

Title: New Assuria Auditor agent for VMware ESX 3.5 released

Number: 94

Date: 30 May 2009

Title New Assuria Auditor agent for VMware ESX released

Introduction This Assuria Bulletin, #94, introduces a new Assuria Auditor agent for the VMware ESX 3.5 environment.

The new VMware ESX 3.5 agent adds to the current virtual environment support by Assuria Auditor of any 'system' running as a 'guest'.

The new agent for VMware ESX provides checks and policies for two distinct areas.

1. ESX Security configuration – checking the configuration of the ESX Hypervisor

and

2. Virtual Machine (VM) configuration settings – checking the VMware ESX configuration settings of guest virtual machines.

The new agent's release 1 content (Checks and Policies) will be enhanced over time. Checks for ESX patches will be added in the next release of the agent via an AutoUpdate (AU).

The VMware ESX agent requires the Assuria Auditor console to have been updated to at least AU #95.

ESX Log collection

Assuria's log management and analysis solutions, Assuria Log Manager (ALM), can collect, store and analyse logs from the VMware ESX environment. User who would like more information about ALM and ESX logs should contact Assuria.

ESX Configuration

The configuration settings of ESX 3.5 are examined. Information sources for the checks include:

- CIS – VMware ESX Server 3.x Benchmark Version 1.0
- VMware best practices security hardening
- VMware Communities forum
- VMware websites technical information
- VMware ESX 3.5 manuals with product
- VMware ESX Server in Enterprise by Edward L. Haletky

The checks are included in a new policy, 'ESX-Configuration Information' and include checks for:

- VM file permissions
- Firewall setup

Title: New Assuria Auditor agent for VMware ESX 3.5 released

Number: 94

Date: 30 May 2009

- Services running
- SSH configuration
- Password security
- Log settings and security

A Policy Navigator for VMware ESX which details the new ESX checks and policies is available in the Assuria Auditor console at AutoUpdate #95 or later.

VM Configuration

In addition to checking the configuration of the VMware hypervisor the configuration settings of guest VMs on the ESX server are examined by Assuria Auditor.

The VMX configuration files are located on the ESX system, Assuria Auditor reads the files and the Assuria Auditor checker examines the configuration settings. A number of specific configuration checks have been developed.

VM Baseline Checks

In addition the configuration settings of all the VMs can be baselined and then monitored for any additions, changes or deletions to the entries in these configuration files.

The baseline checks available are:

- vmconfig-added - Has an entry been added to a VMX file
- vmconfig-changed - Has an entry been changed in a VMX file
- vmconfig-deleted - Has an entry been deleted from a VMX file
- updateVmconfigBaseline - Update the vmconfig baseline

The VM configuration data once baselined can be viewed in the baseline section of the Auditor console.

The view will show a list of all VMs on the server and a double-click on a VM entry will bring up a tabbed notebook showing the configuration settings of that VM.

Assuria is focusing on the information which is relevant to the security of the VM and some additional useful system information.

Assuria Auditor Console – AutoUpdate #95

Assuria Auditor AutoUpdate #95 updated the Console adding the features required to fully support the VMware ESX 3.5 agent. Users should ensure their Console is at AU #95 or later when adding the ESX 3.5 agent to the Console. See Assuria Bulletin #93 for information AU#95.

Title: New Assuria Auditor agent for VMware ESX 3.5 released

Number: 94

Date: 30 May 2009

Download The ESX 3.5 agent is available for download from AssuriaOnline (<https://www.assuriaonline.com>)

Installation Instructions Installation instructions for the agent are available for download from AssuriaOnline.

Enhancement requests and feedback Assuria would like your feedback on the new ESX Agent. Requests for extra checks and policies are also very welcome. Please send your feedback and enhancements requests to 'enhancements@assuria.com'.

Further information For further information regarding the Assuria Auditor VMware ESX 3.5 agent please contact Assuria at support@assuria.com.