ESET Virtualization Security for VMware NSX (vShield) FAQ

Ondersteuning | ESET Nederland - 2025-03-07 - Reacties (0) - ESET Virtual Security

https://support.eset.com/kb5889

Issue

What is ESET Virtualization Security (EVS) for VMware NSX (vShield)
Common questions and solutions

Details

ESET Virtualization Security (EVS) was released globally January 21, 2016, and in North America March 1, 2016.

Solution

Key Benefits and Features of EVS | Licensing | System Requirements | ESET Remote Administrator | Known Issues | Troubleshooting | Support Resources

---

1. **What is ESET Virtualization Security**
   ESET Virtualization Security for VMware vShield is a single ESET appliance that protects all the virtual machines running on the hypervisor. Compatible with ESET Remote Administrator 6, the solution allows drilling down to each virtual machine for rapid task execution.



Figure 1-1
Click the image to view larger in new window

2. **What are the important features in ESET Virtualization Security?**

    - **Quick deployment**—Replacing every virtual appliance is as simple as registering a new security virtual appliance (SVA) within the vShield manager. Once ESET Remote Administrator (which is also available as a virtual appliance) is installed, ESET Virtualization Security appliances can be deployed on multiple hosts at once.
    - **Optimized performance**—VM infrastructure is about optimizing resources and performance, and ESET's scanning engine exactly meets these requirements. It is well known for its low system demands and high speed, thus leaving more resources for other applications and processes.
    - **Remote management**—EVS is compatible with ESET Remote Administrator 6.3, which supports management of both physical and virtual machines.
    - **Server solutions**—Specific solutions for virtual environments included, process exclusions, snapshot independence, native clustering support and Hyper-V storage scan.

3. **How do I deploy ESET Virtualization Security?**
   For detailed instructions, see the following Knowledgebase article: How do I deploy ESET Virtualization Security?

4. **Can I deploy ESET Virtualization Security appliances on multiple hosts at once?**
   Yes. The **ESET Virtualization Security - Deployment Tool** allows administrators to deploy EVS on multiple ESXi hosts. See the following Online Help topic for more information:

    - Installation of ESET Virtualization Security using deployment tool

5. **How does licensing work with ESET Virtualization Security?**
   Licensing options for ESET Virtualization Security may vary depending on your location. Please contact an ESET Sales representative to learn more.

6. **What are the system requirements and supported platform systems for ESET Virtualization Security?**

    - VMware vSphere 5.5 and 6.0 (vCenter Single Sign-On, vSphere Client/Web Client, vCenter Server, vCenter Inventory Service)
    - VMware vShield Manager 5.5.4
    - VMware vShield Endpoint 5.1.0
    - VMware vSphere 5.0 and later

    The following components and infrastructure are needed to deploy ESET Virtualization Security:

    VMware vShield Endpoint installed into VMware environment
    VMware Tools installed on each virtual machine
    ESET Remote Administrator 6 management server installed
    ESET Remote Administrator vAgent Host
    Deployed ESET Virtualization Security that integrates components from VMware (vShield library) and ESET Scanning Engine

    Visit the System Requirements Online Help topic for more detailed system configuration information.

7. **How does ESET Virtualization Security quarantine files?**
    Files infected on virtual machines are automatically transferred to EVS, which stores and tags the file with the virtual machine it belongs to, so centralized quarantine per host can be applied. vMotion allows quarantined files to be on a different EVS than the machine on which it is currently running.

8. **I am an ESET Managed Service Provider (MSP), can I use ESET Virtualization Security?**
    Yes, EVS licensing supports Managed Service Provider licensing.

9. **What protection features does ESET Virtualization Security offer?**
    This solution provides only on-access and on-demand scanning and does not provide the advanced protection features (layered security approach) available in ESET endpoint products.

    - Yes: Heuristics-based detection
    - No: HIPS, Web Access Protection, Device Control, Web Control, Cloud Scanning, Antispam, Local firewall, Network

Attack Blocker, Application Control

10. **What is ESET Shared Local Cache and which virtualization solution should I use?**
    With ESET Shared Local Cache and the protection of an ESET security product (an ESET endpoint product must be present on each virtual machine), you get the same full set of tools and security features that you would have in a physical environment, plus significantly boosted scanning speed. ESET Shared Local Cache comes free with any of the following products: ESET Endpoint Antivirus, ESET Endpoint Security, ESET File Security or ESET Mail Security.

    See the following Knowledgebase article for more information regarding which virtualization solution is best for your network environment:

    - Using ESET version 6 Business products on virtual machines—FAQ.

Using ESET Remote Administrator with ESET Virtualization Security

1. **Do I need to install ESET Remote Administrator in order to manage ESET Virtualization Security on my virtual machines?**
   Yes. EVS is distributed in the form of a GUI-less virtual appliance and only has a basic configuration interface. To initiate scans or enable or disable protection, you must install or deploy ESET Remote Administrator.

   ESET Remote Administrator is also available as a virtual appliance and is compatible with VMware, Hyper-V and Virtualbox virtualized environments, which simplifies the deployment in virtual environment. For detailed instructions to install the ERA Virtual Appliance, see ESET Remote Administrator VA Deployment.

2. **What happens if a virtual machine does not have a**

supported version of VMware Tools installed? Does ESET Remote Administrator report this?
An outdated version of any of the VMware Tools is reported solely to VMware vCenter. If VMware tools does not include EPSEC driver, the solution is not compatible and the machine will not be protected. As there is physically no ESET software installed in protected virtual machines, it is not possible to report this in ESET Remote Administrator. For VMware Tools, updates and reports are handled solely by VMware.

3. **Does ESET Virtualization Security support VMware vMotion?**
   Yes. vMotion migration enables live migration of a virtual machines from one physical server (ESXi server) to another while maintaining continuous service availability. When VMs are moved from one host where ESET Virtualization Security is installed to a different host where ESET is installed, the VM keeps its security settings and remains protected.

4. **What are the Known Issues in ESET Virtualization Security?**
   See the following Knowledgebase article for Known Issues in version 6 business products:

   - Known Issues in ESET Virtualization Security

5. **How are virutal machines identified in ERA?**
   You can view virtual machines in ERA directly from **Dashboard** or from the **Computers** tab in the main menu, using the filter "Agentless virtual machine."

6. **What is the benefit of ESET License Administrator?**
   The ESET License Administrator portal allows a license owner or administrator to view the status of ESET Virtualization Security licenses. Additionally, ELA allows a License Owner to administrate their license usage by creating Security Admin accounts. The License Owner maintains full control of license usage and can delegate control of license credentials to Security Admins who are able to manage specific users. For more information, see the ESET License Administrator User Guide.

Troubleshooting

Cannot register to vShield

Check if network allows communication via port 443 with vShield Manager
Restart vShield Manager VM
Reinstall vShield Endpoint module on ESXi (via VShield Manager Web UI)

ESET Virtualization Security shows zero number of connected/protected VMs

Make sure Guest VMs are running and have installed VMware tools with Endpoint module
Make sure network allows communication via port 48651 to/from EVS
Recheck vShield registration or re-register with vShield (enter management mode - vShield registration)

Errors in trace log:

Error: error[582a0000]: ESET Mdm client: CURL: Error in call easy perform: 3
Possible cause: The hostname/IP address is not configured properly in the ERA policy for EVS machine.
Possible solution: Make sure there is only one policy for ESET Virtualization Security - Security Appliance with proper settings in the Hostname field under VIRTUAL AGENT HOST

Error: error[582a0000]: ESET Mdm client: CURL: Error in call easy perform: 7
Possible cause: EVS is not able to connect to the vAgent Host machine - the machine is not accessible
Possible Solution: Make sure the vAgent Host is turned on and/or try to troubleshoot the network connection problems.

Error: error[582a0000]: ESET Mdm client: CURL: Error in call easy perform : 60
Possible cause: Peer certificate cannot be authenticated with known CA certificates.
Possible Solution: Make sure you are using valid certificates and

CA.

Available support resources

ESET provides support in the form of User Guides, online Knowledgebase, and applicable to your region, chat, email or phone support.

ESET Virtualization Security Online Help contains comprehensive reference information for system settings, configurations, installation scenarios and more.

ESET Virtualization Security: http://help.eset.com/evs/1/en-US/index.html

ESET Remote Administrator Virtual Appliance Deployment: Contains content for deploying ERA in a virtualized environment

Visit www.eset.com/contact to email ESET technical support or for personalized assistance in North America, call 619-630-2400 (6:00am – 6:00pm Pacific Time, Monday – Friday).

For other questions, such as troubleshooting, FAQs and tutorial videos, you can search the ESET Knowledgebase.

- Tags
- NSX
- Virtualization Security