Advanced Malware Detection and Protection

2.0

On-Premises Troubleshooting Guide

Revision A

Contents

- Issues common to manager and engine on page 2
- Manager on page 3
- Engine on page 5

Issues common to manager and engine

Manager/Engine Installation Failure

If the manager/engine installation fails, the below logs can be checked as root user:

/root/amd-wiz-apt.log – To check for any package installation or upgrade failure.

/root/amd-wiz.log – To check for any condition or test during the install that failed and caused installation failure.

/root/amd-wiz-security.log – These logs show that your system's security settings for file permissions, logging, and network configurations have been successfully fixed to meet compliance standards. Any issue related to these configurations will be reported under this.

Package upgrade failure

If automatic upgrade packages are disabled on both the manager and engine.

To upgrade any package on both the manager and engine run the below commands in the same sequence:

apt update	`# updates the information about available updates`
apt list –upgradeable	`# lists packages eligible for update`
apt upgrade	`# upgrade and install all eligible packages`

Currently installed AMDP packages & their versions can be looked up in the output of the following command:

```
apt list
```

As of 11-Dec-2024, the following AMDP packages & versions are listed in the 'apt list' output:

Manager:

- amd-backup/now 2.0.0-1 amd64 [installed,local]
- amd-monitor/now 2.0.0-1 amd64 [installed,local]
- amd-nginx/now 3.0.0-0 amd64 [installed,local]
- amd-python/now 3.0.0-0 amd64 [installed,local]

- python3-amd-config/now 2.0.2-1 all [installed,local]
- python3-amd-license/now 2.0.0-1 all [installed,local]

Engine:

- amd-backup/now 2.0.0-1 amd64 [installed,local]
- amd-monitor/now 2.0.0-1 amd64 [installed,local]
- amd-sandbox-vms/now 2.0.0-1 amd64 [installed,local]
- python3-amd-config/now 2.0.2-1 all [installed,local]
- python3-amd-license/now 2.0.0-1 all [installed,local]

Note

The above packages display a version number of 2.x.x or 3.x.x. Your displayed version number may differ from the version number shown above.

Manager

Manager unable to connect with Engine/ Sandbox

Check for the log lines like below in /var/lib/triage/logs/<YYYYMMDD>.log on manager:

```
{“l”:”debug”,”pkg”:”backends.sandbox”,”backend”:”sandbox1” ,”error”:”HTTP
403 (FORBIDDEN) : Access to this resource is not allowed by this IP
address” ,”ts”:*** ,”msg”:”Control connection error”}
```

During engine registration/installation, the engine IP needs to be an unused IP address in the 10.0.0.0/24 subnet (except 10.0.0.10, which is assigned to the manager).

The above logs would be observed if the IP is set outside of this subnet.

To address this issue, the engine must be removed from the manager configuration and re-installed to assign a new IP within the 10.0.0.0/24 subnet.

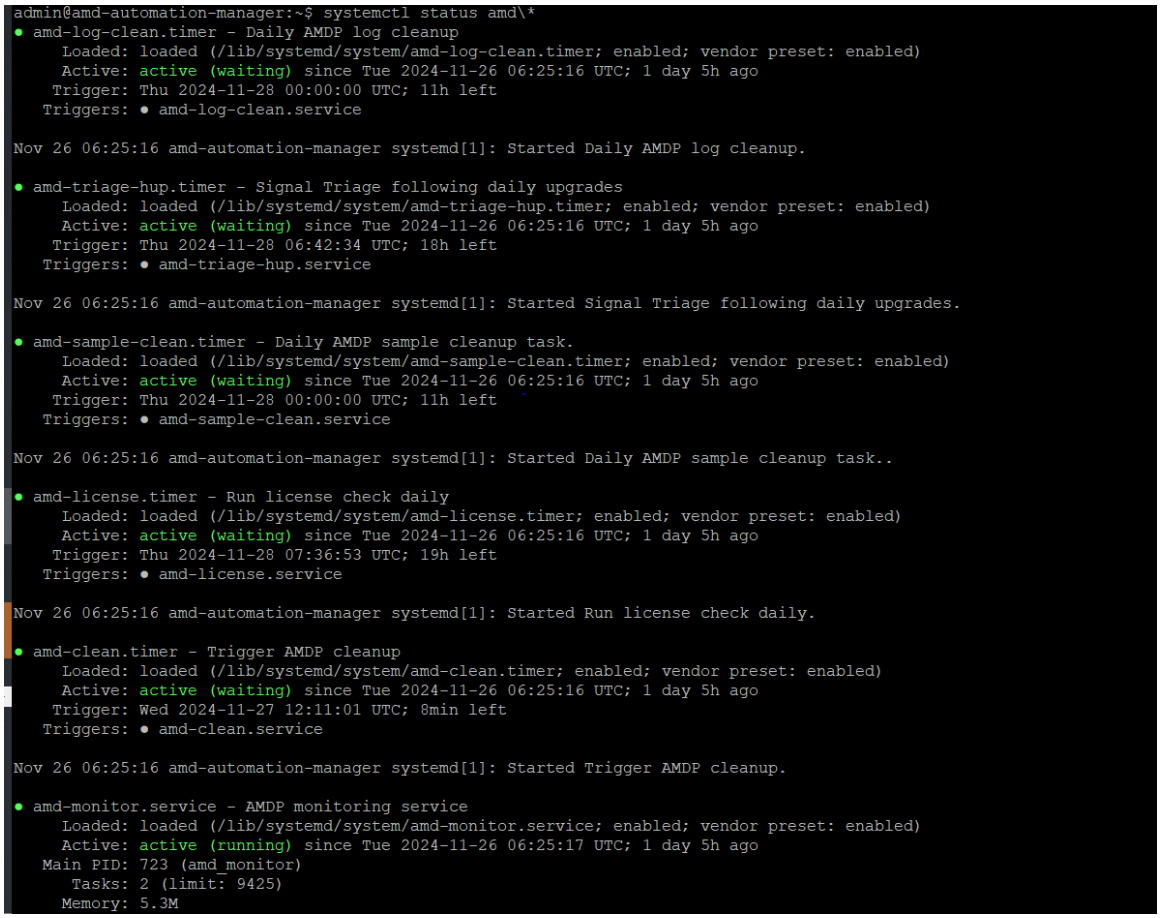
Verifying AMDP Service Status/Health Check

To verify that various AMDP maintenance tasks (log cleanup, triage, sample cleanup, and license check) are scheduled, active, and working as expected to the specific triggers set for their next execution times.

Run the following command as the root user on the manager:

```
systemctl status amd\*
```

Sample output:



File scan issue

If a file scan-related issue is observed, check if the below-mentioned services are active on the manager.

- amd-monitor.service
- tts.service
- triage-frontend.service

Service status can be checked by running the following command as root user on the manager:

```
systemctl status amd-monitor.service tts.service triage-frontend.service
```

If any of the above services are not active or not functioning as desired, run the following command to restart that specific service:

```
systemctl restart <service>
```

Engine

VM build issue

Building sandbox VMs can be time-consuming and may take several hours to complete.

Once the build has started with “amd_setup sandbox –vmbuild”,

The status of the VM installation can be checked with “amd_setup sandbox –vmstatus” to see if it has been completed.

If the build status indicates “UNAVAILABLE” even after waiting for several hours, check the vendor logs by running the below command as root user on the engine:

```
journalctl -u hatching-vms -f
```

If any network connection errors are observed, check and address the following possible reasons:

1) Internet connectivity

2) Firewall rules (if a firewall is being used)

If the issue persists, raise a ticket with the Technical Support team who can raise a case with Hatching for investigation.

Unable to add more than two engines

With a valid non-expired license for 3 or more engines, if the customer is unable to add the third engine.

To add the third engine, the customer license validation test must be completed.

If any network issue persists and the customer license is not being validated. The customer will not be able to add 3 engines.

Error:

```
root@RIFM240BS230V:~# amd_setup engines -l
engine: sandbox1 {'driver': 'sandbox', 'settings': {'sandbox_url': 'http://10.0.0.100:8121'}}
engine: sandbox2 {'driver': 'sandbox', 'settings': {'sandbox_url': 'http://10.0.0.101:8121'}}
root@RIFM240BS230V:~# amd_setup engine -a sandbox3 -i 10.0.0.102
Your license is limited to 2 engines.
root@RIFM240BS230V:~#
```

Note

By default, the Customer can add only 2 Engines.

With a valid license, customers can add up to 6 Engines.

For further investigation, we can run `"amd_backup --logs-only"` command on the manager.

If the issue persists, raise a ticket with the Technical Support team.

Admin Web Portal “password reset” or “send invite” issue

Password reset mail or new user invite mail is not received from the Admin Web Portal after configuring the SMTP server using the “`amd_setup configure-mail`” command.

Possible reasons:

- The SMTP server might not be reachable from the Manager.
- Server/port/username/password configured might be incorrect.

To debug this issue, check the logs in the below log file on Manager:

/var/lib/triage-frontend/logs/<YYYYMMDD>.log

Where YYYMMDD would be the date the configuration was applied or the last manager restart, whichever is the latest.

Verifying AMDP Service Status/Health Check

To verify that various AMDP maintenance tasks (log cleanup, monitoring, and license check) are scheduled, active, and working as expected to the specific triggers set for their next execution times on the engine.

Sample output:

```
admin@amd-automation-engine:~$ systemctl status amd\*
● amd-monitor.service - AMDP monitoring service
     Loaded: loaded (/lib/systemd/system/amd-monitor.service; enabled; vendor preset: enabled)
     Active: active (running) since Tue 2024-11-26 06:29:57 UTC; 3 days ago
   Main PID: 810 (amd_monitor)
      Tasks: 2 (limit: 38410)
     Memory: 7.4M
     CGroup: /system.slice/amd-monitor.service
             ├─   810 /bin/bash /usr/sbin/amd_monitor
             └─804379 sleep 300

Nov 26 06:29:57 amd-automation-engine systemd[1]: Started AMDP monitoring service.

● amd-license.timer - Run license check daily
     Loaded: loaded (/lib/systemd/system/amd-license.timer; enabled; vendor preset: enabled)
     Active: active (waiting) since Tue 2024-11-26 06:29:57 UTC; 3 days ago
    Trigger: Sat 2024-11-30 08:15:18 UTC; 19h left
   Triggers: ● amd-license.service

Nov 26 06:29:57 amd-automation-engine systemd[1]: Started Run license check daily.

● amd-log-clean.timer - Daily AMDP log cleanup
     Loaded: loaded (/lib/systemd/system/amd-log-clean.timer; enabled; vendor preset: enabled)
     Active: active (waiting) since Tue 2024-11-26 06:29:57 UTC; 3 days ago
    Trigger: Sat 2024-11-30 00:00:00 UTC; 11h left
   Triggers: ● amd-log-clean.service
```

File scan issue

For the engine to successfully scan the file below two services should be up and running.

- amd-monitor.service
- hatching-vms.service

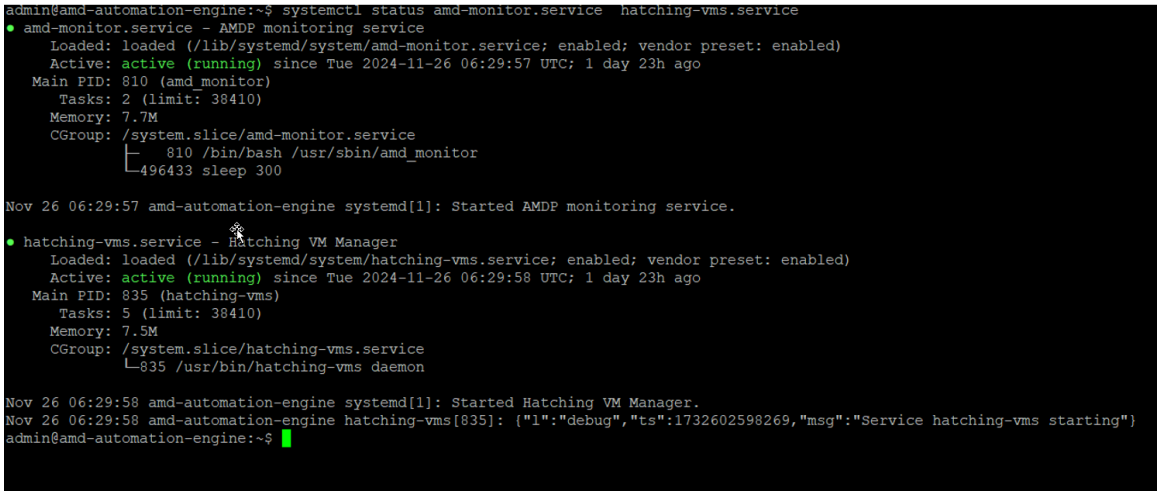
Service status can be checked by running the following command as root user on the manager:

```
systemctl amd-monitor.service hatching-vms.service
```

If any of the above services are not active or not functioning as desired, run the following command to restart that specific service:

```
systemctl restart <service>
```

Sample output:



Published 30 January 2025