FORCEPOINT

POWERED BY Raytheon

Troubleshooting Guide

Advanced Malware Detection On-Premises Manager

v1.1

Published 2019

Every effort has been made to ensure the accuracy of this document. However, Forcepoint makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Forcepoint shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this document or the examples herein. The information in this documentation is subject to change without notice.

Last modified 20-May-2019

Contents

1 Troubleshooting the Lastline Manager virtual machine installation

Troubleshooting Guide | AMD OP | v1.1

The Lastline Manager virtual machine (VM) is created the first time the Advanced Malware Detection On-Premises system reboots, right after the installation of the operating system (OS). The kickstart script responsible for driving the installation of the OS creates an additional installation script under /etc/init.d that is configured to run as a service on first boot via the **chkconfig** tool. The script creates the VM, installs the Lastline software and configures the Advanced Malware Detection On-Premises system to support the Lastline VM. The script removes itself from the services list after execution.

The installation script creates the VM using the **virt-install** command as follows:

```
virt-install --virt-type=kvm --name tmp_lastline --ram 49152
--vcpus=12 --os-variant=ubuntu14.04 --hvm --
network=bridge=virbr0,model=virtio --graphics vnc --disk
path=/data/
lastline.raw,size=4096,bus=ide,format=raw,cache=none,io=nati
ve --cdrom=/data/ISO/LL_ISO --wait=60 --noautoconsole
```

Installation overview

The VM installation process consist of 3 stages:

1. Creation of the VM using the **virt-install** tool.
2. Automated installation of the Lastline software using the same tool that created the VM (**virt-install**). This process requires no input from the user.
3. Upon reboot, the VM obtains an IP from the host system via DHCP.

Scripts

The VM installation involves 2 scripts:

- lastline-virt
- lastline-virt-install

The first script (**lastline-virt**) is configured to be executed as a service upon first boot. The main purpose of this script is to kick off the installation script and detach it from the execution shell, ensuring the OS does not kill the installation service when enforcing the Linux time limit for starting services.

After the child script is detached, the parent removes itself from the list of services so it does not run again in the future. Then, it finishes execution and exits with a success code to let the OS know everything went well, while the actual installation of the VM is still in progress running in the background.

The second script (**lastline-virt-install**) performs the actual creation/installation of the VM.

Installation steps

The lastline-virt-install script creates the VM, installs the Lastline Manager software, configures DHCP in the host system, and updates the VM configuration. It executes as follows:

1. The **lastline-virt-install** script runs the **virt-install** tool as a detached command (notice the parentheses and the '& disown' at the end) to create the VM and install the Lastline software in a single step as described below:

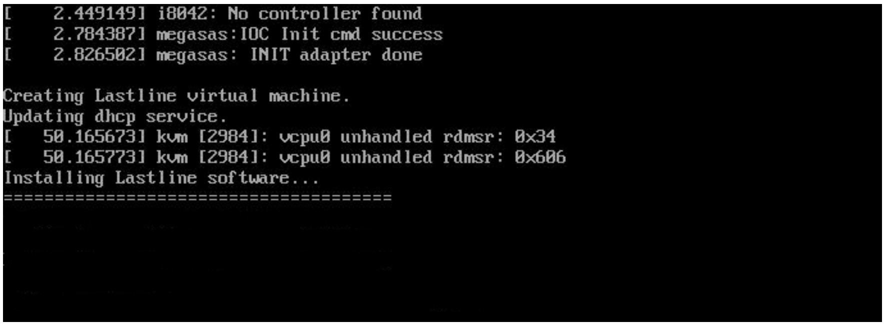
   ```
   (virt-install --virt-type=kvm --name tmp_lastline --ram
   49152 --vcpus=12 --os-variant=ubuntu14.04 --hvm --
   network=bridge=virbr0,model=virtio --graphics vnc --disk
   path=/data/
   lastline.raw,size=4096,bus=ide,format=raw,cache=none,io=nati
   ve --cdrom=/data/ISO/branded_lastline-manager-725~6-6547-
   39c4616.iso --wait=60 --noautoconsole >> ${LOGFILE} 2>&1 &
   disown)
   ```

   The installation process takes approximately 20 minutes to complete. No output is generated since all activity is happening inside the guest VM.

   NOTE: We use the IDE driver for the virtual disk because the guest system cannot detect disks running with the high performance virtual driver (virtio). Ubuntu's 14.04 installation scripts cannot see drives that are named **vda** as required by the virtio driver. Only **sda** and **hda** are supported by the scripts. We update the VM configuration to use the right driver (virtio) in step 4 below, after the installation is complete.
2. After the VM is created, the script updates the DHCP configuration in the host system and assigns the new VM the default IP of 10.0.0.10.
3. The script waits for the VM to become online, then it pings the default IP (10.0.0.10) until the Lastline Manager responds. If the manager does not respond within 30 minutes, the installation fails and exits.
4. After the installation is complete, the VM shuts down to update the configuration of the disk driver from IDE to virtio.
5. The VM is configured to start on boot.
6. The Advanced Malware Detection On-Premises system is rebooted to complete installation.

Troubleshooting a stalled installation

The Advanced Malware Detection On-Premises Manager installation should take approximately 20 minutes. If the installation is taking much longer than 20 minutes and the = ticks have passed the word “unhandled” (shown in the image below) it is likely the installation has stalled.



```
[    2.449149] i8042: No controller found
[    2.784387] megasas:IOC Init cmd success
[    2.826502] megasas: INIT adapter done

Creating Lastline virtual machine.
Updating dhcp service.
[   50.165673] kvm [2984]: vcpu0 unhandled rdmsr: 0x34
[   50.165773] kvm [2984]: vcpu0 unhandled rdmsr: 0x606
Installing Lastline software...
======================================
```

This is known to be caused by not having the Advanced Malware Detection On-Premises Manager ports wired up and active. Specifically, the E port (2nd interface/ bottom port) is not wired to an active switch or Advanced Malware Detection On-Premises Engine port that is ON:

1. Wire the E port as described in the *Quick Start Guide* that was included with your Advanced Malware Detection On-Premises server.
2. Turn on the Advanced Malware Detection On-Premises Engine or switch so that the ports are ON and active.
3. Re-initiate the Advanced Malware Detection On-Premises Manager installation.

2 Troubleshooting registration and configuration

Troubleshooting Guide | AMD OP | v1.1

The **amd_register** script launches the Installation Wizard GUI. Errors by the wizard are logged to: **/root/amd-wiz.log**.

Networking, proxy support, and token registrations are configured by the **amd_setup** script. Actions and errors are logged to: **/root/amd-configuration.log**.

3 Packages

In Advanced Malware Detection On-Premises v1.1, the following packages are installed for shim operation:

```
[root@amd-manager:/usr/local/amd/shim/bin]# rpm -qa | grep
AMD
AMD-rsyslog-client-1.1.0-46.6071fd2.noarch
AMD-dhcp-server-config-1.1.0-46.6071fd2.noarch
AMD-config-1.1.0-46.6071fd2.noarch
AMD-harden-1.1.0-46.6071fd2.noarch
AMD-monitor-1.1.0-46.6071fd2.noarch
AMD-network-config-1.1.0-46.6071fd2.noarch
AMD-shim-1.1.0-46.6071fd2.noarch
AMD-yum-client-1.1.0-46.6071fd2.noarch
```

Note

The above packages display a version number of 1.1.0. Your displayed version number may differ from the version number shown above.

4 Processes

Critical processes include:

- nginx
- uwsgi
- mem-cached

The shim control scripts are located in: **/usr/local/amd/shim/bin/**

Process Logs are located in: **/var/log/amd/**

- shim.log
- uwsgi-daemon.log
- nginx/access.log
- nginx/error.log

5 Workflows

Troubleshooting Guide | AMD OP | v1.1

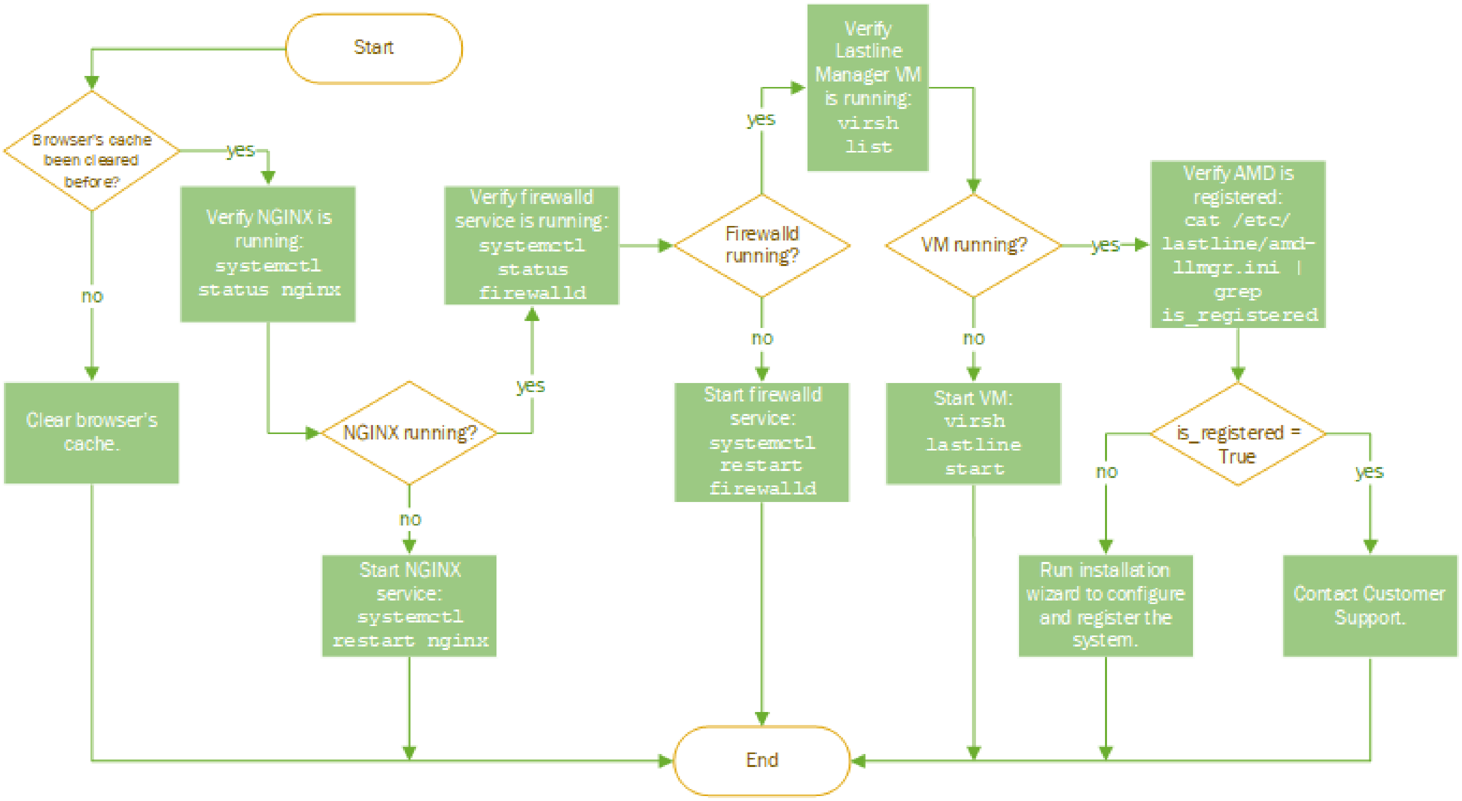
Review the workflow diagrams on the following pages to troubleshoot two common issues found in Advanced Malware Detection On-Premises.

- *Unable to reach the login page*, page 12
- *Unable to send files*, page 13

Unable to reach the login page

If you cannot reach the Advanced Malware Detection On-Premises login page, review the following workflow.

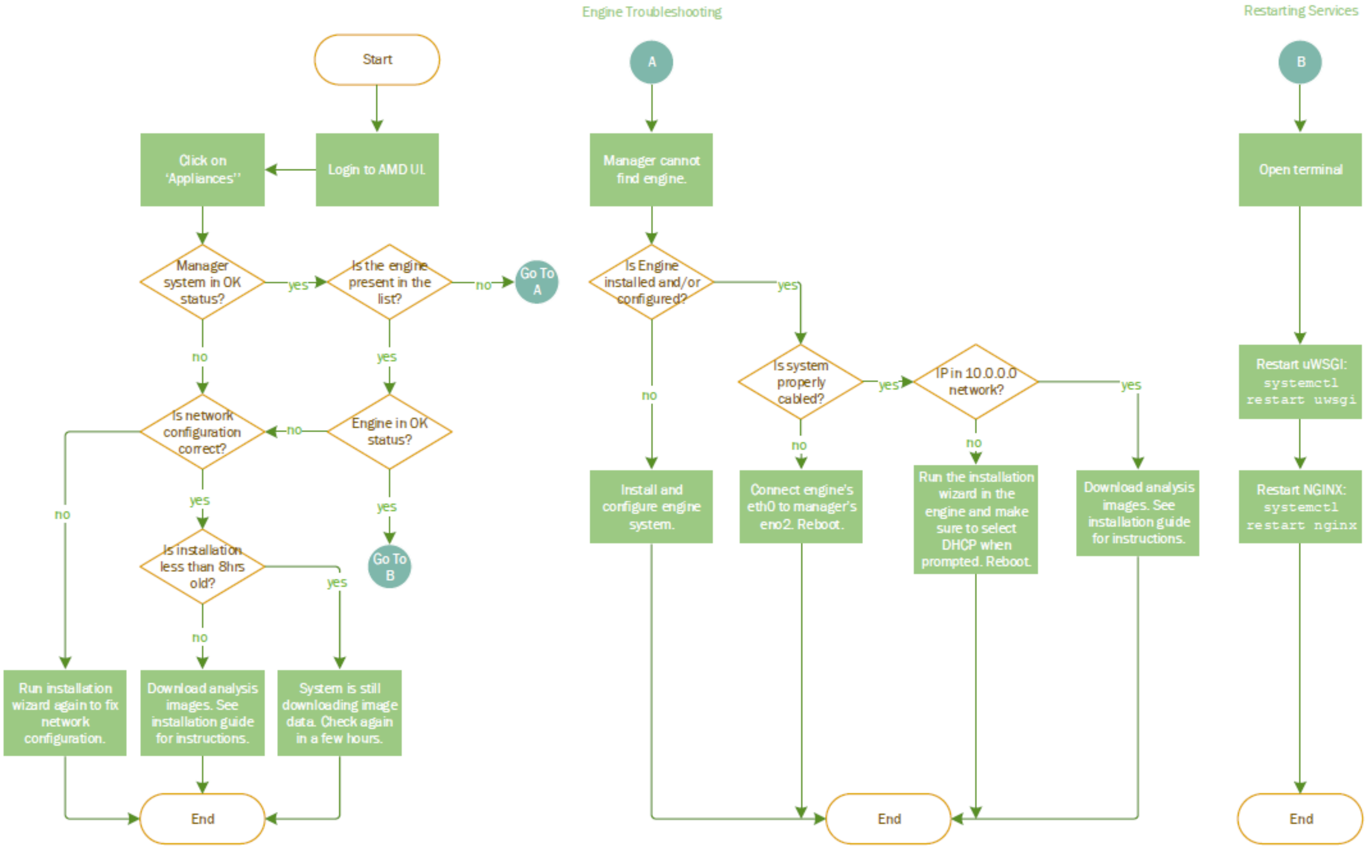
Cannot Reach AMD’s login page


Start
Browser’s cache been cleared before?
yes
no
Clear browser’s cache.
Verify NGINX is running: systemctl status nginx
NGINX running?
yes
no
Start NGINX service: systemctl restart nginx
Verify firewalld service is running: systemctl status firewalld
Firewalld running?
yes
no
Start firewalld service: systemctl restart firewalld
Verify Lastline Manager VM is running: virsh list
VM running?
yes
no
Start VM: virsh lastline start
Verify AMD is registered: cat /etc/lastline/amd-llmgr.ini | grep is_registered
is_registered = True
no
yes
Run installation wizard to configure and register the system.
Contact Customer Support.
End

Unable to send files

If Advanced Malware Detection On-Premises is not accepting files, or the API is unreachable, review the following workflow.

AMD Not Accepting files / API Unreachable


Engine Troubleshooting
Restarting Services
Start
A
B
Login to AMD UI
Click on 'Appliances'
Manager cannot find engine.
Open terminal
Manager system in OK status?
yes
Is the engine present in the list?
no
Go To A
Is Engine installed and/or configured?
yes
no
yes
Is system properly cabled?
yes
IP in 10.0.0.0 network?
yes
Restart uWSGI: systemctl restart uwsgi
Is network configuration correct?
no
Engine in OK status?
no
no
no
no
yes
yes
Install and configure engine system.
Connect engine's eth0 to manager's eno2. Reboot.
Run the installation wizard in the engine and make sure to select DHCP when prompted. Reboot.
Download analysis images. See installation guide for instructions.
Restart NGINX: systemctl restart nginx
Is installation less than 8hrs old?
yes
Go To B
no
Run installation wizard again to fix network configuration.
Download analysis images. See installation guide for instructions.
System is still downloading image data. Check again in a few hours.
End
End
End