



Endace Kemp Flowmon Deployment Guide

EDM07-43 - Version 1

Website

www.endace.com

© Endace Technology Limited 2021, All Rights Reserved.

No part of this document may be reproduced, published or transmitted in any manner without the express written consent of Endace Technology Limited.

Endace™, the Endace logo™, DAG™ and Provenance™ are registered trademarks in New Zealand and/or other countries of Endace Technology Limited. Other trademarks used may be the property of their respective holders.

Use of the Endace products described in this document is subject to the Endace Terms of Trade and the Endace End User License Agreement (EULA).

Disclaimer

This document is provided on an "AS IS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND" basis, including (without limitation) any warranties or conditions as to accuracy, non-infringement, merchantability or fitness or a particular purpose. The documentation is subject to change without notice.

In no event shall Endace Technology Limited or any of its related or affiliated companies be liable for damages, losses (direct or indirect) or costs incurred as a result of the use of this documentation or any inaccuracies or errors contained in the documentation, and use of the documentation is at your own risk.

This document, or any part thereof, may not be copied, modified or distributed without the express written authorization of Endace Technology Limited and may be used only in connection with Endace Technology Limited products and services.

Introduction

This document describes how to deploy and configure a Kemp Flowmon Virtual Probe in an Application Dock on the EndaceProbe, and how to integrate workflows to easily review recorded packet evidence from a Kemp Flowmon Collector event using EndaceVision.

In addition to continuously recording network traffic, EndaceProbe can host a Kemp Flowmon Probe to continuously analyze traffic in real-time. The meta-data or flow data that Kemp Flowmon Probe generates can be forwarded to other systems or collected by Kemp Flowmon Collector for reporting, analysis and storage of metadata relating to network or application performance or security threats. Deploying Kemp Flowmon on EndaceProbes enables scaled network monitoring and agile deployment of sensors when and where they are needed. Kemp Flowmon Probes can be deployed anywhere that EndaceProbe Network Recorders are deployed, enabling increased detection footprints without truck rolls or lengthy hardware deployments.

EndaceProbes are designed to ensure system resources used for capture and recording are separated from the resources used by hosted applications. This means capture performance is never impacted by hosted applications and vice-versa, guaranteeing 100% accurate recording even when the hosted Kemp Flowmon instance is processing heavy traffic loads.

Analysts can leverage workflow integrations using the Pivot-To Vision™ function of the EndaceProbe API to drill down from events in the Kemp Flowmon ADS to analyze relevant packet evidence. The EndaceProbe's built-in investigation tool, EndaceVision, allows analysts to investigate the related, packet data for issues including performance degradations, malware C2 and lateral movement and even data exfiltration.

Important:

- This procedure can only be used on Host EndaceProbe running OSm software 7.0.0 or above.
- Kemp Flowmon version 11.01.06 is supported.

Related Documents

For more information on the installation of Kemp Flowmon, refer to the *Kemp Flowmon documentation*

The following Endace documents provide additional information about how to configure Host EndaceProbes.

- EDM09-146 EndaceProbe User Guide
- EDM09-163 Administrator Guide
- EDM09-21 CLI Command Reference Guide
- EDM07-30 EndaceProbe Performance Guidelines

Support

For assistance with the deployment of the Kemp Flowmon Virtual Probe on an Endace Platform, contact Endace:

Email	support@endace.com
Endace Support Portal	https://support.endace.com
Endace Website	www.endace.com

For assistance with configuring settings for this integration, contact the Kemp Flowmon Support team at: <https://www.flowmon.com/en/company/contact>

Deploying the Kemp Flowmon Virtual Probe

Overview

This section details how to deploy and configure the Kemp Flowmon Probe as a virtual machine on an EndaceProbe.

This deployment requires:

- a zip file from Kemp Flowmon containing:
 - the image file
 - the Kemp Flowmon Virtual Appliance documentation
- a Kemp Flowmon license.

Platform Requirements

The Kemp Flowmon Probe can be deployed as a virtual machine on EndaceProbe platforms that supports a **Quad** Application Dock instance. Osm 7.0.0 and above is supported.

It cannot be deployed on an EndaceCMS.

Refer to *EDM07-30 EndaceProbe Performance Guidelines*, available on the Endace Support Portal, for standard Application Dock sizing information.

Security Considerations

The default GUI account is `admin` and the associated password is `admin`.

The default ssh & CLI user account is `flowmon` and the associated password is `inv3a-t3ch`.

Note:

For security reasons, you need to change the password the first time you log into the virtual machine. In the process of changing this, it is important to ensure that the deployed virtual machine follows your organization's security/hardening policies.

Kemp Flowmon Volume

Download the Flowmon-Probe-Virtual zip file from the Kemp Support website.

<https://support.kemptechnologies.com/hc/en-us/articles/4404209325965-Download-Flowmon-11-1>

This contains the image and the documentation.

Image Filename: Flowmon_probe_virtual-disk-0.qcow2 (~3GB)

Transferring the Image File to the EndaceProbe

The file can be transferred to the EndaceProbe using the EndaceProbe CLI using FTP, SFTP, TFTP, SCP, HTTP or HTTPS, or they can be pushed to the EndaceProbe using an SCP client.

Note: The file is ~3GB, so you may need to plan for the transfer to take some time.

Do one of the following:

Option	Description
Pull from a file server, using HTTP(S) or SCP.	Using the host CLI, transfer the image by running either: <pre>(config) # virt volume fetch url http://<file server name>: <port>/<path>/<file name></pre> or <pre>(config) # virt volume fetch url scp://<user name> [:password]@<file server name>/<path>/<file name></pre>
Push using SCP	Use SCP from a remote system to push the image file onto the host: <pre>\$ scp <file name> <probe user name>@<host probe name>:/endace/vm/pools/default</pre>
Push using SFTP	Use SFTP from a remote system to push the image file onto the EndaceProbe into the /endace/vm/pools/default location. EndaceProbe uses port 22.
Use the GUI .	The <i>Dock > Volumes</i> page enables you to upload the image.

Prerequisites

Check for an existing network bridge:

```
(config) # show bridges
```

Create a network bridge if it one does not already exist.

```
(config) # bridge br0 migrate-from <eth port>
```

where <eth port> is the Ethernet port you want to bind to the Bridge - typically eth0.

For further details on this command, refer to the *Network Bridging* section in *EDM09-21 CLI Command Reference Guide*.

Deploy the Kemp Flowmon Virtual Probe

To deploy the Kemp Flowmon Virtual Probe on an EndaceProbe, complete the following steps:

1. Log into the host EndaceProbe CLI - configure terminal mode.
2. Install the virtual machine , run:

```
(config) # virt vm <virtualMachineName> quick-deploy size quad copy-from
flowmon_probe_virtual-disk0.qcow2
```

Where <virtualMachineName> is the name of the virtual machine you are creating.

Tip: Start typing the file name and press tab to complete the name.

This installation can take a few minutes to complete. The time taken depends on the image file and the available resources on the host EndaceProbe.

3. Review the vDAG assignments:

```
(config) # show virt vdag
```

For example, the following output indicates that vDAG number 16 is assigned and vDags 17 through 31 are unassigned.

```
vDAGs assigned to VMs:
 16 <virtualMachineName> (extension header stripped) (nic-mode disabled)

Unassigned vDAGs: 17 18 19 20 21 22 23 24 25 26 27 28 29 30
31
```

a. Identify the single vDAG that has been assigned to the Kemp Flowmon virtual machine.

Nic-mode must be enabled to ensure this interface appears as the **eth2** interface inside the Kemp Flowmon Virtual Probe.

Run the following on the Kemp Flowmon vDAG:

```
(config) # virt vdag <vdag number> nic-mode enable
(config) # virt vdag <vdag number> nic model virtio
```

4. Save the running configuration.

```
(config) # configuration write
```

5. If the Kemp Flowmon Virtual Probe will be configured using DHCP, run the following command and note the MAC address of **Interface 1**.

```
(config) # show virt vm <virtualMachineName> detail
```

6. Power on the virtual machine:

```
(config) # virt vm <virtualMachineName> power on
```

Configure the Kemp Flowmon Virtual Probe

To configure and license the Kemp Flowmon Virtual Probe, you need to have an IPv4 address on the first virtual interface.

- If you are using DHCP, use the MAC address of Interface 1 (See step 5 above) to register the virtual machine with a DHCP server.
- If you are using a static IP address, do this via console access from the EndaceProbe CLI.

```
(config) # virt vm <virtualMachineName> console connect text
```

Follow the Post-installation steps in the **Kemp Flowmon Virtual Appliances** documentation to configure new passwords, other network related settings, and the time/date.

Send Data to the Kemp Flowmon Virtual Probe

The traffic captured by the EndaceProbe needs to be sent to the Kemp Flowmon Virtual Probe so it can be processed. This requires the creation of a Data Pipe on the host EndaceProbe. For details on creating a Data Pipe, refer to the *Data Pipe* chapter in your *EndaceProbe User Guide*.

1. On the EndaceProbe, create a Data Pipe with:

- the input (sink) as the DAG module - In the example below DAG module 1 port A.
- the output (source) as the vDAG.

For example, in the CLI:

```
(config) # erfstream pipe <pipeName> source dag dagmod.1.a sink vdag.<virtualMachineName>.1
```

The Data Pipe can also be created on the GUI.

2. On the EndaceProbe, save the running configuration.

```
(config) # configuration write
```

3. Log into the Kemp Flowmon Virtual Probe GUI.
4. Navigate to the Configuration Centre page and:

- a. Install the Kemp Flowmon license
- b. Check that the network interface eth2 is receiving traffic.

This interface is mapped to the EndaceProbe's vDAG configured earlier.

5. Log into the Kemp Flowmon Collector.
6. Navigate to the Configuration Centre page and verify that traffic is being received from the Kemp Flowmon Virtual Probe

Event Workflow Integration

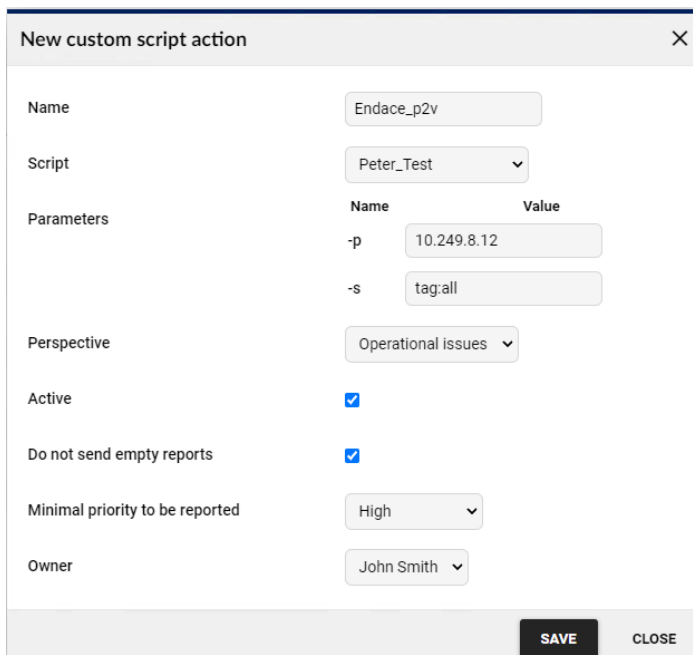
The Kemp Flowmon Pivot-to-Vision integration provides you with the ability to go from an event in the Kemp Flowmon ADS to viewing packet level details in an EndaceVision Investigation.

1. Go to the Kemp Flowmon Collector home page and check if the ADS is installed
 - a. If it is not installed, download it from the Kemp Flowmon Support Portal and import it as a package.
2. Install the Endace Package via the Kemp Flowmon Collector Configuration Center > Versions.
3. SSH into the Kemp Flowmon Collector and save a local copy of `/data/components/endace/add-comment.py`.
4. On the Kemp Flowmon Collector, upload the `add-comment.py` script to the ADS by Settings > System Settings > Custom Scripts > New Custom Script.
5. Fill in the parameter names and values
 - p is the FQDN of the EndaceProbe or InvestigationManager
 - s is the name of the Data Source. You can use `tag:all` to select all Data Sources on that EndaceProbe.



Name	Value
-p	10.249.8.12
-s	tag:all

6. Create a Custom Script Action via Settings > Processing > Custom scripts > New Custom Script Action.



Name	Value
-p	10.249.8.12
-s	tag:all

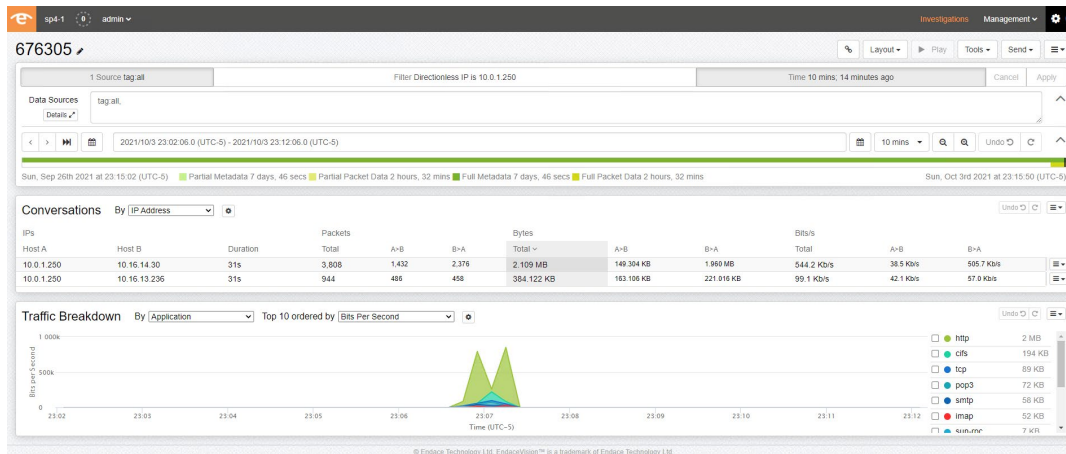
7. Ensure the Active checkbox is ticked.

Launch an Investigation

Once the Kemp Flowmon integration is set up, there will be a link to EndaceVision in the event details in the Kemp Flowmon ADS, where you can view or download the captured data from before, during and after an event. This simple click-through integration makes investigation of events extremely efficient.

To do this, on the Kemp Flowmon ADS:

1. View the events and click on an EventID.
2. Select the Comments tab. Highlight the text and Right-click for the option to open the hyperlink.
3. An EndaceVision Investigation will be initiated in a new browser tab. From here you can further refine the Investigation.



Version History

Version	Date	Reason
1	October 2021	First release.

