ESET Tech Center

Using ESET version 6 Business products on virtual machines—FAQ

Ondersteuning | ESET Nederland - 2017-11-08 - Reacties (0) - Legacy ESET Remote Administrator (6.x / 5.x / 4.x)

https://support.eset.com/kb3674

Issue

Install the ESET Remote Administrator Virtual Appliance

Best practices for ESET endpoint/server solutions on virtual machines (VMware, Vsphere, Virtualbox etc.)

Compare ESET Shared Local Cache, ESET Virtualization Security, ESET File Security for Microsoft Windows Server for Azure

Supported hypervisors

Solution

ERA installation | Supported hypervisors | Active Directory | Which virtualization solution to use | Troubleshooting ERA OVA

1. **How can I deploy ESET Remote Administrator and ESET endpoint/server solutions in a virtualized environment?**
   ESET Remote Administrator (ERA) can be installed in a virtual environment using the same procedure that you would use when installing on a physical server. ERA 6 is compatible with VMware, Hyper-V and Virtualbox virtualized environments (see number 2 below).

   Additionally, ERA is available for download as an Open Virtualization Appliance (OVA) file. This file is a template that contains ERA pre-installed on a CentOS operating system. See

the following resources for more information on how to install ESET Remote Administrator:

- How do I install ESET Remote Administrator? (6.x)—Standard installation
- How do I install ESET Remote Administrator Virtual Appliance—Virtual appliance deployment
- ESET Remote Administrator 6 Virtual Appliance Installation Manual and User Guide

2. **What virtual environments and hypervisors are supported by ESET Remote Administrator?**
   The following viritualization solutions are supported by ESET Remote Administrator:

   - VMware ESXi 5.0 and later
   - VMware Workstation 6.5 and later
   - VMware Player
   - vSphere
   - Microsoft Hyper-V
   - Oracle Virtualbox

3. **What are the best practices for ESET endpoint/server solutions installed on a virtual client?**
   Version 6 ESET endpoint/server solutions are optimized for operation in virtualized environments and do not require any customization to function correctly on a virtual client. In applications where ESET products are installed on both a physical host and virtual machine, some files may be scanned twice, however this should not result in a noticeable impact on system performance.

   To avoid overuse of resources in a virtualized environment, we recommend that you install ESET products on virtual client computers in small derivations. Installing ESET on all virtual clients at once will result in a large number of initial scans, which can affect performance on the host computer.

   See the resources available below to make sure that your virtual

machine satisfies the minimum system requirements for ERA and ESET endpoint/server solutions.

- View system requirements for ESET Remote Administrator 6.x
- View system requirements for ESET Endpoint Security and ESET Endpoint Antivirus
- View system requirements for ESET Endpoint Security and ESET Endpoint Antivirus for Mac OS X

4. **Can I link my existing ESET Remote Administrator (ERA) Virtual Appliance to a Windows Domain to allow ERA to map security groups?**
   Your windows domain should be specified during deployment of the ERA Virtual Appliance. We recommend that you uninstall your ERA Virtual Appliance and then redeploy it if you need to link to a new Windows domain.

5. **How do I configure LDAP to allow for Static Group synchronization on ERA virtual appliance?**
   See the following Knowledgebase article for instructions to configure the ESET Remote Administrator appliance to join a domain:

   How do I configure LDAP to allow for Static Group synchronization on ERA virtual appliance? (6.x)

6. **How do I configure communication between ERA VA or ERA for Linux with Active Directory?**
   See the following Knowledgebase article for instructions to create a synchronization task to sync the ERA OVA or ERA for Linux with Active Directory:

   How do I create a task to sync ESET Remote Administrator VA with Active Directory? (6.x)

7. **I am using dual-boot software such as Mac Boot Camp or Parallels—do I need separate licenses for my Mac operating system and Windows operating system?**
   North American Customers: Yes, you will need to purchase ESET Cyber Security/ESET Cyber Security Pro and an ESET product for

Windows.

Customers outside North America: No, you do not need to purchase ESET Cyber Security / ESET Cyber Security Pro and an ESET product for Windows. You can extend the protection of your ESET product to a parallel operating system on the same computer.

8. **What is ESET Shared Local Cache and how can I use it with my ESET products in a virtualized setting?**
   ESET Shared Local Cache (ESLC) is a utility that can be installed in your virtual environment to significantly boost the performance of ESET products installed on virtualized client machines. In virtualized environments, multiple computers are often based on the same base image. This results in a large number of identical files stored on different virtual machines. ESLC monitors these duplicate files and records those files that are declared clean after being scanned by an ESET product. Once recorded, this information is available to all clients in the virtual environment that are in communication with ESLC. Unaltered files that have already been declared clean will not be scanned by other clients.

   For instructions to install and configure ESLC, see the ESET Shared Local Cache User Guide.

9. **What is ESET Virtualization Security for VMware vShield?**
   ESET Virtualization Security for VMware vShield is a single ESET appliance that protects all the virtual machines running on the hypervisor.

   For more information, see ESET Virtualization Security for VMware vShield FAQ.

Which virtualization solution should I use?

The following three solutions are available for virtual environments:

ESET Shared Local Cache (ESLC)—ESLC is a free plug-in to cache files and optimize scanning for all connected Windows/Mac endpoints and Windows servers. Using ESLC will boost performance in your network and is recommended if you are

running virtual machines in a mixed or hypervisor agnostic environment.

ESET Virtualization Security (EVS)—EVS is the recommended solution when specifically protecting vShield endpoints using the ESX hypervisor from VMware as part of the vSphere solution.

ESET File Security for Microsoft Windows Server for Azure (EFSW for Azure)—If you are building Microsoft Azure workloads in the cloud, you can deploy ESET File Security for Microsoft Windows Server for Azure as a VM security extension, which is available from the the Azure Marketplace.

Virtual environment	Recommended ESET solution
Physical endpoints/servers	ESET Endpoint Antivirus/Security (endpoints)/ESET File Security (servers)
Physical and virtual machines (hypervisor agnostic)	• ESET Shared Local Cache • ESET Endpoint Antivirus/Security (endpoints)/ESET File Security (servers)
Virtual machines using ESX hypervisor (vSphere/vShield)	ESET Virtualization Security
Virtual servers in Microsoft Azure	ESET File Security for Microsoft Windows Server for Azure
VDI (persistent-state VMs)	• ESET Shared Local Cache • ESET Endpoint Antivirus/Security (endpoints)/ESET File Security (servers)
VDI (non-persistent-state VMs using ESX hypervisor)	ESET Virtualization Security

For answers to questions regarding which product is recommended for your virtual environment, see below:

1. **Can I run ESET Shared Local Cache and ESET Virtualization Security for mixed operating system environments?**
   Yes. You can combine EVS and ESLC virtual appliances on the same host. EVS would be used in conjunction with the virtual machines that have VMware tools installed and ESLC would be used with VMs that have standard AV products installed (for instance, ESET Endpoint Antivirus/Security for OS X, ESET Mail Security for Microsoft Exchange). "Agentless" AV scanning for vShield-based VMs are connected to EVS and "agented" AV scanning for other VMs with the standard ESET solution.

2. **For a cluster of three hosts, do I need to deploy ESET Virtualization Security appliance or ESET Shared Local Cache on each host or only one EVSA/ESLC per cluster?**
   EVS requires a security appliance (EVSA) to be installed on each host. Because the scanning introspection is limited to host, it cannot scan VMs on other hosts. However, ESLC can be installed once in your network and would be accessible from all virtual machines (across hosts) that have an ESET-compatible business product installed on it (for instance, ESET Endpoint Security, ESET File Security for Microsoft Windows Server).

3. **Can I run EVSA on some hosts and ESLC on others?**
   Yes. For example, if you have a cluster of three hosts, it is possible to run EVSA on two hosts and ESLC on the third. You can have two hosts with EVS (with virtual machines and with vMotion connecting them) and ESLC on the other host. If the ESLC appliance is set to have hostname (which is not changed), ESLC can also be vMotioned. However, you need to take into account the short downtime for usage of the ESLC service during the time it is being vMotioned.

The following video animations demonstrate the system architectures of ESET Shared Local Cache and ESET Virtualization Security and how they use system resources.

ESET Virtualization Security—System Architecture and Resource Allocation

ESET Shared Local Cache System—System Architecture and Resource Allocation

---

Troubleshooting ERA VA

1. **Client computers appear twice in ESET Remote Administrator installed on my vSphere environment that is synced with my Active directory (AD)—why does this occur and how can I resolve it?**
   To avoid having clients appear twice in virtualized environments

that are synced with AD, perform VMware synchronization first and then perform AD synchronization with ESET Remote Administrator in vSphere. VMware synchronization identifies computers based on the UUID of virtual machines (VMs), whereas AD synchronization identifies computers based on DNS names. Performing VMware synchronization first, your vSphere environment will allow you to select **Host Name** as the identifier for client computers, which will in turn allow AD synchronization to run without finding duplicates.

See ESET Virtualization Security vCenter and Active Directory synchronization.

2. **Which log files can I access for troubleshooting the ERA Virtual Appliance?**

   The following log files can be used to troubleshoot the ERA Virtual Appliance:

   If ERA VA deployment fails, do not restart the appliance but first check this log file:

   `/root/appliance-configuration-log.txt`

   ERA Server installation log:

   `/var/log/eset/RemoteAdministrator/EraServerInstaller.log`

   ERA Server trace logs:

   trace.log, status.html and last-error.html located in `/var/log/eset/RemoteAdministrator/Server/`

   ERA Server dumps:

   `/var/opt/eset/RemoteAdministrator/Server/Dumps/`

Related articles:

Migrate the ESET Virtual Appliance from an earlier version of 6.x to the latest

Tags
Virtual Appliance