.

6 Install the host module using the following command.

```
esxcli software vib install -d <path-to-zip>
```

The host module starts automatically after installed.

7 Use the `/etc/init.d/glxhostuwd status` command to verify.

8 Use the ESXi command line to set up the host configuration variables (glxHostId, glxAppIP, and glxAppPort).

AppDefense uses ESXi advanced configuration variables to pass configuration settings to the AppDefense Host Module.

Note Enable Secure Shell (SSH) and ESXi Shell for the ESXi hosts from the vCenter Server.

a **Setting *glxHostId***:

- Log in to the ESXi host by SSH using the *root* user
- Set the AppDefense Host Identifier (Host *MoRef ID* from vCenter Server) using the `esxcfg-advcfg /UserVars/glxHostId -s <host-id>` command. AppDefense Host Identifier is used while sending host heartbeat messages.
- Find the *MOID* value from the vCenter Server Operations Manager Dashboard available at **`https://<vcenter-ip>/vod/index.html?page=hosts`**. *MOID* is used by vCenter Server to identify the hosts (for example: “host-10”).
- Replace <*host-id*> with the current host *MOID* from the vCenter Server.

b **Setting *glxAppIP***:

- Replace the <*ip-address*> with the IP address of the AppDefense Appliance using the `esxcfg-advcfg /UserVars/glxAppIP -s <ip-address>` command.

  If you do not know the IP address of the appliance, you can get it through vCenter Server.

c **Setting *glxAppPort***:

- Set the AppDefense Appliance port number using the `esxcfg-advcfg /UserVars/glxAppPort -s 80` command.

  Port number is configurable, but must be set to port *80*.

You can verify if the values are configured correctly using the following commands:

```
 esxcfg-advcfg /UserVars/glxHostId -g
#(Output example: Value of glxHostId is host-10)

esxcfg-advcfg /UserVars/glxAppIP -g
```

```
#(Output example: Value of glxAppIP is 192.168.201.67)

esxcfg-advcfg /UserVars/glxAppPort -g
#(Output example: Value of glxAppPort is 80)
```

Install the Guest Module

You can install AppDefense Guest Module on the guest virtual machines (VM) where your application workloads are running. You can install AppDefense Guest Module on Windows and Linux systems. The AppDefense solution works with Guest Introspection for VMware NSX (VMware open-source product) to provide a network attestation service.

Important AppDefense does not work in virtual machines that have Fault Tolerance enabled. The underlying infrastructure required by AppDefense does not work with Fault Tolerant virtual machines. This limitation applies to both Linux and Windows guest virtual machines.

Guest Virtual Machine	Install Steps
Windows System	■ Guest Module Install Prerequisites for Windows Systems ■ Install the Guest Module on Windows System
Linux System	■ Guest Module Install Prerequisites for Linux Systems ■ Install Guest Module on Linux System Using VMware Package Repository

Guest Module Install Prerequisites for Windows Systems

You must satisfy these prerequisites before installing the AppDefense Guest Module.

Prerequisites

- These steps assume you have Windows 2008 R2 or Windows 2012 or Windows 2016 workloads running on the host(s) where you have configured the AppDefense Host Module.
- You have installed VMware Tools and is running on the VMs where you want to install the AppDefense Guest Module.

Procedure

1. While creating a new VM, set the compatibility to ESXi 6.5 and later.
2. If the VM version is lower than 13, upgrade the VM hardware version to 13 or later.

   Follow the Knowledge Base Article for upgrading a VM to the latest hardware version.
3. Enable the Guest Integrity feature as follows.
   a. Log in to the AppDefense Manager.
   b. At the bottom of the left navigation pane, click the setting () icon.
   c. Click **Inventory**, and then click the **VMs** tab.

d Select the required VM, and then click **Enable Guest Integrity**.

A confirmation window to restart the VM after enabling the Guest Integrity appears.

e Click **Submit**.

Note Depending on activity currently going on inside the VM, use this option judiciously. If you defer restarting the VM , then perform the restart through the vCenter Server console. For Guest Integrity to take effect, you must restart the VM at least once.

The Recent Infrastructure Action column displays the status. Refresh the page after few minutes to verify the updated status.

What to do next

Install AppDefense Guest Module.

Install the Guest Module on Windows System

You must install AppDefense Guest Module on the guest virtual machines (VM) where your application workloads are running. You can install AppDefense Guest Module using AppDefense Manager GUI or using command-line interface.

Prerequisites

- You have satisfied all the Guest Module Install Prerequisites for Windows Systems.
- You have Uninstall the AppDefense Guest Module.

Procedure

1 Log in to the AppDefense Manager.

2 At the bottom of the left navigation pane, click the setting ( ) icon.

3 Click **Downloads**, and then click the **Guest Module** tab.

The *AppDefense msi installer* for the Windows operating system is available for download. Example, *AppDefense-x64-1.2.0.2-8845982.msi*.

4 To download the latest build (one with the highest build number), click the **Download** link. The *AppDefense msi installer* is downloaded. Save the installer on the guest VM.

5 Go to the guest VM. You can either use the installer UI or command prompt for installation.

If you have older version of driver (installed using batch installer, or manual), uninstall the older version and delete all the related files. For details, refer to Uninstall the AppDefense Guest Module.

6 To install using the installer UI:

a Run the *AppDefense msi installer*.

b Accept the license agreement, and click **Install**.

c Accept the license agreement, and click **Install**.

Installer installs all the components.

d To complete the installation, click **Finish** .

Installer prompts to restart the system. To restart the system, click **Yes**.

7 (Optional) To install using the command prompt:

a Open the command prompt.

b Install the AppDefense Guest Module using the `AppDefense-x64-XXXXX.msi /qn` command.

Command installs the guest module and restarts the VM.

8 After the system restarts, guest driver and the probabilistic risk assessment (PRA) service starts running. You can verify using the following commands:

```
sc query glxgi
sc query gisvc
```

The status displays as `running`.

The AppDefense Guest Module is installed on the guest VM where your application workloads are running.

What to do next

You can now configure the AppDefense Guest Module to be protected by AppDefense.

Installing the AppDefense Guest Module on Linux System

You can install AppDefense Guest Module on the supported Linux system. The installation ofAppDefense Guest Module installs the AppDefense package, Guest Introspection package, and the *netfilter* dependencies.

Guest Introspection is a service that is deployed to offload security functions to a dedicated security appliance on each host. As a result Guest Introspection removes the need for an antivirus agent within the guest operating system.

Guest Introspection uses the following *netfilter* libraries to provide connection control and connection monitoring capability to the AppDefense.

- *libnetfilter_queue*: Provides APIs to capture network packets.
- *libnetfilter_conntrack*: Provides APIs to track network connection status.

Linux Installation Package

The Linux installation packages are available at the following two locations.

1 **Package Repository**: https://packages.vmware.com/appdefense/latest/

2 **Downloads Repository**: http://downloads.vmwaredrx.com/repository/

Linux Installation Options

You have the following options to install AppDefense Guest Module on the supported Linux system.

- Install Guest Module on Linux System Using VMware Package Repository: Preferred method for installation.
- Install Guest Module on Linux System Using the Downloads Repository: If you cannot access the VMware package repository (*https://packages.vmware.com*) or you cannot access the operating system (OS) repository to install the *netfilter* dependencies, then you can install AppDefense Guest Module on guest Linux virtual machines (VM) using the Downloads *(downloads.vmwaredrx.com)* repository.
- Install Guest Module on Linux System Using Local Download: If you do not have Internet access, then you can download the complete installation package and then configure the AppDefense Guest Module on the required guest Linux virtual machines (VM) pointing to the local repository.
- Install Guest Module Using Package Manager Command: Alternate method for installation. You can use this method if you do not want to configure the repository.

Known Limitations for Linux VMs

There are few known limitations for AppDefense to work with Linux VM. For details, refer to the Known Limitation with Linux VMs.

Guest Module Install Prerequisites for Linux Systems

You must complete these prerequisites before the actual installation. The AppDefense solution works with Guest Introspection for VMware NSX (VMware open-source product) to provide a network attestation service.

Ensure that the guest virtual machine (VM) has:

1 ESXi 6.5 or later installed.

2 A supported version of Linux installed.

  See System Requirements for the list of supported Linux distributions and versions.

3 *iptables* package of 1.4.11 version or later is installed.

Known Limitations for Linux VMs

There are few known limitations for AppDefense to work with Linux VM. For details, refer to the Known Limitation with Linux VMs.

Install Guest Module on Linux System Using VMware Package Repository

You can install AppDefense Guest Module on guest Linux virtual machines (VM) where your application workloads are running using the VMware package repository. The Linux VM (or server that is used to supply binaries to VMs) must be able to access *https://packages.vmware.com*. The installation of AppDefense Guest Module installs the AppDefense package, and the Guest Introspection package.

Perform the steps as applicable for your Linux distribution.

Prerequisites

- You must complete the prerequisites before the actual installation. For details, refer to Guest Module Install Prerequisites for Linux Systems.
- The Linux VM (or server that is used to supply binaries to VMs) must have access to https://packages.vmware.com. To verify accessibility to *packages.vmware.com*, use the `ping packages.vmware.com` command. Then run the `curl –Is https://packages.vmware.com/appdefense` command. The curl request returns the `HTTP/1.1 200 OK` status code.

Procedure

1 **For Ubuntu systems**:

a Obtain and import the VMware packaging public keys using the following commands.

```
wget https://packages.vmware.com/appdefense/key/VMWARE-APPD-PACKAGING-GPG-RSA-KEY.pub
apt-key add VMWARE-APPD-PACKAGING-GPG-RSA-KEY.pub
```

b Create a file named *appdefense.list* under `/etc/apt/sources.list.d`.

Note The Linux VM, where you want to deploy AppDefense, must have *netfilter* dependency installed. If not, the VM must have access to the OS repository to install the *netfilter* package.

c Edit the *appdefense.list* file with the following contents:

```
 vi /etc/apt/sources.list.d/appdefense.list

deb [arch=amd64] https://packages.vmware.com/appdefense/latest/ubuntu trusty main
deb [arch=amd64] https://packages.vmware.com/guest-introspection-for-vmware-nsx/latest/ubuntu
trusty main
```

d Install the AppDefense Guest Module package using the following commands.

```
apt-get update
apt-get install vmw-glx
```

Note To upgrade or install a specific version, run the following command.

```
apt-get install vmw-glx-<version>
```

2 **For RHEL systems**:

a Obtain and import the VMware packaging public keys using the following commands.

```
wget https://packages.vmware.com/appdefense/key/VMWARE-APPD-PACKAGING-GPG-RSA-KEY.pub
rpm --import VMWARE-APPD-PACKAGING-GPG-RSA-KEY.pub
```

b Create a file named *appdefense.repo* under `/etc/yum.repos.d`.

c Edit the *appdefense.repo* file with the following contents:

```
 vi /etc/yum.repos.d/appdefense.repo
[repo-appdefense]
name=AppDefense repo
baseurl=https://packages.vmware.com/appdefense/latest/
enabled=1
gpgcheck=1

[guest-introspection-for-vmware-nsx]
name=Guest Introspection for VMware NSX
baseurl=https://packages.vmware.com/guest-introspection-for-vmware-nsx/latest/rhel/x86_64/
enabled=1
gpgcheck=1
```

d Install the AppDefense Guest Module package using the following commands.

```
yum install vmw-glx
```

Note To upgrade or install a specific version, run the following command:

```
yum install vmw-glx-<version>
```

3 **For CentOS systems**:

a Obtain and import the VMware packaging public keys using the following commands.

```
wget https://packages.vmware.com/appdefense/key/VMWARE-APPD-PACKAGING-GPG-RSA-KEY.pub
rpm --import VMWARE-APPD-PACKAGING-GPG-RSA-KEY.pub
```

b Create a file named *appdefense.repo* under `/etc/yum.repos.d`.

c Edit the *appdefense.repo* file with the following contents:

```
 vi /etc/yum.repos.d/appdefense.repo
[repo-appdefense]
name=AppDefense repo
baseurl=https://packages.vmware.com/appdefense/latest/
enabled=1
gpgcheck=1

[guest-introspection-for-vmware-nsx]
name=Guest Introspection for VMware NSX
baseurl=https://packages.vmware.com/guest-introspection-for-vmware-nsx/latest/centos/x86_64/
enabled=1
gpgcheck=1
```

d Install the AppDefense Guest Module package using the following commands.

```
yum install vmw-glx
```

Note To upgrade or install a specific version, run the following command.

```
yum install vmw-glx-<version>
```

4 **For SLES systems**:

a Obtain and import the VMware packaging public keys using the following commands.

```
wget https://packages.vmware.com/appdefense/key/VMWARE-APPD-PACKAGING-GPG-RSA-KEY.pub
rpm --import VMWARE-APPD-PACKAGING-GPG-RSA-KEY.pub
```

b Add the following repository:

```
zypper ar "https://packages.vmware.com/appdefense/latest/" appdefense
zypper ar "https://packages.vmware.com/guest-intappdefense.reporospection-for-vmware-
nsx/latest/sles/x86_64/"
guest-introspection-for-vmware-nsx
```

c Install the AppDefense Guest Module package using the following commands.

```
zypper install vmw-glx
```

Note To upgrade or install a specific version, run the following command.

```
zypper install vmw-glx-<version>
```

5 To verify if AppDefense Guest Module is installed, run the following command with the root privilege.

```
/etc/init.d/vmw_glxd status
```

6 To verify if the Guest Introspection is installed, run the following command with the root privilege.

```
/etc/init.d/vmw_conn_notifyd status
```

The status is running.

What to do next

If you cannot access the VMware package repository (*https://packages.vmware.com*), then install AppDefense Guest Module on guest Linux virtual machines (VM) using the Downloads *(downloads.vmwaredrx.com)* repository.

Install Guest Module on Linux System Using the Downloads Repository

If you cannot access the VMware package repository (*https://packages.vmware.com*) or you cannot access the operating system (OS) repository to install the *netfilter* dependencies, then you can install AppDefense Guest Module on guest Linux virtual machines (VM) using the Downloads *(downloads.vmwaredrx.com)* repository. The installation of AppDefense Guest Module installs the AppDefense package, Guest Introspection package, and the *netfilter* dependencies.

Perform the steps as applicable for your Linux distribution.

Prerequisites

- You must complete the prerequisites before the actual installation. For details, refer to Guest Module Install Prerequisites for Linux Systems.
- The Linux VM (or server that is used to supply binaries to VMs) must have access to *http://downloads.vmwaredrx.com/repository/*.

Procedure

1 **For Ubuntu systems**:

   a Obtain and import the VMware packaging public keys using the following commands.

```
wget https://downloads.vmwaredrx.com/repository/appdefense/key/VMWARE-APPD-PACKAGING-GPG-RSA-KEY.pub
apt-key add VMWARE-APPD-PACKAGING-GPG-RSA-KEY.pub
```

   b Create a file named *appdefense.list* under `/etc/apt/sources.list.d`.

c Edit the *appdefense.list* file with the following contents:

```
vi /etc/apt/sources.list.d/appdefense.list
```

For Ubuntu 14.04:

```
deb [arch=amd64] http://downloads.vmwaredrx.com/repository/guest-introspection-os-
bundle/ubuntu trusty main
deb [arch=amd64] https://downloads.vmwaredrx.com/repository/appdefense/latest/ubuntu trusty
main
deb [arch=amd64] https://downloads.vmwaredrx.com/repository/guest-introspection-for-vmware-
nsx/latest/ubuntu trusty main
```

-Or-

For Ubuntu 16.04:

```
deb [arch=amd64] http://downloads.vmwaredrx.com/repository/guest-introspection-os-
bundle/ubuntu xenial main
deb [arch=amd64] https://downloads.vmwaredrx.com/repository/appdefense/latest/ubuntu trusty
main
deb [arch=amd64] https://downloads.vmwaredrx.com/repository/guest-introspection-for-vmware-
nsx/latest/ubuntu trusty main
```

d Install the AppDefense Guest Module package using the following commands:

```
apt-get update
apt-get install vmw-glx
```

Note To upgrade or install a specific version, run the following command:

```
apt-get install vmw-glx-<version>
```

2 **For RHEL systems**:

a Obtain and import the VMware packaging public keys using the following commands:

```
wget http://downloads.vmwaredrx.com/repository/appdefense/key/VMWARE-APPD-PACKAGING-GPG-RSA-
KEY.pub
rpm --import VMWARE-APPD-PACKAGING-GPG-RSA-KEY.pub
```

b Create a file named *appdefense.repo* under `/etc/yum.repos.d`.

c Edit the *appdefense.repo* file with the following contents:

```
 vi /etc/yum.repos.d/appdefense.repo
[repo-appdefense]
name=AppDefense repo
baseurl=http://downloads.vmwaredrx.com/repository/appdefense/latest/
enabled=1
gpgcheck=1

[guest-introspection-for-vmware-nsx]
name=Guest Introspection for VMware NSX
baseurl=http://downloads.vmwaredrx.com/repository/guest-introspection-for-vmware-
nsx/latest/rhel/x86_64/
enabled=1
gpgcheck=1
```

d For RHEL 7.0, 7.3 or 7.4: To install a dependent component, add the following line in the *appdefense.repo* file created in the previous step c.

```
===

[guest-introspection-os-bundle]

name=Guest Introspection OS Bundle

baseurl= http://downloads.vmwaredrx.com/repository/guest-introspection-os-bundle/rhel/7.0/

enabled=1

gpgcheck=0

===
```

Note The *baseurl* parameter is represented as *http://downloads.vmwaredrx.com/repository/guest-introspection-os-bundle/rhel/<os_version>*. The *os_version* can be RHEL 7.0, 7.3, or 7.4.

e Install the AppDefense Guest Module package using the following commands:

```
yum install vmw-glx
```

Note To upgrade or install a specific version, run the following command:

```
yum install vmw-glx-<version>
```

3 **For CentOS systems**:

a Obtain and import the VMware packaging public keys using the following commands:

```
wget http://downloads.vmwaredrx.com/repository/appdefense/key/VMWARE-APPD-PACKAGING-GPG-RSA-
KEY.pub
rpm --import VMWARE-APPD-PACKAGING-GPG-RSA-KEY.pub
```

b Create a file named *appdefense.repo* under `/etc/yum.repos.d`.

c Edit the *appdefense.repo* file with the following contents:

```
 vi /etc/yum.repos.d/appdefense.repo
[repo-appdefense]
name=AppDefense repo
baseurl=http://downloads.vmwaredrx.com/repository/appdefense/latest/
enabled=1
gpgcheck=1

[guest-introspection-for-vmware-nsx]
name=Guest Introspection for VMware NSX
baseurl=http://downloads.vmwaredrx.com/repository/guest-introspection-for-vmware-
nsx/latest/centos/x86_64/
enabled=1
gpgcheck=1
```

d For CentOS 7.1, 7.2, 7.3, or 7.4: To install a dependent component, add the following line in the *appdefense.repo* file created in the previous step c.

```
===

[guest-introspection-os-bundle]

name=Guest Introspection OS Bundle

baseurl= http://downloads.vmwaredrx.com/repository/guest-introspection-os-bundle/centos/7.1/

enabled=1

gpgcheck=0

===
```

Note The *baseurl* parameter is represented as *http://downloads.vmwaredrx.com/repository/guest-introspection-os-bundle/centos/<os_version>*. The *os_version* can be CentOS 7.1, 7.2, 7.3, or 7.4.

e Install the AppDefense Guest Module package using the following commands:

```
yum install vmw-glx
```

Note To upgrade or install a specific version, run the following command:

```
yum install vmw-glx-<version>
```

4 **For SLES systems**:

a Obtain and import the VMware packaging public keys using the following commands:

```
wget http://downloads.vmwaredrx.com/repository/appdefense/key/VMWARE-APPD-PACKAGING-GPG-RSA-
KEY.pub
rpm --import VMWARE-APPD-PACKAGING-GPG-RSA-KEY.pub
```

b Add the following repository:

```
zypper ar "http://downloads.vmwaredrx.com/repository/appdefense/latest/" appdefense
zypper ar "http://downloads.vmwaredrx.com/repository/guest-intappdefense.reporospection-for-
vmware-nsx/latest/sles/x86_64/"
guest-introspection-for-vmware-nsx
```

c For SLES 11.4, 12.2, or 12.3: To install a dependent component, add the following line in the *appdefense.repo* file created in the previous step b.

```
zipper ar "http://downloads.vmwaredrx.com/repository/guest-introspection-os-bundle/sles/11.4/"
```

Note The *baseurl* parameter is represented as *http://downloads.vmwaredrx.com/repository/guest-introspection-os-bundle/sles/<os_version>*. The *os_version* can be SLES 11.4, 12.2, or 12.3.

d Install the AppDefense Guest Module package using the following commands:

```
zypper install vmw-glx
```

Note To upgrade or install a specific version, run the following command:

```
zypper install vmw-glx-<version>
```

5 To verify if AppDefense Guest Module is installed, run the following command with the root privilege:

```
/etc/init.d/vmw_glxd status
```

6 To verify if the Guest Introspection is installed, run the following command with the root privilege:

```
/etc/init.d/vmw_conn_notifyd status
```

The status is running.

Install Guest Module on Linux System Using Local Download

If you do not have Internet access, then you can download the complete installation package and then configure the AppDefense Guest Module on the required guest Linux virtual machines (VM) pointing to the local repository.

Perform the steps as applicable for your Linux distribution.

Prerequisites

Linux installation

- You must complete the prerequisites before the actual installation. For details, refer to Guest Module Install Prerequisites for Linux Systems.

Procedure

1 This step is a common step for any Linux distribution. Download and import the complete VMware package using the following URLs. Expand the repository using the `unzip` and `untar` command.

```
http://downloads.vmwaredrx.com/repository/packages/appdefense.tar.gz
http://downloads.vmwaredrx.com/repository/packages/guest-introspection-for-vmware-nsx.tar.gz
http://downloads.vmwaredrx.com/repository/packages/guest-introspection-os-bundle.tar.gz
```

2 **For Ubuntu systems**:

a Obtain and import the VMware packaging public keys using the following commands.

```
wget file:/HOME/Downloads/repository/appdefense/key/VMWARE-APPD-PACKAGING-GPG-RSA-KEY.pub
apt-key add VMWARE-APPD-PACKAGING-GPG-RSA-KEY.pub
```

b Create a file named *appdefense.list* under `/etc/apt/sources.list.d`.

c Edit the *appdefense.list* file with the following contents:

```
vi /etc/apt/sources.list.d/appdefense.list
```

For Ubuntu 14.04:

```
deb [arch=amd64] file:/HOME/Downloads/guest-introspection-os-bundle/ubuntu trusty main
deb [arch=amd64] file:/HOME/Downloads/appdefense/latest/ubuntu trusty main
deb [arch=amd64] file:/HOME/Downloads/repository/guest-introspection-for-vmware-
nsx/latest/ubuntu trusty main
```

-Or-

For Ubuntu 16.04:

```
deb [arch=amd64] file:/HOME/Downloads/guest-introspection-os-bundle/ubuntu xenial main
deb [arch=amd64] file:/HOME/Downloads/appdefense/latest/ubuntu trusty main
deb [arch=amd64] file:/HOME/Downloads/guest-introspection-for-vmware-nsx/latest/ubuntu trusty
main
```

d Install the AppDefense Guest Module package using the following commands:

```
apt-get update
apt-get install vmw-glx
```

Note To upgrade or install a specific version, run the following command:

```
apt-get install vmw-glx-<version>
```

3 **For RHEL systems**:

a Obtain and import the VMware packaging public keys using the following commands:

```
wget file:/HOME/Downloads/appdefense/key/VMWARE-APPD-PACKAGING-GPG-RSA-KEY.pub
rpm --import VMWARE-APPD-PACKAGING-GPG-RSA-KEY.pub
```

b Create a file named *appdefense.repo* under `/etc/yum.repos.d`.

c Edit the *appdefense.repo* file with the following contents:

```
 vi /etc/yum.repos.d/appdefense.repo
[repo-appdefense]
name=AppDefense repo
baseurl=file:/HOME/Downloads/appdefense/latest/
enabled=1
gpgcheck=1

[guest-introspection-for-vmware-nsx]
name=Guest Introspection for VMware NSX
baseurl=file:/HOME/Downloads/guest-introspection-for-vmware-nsx/latest/rhel/x86_64/
enabled=1
gpgcheck=1
```

d For RHEL 7.0, 7.3 or 7.4: To install a dependent component, add the following line in the *appdefense.repo* file created in the previous step c.

```
===

[guest-introspection-os-bundle]

name=Guest Introspection OS Bundle

baseurl= file:/HOME/Downloads/guest-introspection-os-bundle/rhel/7.0/

enabled=1

gpgcheck=0

===
```

Note The *baseurl* parameter is represented as *file:/HOME/Downloads/guest-introspection-os-bundle/rhel/<os_version>*. The *os_version* can be RHEL 7.0, 7.3, or 7.4.

e Install the AppDefense Guest Module package using the following commands:

```
yum install vmw-glx
```

Note To upgrade or install a specific version, run the following command:

```
yum install vmw-glx-<version>
```

4 **For CentOS systems**:

a Obtain and import the VMware packaging public keys using the following commands:

```
wget file:/HOME/Downloads/appdefense/key/VMWARE-APPD-PACKAGING-GPG-RSA-KEY.pub
rpm --import VMWARE-APPD-PACKAGING-GPG-RSA-KEY.pub
```

b Create a file named *appdefense.repo* under `/etc/yum.repos.d`.

c Edit the *appdefense.repo* file with the following contents:

```
 vi /etc/yum.repos.d/appdefense.repo
[repo-appdefense]
name=AppDefense repo
baseurl=file:/HOME/Downloads/appdefense/latest/
enabled=1
gpgcheck=1

[guest-introspection-for-vmware-nsx]
name=Guest Introspection for VMware NSX
baseurl=file:/HOME/Downloads/guest-introspection-for-vmware-nsx/latest/centos/x86_64/
enabled=1
gpgcheck=1
```

d For CentOS 7.1, 7.2, 7.3, or 7.4: To install a dependent component, add the following line in the *appdefense.repo* file created in the previous step c.

```
===

[guest-introspection-os-bundle]

name=Guest Introspection OS Bundle

baseurl= file:/HOME/Downloads/guest-introspection-os-bundle/centos/7.1/

enabled=1

gpgcheck=0

===
```

Note The *baseurl* parameter is represented as *file:/HOME/Downloads/guest-introspection-os-bundle/centos/<os_version>*. The *os_version* can be CentOS 7.1, 7.2, 7.3, or 7.4.

e Install the AppDefense Guest Module package using the following commands:

```
yum install vmw-glx
```

Note To upgrade or install a specific version, run the following command:

```
yum install vmw-glx-<version>
```

5 **For SLES systems**:

a Obtain and import the VMware packaging public keys using the following commands:

```
wget file:/HOME/Downloads/appdefense/key/VMWARE-APPD-PACKAGING-GPG-RSA-KEY.pub
rpm --import VMWARE-APPD-PACKAGING-GPG-RSA-KEY.pub
```

b Add the following repository:

```
zypper ar "file:/HOME/Downloads/appdefense/latest/" appdefense
zypper ar "file:/HOME/Downloads/guest-intappdefense.reporospection-for-vmware-
nsx/latest/sles/x86_64/"
guest-introspection-for-vmware-nsx
```

c For SLES 11.4, 12.2, or 12.3: To install a dependent component, add the following line in the *appdefense.repo* file created in the previous step b.

```
zipper ar "file:/HOME/Downloads/guest-introspection-os-bundle/sles/11.4/"
```

Note The *baseurl* parameter is represented as *file:/HOME/Downloads/guest-introspection-os-bundle/sles/<os_version>*. The *os_version* can be SLES 11.4, 12.2, or 12.3.

d Install the AppDefense Guest Module package using the following commands:

```
zypper install vmw-glx
```

Note To upgrade or install a specific version, run the following command:

```
zypper install vmw-glx-<version>
```

6 To verify if AppDefense Guest Module is installed, run the following command with the root privilege:

```
/etc/init.d/vmw_glxd status
```

7 To verify if the Guest Introspection is installed, run the following command with the root privilege:

```
/etc/init.d/vmw_conn_notifyd status
```

The status is running.

Install Guest Module Using Package Manager Command

This method is an alternate method to install AppDefense Guest Module on guest Linux virtual machines (VM) where your application workloads are running. You can use this method if you do not want to configure the repository. The installation of AppDefense Guest Module installs the AppDefense package, and the Guest Introspection package.

- You must complete the prerequisites before the actual installation. For details, refer to Guest Module Install Prerequisites for Linux Systems.
- The Linux VM (or server that is used to supply binaries to VMs) must have access to https://packages.vmware.com. To verify accessibility to *packages.vmware.com*, use the `ping packages.vmware.com` command. Then run the `curl –Is https://packages.vmware.com/appdefense` command. The curl request returns the `HTTP/1.1 200 OK` status code.

Perform the steps as applicable for your Linux distribution.

1 Go to the Linux VM.

2 Go to the link provided in the table and download the Guest Introspection and AppDefense packages for the relevant Linux distribution.

3 To install Guest Introspection andAppDefense Guest Module, run the commands for the appropriate Linux distribution in the **Command to Download Package** column.

Table 3-2. Linux Package and Command to Use for Installation

Linux Distribution	Link to Download Package	Command to Use for Installation
Ubuntu	■ https://packages.vmware.com/guest-introspection-for-vmware-nsx/latest/ubuntu/dists/trusty/main/binary-amd64/Guest-Introspection-for-VMware-NSX-1.0.0.1.9050537-1.ubuntu_x86_64.deb ■ https://packages.vmware.com/appdefense/latest/ubuntu/dists/trusty/main/binary-amd64/vmw-glx_1.2.0.1-9050537_amd64.deb	■ `dpkg –i Guest–Introspection–for–VMware–NSX–1.0.0.0.8809351–1.ubuntu_x86_64.deb` ■ `dpkg –i vmw–glx_1.2.0.0–8809351_amd64.deb`
SLES	■ https://packages.vmware.com/guest-introspection-for-vmware-nsx/latest/sles/x86_64/Guest-Introspection-for-VMware-NSX-1.0.0.0.8809351-1.sles.x86_64.rpm ■ https://packages.vmware.com/appdefense/latest/vmw-glx-1.2.0.0-8809351.x86_64.rpm	■ `rpm –Uvh Guest–Introspection–for–VMware–NSX–1.0.0.0.8809351–1.sles.x86_64.rpm` ■ `rpm –Uvh vmw–glx–1.2.0.0–8809351.x86_64.rpm`

Table 3-2. Linux Package and Command to Use for Installation (Continued)

Linux Distribution	Link to Download Package	Command to Use for Installation
RHEL	■ https://packages.vmware.com/guest-introspection-for-vmware-nsx/latest/rhel/x86_64/Guest-Introspection-for-VMware-NSX-1.0.0.0.8809351-1.rhel.x86_64.rpm ■ https://packages.vmware.com/appdefense/latest/vmw-glx-1.2.0.0-8809351.x86_64.rpm	■ `rpm –Uvh Guest–Introspection–for–VMware–NSX–1.0.0.0.8809351–1.rhel.x86_64.rpm` ■ `rpm –Uvh vmw–glx–1.2.0.0–8809351.x86_64.rpm`
CentOS	■ https://packages.vmware.com/guest-introspection-for-vmware-nsx/latest/centos/x86_64/Guest-Introspection-for-VMware-NSX-1.0.0.0.8809351-1.centos.x86_64.rpm ■ https://packages.vmware.com/appdefense/latest/vmw-glx-1.2.0.0-8809351.x86_64.rpm	■ `rpm –Uvh Guest–Introspection–for–VMware–NSX–1.0.0.0.8809351–1.centos.x86_64.rpm` ■ `rpm –Uvh vmw–glx–1.2.0.0–8809351.x86_64.rpm`

4 To verify if AppDefense Guest Module is installed, run the following command with the root privilege:

```
/etc/init.d/vmw_glxd status
```

5 To verify if the Guest Introspection is installed, run the following command with the root privilege:

```
/etc/init.d/vmw_conn_notifyd status
```

The status is running.

Integrate Applications

4

You can optionally integrate AppDefense with other provisioning systems that can help to define appropriate and allowed behaviors such as NSX Data Center for vSphere, vRealize Automation, and Puppet Enterprise. AppDefense supports integration with partner security vendors, such as Splunk, IBM QRadar, NetWitness, Carbon Black, Aqua Security, and SecureWorks.

This chapter includes the following topics:

Configuring AppDefense with NSX Data Center for vSphere

AppDefense uses NSX Data Center for vSphere to handle the network virtualization and isolation. Taken together, vSphere and NSX Data Center for vSphere provides a platform required to completely isolate each application from other workloads and underlying system components. AppDefense offers an extra layer to establish the *normal* operating behaviors for each isolated application, and can take varied responses when an application deviates from its *normal* behaviors. Since AppDefense sits between the hypervisor and NSX Data Center for vSphere, it is immune from attack or compromise even when a workload is afflicted.

When AppDefense detects a threat, it uses vSphere and NSX to act automatically. NSX is used for the quarantine remediation action.

Configuring NSX Data Center for vSphere

To quarantine virtual machines using AppDefense, you can set up NSX Data Center for vSphere as follows:

- Prepare Host Clusters for NSX Data Center for vSphere. For more details, refer to NSX documentation.
- NSX Data Center for vSphere is configured as per details mentioned in the Configure the AppDefense Appliance.

View the Quarantined VMs in NSX Data Center for vSphere

1 Log in to the vSphere Client.

2 Navigate to **Networking & Security** > **Groups and Tags**.

3 Click the **Security Tags** tab.

VMs quarantined by AppDefense appears under the *AppDefense.VulnerabilityFound* tag.

Configuring AppDefense with Splunk

This section covers the steps required to configure AppDefense to integrate with Splunk. After integration, the alarms (and the metadata) from AppDefense can be viewed on Splunk interface.

Prerequisites

You have installed and configured Splunk. Based on the Splunk documentation, install the *REST API Modular Input* endpoint on an Indexer/Forwarder and the Application on a Search Head. For more details, refer to the Splunk documentation (the basics of indexer cluster architecture).

Procedure

1 To integrate Splunk from the AppDefense Manager, provision the API Key.

a Log in to the AppDefense Manager.

b At the bottom of the left navigation pane, click the setting ( ) icon.

c Click **Integrations**, and then click **Provision New API Key**.

The **New Integration** window appears.

d In the **New Integration** window, select the following parameters.

Parameter	Description
Integration Name	Enter a name for your integration.
Integration Type	Select the partner security vendor that you want to integrate. Select **Splunk**.

e Click **Provision**.

The **New integration Created** window displays the URL and the Authorization/API key. Keep this window open until the integration is done, or note down the information and preserve to be used during integration.

Following is the example of the information available in the **New integration Created** window:

```
Endpoint URL=https://appdefense.vmware.com/partnerapi/v1/orgs/13

API Key=Bearer xxxxxxxxxxxxxx9.exxxxxxxxxxxxxxx.xxxxxxxxx_xxxxxxx_xxxxxxxxxxw-
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

Important When you close the **New integration Created** window, there is no way to get back to the authorization/API key. If you lose the authorization/API key, contact AppDefense support team at *appdefense_support@vmware.com*.

f Click **OK** ONLY when you have saved the information.

2 Go to Splunk, and integrate Splunk to use with AppDefense.

a Download and install the Splunk REST API Modular Input from the Splunkbase.

b (Optional) Create an index to be used when configuring the REST API Modular Input endpoint.

c To configure a new REST API Input, go to Splunk **Settings** > **Data inputs > REST**, and click **New**. Configure the following parameters.

Option	Description
Endpoint URL	Paste the URL that was exposed by AppDefense Manager when a new integration was provisioned for Splunk.
HTTP Method	Select **GET** from the drop-down menu.
Authentication Type	Select **None** from the drop-down menu.
HTTP Header Properties	The Authorization property is exposed by AppDefense Manager when a new integration was provisioned for Splunk followed by the key. For example: *Authorization=Bearer eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJQcmluY2lwYWwvMjQ4MCJ9.cbBLUCLfHElpv9NMZmvUQPhCtgnkdg9wmTSXHSrojJSDKtuY0NzHEHeStkQnP16wLQeGKRtDIISbGdEispbvPw.* **Note** Append *Authorization=Bearer* in the beginning followed by the key.
Response Type	Select **json** from the drop-down menu.
Source Type > Set source type	Select **Manual** from the drop-down menu.
Source Type > Source type	Enter **app_defense_alarms**.
More settings	Click **More settings**.
More settings > Index	To store the data in AppDefense, select an index from the drop-down menu. For example, *appd*.

After the new REST endpoint is created, new alarms from AppDefense start to show up on Splunk. You can search and analyze the alarms using the Splunk query language.

Configure Puppet

You can integrate Puppet Enterprise with AppDefense optionally. AppDefense uses the Puppet orchestrator to get the application scope and members. Puppet configuration takes precedence over scope, service definitions, and virtual machine (VM) assignments done directly from the AppDefense Manager. AppDefense supports a VM that is being associated with a single service.

Prerequisites

You have installed and configured Puppet Enterprise.

Procedure

1 Log in to the AppDefense Appliance virtual appliance.

Make sure that you are in the **AppDefense > Status** tab.

2 Click the **Configuration** tab, and enter information in all the parameters under **Puppet Configuration** as follows.

Option	Description
Puppet Master URL	Enter the authentication RBAC URL. For example: *https://{puppetMasterIP}:4433/rbac-api/v1/auth/token*.
Puppet Orchestrator URL	Enter the puppet orchestrator URL. For example: *https://{orchestratorIP}:8143/orchestrator/v1*.
Puppet DB URL	Enter the puppet database query URL. For example: *https://{DB IP}:8081/pdb/query/v4*.
Puppet Master username	Enter user name for the Puppet Enterprise user account.
Puppet Master Password	Enter a password the for Puppet Enterprise user account.
Puppet Configured	Set to *true* to start connecting to puppet.

You can now get the application scope and members from the Puppet orchestrator.

Configuring AppDefense to Integrate with vRealize Automation

You can optionally configure AppDefense with vRealize Automation to capture application context as an XaaS Blueprint.

You must first import and configure AppDefense workflows in vRealize Orchestrator (vRO) Plug-In.

Now use vRealize Automation (vRA) to capture application context as an XaaS Blueprint.

Configure AppDefense Workflow in vRealize Orchestrator

You can import and configure AppDefense workflows in vRealize Orchestrator Plug-In, and then use vRealize Automation (vRA) to capture the application context as an XaaS blueprint.

Prerequisites

You have installed and configured vRA and vRO Plug-In for vCenter Server.

Procedure

1 Log in to AppDefense Appliance.

   a Create a public/private key pair using OpenSSL. For example, `openssl genrsa –aes256 –out vro.pem 2048`.

   b When prompted, enter a password. You need this password later.

   c Convert the key pair to Privacy Enhanced Mail (PEM) certificate using OpenSSL. For example, `openssl req –new –x509 –key vro.pem –out vro_public.cer`.

   d Keep all the parameters as default except for the Common Name parameter, which needs a value. The value is not important to AppDefense Appliance, so enter any convenient string as the Common Name parameter value.

   e Copy the PEM certificate to the AppDefense Appliance host under any temporary folder.

   f Go to `/opt/vmware/goldilocks/etc` and open *application.properties* file. Look for *server.ssl.trust-store* and *server.ssl.trust-store-password* properties.

   g Use the `keytool` command to import the certificate to the AppDefense Appliance TrustStore. For example, `keytool –importcert –file vro_public.cer –keystore <trust Store> –storepass <TrustStore password>.`

   h Restart the AppDefense Appliance service (*glx.service*) using the `sudo systemctl start glx.service` command.

2 Log in to vRealize Orchestrator (vRO) client.

   a Connect to the vRealize Orchestrator client in a Web browser. For example, *https://vRO_appliance_ip:8281/vco*.

   b Click **vRealize Orchestrator Client**.

   The client file is downloaded.

   c (Optional) Click the download and follow the prompts.

   d Log in by using the Orchestrator client user name and password.

3 In the vRO client, use the **Create a keystore** workflow as follows.

   a Click the **Workflows** view in the Orchestrator client.

   b In the workflow hierarchical list, expand **Library > Configuration > Keystores**.

   c Right-click the **Create a keystore** workflow, and click **Start workflow**.

   d Enter a name for keystore, for example, **`AppDefense–keystore`**, and click **Submit**.

4 In the vRO client, use the **Add key** workflow as follows.

   a Click the **Workflows** view in the Orchestrator client.

   b In the workflow hierarchical list, expand **Library > Configuration > Keystores**.

   c Right-click the **Add key** workflow, and click **Start workflow**.

   d Enter a name for keystore, for example, **`AppDefense-keystore`**, and click **Submit**.

   e Click the **Not set** link.

   f Expand the **Keystores** folder and select the **`AppDefense-keystore`** keystore created earlier.

   g In the **Common parameters** window, enter the following parameters.

Option	Description
Key alias	Give any alias name.
PEM encoded key and certificate chain	Paste the PEM-encoded private key and public certificate created in step 1. First paste the private key, and then paste the public certificate below the private key.
Key password if any	Enter the password created in step 1 b.

   h Click **Submit**.

5 Download the vRO package for AppDefense as follows.

   a Go to the vRO package downloads page (http://downloads.vmwaredrx.com/vro-plugin/1.1.0-GA/vro-workflow-1.1.0.0.package).

   b The vRO package is downloaded.

   The package contains the required Workflows and Actions (namely *ApplicationContext*, *Scope*, *ApplicationContext_PostProvisioning* workflow, four actions, and a configuration element.

6 In the vRO client, import the downloaded package as follows.

   a Click **Design** from the list, and then click the **Packages** icon.

   b Click **Import package**.

   c Select and import the vRO package downloaded in step 5.

   d Go to **Library > HTTP-REST > Configuration**.

e Right-click **Add a REST host** workflow, and click **Start workflow**.

f Enter details as follows.

Option	Description
Add a REST host	■ Enter name of the host as **`Appliance`**. ■ Enter details of the AppDefense Appliance host URL. For example, *https://<Appliance_IP>:port*. ■ Click **Yes** for **If set to true, certificate is accepted silently and the certificate is added to the trusted store**. ■ Keep other parameters by default, and click **Next**.
Host Authentication	Keep the default parameter, and click **Next**.
Proxy Settings	Enter proxy settings, if any.
Advanced	■ Click **Yes** for the **Verify whether the target hostname matches the names stored inside the server's X.509 certificate**. ■ Click **Not set** for **The PrivateKeyEntry to use for client certificate authemtication**. ■ Expand **Keystores**, and select the keystore and key created in step 4. ■ Click **Select** and then click **Submit**.

A new HTTP-REST host named **`Appliance`** is added to the vRO inventory.

7 Configure the **`Appliance`** for vCenter Server as follows.

a Click the **Workflows** view in the Orchestrator client.

b In the workflow hierarchical list, expand **Library > vCenter > Configuration**.

c Right-click the **Add a vCenter Server instance** workflow, and click **Start workflow**.

d Enter details as follows.

Option	Description
Set the vCenter Server instance properties	■ Enter the details of vCenter Server host IP and port number. ■ Click **Yes** for **Will you orchestrate this instance**. ■ Click **Yes** for **Do you want to ignore certificate warnings**. ■ Click **Next**.
Set the connection properties	■ Click **No** for **Do you want to use a session per user method to manage user access to the vCenter Server system**. ■ Enter vCenter Server administrator credentials. ■ Click **Next**.
Additional Endpoints	Keep the default parameter, and click **Submit**.

8 Configure the **`Appliance`** for vRA as follows.

a Click the **Workflows** view in the Orchestrator client.

b In the workflow hierarchical list, expand **Library > vRealize Automation > Configuration**.

c Right-click the **Add a vRA host** workflow, and click **Start workflow**.

d Enter details as follows.

Option	Description
Add a vCAC host	■ Enter the details of vRA host name and URL. ■ Click **Yes** for **Automatically install SSL certificates**. ■ Keep other parameters by default, and click **Next**.
Host Authentication	■ Enter the **Tenant** details. ■ Enter the vRA credentials. ■ Click **Submit**.

9 Configure the **Appliance** for IaaS host of a vRA host as follows.

a Click the **Workflows** view in the Orchestrator client.

b In the workflow hierarchical list, expand **Library > vRealize Automation > Configuration**.

c Right-click the **Add the IaaS host of a vRA host** workflow, and click **Start workflow**.

d Enter details as follows.

Option	Description
Common parameters	Click **Not set** and then select the vRA host added in step 8.
Add a IaaS host	Keep other parameters by default, and click **Next**.
Host Authentication	■ Enter the **IaaS** host credentials. Enter vRA credentials, typically user name as *administrator* and password as *VMware1!*. ■ Keep other parameters by default, and click **Next**. ■ Enter the **Domain** as *VMWAREM*. ■ Click **Submit**.

10 Configure the **ApplicationContext_PostProvisioning** as follows.

a Click the **Workflows** view in the Orchestrator client.

b In the workflow hierarchical list, expand **Goldilocks > ApplicationContext_PostProvisioning**.

c Click **Edit**.

d Go to **Attributes** section at the bottom.

Option	Description
applianceHost	Click **Value** and then select the REST host (**HTTP-REST** section) added in step 6.
host	Click **Value** and then select the vRA host added in step 8.
	■ Enter the **IaaS** host credentials. Enter vRA credentials, typically user name as *administrator* and password as *VMware1!*. ■ Keep other parameters by default, and click **Next**. ■ Enter the **Domain** as *VMWAREM*. ■ Click **Submit**.

What to do next

Configure the XaaS blueprint in vRA.

Configure XaaS Blueprints in vRealize Automation

AppDefense uses vRealize Automation (vRA) Plug-In to capture the application context as an XaaS blueprint in vRA. After importing and configuring a workflow in vRO, capture application context as an XaaS blueprint in vRA.

Prerequisites

- You have installed and configured vRA and vRO Plug-In for vCenter Server.
- You have imported and configured a workflow in the vRO client.

Procedure

1. Log in to the vRealize Automation client.
2. Go to **Design > XaaS > XaaS Blueprints**.
3. Configure the **ApplicationContext** workflow as follows.
   a. Click **New**, and then select the **Orchestrator > AppDefense > ApplicationContext** workflow.
   b. Enter the name and click **Next**.
   c. (Optional) In case the XaaS blueprint exists, select the XaaS blueprint and click **Next**. On the next page, click the **Refresh** icon.
   d. Click **Next**, and then click **Finish**.
   e. Select the XaaS Blueprint and click **Publish**.
4. Go to **Design > XaaS > XaaS Blueprints**.
5. Configure the **Scope** workflow as follows.
   a. Click **New**, and then select the **Orchestrator > AppDefense > Scope** workflow.
   b. Enter a name for the scope and click **Next**.
   c. (Optional) In case the XaaS blueprint exists, select the XaaS blueprint and click **Next**. On the next page, click the **Refresh** icon.
   d. Select **Conditional** from the **Visible** drop-down menu.
   e. Click **Edit Condition**, and select the following options.

Option	Description
First drop-down menu	Scope
Second drop-down menu	Equals
Third drop-down menu	Constant
Text field	Other

f Click **Apply**. Click **Next**, and then click **Finish**.

g Select the XaaS blueprint and click **Publish**.

6 Use any of your existing blueprints (if you have one already) or repeat all the preceding steps to create a blueprint.

7 Go to **Design > Blueprints** , and click **ApplicationContext** XaaS blueprint.

a In the **Design Canvas**, drag the created **ApplicationContext** XaaS blueprint and drop in the **Design Canvas**, one each for every type of provisioning blueprint.

b Create a dependency from XaaS blueprint to the Provisioning blueprint.

c Click **ApplicationContext** XaaS blueprint, and enter the relevant values for following fields.

- Service Name
- Service Type
- Service Description
- OpenSourceComponent
- GeoLocation

d In the **Design Canvas**, for each provisioning element (for example, *vsphere_machine*), select the **Properties** tab.

e Click the**Custom Properties** tab, and click **New**.

Option	Description
Name	Extensibility.Lifecycle.Properties.VMPSMasterWorkflow32.MachineProvisioned
Value	__*,*

f Click **Save**, and then click **Finish**.

8 Go to **Design > Blueprints** , and click **Scope** XaaS Blueprint.

a Enter the relevant value for the **Scope** parameter.

b Click **Save**, and then click **Finish**.

9 Create an Event Subscription as follows.

a Go to **Administration > Events > Subscriptions**.

b On the **Event Topic** tab, click **New**, and then click **Machine provisioning**. Click **Next**.

c On the **Conditions** tab, click **Run based on conditions**.

d In the drop-down menu, click **All of the following** and select the following parameters.

Option 1	Option 2	Option 3
Data > Lifecycle State > Lifecycle state name	Equals	Click **Constant** and select **VMPSMasterWorkflow32.MachineProvisioned** from the drop-down menu.

e Click **Add expression** and select the following parameters.

Option 1	Option 2	Option 3
Data > Lifecycle State > State phase	Equals	Click **Constant** and select **PRE** from the drop-down menu.

f Click **Add expression** and select the following parameters.

Option 1	Option 2	Option 3
Data > Lifecycle State > State phase	Equals	Click **Constant** and select **PRE** from the drop-down menu.

Click **Next**.

g On the **Workflow** tab, expand the **Orchestrator** folder and select **AppDefense > ApplicationContext_PostProvisioning**.

Click **Next**.

h On the **Details** tab, select the **Blocking** check box.

i Click **Finish**, and then click **Publish** the event subscription.

Blueprint is created and configured.

10 Provision the new instance using the created blueprint as follows.

a Click **Catalog**. Locate the published blueprint and click **Request** and respond to prompts.

Verify the progress.

You can now capture the application context as an XaaS blueprint in vRA.

What to do next

For more details on blueprints, refer to vRealize Automation documentation.

Uninstalling AppDefense Modules

5

You must uninstall earlier deployed AppDefense Modules, before installing the new version.

This chapter includes the following topics:

Uninstall the AppDefense Host Module

You must uninstall earlier deployed AppDefense Host Module, before installing the new version.

Prerequisites

AppDefense Host Module is installed on the ESXi host.

Procedure

1. Go to the ESXi host, and open the control panel.
2. Go to **Programs and Features**.
3. Select **VMware AppDefense**, and click **Uninstall**.

What to do next

Uninstall AppDefense Guest Module from the guest virtual machines.

Uninstall the AppDefense Guest Module

You must uninstall earlier deployed AppDefense Guest Module, before installing the new version.

Uninstall the AppDefense Guest Module for the Windows System

If you have an earlier version of the guest module, then you must uninstall the earlier version before installing the new version. If you had a beta set up, this step is optional. You can uninstall using control panel or command prompt.

- To uninstall using control panel:
  a. Go to the guest VM, and open control panel.

b Go to **Programs and Features**.

c Select VMware AppDefense, and click **Uninstall**. Follow the prompts to uninstall AppDefense.

- To uninstall using command prompt:

a Go to the guest VM, and open command prompt with the administrator privilege.

b Run the `msiexec /x AppDefense-x64-XXXXX.msi /qn` command.

The AppDefense Guest Module components are removed from the system.

Uninstall the AppDefense Guest Module for the Linux System

Prerequisites: AppDefense Guest Module is installed. You have root privileges on the Linux system.

To uninstall the guest module using the command prompt, perform the following steps.

- For uninstalling package from Ubuntu system, run the `apt-get remove vmw-glx Guest-Introspection-for-VMware-NSX` command.
- For uninstalling package from RHEL system, run the `yum remove vmw-glx Guest-Introspection-for-VMware-NSX` command.
- For uninstalling package from SLES system, run the `zypper remove vmw-glx Guest-Introspection-for-VMware-NSX` command.

The AppDefense Guest Module components installed on the Linux system are uninstalled.

Upgrading AppDefense

6

If you have earlier version or a beta set up for AppDefense Appliance and AppDefense Modules, you must upgrade to latest available version.

This chapter includes the following topics:

- Upgrade the AppDefense Appliance
- Upgrade Host Module
- Upgrade Guest Module for Windows System

Upgrade the AppDefense Appliance

You must upgrade previous version or beta set up for AppDefense Appliance.

Prerequisites

You have previous version or beta set up for AppDefense Appliance.

Procedure

1. Log in to the AppDefense Appliance from vCenter Server using the *admin* credentials.
2. Stop the running appliance using the `sudo systemctl stop glx.service` command.
3. Open the `/opt/vmware/goldilocks/etc/application.properties` file.
4. Copy and save the *goldilocks.appliance.uuid* and *goldilocks.appliance.api-key* to your local desktop or laptop to use later.

   For example:

   ```
   goldilocks.appliance.uuid=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
   goldilocks.appliance.api-key=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
   xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
   xxxx
   ```

5. Copy the NSX and vCenter Server configuration settings from the `application.properties` file.
6. Power off the appliance.

7 Deploy AppDefense Appliance in the vCenter Server.

Note Do NOT Provision the Deployed AppDefense Appliance.

8 Delete the older appliance from vCenter Server after you complete deploying the new appliance.

9 Configure the AppDefense Appliance. In the **AppDefense Manager Configuration** settings, use the *goldilocks.appliance.uuid* and *goldilocks.appliance.api-key* saved in step 4.

AppDefense Appliance is upgraded.

What to do next

Upgrade host and guest modules.

Upgrade Host Module

You must update configuration for AppDefense Host Module when a newer version is available.

Prerequisites

Newer version of AppDefense Host Module is available.

Procedure

1 Log in to the vCenter Server and note down the IP address of the host.

2 Log in to the AppDefense Manager.

3 At the bottom of the left navigation pane, click the setting () icon.

4 Click **Inventory**, and then click the **Hosts** tab.

5 Search and select the host with an IP address noted down in the step 1.

6 To upgrade the host, select one of the following options.

Parameter	Description
Install/Update	To update the host module, select the required host version. You can schedule the upgrade as **Immediate** or **Schedule** later by specifying hour and day.
Auto-Update	Select the option if you want to update the host module automatically when a newer version is released. You can schedule the upgrade as follows: ■ **Immediate**: When a new version is released, host module gets automatically upgraded. ■ **Schedule**: Schedule the upgrade later by specifying hour and day. ■ **Disable**: Disable the automatic upgrade or a scheduled upgrade.
Update Configuration	If there is any mismatch, update the host module configuration. You can update configuration only for the pre-installed host modules.

7 To upgrade the host module, click **Confirm** or **OK**.

You can view the status of the upgrade as initiated, queued, or success with details. It takes few minutes to complete. Refresh the page after few minutes. You see that the action is finished successfully and AppDefense Host Module version appears.

8 Verify if the AppDefense Host Module is upgraded correctly.

a Log into the ESXi host.

b Use the `esxcli software lib list | grep glxhost` command to verify.

AppDefense Host Module is upgraded.

What to do next

Upgrade the AppDefense Guest Module.

Upgrade Guest Module for Windows System

You must upgrade AppDefense Guest Module on the guest virtual machines (VM) where your applications are running.

This upgrade procedure is applicable for the Windows system.

Prerequisites

- You have satisfied all the Guest Module Install Prerequisites for Windows Systems.
- You have Uninstall the AppDefense Guest Module.

Procedure

1. Log in to the AppDefense Manager.
2. At the bottom of the left navigation pane, click the setting () icon.
3. Click **Downloads**, and then click the **Guest Module** tab.

   The *AppDefense msi installer* for the Windows operating system is available for download. Example, *AppDefense-x64-1.2.0.2-8845982.msi*.
4. Download the latest *AppDefense msi installer*.
5. Install the Guest Module on Windows System using UI or command prompt.

AppDefense Guest Module are upgraded on the guest virtual machines.

Troubleshooting AppDefense 7

This section describes how to monitor and troubleshoot the AppDefense by using the AppDefense Manager, AppDefense Appliance, vSphere Web Client, vCenter Server, and other AppDefense components, as needed.

This chapter includes the following topics:

Collecting Logs Manually

You can manually collect the support bundle data for the ESXi hosts on which AppDefense is running. This diagnostic information contains AppDefense specific logs and configuration files that a VMware Technical Support uses when addressing a support request.

Prerequisites

- You have not enabled the automatic log collection feature from AppDefense Manager.
- You are requested to upload the support bundle from VMware Technical Support.

Procedure

1. Log in to the vSphere Web Client.

   Your account must have *administrative* privileges, or has the *Global.Diagnostics* permission.
2. Select the required ESXi host or data center for which you want to collect the logs, and then click **Actions** > **Export System Logs**.
3. If a group of ESXi hosts are available, select the host or group of hosts from the list.
4. Select the required logs. The default selection contains many files. You must select **Logs > System** and **Virtual Machines > logs**.
5. To download the support bundle, select the required location.

6 You can attach the file to your service request. You can attach the generated support bundle to the service request using vSphere Web Client.

   a Go to **Administration** > **Support > Upload File to Service Request**.

   b Enter your service request ID.

   c Click **Choose File**, and select the downloaded support bundle.

   d Click **OK**.

   For more details, refer to the Knowledge Base article.

Troubleshooting AppDefense Appliance

This section describes how you can troubleshoot problems related to configuration, connectivity, or password for the AppDefense Appliance.

How to Verify Appliance Connectivity Manually

You can verify connectivity for the AppDefense Appliance manually.

Problem

You want to verify connectivity for the AppDefense Appliance.

Solution

1 Log in to the AppDefense Appliance VA from vCenter Server using the *admin* credentials.

2 Verify the connectivity to the AppDefense Manager using the `S` command.

   Output must be `200 OK`.

3 Log in to vCenter Server (https://<vCenter FQDN or IP address>:9443), and verify the connectivity using the following command:

```
wget --spider --no-check-certificate --tries 3 --timeout=10
```

   Output must be `302 Found`.

   If you find issues related to vCenter Server connectivity testing, refer to the vCenter Server online documentation.

4 If the vCenter Server is configured with fully qualified domain name (FQDN) but not resolvable by DNS, or the AppDefense Manager host name is not resolvable by DNS, add FQDN and IP address mapping for the vCenter Server in the `/etc/hosts` file on the AppDefense Appliance. Go to the`/etc/hosts` file using the `sudo` command, and verify or add FQDN and IP address mapping as given in the following example:

   <vCenter IP address> <vcenter FQDN>

   <AppDefense Manager IP address> appdefense.vmware.com

Appliance Not Getting an IP Address from DHCP Server

After deploying AppDefense Appliance in the vCenter Server, the appliance is not getting IP address from the DHCP server.

Solution

1. Log in to the AppDefense Appliance from the vCenter Server using the *admin* credentials.
2. Modify the `10-eth0.network` file using the `sudo` command as follows:

   ```
   sudo vi /etc/systemd/network/10-eth0.network
   ```

   File content should be similar as the following example:

   ```
   [Match]
   Name=eth0

   [Network]
   DHCP=ipv4
   [DHCP]
   UseDomains=true
   ClientIdentifier=mac
   ```

3. Restart the network service using the `sudo systemctl restart systemd-networkd` command.

If you are still facing problems, refer to the Photon documentation to configure IP address, DNS, and gateway manually.

Configured Static IP Address for AppDefense Appliance Is Not Working

After deploying AppDefense Appliance in the vCenter Server, the appliance is not getting IP address.

Solution

1. Log in to the AppDefense Appliance from the vCenter Server using the *admin* credentials.
2. Modify the `10-eth0.network` file using the `sudo` command as follows:

   ```
   sudo vi /etc/systemd/network/10-eth0.network
   ```

   File contents are similar as the following example:

   ```
   [Match]
   Name=eth0

   [Network]
   Domains=dom1.example.com dom2.example.com
   Gateway=192.168.139.253
   ```

```
Address=192.168.139.195/22
DHCP=no
[DHCP]
Use DNS=false
```

3 Modify the `/etc/systemd/resolvd.conf` and make sure set the DNS entries as similar as the following example:

```
[Resolve]
DNS=192.168.140.1 192.168.140.2
```

4 Restart the network service using the `sudo systemctl restart systemd–networkd` command.

AppDefense Appliance Is Not Connecting to vCenter Server Due to SSL Handshake Error

AppDefense Appliance is not getting connected to vCenter Server due to the SSL handshake error.

Problem

You see an error similar to:

`javax.net.ssl.SSLHandshakeException:`

`sun.security.validator.ValidatorException: PKIX path building failed:`

`sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target.`

Solution

1 Stop the *glx* service using the `sudo systemctl stop glx.service` command.

2 Delete the *vmwarecerts* file using the `rm /opt/vmware/goldilocks/etc/vmwarecerts` command.

3 Start the *glx* service using the `sudo systemctl start glx.service` command.

If these steps do not solve the problem, then see the `/var/log/goldilocks/pre–start.log` file and report the error to the AppDefense support team.

Hardware and Product Version Information Shows as Unknown

Hardware and the product version information on a virtual machine (VM) is shown as `Unknown`.

Cause

This problem might happen because the VM firewall setting blocks the outgoing connection to the AppDefense Appliance.

Solution

These steps are applicable for the Windows VM.

Procedure

1. Go to the VM and open the Firewall settings from the **Advanced Configuration** menu.
2. If the Windows firewall parameter is **ON**, remove any rule that is blocking the connection between the VM and the AppDefense Appliance.

How to Reset Password For AppDefense Appliance Administrator

You are locked out of AppDefense Appliance that has *admin* privileges.

Cause

You entered incorrect password for the AppDefense Appliance for three times.

Solution

1. Log in to the AppDefense Appliance from vCenter Server using the *root* credentials.
2. Verify if the *admin* account is locked using the `pam_tally2 –u admin` command.
3. If the *admin* account is locked, then use the following command to reset the password.

   ```
   pam_tally2 –r –u admin
   ```

4. If necessary, change the *admin* user password using the `passwd admin` command.

   AppDefense Appliance *admin* user password is changed.

Troubleshooting AppDefense Modules

This section describes how you can troubleshoot problems related to installation, or configuration for the AppDefense Host Module or AppDefense Guest Module.

Known Limitation with Linux VMs

The following section describes the known problems of AppDefense with Linux VM.

Solution

1. **Problem**: Guest driver uses the VMware Virtual Machine Communication Interface (VMCI) channel to communicate with the host.

   Virtual Machine Communication Interface (VMCI) is an upstream gateway and has a known problem with the *VMCI with vsock (1.0.1.0-k)*, *vmw_vsock_vmci_transport (1.0.2.0-k)*, and *vmw_vmci (1.1.3.0-k)* drivers.

   To work around this problem, upgrade the mentioned drivers to the versions suggested by the Linux distribution.

2 **Problem**: AppDefense does not work in virtual machines that have Fault Tolerance enabled.

The underlying infrastructure required by AppDefense does not work with Fault Tolerant virtual machines. This limitation applies to both Linux and Windows guest virtual machines. On fault tolerant systems, AppDefense drivers do not run due to VMCI Interop issues. You must disable Fault tolerance (FT). For more information about disabling FT, refer to the Knowledge base article.

3 **Problem**: The parent process command-line Information is shown to provide more information about the process. Sometimes, the parent process command-line Information is not correct or reliable.

The parent process information is not being used for any policy making or decision. Following information is displayed for the processes that exist when the AppDefense guest agent starts:

- Process binary absolute path
- Process MD5 and SHA256 hashes
- Command line the process started with PID (process identity)

Following information is displayed for the processes that are created after the AppDefense guest agent starts:

- Parent Process binary absolute path
- Parent Process MD5 and SHA256 hashes
- Parent Command line the process started with PPID (parent process identity)

AppDefense Guest Module Installation Fails

You have a beta set up for the AppDefense Guest Module, and installation of the latest version of the AppDefense Guest Module fails.

Solution

1 Go to the virtual machine where AppDefense Guest Module is installed and uninstall the earlier version for AppDefense Guest Module using the following commands.

```
GIInstaller.bat uninstall glxgi
 GIInstaller.bat uninstall gisvc
```

2 Install the latest version of the AppDefense Guest Module based on the operating system of your virtual machine. For details, refer to Install the Guest Module.

Virtual Machine Shows Status as Critical

Guest virtual machine shows status as *critical*.

Solution

1 In the guest virtual machine (VM), run the `sc query glxgi` command.

Verify if the status shows as `running`. If the status is not `running`, then verify that the VM hardware version is 13 or later.

2 Enable the guest integrity feature for a VM using the vCenter Server.

   a Ensure that the VM is powered off.

   b Go to the required VM in thevCenter Server, and then click the **Configure** tab.

   c Go to **Settings > VM Options**, and click **Edit**.

   d Go to **Advanced > Configuration Parameters**, and click **Edit Configuration**.

   e Add a parameter named **`guestIntegrity.enable`**, and set the values as **`TRUE`**. Click **OK**.

   f Power on the VM.

3 In the ESXi host, run the `/etc/init.d/glxhostuwd status` command.

   Verify if the status shows as `running`. If status is not displayed, then the host module is not installed. Install the host module. For details, refer to Install the Host Module.

4 Update the host module configuration. For details, refer to Upgrade Host Module.