

Technical Note: Virtualizing ESM with CORRE

The information in this technical note applies to ESM with CORR-Engine 6.0c and later.

Overview

Running ESM with CORR-Engine on a virtual machine (VM) may be sensitive to any environmental differences between the operating system on the VM and the same operating system on a stand-alone machine. This document describes the system that HP ArcSight tested and the result for running ESM with CORR-Engine on a VM.

In a computer set up to run virtual machines, the computer's CPU, memory, hard disk space, and other resources are shared by the VM manager application and any other VMs on that computer. Make sure the VM itself meets or exceeds all the ESM system requirements as specified in the *ESM Installation and Configuration Guide*.

Policy on Virtual Environments

HP ArcSight does limited testing and with a specific virtualization platform provider - VMware ESXi, in this case.

Instead of testing different virtualization vendors, our policy is to verify the functionality of ESM with CORR-Engine running as an application on our supported operating system such that the virtualization layer is completely transparent to ESM. Expect there to be an impact on performance as a result of virtualization.

Our recommendation is that you provide dedicated CPU and I/O resources to the VM where ESM is installed.

ESM with CORR-Engine scales better on virtualized environment compared to ESM with Oracle, especially with more and faster cores. ESM with CORR-Engine is less I/O-intensive than ESM with Oracle.

We expect customers to engage their own IT in resolving performance issues or any vendor-specific virtualized environment issues.

Tested Virtual Environment

HP ArcSight tested ESM 6.0c on a virtual machine running on VMware ESXi 4.1.0.659051. This VM environment and the ESM installation had the following characteristics:

- 8-core processor.
- 36 GB of memory
- 250 GB of available disk space
- 10,000 actors defined
- 10,000 assets defined

This environment passed basic testing. It met our minimum requirements for processing events and providing platform for ESM.

Users must use a virtual machine that by *itself* meets the minimum requirements specified in the *Installation and Configuration Guide*.

Copyright © 2012 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Follow this link to see a complete statement of copyrights and acknowledgements:
<http://www.hpenterprisesecurity.com/copyright>

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

This document is confidential.

October 2012