Anti-Virus Software Guidelines for Virtualization Environment

Document Contact: SUIT
Major Contributors: SUIT
Last Revision Date: July 2020
Revision: 1.7
9.2.1 Remove NSX from vSphere Web Client ................................................................. 90
9.2.2 Verify that MOVE has been successfully uninstalled ........................................ 94
9.3 Remove an individual host from NSX Prepared Cluster ........................................... 94
10 Known issues & References .................................................................................. 95
10.1 Known issues ........................................................................................................ 95
10.2 References ........................................................................................................... 95
1 Introduction

1.1 Scope
This document guides installation and configuration of McAfee MOVE AntiVirus (Agentless) in an NSX for virtualized environment.

1.2 Revision History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.7</td>
<td>July 2020</td>
<td>Added Migration support from VMWare NSX 6.3.3 with McAfee MOVE 4.5.x to VMware NSX 6.4.5 with McAfee MOVE 4.8.x</td>
</tr>
<tr>
<td>1.6</td>
<td>March 2020</td>
<td>Added Migration support from VMWare NSX 6.3.3 with McAfee MOVE 4.5.x to VMware NSX 6.4.5 with McAfee MOVE 4.8.x</td>
</tr>
<tr>
<td>1.5</td>
<td>October 2019</td>
<td>Added NSX manager upgrade procedure.</td>
</tr>
<tr>
<td>1.4</td>
<td>June 2019</td>
<td>Added qualification of VMware NSX 6.4.5.13282012 with McAfee MOVE AL 4.8.0.168</td>
</tr>
<tr>
<td>1.3</td>
<td>September 2018</td>
<td>Updated review comments, added qualification of VMware NSX Manager 6.3.3 with McAfee MOVE AL 4.5.1 302</td>
</tr>
<tr>
<td>1.2</td>
<td>September 2017</td>
<td>Added section to upgrade NSX Manager 6.2.5 to NSX Manager 6.3.3</td>
</tr>
<tr>
<td>1.1</td>
<td>July 2017</td>
<td>Antivirus software guidelines for virtualization environment in NSX environment</td>
</tr>
<tr>
<td>1.0</td>
<td>January 2017</td>
<td>Antivirus software guidelines for virtualization environment</td>
</tr>
</tbody>
</table>

1.3 Terms and Acronyms

<table>
<thead>
<tr>
<th>Terms and Acronyms</th>
<th>Abbreviations</th>
</tr>
</thead>
<tbody>
<tr>
<td>AL</td>
<td>Agentless</td>
</tr>
<tr>
<td>AV</td>
<td>AntiVirus</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>DRS</td>
<td>Distributed Resource Scheduler</td>
</tr>
<tr>
<td>EAM</td>
<td>ESX Agent Manager</td>
</tr>
<tr>
<td>ePO</td>
<td>ePolicy Orchestrator</td>
</tr>
<tr>
<td>ERICA</td>
<td>European Institute for Computer Antivirus Research</td>
</tr>
<tr>
<td>GI</td>
<td>Guest Introspection</td>
</tr>
<tr>
<td>HA</td>
<td>High Availability</td>
</tr>
<tr>
<td>MDCC</td>
<td>McAfee Data Center Connectors</td>
</tr>
<tr>
<td>MOVE</td>
<td>Management for Optimized Virtual Environments</td>
</tr>
</tbody>
</table>
1.4 Overview of NSX

VMware NSX is a software networking and security virtualization platform that delivers the operational model of a virtual machine for the network. Virtual networks reproduce the Layer2 - Layer7 network model in software, allowing complex multi-tier network topologies to be created and provisioned programmatically in seconds. NSX also provides a new model for network security. Security profiles are distributed to and enforced by virtual ports and move with virtual machines.

NSX supports VMware's software-defined data center strategy. By extending the virtualization capabilities of abstraction, pooling and automation across all data center resources and services, the software-defined data center architecture simplifies and speeds the provisioning and management of computing, storage, and networking resources through policy-driven automation. By virtualizing the network, NSX delivers a new operational model for networking that breaks through current physical network barriers and enables datacenter operators to achieve better speed and agility with reduced costs.

**NSX Manager**

The NSX Manager is the centralized network management component of NSX. It provides the single point of configuration and REST API entry-points.

The NSX Manager is installed as a virtual appliance on any ESXi host in your vCenter Server environment’s Manager and vCenter have a one-to-one relationship. For every instance of NSX Manager, there is one vCenter Server.

**Service Composer**

Service Composer helps you provision and assign network and security services to applications in a virtual infrastructure. You map these services to a security group, and the services are applied to the virtual machines in the security group using a Security Policy.

Data Security provides visibility into sensitive data stored within your organization's virtualized and cloud environments and reports any data security violations.
2  Planning your Installation

Security Virtual Machine (SVM) and virtual systems must have specific hardware and software to run McAfee MOVE AntiVirus. Review these requirements and recommendations before installing the software to make sure that your installation is successful.

2.1  Deployment Topology and Considerations

Below topology indicates a typical deployment of Guest Introspection and McAfee Move Appliance modules on Management and Production nodes for each ESXi host in an Experion virtualized system.

**Note:** Each host could be a standalone server such as a Dell PowerEdge 720 or a blade in a Dell FX2 or IBM/Lenovo BladeCenter S, storage could be local or shared.

**Figure 2-0. Deployment Topology**

The system shall be installed with a single NSX Manager and ePO per vCenter Server. In addition, each ESXi host to be protected by MOVE shall have an instance of the Guest Introspection and McAfee MOVE Appliances installed.

**NOTE:** ESXi hosts must be configured in a vSphere cluster.
2.2 About McAfee MOVE
Management for Optimized Virtual Environments (MOVE) AntiVirus is optimized for protecting virtual environments such as Virtual Machines running virtualization (hypervisor) software like VMware ESXi. It removes the need to install an anti-virus application on every virtual machine (VM) by offloading all scanning to a dedicated security virtual machine (SVM) so that customers get the protection they need without sacrificing performance.

McAfee MOVE AV brings advanced malware protection to your virtualized environments and integrates real-time threat intelligence with security management across your physical and virtual infrastructure.

McAfee MOVE AV provides two deployment options: Agentless and Multi-Platform. Both deployment options provide consistent protection and are managed and reported by McAfee ePolicy Orchestrator (McAfee ePO).

Agentless deployment
This deployment method integrates with VMware NSX Manager. It protects your virtual environment from malware without a McAfee Agent for easy deployment and setup. This deployment provides virus protection for VMs on the hypervisor.

Agentless components

ePolicy Orchestrator - A management platform that allows you to configure policies to manage Agentless configuration and provides reports on malware discovered in your virtual environment.

Security Virtual Machine (SVM) - The McAfee MOVE AntiVirus service package that provides anti-virus protection for VMs and communicates with the loadable kernel module on the hypervisor and McAfee ePO. The SVM is the only system directly managed by McAfee ePO. VirusScan Enterprise for Linux, McAfee Agent and McAfee MOVE AntiVirus (Agentless) are pre-installed.

VMware NSX Manager - Console that allows you to configure, provision, and automate the protection on the endpoints in a datacenter.

Virtual Machines (VMs) - Completely isolated guest operating system installations in a normal host operating system that support both virtual desktops and virtual servers.

2.3 System Requirements for NSX

System Requirements before you install NSX in your vCenter Server environment, consider your network configuration and resources.
Hardware Requirements

Table 1 H/W Details

<table>
<thead>
<tr>
<th></th>
<th>Memory</th>
<th>Disk</th>
<th>vCPU</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX Manager</td>
<td>16 GB allocated</td>
<td>60 GB</td>
<td>4</td>
<td>1 per vCenter</td>
</tr>
<tr>
<td>Guest Introspection</td>
<td>2 GB</td>
<td>6 GB</td>
<td>2</td>
<td>1 per host</td>
</tr>
</tbody>
</table>

Note: If your NSX managed environment contains more than 256 hypervisors, we recommend increasing NSX Manager Resources to 8 vCPU and 24 GB of RAM.

Software Requirements

For the latest interoperability information, see the Product Interoperability Matrix at https://www.vmware.com/resources/compatibility/sim/interop_matrix.php

These are the minimum required versions of VMware products.

- VMware vCenter server 6.0U2 or 6.5 U1
- VMware vSphere Client 6.0U2 or 6.5 U1
- VMware ESXi 6.0U2 or 6.5 U1
- VMware Tools
- Browser Support
  - Mozilla Firefox version 62 and later.
  - Microsoft Edge version 38 and later.
  - Google Chrome version 50 and later.

Note:

1. VMware ESXi 5.5 is not supported with VMware NSX 6.4.5.
2. VMware NSX Security Appliance is not compatible with Internet Explorer 11 v11.0.9600.16384 RTM Build KB2841134 only, other upgraded versions are successfully working

Client and User Access

- If you added ESXi hosts by name to the vSphere inventory, ensure that forward and reverse name resolution is working. Otherwise, NSX Manager cannot resolve the IP addresses
• User must have permissions to add and power on virtual machines
• Access to the data store where you store virtual machine files and the account permissions to copy files to that data store
• Cookies enabled on your Web browser, to access the NSX Manager user interface
• From NSX Manager, ensure port 443 is accessible from the ESXi host, the vCenter Server, and the NSX appliances to be deployed. This port is required to download the OVF file on the ESXi host for deployment.
• A Web browser that is supported for the version of vSphere Web Client you are using. See the vCenter Server and Host Management documentation for details:

### Ports and Protocols Required by NSX

The following ports must be open for NSX to operate properly

**Table 2. Ports and Protocols required by NSX.**

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
<th>Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESXi Hosts</td>
<td>NSX Manager</td>
<td>5671</td>
<td>TCP</td>
<td>Rabbit MQ (messaging bus technology)</td>
<td>Rabbit MQ</td>
</tr>
<tr>
<td>ESXi Host</td>
<td>NSX Controllers</td>
<td>1234</td>
<td>TCP</td>
<td>Communication between ESXi Host and NSX Controller Clusters</td>
<td></td>
</tr>
<tr>
<td>Client PC</td>
<td>NSX Manager</td>
<td>443</td>
<td>TCP</td>
<td>NSX Manager Admin Interface</td>
<td>HTTPS</td>
</tr>
<tr>
<td>REST Client</td>
<td>NSX Manager</td>
<td>443</td>
<td>TCP</td>
<td>NSX Manager REST API</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Client PC</td>
<td>NSX Manager</td>
<td>80</td>
<td>TCP</td>
<td>NSX Manager VIB Access</td>
<td>HTTP</td>
</tr>
<tr>
<td>NSX Manager</td>
<td>vCenter Server</td>
<td>443,80</td>
<td>TCP</td>
<td>vSphere Web Access</td>
<td>HTTPS</td>
</tr>
<tr>
<td>NSX Manager</td>
<td>vCenter Server</td>
<td>902</td>
<td>TCP</td>
<td>vSphere Web Access</td>
<td>VMware Internal</td>
</tr>
<tr>
<td>NSX Manager</td>
<td>ESXi Host</td>
<td>443</td>
<td>TCP</td>
<td>Management and provisioning connection</td>
<td>HTTPS</td>
</tr>
<tr>
<td>NSX Manager</td>
<td>ESXi Host</td>
<td>Port</td>
<td>Protocol</td>
<td>Description</td>
<td>Service</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------</td>
<td>------</td>
<td>----------</td>
<td>--------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td>DNS Server</td>
<td>53</td>
<td>TCP/UDP</td>
<td>DNS client connection</td>
<td>DNS</td>
</tr>
<tr>
<td>NSX Manager &amp; NSX Controller</td>
<td>NTP Time Server</td>
<td>123</td>
<td>TCP/UDP</td>
<td>NTP client connection</td>
<td>NTP</td>
</tr>
<tr>
<td>NSX Manager</td>
<td>Syslog Server</td>
<td>514</td>
<td>TCP/UDP</td>
<td>Syslog connection</td>
<td>Syslog</td>
</tr>
<tr>
<td>NSX Manager</td>
<td>vCenter Server</td>
<td>443</td>
<td>TCP</td>
<td>vSphere API</td>
<td></td>
</tr>
<tr>
<td>ESXi Host</td>
<td>NSX Manager</td>
<td>5671</td>
<td>TCP</td>
<td>AMQP</td>
<td></td>
</tr>
<tr>
<td>ESXi Host</td>
<td>vCenter Server</td>
<td>443</td>
<td>TCP</td>
<td>VIB deployment/Host preparation</td>
<td>EAM Service</td>
</tr>
<tr>
<td>vCenter Server</td>
<td>NSX Manager</td>
<td>443</td>
<td>TCP</td>
<td>Download Web Client plugin(vsmext.zip)</td>
<td>Web Client</td>
</tr>
<tr>
<td>ESXi Host</td>
<td>NSX Manager</td>
<td>8301 and 8302</td>
<td>UDP</td>
<td>DVS Sync</td>
<td></td>
</tr>
<tr>
<td>NSX Manager</td>
<td>ESXi Host</td>
<td>8301 and 8302</td>
<td>UDP</td>
<td>DVS Sync</td>
<td></td>
</tr>
<tr>
<td>USVM</td>
<td>NSX Manager</td>
<td>5671</td>
<td>TCP</td>
<td>Guest Introspection</td>
<td></td>
</tr>
</tbody>
</table>

See the Network port requirements KB for more details.
https://kb.vmware.com/s/article/2079386
2.4 System and hardware requirements for SVM

SVM requirements (Agentless)

- You must use the virtual machine we provide for Agentless SVM. This system is a dedicated virtual appliance with Endpoint Security for Linux Threat Prevention installed.
- The McAfee Security Virtual Machine (SVM) package must be checked in to McAfee ePO.
- The SVM VM is built to meet these minimum hardware requirements:

<table>
<thead>
<tr>
<th>Table 3. SVM H/W requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CPU</strong></td>
</tr>
<tr>
<td>SVM</td>
</tr>
</tbody>
</table>

These items come pre-installed:

- Operating system Ubuntu 16.04
- Endpoint Security for Linux Threat Prevention 10.5.3
- McAfee Agent McAfee MOVE AntiVirus (Agentless)

Client system requirements

The McAfee MOVE AntiVirus client software requires one of these operating systems:

<table>
<thead>
<tr>
<th>Table 4. SVM OS details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OS</strong></td>
</tr>
<tr>
<td>Windows Vista</td>
</tr>
<tr>
<td>Windows Server 2008 SP2</td>
</tr>
<tr>
<td>Windows 7</td>
</tr>
<tr>
<td>Windows 2008 R2 SP1</td>
</tr>
<tr>
<td>Windows 8</td>
</tr>
<tr>
<td>Windows 2012</td>
</tr>
<tr>
<td>Windows 8.1</td>
</tr>
<tr>
<td>Windows 2012 R2</td>
</tr>
<tr>
<td>Windows 10</td>
</tr>
<tr>
<td>Windows Server 2016</td>
</tr>
</tbody>
</table>
Supported VMware management platform and software

**Table 5** Appliance

<table>
<thead>
<tr>
<th>Appliance and software</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware vCenter</td>
<td>6.0 U2 or 6.5 U1</td>
</tr>
<tr>
<td>VMware ESXi</td>
<td>6.0 U2 or 6.5 U1</td>
</tr>
</tbody>
</table>

Supported McAfee management platform and software

**Table 6.** Supported McAfee software

<table>
<thead>
<tr>
<th>Software</th>
<th>Agentless Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee ePO</td>
<td>5.3.3, 5.9.0,5.9.1, or 5.10.0 Update 3</td>
</tr>
<tr>
<td>MDCC</td>
<td>5.3.1.216</td>
</tr>
<tr>
<td>McAfee Agent</td>
<td>5.5.1.342</td>
</tr>
<tr>
<td>VirusScan Enterprise</td>
<td>NA</td>
</tr>
</tbody>
</table>

2.5 Downloading software extensions and packages

You must download these software extensions and product packages before the components can be deployed to virtual systems or installed on McAfee ePO.

From the Software Manager or McAfee download site


download these packages.

**Table 7.** Software extensions and product details

<table>
<thead>
<tr>
<th>Package name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOVE-AV_Meta_Package_Ext_4.8.0.104.zip</td>
<td>This main extension includes these extensions:</td>
</tr>
<tr>
<td></td>
<td>• McAfee MOVE AntiVirusCommon — Extension for product installation and deployment</td>
</tr>
<tr>
<td></td>
<td>• McAfee MOVE AntiVirus — Extension for configuring and managing policies</td>
</tr>
<tr>
<td></td>
<td>• McAfee MOVE AntiVirusLicense — License extension; upgrades evaluation extension to a fully licensed extension</td>
</tr>
<tr>
<td></td>
<td>• vSphere Connector — Data Center discovery software</td>
</tr>
<tr>
<td></td>
<td>• McAfee Data Center Control — It is a dependency software for vSphere Connector</td>
</tr>
<tr>
<td></td>
<td>• Product Help extension</td>
</tr>
<tr>
<td>MOVE-AV-AL_SVM_OVF_4.8.0.168.zip</td>
<td>Agentless SVM OVF package — McAfee ePO deployable package</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------------------------------------</td>
</tr>
<tr>
<td>MDCC_5.3.1.zip</td>
<td>MDCC is the base management extension for all Cloud Workload Discovery. Install this extension to discover the VM information and import it to the System Tree.</td>
</tr>
<tr>
<td>MOVE AntiVirus Common Extension Version 4.8.0.135.zip</td>
<td>Common UI Core extension. This extension must be installed on McAfee ePO to install Cloud Workload Discovery.</td>
</tr>
<tr>
<td>vSphere Connector Extension Version 5.3.1.206.zip</td>
<td>vSphere Connector — Data Center discovery software</td>
</tr>
<tr>
<td>MOVE- AV_DOCS_4.8.0.zip</td>
<td>Product documentation package</td>
</tr>
</tbody>
</table>
2.6 Special HA and DRS considerations

On a cluster utilizing DRS and HA, ensure the MOVE Appliance and Guest Introspection appliances are excluded from DRS and HA, as they should always only be run on the specific hosts they are deployed to.

Note: When a host using DRS/HA with MOVE and Guest Introspection appliances running on it is put into Maintenance mode these appliances will need to be manually shutdown after the other VMs on this host have been migrated to other hosts.
3 Installing and Configuring a new NSX Manager

This section describes for new installation, and refer section 7 to upgrade the existing installs.

The NSX Manager provides the graphical user interface (GUI) and the REST APIs for creating, configuring and monitoring NSX components, such as controllers, logical switches, and edge services gateways. The NSX Manager provides an aggregated system view and is the centralized network management component of NSX. NSX Manager is installed as a virtual appliance on any ESXi host in your vCenter environment.

For high availability, VMware recommends that you deploy NSX Manager in a cluster configured with HA and DRS.

**NOTE:** The NSX Manager virtual machine installation includes VMware Tools. Do not attempt to upgrade or install VMware Tools on the NSX Manager.

**Obtain the NSX Manager OVA File**

The NSX Manager virtual machine is packaged as an OVA file which allows you to use the vSphere Web Client\Client to import the NSX Manager into the datastore and virtual machine inventory.

Go to “my.vmware” website, enter your login credentials, and download the [VMware-NSX for vSphere 6.4.5](https://my.vmware.com/group/vmware/details?downloadGroup=NSXV_645&productId=614) Or refer the following link.

**Image 3-1.** Download NSX Manager
<table>
<thead>
<tr>
<th>File</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NSX for vSphere 6.4.5</strong>&lt;br&gt;File size: 2.32 GB&lt;br&gt;File type: ova</td>
<td><img src="download.png" alt="Download Now" /></td>
</tr>
<tr>
<td><strong>NSX for vSphere 6.4.5 Upgrade Bundle</strong>&lt;br&gt;File size: 2.22 GB&lt;br&gt;File type: tar.gz</td>
<td><img src="download.png" alt="Download Now" /></td>
</tr>
<tr>
<td><strong>Standalone Edge - Client</strong>&lt;br&gt;File size: 140.26 MB&lt;br&gt;File type: tar.gz</td>
<td><img src="download.png" alt="Download Now" /></td>
</tr>
</tbody>
</table>
3.1 Installing and Configuring the NSX Manager

Adding a new NSX Manager
Install the NSX Manager virtual machine on an ESXi host that is configured in a vSphere cluster.

- Log into the VMware vSphere web client to deploy NSX manager ova template.
- After logging in, Select Cluster | Actions | All vCenter Actions | Deploy OVF. Image

Image 3-2. Deploy OVF
• Specify the **source location** (Browse your file system for an OVF or OVA template) and click “Next”.

• In the **1b Review Details** page, select the “Accept extra configuration options” and then press “Next”.

**Image 3-3. Review details**

Agree to accept the terms of the end user license agreements, and click “Next”.

• Edit the **name** and select the folder location within the inventory where the VM will reside, and click “Next”.

• In the **Select Storage** page, select the **VM Storage Policy** and the **Destination Datastore** for the NSX Manager virtual appliance. Then press “Next”.

• Select a network by right-clicking the **Destination Network** column in your infrastructure to set up the network mapping and click “Next”.

**Image 3-4. Setup networks**

In the **2e Customize template** page, enter the CLI Admin User and CLI Privilege Mode passwords and then expand the Network properties object.
Image 3-5. Configure passwords

- Enter the Hostname, Network 1 IPv4 Address, Network1 Netmask, and Default IPv4 Gateway and then expand the DNS object.

Image 3-6. Configure network

- Enter the DNS Server list, Domain Search list and then expand the Services Configuration object.
- Enter the NTP Server list and then press the Next button.

In the Ready to complete page, review the configuration, select Power on after deployment and
then press Finish.

- Once the NSX Manager appliance is deployed and powered on open a web browser to the specified IP address, which is configured during customize template page.

**Image 3-7. NSX Login**

![NSX Login Image]

- Enter Username (admin by default) and Password (as configured in section 4, image 1.4) and click the Login button.
- Click on Manage Appliance Settings button
- In Time Settings section, click Edit and type the Name\IP address of your NTP server and click OK. The NTP server establishes a common network time.

**Image 3-8. NTP settings**
Note: It is recommended that you use the NTP server used by the SSO server so that the time on the NSX Manager server is in sync with the NTP server.

- Navigate to Network page, and re-check the configured details (as configured, while deploying NSX in section 4, image 1.5) or configure Netmask, Default Gateway, and DNS server Details.

Image 3-9 Review Network Details
- Navigate to NSX Management service page, click on **Edit** in **Lookup Service URL** section and enter the appropriate **lookup service host**, credentials and then click **OK**.

**Image 3-10.** Edit Lookup Service URL

![Lookup Service URL form](image)

- Click **yes** for security token pop service.

Once, lookup service status turns to connected, click on **Edit** in **vCenter Server** section and enter the appropriate credentials to connect to vCenter Server then click **OK**.

**Image 3-11.** Edit vCenter Credentials

![vCenter Server form](image)

- Click **yes** in Trust Certificate window.
Once the registration is successful, both the **Lookup Service URL** and **vCenter Server** status should be **connected** (In green)

**Image 3-13 Status**

*Note: After configuring NSX Manager restart the VMware vSphere Web Client on the vCenter Server the NSX Manager was registered with.*

- Log in to the vSphere web client and browse to **Networking & Security**, click **NSX Managers** and verify the newly deployed NSX Manager is present.

**Image 3-14 Verify NSX Manager**
3.2 Install Guest introspection

NOTE

This section describes for new installation, and refer section 6 to upgrade the existing installs.

Installing Guest Introspection automatically installs a new VIB and a service virtual machine on each host in the cluster.

Prerequisites:

The installation instructions that follow assume that you have the following system:

- A datacenter with supported versions of vCenter Server and ESXi installed on each host in the cluster.
- ESXi hosts must be configured in a vSphere cluster.
- All the necessary ports are open as mentioned in section 2.1, table 2.
- Hosts in the cluster where you want to install Guest Introspection have been prepared for NSX. **Note:** Guest Introspection cannot be installed on standalone hosts.

- Ensure the NSX Manager and the prepared hosts that will run Guest Introspection services are linked to the same NTP server and that time is synchronized. Failure to do so may cause VMs to be unprotected by antivirus services, although the status of the cluster will be shown as green for Guest Introspection and any third-party services.

  NTP server details configured in NSX as shown in section 4, Image 1-7 and the ESXi host should be linked to the same NTP server and the time should be in sync.

Follow the steps specified in the below link, to see/configure the NTP server details in ESXi host

https://kb.vmware.com/s/article/2012069

If you want to assign an IP address to the NSX Guest Introspection service virtual machine from an IP pool, create the IP pool before installing NSX Guest Introspection. See Working with IP Pools in the NSX Administration Guide.

Procedure

Log on to vSphere web client as an administrator.

Go to Home | Networking & Security | Installation, then click the Service Deployments tab.

- Click on New Service Deployment (+) icon.

  Image 3-15. Service Deployment
• In the Deploy Network and Security Services dialog box, select **Guest Introspection**, select **Deploy now** to deploy Guest Introspection and click **Next**.

**Image 3-16. Select Services**

• Select the **datacenter and cluster(s)** where you want to install Guest Introspection, and click “Next”.
• On the Select storage and Management Network Page, select the datastore on which to add the service virtual machines storage or select “Specified on host”.

If you selected Specified on host, follow the steps below for each host in the cluster.

  On the vSphere Web Client home page, click vCenter and then click Hosts.
  - Click a host in the Name column and then click the Manage tab.
  - Click Agent VM Settings and click Edit.
Image 3-18. Agent VM settings

- Select the **datastore** and **Network** then, click **OK**.

  - Set datastore as **Specified on host**, and the network as **Specified on host**.
  - In IP assignment, select one of the following:

**DHCP**: Assign an IP address to the NSX Guest Introspection service virtual machine through Dynamic Host Configuration Protocol (DHCP). Select this option if your hosts are on different subnets.

**An IP pool**: Assign an IP address to the NSX Guest Introspection service virtual machine from the selected IP pool.
• Click Next and then click Finish on the Ready to complete page.
• Monitor the deployment until the Installation Status column displays Succeeded.

**Image 3-20. Status GI**
• After successful deployment GI, each host will now contain an ESXi Agents resource group with the installed service deployments.

**Image 3-21. Deployed Services in vCenter**
4 Upgrade VMware NSX Manager

This section describes how to upgrade the VMware NSX for vSphere system using the NSX Manager user interface and the vSphere Web Client. The information includes step-by-step upgrade instructions and suggested best practices.

<table>
<thead>
<tr>
<th>NOTE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. If you are upgrading NSX Manager 6.3.3 to NSX Manager 6.4.5, then follow the instructions in this section. Otherwise, skip to Section 7 to Install VMware Tools.</td>
</tr>
<tr>
<td>2. Before upgrading to VMware NSX 6.4.5, please make sure policies, policy assignment, client tasks and preconfigured queries and reports are taken backup in McAfee MOVE ePO.</td>
</tr>
<tr>
<td>Link for how to migrate policies: <a href="https://kc.mcafee.com/corporate/index?page=content&amp;id=KB88822">https://kc.mcafee.com/corporate/index?page=content&amp;id=KB88822</a></td>
</tr>
</tbody>
</table>

Download the NSX upgrade bundle:


2. Download [NSX for vSphere 6.4.5 Upgrade Bundle](https://www.honeywellprocess.com/library/support/security-updates/Customer/VMware-NSX-Manager-upgrade-bundle-6.4.5-13282012.tar.gz) and Confirm the file name: VMware-NSX-Manager-upgrade-bundle-6.4.5-13282012.tar.gz

Refer the instruction given in the Pdf file to download VMware-NSX-Manager-upgrade-bundle-6.4.5-13282012.tar.gz.

4.1 Steps to Upgrade NSX Manager 6.3.3 to 6.4.5

Perform the following procedure to Upgrade NSX Manager 6.3.3 to 6.4.5:

2. Verify McAfee MOVE AV and Guest Introspection services are up and running, before start upgrading to NSX 6.4.5

Image 4-1.
3. Log into the NSX manager with your credentials, select **Manage | Under settings | Upgrade | click on Upload Bundle**

**Image 4-2.**

4. Browse for the **NSX for vSphere 6.4.5 Upgrade Bundle** file path and click on **Continue**

**Image 4-3.**

**Image 4-4.**
5. Once the VMware NSX uploading is completed, click on **Upgrade** button to initiate the upgrade from VMware NSX 6.3.3 to VMware NSX 6.4.5.

Image 4-5.

6. The uploaded bundle will be validated & continue to upgrade by selecting **Upgrade** option.

Image 4-76.

**NOTE**
The SSH option also can be enabled/Disabled over here, and click on Upgrade button.
7. Wait for the upgrade for the NSX Manager to complete and go to NSX Manager | View Summary | check for Current software version & upgrade state as shown below

**Image 4-7.**

![NSX Manager Virtual Appliance](image)

**NOTE**
After the upgrade some services might get stopped, restart all the services and ensure that all services are running before proceeding with next steps.

4.2 Upgrading the VMware NSX manager from the vCenter Web client

Precondition: VMware NSX Appliance should be upgraded to latest version as shown in the above section 6.1, else Upgrade icon will not be appeared in vSphere Web client

1. Log in to vCenter Server, navigate to Home | Networking & security | installation | service deployment.
2. Under Service Deployment tab, search for Upgrade Available option under Guest Introspection | click on upgrade. (up arrow)

**Image 4-8.**
3. Wait for the upgrade process to complete and verify the latest version of VMware NSX 6.4.5 is updated as shown below

Image 4-9

The EAM status is available from 6.3.3 and later versions of the NSX manager
4.3 Upgrade McAfee MOVE 4.5.x to 4.8.0

This section describes the users for upgrading to McAfee MOVE 4.8.0. For users to configure the fresh installation of McAfee MOVE 4.8.0, please refer to section 8.

Preconditions:
1. Download the latest MOVE extensions from the [McAfee Products](#) download, by providing the grant number.
   - VSHEREDEXTN_5.3.2.111.zip
   - DC_GS_4000_4.8.1.16.zip
   - DC_AM_4000_4.8.1.30.zip
   - MDCC_5.3.2.270.zip
   - MOVEAVLIC400_4.8.1.28.zip
   - MOVE-AV_Meta_Package_Ext_4.8.0.104.zip
   - MOVE-AV_AL_SVM_OVF_4.8.0.168.zip

   (Or)
   - MOVE-AV_Meta_Package_Ext_4.8.0.104.zip
   - MOVE-AV_AL_SVM_OVF_4.8.0.168.zip

   user can individually check-in the respective MOVE extension in McAfee ePO from 1 to 5 or else check-in the “MOVE-AV_Meta_Package_Ext_4.8.0.104.zip” which includes all the latest updates of extensions for McAfee MOVE 4.8.0

2. Login to McAfee MOVE ePO, select HOME | software | Extensions

   ![Image 4-110](#)

   Click on Install Extensions

3. Click on Install Extensions
4. Click on **Choose File** and provide the file path of latest downloaded extensions.

5. Click on **OK** button to replace the extensions with latest versions
NOTE

User can individually choose to upgrade the extensions or check-in MOVE-AV_Meta_Package_Ext_4.8.0.104.zip to upgrade to latest extensions.

6. Click on HOME | software | Extensions | Data Center Security, verify upgrade extensions are reflecting with latest versions.

Image 4-14

7. Click on HOME | Automation | MOVE AntiVirus Deployment for deploying the McAfee MOVE Agentless SVM 4.8.
8. Click on Configuration | SVM Repository | Actions | Add SVM

9. Click on Choose File, browse the file path for MOVE-AV-AL_SVM_OVF_4.8.0.168.zip, click on OK
10. Click on **Service | NSX Manager | click on Upgrade**

Image 4-18
11. Wait for the McAfee SVM Upgrade to be completed and verify the versions as shown below

Image 4-19

12. Log in to vCenter Server, navigate to Home | Networking & security | installation | Service Deployment. Under Service Deployment tab, search for Upgrade Available option under McAfee MOVE AV | click on upgrade. (up arrow)

Image 4-20

13. Select the IP assignment pool | click on Upgrade Now | OK
14. Verify the McAfee MOVE AV deployment progressing as shown in the below, and wait for the MOVE upgrade to be completed

15. After successful upgrade verify Guest introspection and McAfee MOVE AV services to be GREEN(UP)
1. VMware announced [https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/support/product-lifecycle-matrix.pdf](https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/support/product-lifecycle-matrix.pdf) on February 2020 to NSX 6.2.x and VMware NSX 6.3.x releases. If the customers are on these releases, upgrade the VMware NSX to latest SUIT qualified versions.

2. McAfee announced [https://www.mcafee.com/enterprise/en-in/support/product-eol.html](https://www.mcafee.com/enterprise/en-in/support/product-eol.html) on December 2019 to MOVE 4.5.x releases. If the customers are on these releases, upgrade the McAfee MOVE to latest SUIT qualified versions.
5 Install and configure McAfee MOVE

In preparation for the McAfee Move virtual security appliances (VSA) on each ESXi host, McAfee ePolicy Orchestrator software, which acts as the management station for the solution needs to be deployed.

McAfee MOVE Agentless is controlled from the ePO server, which must first be configured. The ePO server continuously communicates with all Scan Virtual Appliances (SVA) across hypervisors. The basic policy configuration and event gathering data will come from the SVAs.

Prerequisites

Ensure McAfee ePolicy Orchestrator server (5.10 Update 3) installed on a Windows VM on your management ESXi host.

For more information on setting up the ePO server, refer McAfee ePO installation guide


Ensure the necessary ports for successful McAfee Agent registration and communication opened for inbound access on the Windows firewall on the ePO.

Table 8. Ports needed by ePO for communication through a firewall

<table>
<thead>
<tr>
<th>TCP Port</th>
<th>Details</th>
<th>Traffic Direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>McAfee Agent communication port with ePO (downloads).</td>
<td>Inbound connection to the Agent Handler and the ePO server from the McAfee Agent. Inbound connection to the ePO server from the remote Agent Handler.</td>
</tr>
<tr>
<td>443</td>
<td>McAfee Agent secure communication port with ePO.</td>
<td>Inbound connection to the Agent Handler and the ePO server from the McAfee Agent. Inbound connection to the ePO server from the remote Agent Handler. Outbound connection from the ePO server to McAfee servers.</td>
</tr>
<tr>
<td>8443</td>
<td>McAfee Agent registration port with ePO.</td>
<td>Inbound connection to the ePO server from the ePO console.</td>
</tr>
<tr>
<td>8081</td>
<td>The port that provides the ability to send a wake-up call to the McAfee Agent installed on the SVAs/SVMs, using ePO.</td>
<td>The inbound connection from the ePO server/Agent Handler to the McAfee Agent. The inbound connection from client machines to Super Agents configured as repositories.</td>
</tr>
</tbody>
</table>
For more information, refer below the article.
https://kc.mcafee.com/corporate/index?page=content&id=KB66797

5.1 Overview of MOVE AV deployment process
Using McAfee ePO and vSphere Web Client, you can register the McAfee MOVE AntiVirus SVM with VMware NSX Manager, configure it, and deploy it to your clusters. This deployment automatically provides virus protection for virtual machines on a new hypervisor from the moment the hypervisor is added to the cluster.

**Note:** This assumes that the user has already configured and installed McAfee ePO.

The overall McAfee MOVE AntiVirus service deployment in an NSX environment consists of the following tasks.

1. Register vCenter Server with NSX Manager.
2. Install the extensions for Cloud Workload Discovery and McAfee MOVE AntiVirus on McAfee ePO in this order:
   - Cloud Workload Discovery
   - McAfee MOVE AntiVirus
3. Register a VMware vCenter account with McAfee ePO.
4. Set up a common configuration for McAfee ePO and McAfee MOVE AntiVirus SVM on the McAfee ePO server.
5. Check in the McAfee MOVE AntiVirus SVM package to McAfee ePO.
6. Test the NSX Manager connection to the McAfee ePO server by validating the credentials of the NSX Manager.
7. Register the McAfee MOVE AntiVirus service with NSX Manager using McAfee ePO.
8. Verify the policy export details in vSphere Web Client.
10. Apply the NSX Security Policy to the NSX Security Group.
11. Deploy the McAfee MOVE AntiVirus service using vSphere Web Client.
12. Apply McAfee MOVE AntiVirus (Agentless) protection to your VMs.
Below diagram indicates the overall deployment process of MOVE AntiVirus service (NSX)

**Figure 5-1. Deployment Process of MOVE AV Service**

5.2 Deploying McAfee MOVE AntiVirus (Agentless) in an NSX environment

The extensions for Cloud Workload Discovery and McAfee MOVE AntiVirus allow you to register the vCenter account and set up the NSX requirements. You must complete this process before deploying the McAfee MOVE AntiVirus service and configuring the policies.

Using McAfee ePO and vSphere Web Client, you can register the McAfee MOVE AntiVirus SVM with VMware NSX Manager, configure it, and deploy it to your clusters.

This deployment automatically provides virus protection for virtual machines on a new hypervisor from the moment the hypervisor is added to the cluster.

Register vCenter Server with NSX Manager

Refer Section 4, Page no 21 to register vCenter Server with NSX Manager. Otherwise, skip to next step.

5.2.1 Install the product extension files on the management (ePO) server

The product extensions for Cloud Workload Discovery, McAfee MOVE AntiVirus must be installed on the McAfee ePO server before you can manage McAfee MOVE AntiVirus on your virtual machines.

**Note:** Before you begin, ensure extension files are in an accessible location on the network.
Procedure

- Log on to McAfee ePO server as an administrator
- Select **Menu | Software**, then click **Extensions** to open Extensions page.

You must install the product extensions in the below-specified order.

- MOVE-AV_Meta_Package_Ext_4.8.0.104.zip
- MDCC_5.3.1.zip
- DC GS 4000_4.8.0.135_HF1264345.zip
- VSPHEREDCEXTN.zip

- Click **Install Extension**, browse and select the **MOVE-AV_Meta_Package_Ext_4.8.0.104** extension file, then click **OK**.

**Figure 5-2. Browse Extensions**

- After a confirmation message, click **OK**.
- Repeat the process to install the extension of **MDCC_5.3.1.zip**, **DC GS 4000_4.8.0.135_HF1264345.zip**, and **VSPHEREDCEXTN.zip** files extension.
- Once, extensions are installed successfully, this extension will be visible under extension page.
### Image 5-3. Installed extensions

<table>
<thead>
<tr>
<th>Name:</th>
<th>MOVE AntiVirus</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version:</td>
<td>4.8.0.131</td>
</tr>
<tr>
<td>Installed by:</td>
<td>admin - May 27, 2019 5:31:21 AM PDT</td>
</tr>
</tbody>
</table>

#### 5.2.2 Register a VMware vCenter account with McAfee ePO (5.10 Update 3)

To enable and manage the security of the virtual machines in your datacenter with McAfee MOVE AntiVirus (Agentless), you must first add the vCenter to the McAfee ePO server. This is the same vCenter account that you already registered with NSX Manager.

Note: Before you begin, ensure you have installed the Cloud Workload Discovery or MDCC extension on the McAfee ePO server. Configured your VMware vCenter server that manages the ESXi servers, which host the guest VMs.

- Log on to McAfee ePO as an administrator.
- Select **Menu > Configuration > Registered Cloud Accounts**, then click **Add Cloud Account** to open the **Add Cloud Account** page.

### Image 5-4. Add cloud Account
• From the **Choose Connector** drop-down list on the **Description** page, select **VMware vSphere**, then click **OK**.
• On the **vCenter Account Details** page, type **Account Name**, **Server IP Address**, **vCenter Username**, and **vCenter Password**, **Port No.**, and **Sync interval** details.

**Image 5-5. Register Cloud Account**

1. Click **Test Connection** to validate VMware vCenter account details and verify the connection to the VMware vCenter, then click **Next** to open the **Validate Certificate** page.
2. Click **Accept** to validate the certificate, then click **Finish**.
3. When prompted to confirm, click **OK** to register the vCenter account.

**Note**: This action registers the VMware vCenter and imports all discovered virtual machines, which are unmanaged, into the System Tree. The instances are imported with the same organization as the VMware vCenter.

4. After configuring and registering the VMware vCenter account with McAfee ePO, the account details of the registered vCenter are displayed in McAfee ePO. You can see information such as the number of VMs that are available under the registered vCenter. How many VMs are up and running under the registered vCenter and how many VMs are managed by McAfee ePO. If the number of Total VMs show 0, click on sync at the far right of the console to initiate an immediate discovery.
5. To verify that the VMs were imported, select **Menu | Systems | System Tree**. After the discovery, you can find your vCenter account under the group vSphere. The clusters and hosts from vCenter are logically grouped under each datacenter group in the System Tree.

**Image 5-7 Imported VMs**

**Note:** Once the McAfee MOVE AntiVirus (Agentless) product setup is done and running, you must not delete the Registered Cloud Account.
5.2.3 Set up a common configuration for McAfee MOVE AntiVirus SVM deployment

Before deploying the McAfee MOVE AntiVirus SVM, configure these settings on the McAfee ePO server, so that they are retrieved and used for every McAfee MOVE AntiVirus SVM deployment, from the same McAfee ePO server.

Prerequisite

McAfee MOVE AntiVirus extension should be installed on the McAfee ePO server.

Procedure

1. Log on to McAfee ePO as an administrator.
2. Select Menu | Automation | MOVE AntiVirus Deployment.
   
   **Note:** MOVE AntiVirus Deployment option will be enabled only after installing MOVE AV License extension in ePO server.

3. On the Configuration tab, click General and configure credentials for McAfee ePO and SVA.
4. Click Save to store these configurations, so that you can use them for every McAfee MOVE AntiVirus SVM deployment.

**Image 5-8. General Configuration**
5.2.4 Check in the McAfee MOVE AntiVirus SVM package to McAfee ePO

Check in the McAfee MOVE AntiVirus SVM package to McAfee ePO, so that it is available with VMware NSX Manager to deploy it to the cluster. You can view and delete the McAfee MOVE AntiVirus SVM package using McAfee ePO.

- Log on to McAfee ePO as an administrator.
- Select Menu | Automation | MOVE AntiVirus Deployment.
- On the Configuration tab, click SVM Repository to open the SVM Repository page.
- Click Actions | Add SVM to open the Check-in SVM (zip) File page.

Image 5-9. Add SVM

- From Select SVM (zip) file to check-in under SVM Repository Details, browse to and select the McAfee MOVE AntiVirus SVM package, then click OK. This action checks in the McAfee MOVE AntiVirus SVM package to McAfee ePO. Once the file check in successful, SVM package should be listed under SVM Repository as shown in the below screen shot.
5.2.5 Validate your NSX Manager using McAfee ePO

The Cloud Workload Discovery or MDCC extension automatically detects and sends the details of your NSX Managers to the McAfee ePO server. But, these NSX servers are not yet registered with McAfee ePO.

Before You Begin:

- You created and configured NSX Manager.
- You registered the vCenter account with NSX Manager.
- You installed the McAfee MOVE AntiVirus extension on the McAfee ePO server.

Using this configuration available on the McAfee ePO server, you can edit the details and validate the credentials of your NSX Manager. From here, you can also register your vCenter server with NSX Manager.

Procedure:

- Log on to McAfee ePO as an administrator.
- Select Menu | Automation | MOVE AntiVirus Deployment.
- On the Configuration tab, click NSX Manager. The NSX Manager: Registration page appears with these details.
- Click Edit under Action to open the Edit NSX Manager Details dialog box and edit these NSX Manager Account details.
- Configure NSX Manager Name, NSX Manager Address, Port, Username, and Password details.
Image 5-11. Edit NSX Manager Details

<table>
<thead>
<tr>
<th>Automation</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOVE AntiVirus Deployment</td>
</tr>
</tbody>
</table>

### Edit NSX Manager Details

<table>
<thead>
<tr>
<th>vCenter Account:</th>
<th>NSX-MOVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX Manager Name:</td>
<td>SUIT-NSX-MGR</td>
</tr>
<tr>
<td>NSX Manager Address:</td>
<td>192.168.85.231</td>
</tr>
<tr>
<td>NSX Manager Port:</td>
<td>443</td>
</tr>
<tr>
<td>NSX Manager Username:</td>
<td>admin</td>
</tr>
<tr>
<td>NSX Manager Password:</td>
<td>**********</td>
</tr>
</tbody>
</table>

- Click **Validate** to verify the credentials of the NSX Manager and check that the connection to the NSX Manager works.
- Click **Save** to store the NSX Manager account details.

#### 5.2.6 Register the McAfee MOVE AntiVirus service with NSX Manager using McAfee ePO

After registering your vCenter account details on NSX Manager and McAfee ePO, use McAfee ePO to enable the registration of McAfee MOVE AntiVirus (Agentless) as a service in NSX Manager. The details of the registered vCenter, SVM, and NSX Manager are automatically retrieved and displayed on the McAfee ePO server. But you must register the McAfee MOVE AntiVirus service with the vCenter account using McAfee ePO. This registration permits the deployment of the McAfee MOVE AntiVirus service to the ESXi servers.
Procedure:

- Log on to McAfee ePO as an administrator.
- Select Menu | Automation | MOVE AntiVirus Deployment.
- On the Service tab, click NSX Manager to open the MOVE Service Registration page with these details.

Table 9. Configuration Field details

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX Manager Name</td>
<td>Displays the name of the registered NSX Manager.</td>
</tr>
<tr>
<td>NSX Manager Address</td>
<td>Displays the IP address of your NSX Manager.</td>
</tr>
<tr>
<td>vCenter Account</td>
<td>Displays the name of the vCenter account that is registered with NSX Manager and McAfee ePO.</td>
</tr>
<tr>
<td>Registered SVM Version</td>
<td>Displays the version of the McAfee MOVE AntiVirus SVM package checked in to McAfee ePO.</td>
</tr>
<tr>
<td>Service Registration Status</td>
<td></td>
</tr>
</tbody>
</table>
  - **Registered** - Indicates that the McAfee MOVE AntiVirus service is registered and ready for deployment.  
  - **Not Registered** - Indicates that the McAfee MOVE AntiVirus service is not registered.  
  - **Registration Failed** - Indicates that the McAfee MOVE AntiVirus service failed. |
| Actions                  |  
  - **Register** - Click to select the latest McAfee MOVE AntiVirus SVM and register it to the vCenter that is added to your NSX Manager.  
  - **Unregister** - Click to unregister the McAfee MOVE AntiVirus service and to remove it from the vCenter that is added to your NSX Manager.  
  - **Upgrade** - Click to upgrade the McAfee MOVE AntiVirus service. |
• Click Register under Actions to open the MOVE Service Registration dialog box.

**Image 5-12. NSX Manager Registration Details**

<table>
<thead>
<tr>
<th>Service</th>
<th>NSX Manager</th>
<th>vCenter Account</th>
<th>Service Registration</th>
<th>Service Registration Status</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOVE AntiVirus Deployment</td>
<td>NSX Manager 1</td>
<td>vCenter 1</td>
<td>4.8.0.168</td>
<td></td>
<td>Update</td>
</tr>
</tbody>
</table>

**Image 5-13. MOVE Service Registration**

• Select the latest McAfee MOVE AntiVirus SVM and click OK. The McAfee MOVE AntiVirus service is now registered with the vCenter account that is registered with your NSX Manager.
• Once the MOVE Antivirus service is registered successfully, The McAfee MOVE AV service should now be listed in the vSphere web client under **Networking & Security, Service Definitions**.

**Procedure:**

• Log on to vSphere web client as an administrator.
• **Select** Networking & Security | Service Definitions.
5.2.7 **On-access scan policy export to NSX**

After you register the McAfee MOVE AntiVirus service on McAfee ePO server, the On Access Scan policies for McAfee MOVE AntiVirus are exported from McAfee ePO to NSX in real time.

The exported policies are available in Profile Configurations under Networking & Security | Service Definitions | McAfee MOVE AV | Actions | Edit settings | Manage | Profile Configurations with a policy ID and description.
Note: Only the On Access Scan policies are exported from McAfee ePO to NSX Manager. If you need to assign the On Demand Scan policies, assign them manually on McAfee ePO.

When you create or change an On Access Scan policy in McAfee ePO, it is immediately exported to Profile Configurations in vSphere Web Client. This real-time policy export helps the VMware administrator understand the different set of policies created and changed by the administrator.

Note: Changes to On Access Scan policy names in McAfee ePO are not updated in NSX. You must manually update the name changes in NSX.

When you delete an On Access Scan policy from McAfee ePO, it is deleted from NSX Manager if it is not included in any of the NSX security policies. You can't delete the exported On Access Scan policy in NSX Manager when it is included in any NSX security policy. You must remove all configuration referring to this policy before deleting it.

### 5.2.8 Deploy McAfee MOVE AntiVirus Service

To provide McAfee MOVE AntiVirus (Agentless) protection to the virtual machines on your ESXi servers, you must install the McAfee MOVE AntiVirus service (McAfee MOVE AntiVirus SVM) on your ESXi servers.

Before you begin

- Ensure the host, where you are deploying the SVM using NSX Manager, is part of a cluster.
- Guest Introspection service is installed on all ESXi servers as in section 5.
- Virtual machines have the latest VMware Tools installed, including the vShield Driver as in section 6.
- You have appropriate permission to perform the SVM deployment using McAfee ePO.

Info: You can enable this permission by navigating through Menu | Users | Permission Sets | MOVE AV [Agentless] SVM Deployment | Edit.
Using the VMware vSphere Web Client console, you can deploy the McAfee MOVE AntiVirus services on a set of clusters. Manage service deployments here by adding new services or deleting existing ones.

This deployment automatically provides virus protection for virtual machines on a new hypervisor from the moment the hypervisor is added to the clusters. When a new cluster is added, deploy the McAfee MOVE AntiVirus SVM again.

Procedure:

- Log on to vSphere web client as an administrator.
- Go to Home | Networking & Security | Installation, then click the Service Deployments tab.
- Click on New Service Deployment (+) icon, as shown in section 5, image 2-4.
- In the Deploy Network and Security Services dialog box, select McAfee MOVE AV, select Deploy now to deploy McAfee MOVE AV and click “Next”.

Image 5-16. Select MOVE AV Service

- Select the cluster(s) where you want to install McAfee MOVE AV, and click Next. As shown in section 5, image 2-6.

- From Select storage and Management Network, for each cluster, select a datastore on which to store the McAfee MOVE AntiVirus SVM, the network and the IP assignment for the McAfee MOVE AntiVirus service to use.
If you are assigning static IP pools in the **IP Assignment** column to the McAfee MOVE AntiVirus service or Guest Introspection service, make sure that your default gateway and DNS is reachable/resolvable and the prefix length is correct. If not, the McAfee MOVE AntiVirus and Introspection service VMs are not activated and they can't communicate to the NSX manager or McAfee ePO because their IPs are not on the same network as McAfee ePO or the NSX Manager.

- Review the settings and click Finish to complete the deployment of McAfee MOVE AntiVirus service.

**Image 5-17.**

When deployment is complete, the McAfee MOVE AntiVirus service appears in the list of Network & Security Service Deployments. This action initiates the SVM deployment to all hypervisors in the selected cluster. The SVM deployment might take a few minutes to complete.

- The McAfee MOVE AntiVirus service is now deployed to the cluster when the Installation Status is Successful and view these Service status details on the VMware vSphere Web Client console.
Table 10. Service Status

<table>
<thead>
<tr>
<th>Service Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNKNOWN</td>
<td>Specifies that the McAfee MOVE AntiVirus service status is unknown.</td>
</tr>
<tr>
<td>UP</td>
<td>Up and running</td>
</tr>
<tr>
<td>DOWN</td>
<td>Specifies that the McAfee MOVE AntiVirus service is stopped.</td>
</tr>
</tbody>
</table>

Image 5-18. Service Status

After successful deployment, each host will now contain an ESXi Agents resource group with the installed service deployments.

Image 5-19. Service deployments VM in vCenter
Once the MOVE SVM Deployed successfully, MOVE SVA should be in **Managed** mode and should be communicating successfully.

Deployed MOVE SVA status also can be seen in the configured ePO
- Log on to McAfee ePO as an administrator.
- Select Menu | System Tree to the see the deployed SVA. Image 5-7. SVA Managed State

**Image 5-20**

![System Tree](image)

<table>
<thead>
<tr>
<th>System Name</th>
<th>Managed State</th>
<th>IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUIT-NX-MNGR-SVA-vanagent-17</td>
<td>Managed</td>
<td>dc_vm_auto, linux, NSX-MOVE, Work</td>
</tr>
<tr>
<td>DOWIN2016</td>
<td>Unmanaged</td>
<td>dc_vm_auto, NSX-MOVE, windows</td>
</tr>
<tr>
<td>ePG-Manager 5.5.1</td>
<td>Unmanaged</td>
<td>dc_vm_auto, NSX-MOVE, windows</td>
</tr>
<tr>
<td>EDS-MOVE</td>
<td>Unmanaged</td>
<td>dc_vm_auto, NSX-MOVE, windows</td>
</tr>
<tr>
<td>EDSIS-SRV</td>
<td>Unmanaged</td>
<td>dc_vm_auto, NSX-MOVE, windows</td>
</tr>
<tr>
<td>MOVE-REPLACE</td>
<td>Unmanaged</td>
<td>dc_vm_auto, NSX-MOVE, windows</td>
</tr>
</tbody>
</table>

Note: If the Managed State of MOVE SVA is in “unmanaged” state, then try to re-configure the network and register MOVE SVA with ePO manually as shown in the below steps.

- Open the console of MOVE SVA.
- At the prompt, log on with these credentials: User name: **svaadmin**
  - Password: (As configured in **section 8.2, image 4-3** or **admin** by default)
- Run `sudo /opt/McAfee/move/bin/sva-config`.
- Enter **Password** (As configured in **section 8.2, image 4-3** or **admin** by default) and click enter.
- Pass “**y or yes**” to proceed.
- Pass “**n or no**” to open SSH port on the firewall.
- Pass “**y or yes**” to continue with other configurations.
- Pass “**n or no**” to configure hostname
- Pass “**y or yes**” to configure the network.
- Pass “**static**” for Network IP configuration.
- Configure **IP address, Network Mask, Network, Broadcast Address, Gateway** and enter.
- Pass “**y or yes**” to configure DNS address.
- Configure the **DNS address** and enter.
• Pass “y or yes” to register McAfee Agent with ePO server.

**Image 5-21. SVA Manual Registration**

```
swadmin#NSManager-SVA-vmagent-39:~$ sudo /opt/McAfee/move/bin/sva-config
(sudo) password for swadmin:
Checking if this SUM deployment is done from NSX manager
This SUM is deployed using NSX Manager. MOVE SUM register or un-register with
uable using this script.
Would you like to proceed? yes/no [nol]: y

Executing the SUM configuration utility.
Open SSH port on firewall? yes/no [nol]: n
Do you want to continue with other configurations? yes/no [yes]: y

Configure host name? yes/no [nol]: n

Configure Network? yes/no [nol]: y
Network IP Address configuration. dhcp/static [static]: static
IPv4 Address (192.168.0.231): 192.168.0.231
Network Mask (255.255.255.0): 255.255.255.0
Gateway (192.168.0.1): 192.168.0.1
Restarting the network interfaces. Please wait...

Configure DNS servers? yes/no [nol]: y
[ok] Starting resolvconf (via systemd): resolvconf.service.
Nameserver 1 (Enter 'none' to delete) (192.168.0.61): 192.168.0.6
Nameserver 2 (Enter 'none' to delete): 
DNS Domain (Enter 'none' to delete): 
```

• Configure ePO server IP address, Port, Username, and Password.

**Image 5-22. SVA Registration**

```
Would you like to register McAfee agent with ePO server? yes/no [nol]: y
Enter ePO Server IP address or DNS name: 192.168.0.223
Enter ePO Server Port (0001): 9413
Enter ePO Server Administrator user name (admin): admin
Enter ePO password:
Is the ePO server running in FIPS mode? yes/no [nol]: n

McAfee Agent registration is complete.if this SUM is not communicating with the ePO server,
please check the log file /opt/McAfee/move/log/mcafee_agent_registration.log for any errors.

Restoring McAfee MOVE service...
Shutting down move monitor service... move is stopped
Shutting down move monoray service... monoray is stopped
Shutting down move javamove service... javamove is stopped
Shutting down move MoveAMAgentless service... javamove is stopped
Setting MOVE Service to Down
MoveAMAgentless is started
2017-07-10 06:36:12 (13070) MoveAMAgentless: Startup moved
2017-07-10 06:36:12 (13070) cmagent.info: Refresh policy command initiated by cmagent.
2017-07-10 06:36:12 (13070) cmagent.info: Policy enforcement command initiated by cmagent.
```

Once the McAfee Agent registration and are started successfully, the SVA machine should be able to
communicate with ePO (If not any error).
5.3 Configuring the Security Group and Security Policy

You must create the security policy and apply it to the security group of VMs that you want to protect. The security policies for McAfee MOVE AntiVirus are automatically exported from McAfee ePO after you register the McAfee MOVE AntiVirus service on McAfee ePO. This configuration is a one-time initial activity for a vCenter.

Note: You must repeat this configuration when a new datacenter is added.

Create an NSX security policy in the NSX Manager

Create an NSX security policy with McAfee MOVE AntiVirus (Agentless) enabled as a Guest Introspection Service.

Note: Ensure MOVE Antivirus extensions are installed and MOVE service is registered with the McAfee ePO Server.

Procedure:

1. Log on to vSphere web client as an administrator.

Image 5-23. Add Security Policies

- Specify a unique user-friendly name and any details to identify the security policy, then click Next to open the Guest Introspection Service page.
Click the green plus (+) sign to add a Guest Introspection Service. Provide a name for the Guest Introspection Service and define these settings and click OK:
### Table 11. New Policy Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Select Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type the name of the McAfee MOVE AntiVirus service.</td>
</tr>
<tr>
<td>Description</td>
<td>Anything, which helps you to identify the SVM.</td>
</tr>
<tr>
<td>Action</td>
<td>Apply</td>
</tr>
<tr>
<td>Service Type</td>
<td>AntiVirus</td>
</tr>
<tr>
<td>Service Name</td>
<td>McAfee MOVE AV</td>
</tr>
<tr>
<td>Service Profile</td>
<td>McAfee MOVE AV_[Policy Name]-XX (AntiVirus)</td>
</tr>
</tbody>
</table>

These are the profile configurations exported from McAfee ePO. If you create a policy or change an existing On Access Scan policy using McAfee ePO, it is immediately exported and available here to include for creating the security policy. But, any change to the name and description is not updated to NSX. You must manually update them if needed.

<table>
<thead>
<tr>
<th>State</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enforce</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Image 5-26. Configure and Enforce Policies

- Click **Finish** to complete and close the New Security Policy page, same can be viewed in the Security Policies tab.
5.3.1 Create a Global Security Group

Select the needed datacenters or their clusters from the available vCenter and configure them as a security group. This configuration allows you to assign the security policy to the group and protect its VMs.

Procedure:

3. Log on to vSphere web client as an administrator.
4. Go to Home | Networking & Security | Service Composer and click the Security Groups tab, then click the New Security Group icon
Image 5-29 Add Security Groups

- Specify a unique user-friendly name and any details to identify the Security Group, then click Next to open the Define dynamic membership page.
- Keep the default configuration for the dynamic membership criteria that objects must meet to be part of this security group, then click Next to open the Select objects to include page.
- From the Object Type drop-down list, select the required datacenter or cluster and select your objects to be protected, then click Next to open the Select objects to exclude page.

Image 5-30. Select objects to Include

- Select the objects to exclude, then click Next to open the Ready to complete page.
**Info:** If you include and exclude a cluster in the same **Security Group**, the exclusion takes priority. Objects that are excluded are not protected.

**Example:** If we want to exclude the VMs from the cluster, then those VMs are not protected.

- Review the **Settings**, then click **Finish** to create the security group, same can be viewed in the **Security Groups** tab.

**Image 5-31. Created Security Policies**

5.3.2 **Apply the NSX security policy to the NSX security group**

Apply the security policy to the security group of VMs that you want to protect.

Map a security policy (for example, **Mcafee-test**) to a security group (for example, **MOVEAVScan Policies**). The McAfee MOVE AntiVirus service and policy settings from McAfee ePO configured for **Mcafee-test** are applied to all virtual machines that are members of **MOVEAVScan Policies**.

**Procedure:**

1. Log on to vSphere web client as an administrator.
2. Navigate to **Home > Networking & Security > Service Composer**, click the **Security Groups** tab, select the **New security policy (Mcafee-test)** you have created, and then click the **Apply Security Policy** icon.

**Image 5-32. Apply Security Policy**
• In the **Apply Policy to Security Groups window**, select the **security group** (created SG) that contains the VMs that you want to protect, then click **OK**.

**Image 5-33. Select Security Group**

The selected NSX security policy is now applied to all VMs in the selected NSX security group. The VMs from the selected security group are now protected according to the **On Access Scan** policy that is exported from McAfee ePO.

**Image 5-34 View Applied Policy**
5.3.3 Enable NSX tagging through McAfee ePO

After installing the McAfee MOVE AntiVirus extension and registering the McAfee MOVE AntiVirus service in McAfee ePO, the tag applied in your environment appears with details about the virtual machines where the tag was applied. MCAFEE.MOVE.unprotected=yes is the McAfee MOVE AntiVirus (Agentless) tag.

Before you begin

- You have registered the McAfee MOVE AntiVirus service with McAfee ePO.
- You specified your vCenter details under SVM Configuration in the McAfee MOVE AntiVirus SVM Settings policy in McAfee ePO.

Registering the McAfee MOVE AntiVirus service exports all On Access Scan policies of McAfee MOVE AntiVirus from McAfee ePO to NSX. When a new scan policy is added or an existing scan policy is changed, all updates are immediately exported to NSX. These policies are included in the NSX security policy. Using the NSX tagging option, this policy can be automatically assigned to a VM that has been tagged as MCAFEE.MOVE.unprotected=yes or ANTI_VIRUS.VirusFound.threat=high.

Procedure:

1. Log on to McAfee ePO as an administrator.
2. Select Menu | Automation | MOVE AntiVirus Deployment.
3. On the Configuration tab, click Server Settings and select these tagging options under NSX tagging.
   - NSX Virus Found Tag — Enable this option so that the VM is tagged with ANTI_VIRUS.VirusFound.threat=high on detecting a malware.
   - Unprotected Tag — Enable this option to automatically retrieve the details of the unprotected VMs, tag them with MCAFEE.MOVE.unprotected=yes, and display them on the NSX Manager. This tag resource indicates that these VMs are not protected by McAfee MOVE AntiVirus. By default, this option is enabled. The MCAFEE.MOVE.unprotected=yes tag is automatically removed from the VMs when they are protected.
5.4 Configuring MOVE Policies

Manage the policies via the Policy Catalog in ePO.

- Log on to McAfee ePO as an administrator.
- Go to **Menu > Policy Catalog**, and select MOVE Antivirus 4.5.10 from the product drop down list.

Select My Default (on Access Scan) policy, click on Show Advanced option and Enable on-access option.
**Image 5-37. Scan Policy configuration**

**Honeywell**

**Image**

**5-37. Scan Policy configuration**

Honeywell SUIT 68

Revision 1.6

![Image of Honeywell SUIT 68 Revision 1.6](image)

- Select *File Types to Scan* "All files" and *Threat detection first response* as "deny access to files" and click *Save* as shown in the below screen shot.

**Image 5-38. File Types**

- The malware that is detected on any virtual machine is quarantined only when you have enabled the Quarantine configuration option under Scan Policy and the Quarantined files are stored on the specified network share. Select My Default (Options) policy, configure Quarantine network share, Network domain and username, Network password options in Quarantine manager (Agentless only) group and click save button.

**Note:** Make sure that you enter the server name in a manner that can be resolved by the SVM. How this is entered depends on the environment and how the SVM is configured.
**Image 5-39. Options policy**

- Select My Default (SVM settings) policy, configure the relevant details of your vCenter Server and credentials. Use the ‘Test connection settings’ to verify this setting and click on save to save the policy.

**Image 5-40. SVM Configuration**

- Once the policy settings are done, assign the policies under system tree.

**Note:** When you change policies in the ePolicy Orchestrator console, the changes take effect on the SVM at the next agent-server communication. To enforce policies immediately, send an agent wake-up call to the targeted SVM from the ePolicy Orchestrator console.

**Assign a policy**

You must assign a policy to the client systems for it to take effect.

- Log on to McAfee ePO as an administrator.
- In the System Tree, select the group containing the virtual machines where you want to apply the policy.
• Select the SVM machines, click on Action | Agent | Set Policy & Inheritance.

**Image 5-41. Set Policy & Inheritance**

- Select Policy, Break inheritance and click on Save as shown below.
To apply the policy immediately, send an agent wake-up call and click Ok in McAfee Agent page.

Image 5-43. Wake up agents
5.5 Keeping your protection up to date

McAfee MOVE AntiVirus depends on the engine and information in the content files to identify and act on threats. Every day, McAfee Labs releases new content files to address new threats.

To update systems managed by McAfee ePO, use the Master Repository. The Master Repository on the McAfee ePO server maintains the latest versions of the engine and content files.

For Agentless SVM, the AutoUpdate for DAT files is disabled. Use McAfee ePO to create a client task and update to the latest versions of the engine and DAT files.

Procedure:

- Download V2 Virus Definition Updates (DATs) to check-in to ePO.

  **Note:** Ensure V2 DAT file is downloaded as shown in the below screen shot

**Image 5-44. Virus Definitions**

**Download V2 Virus Definition Updates (DATs)**

<table>
<thead>
<tr>
<th>DAT File</th>
<th>Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>8596x.dat.exe</td>
<td>Windows-Intel</td>
</tr>
<tr>
<td><strong>DAT Package For Use with McAfee ePO</strong></td>
<td>-</td>
</tr>
</tbody>
</table>

- Go to **Menu | Master Repository**, then click on Check in Package and browse the downloaded V2 DAT file.

**Image 5-45. Check-in Package**

Software

Master Repository

Check In Package

What package are you checking in?

Note: If distributed repositories are set up to replicate only selected packages, your newly check-in package will be replicated by default. To avoid replicating a newly check-in package, select the checkbox for Product or Update (zip).

Package type

- Product or Update (.zip)
- Extra.DAT
- Super.DAT

File path

Browse...
• Click on **Next** and **Save** button to complete the Check-in Process.

**DAT ePO Update task**

**Procedure:**

Log on to the ePO server as an Administrator.

Click Menu| System Tree and select a group or systems (MOVE SVA) for which you want to create the Product Update task.

To create a client update task and access the Client Task Builder page, click Assigned Client Tasks, Actions, and select New Client Task Assignment.

• To select the product update task:
  - Under Task to schedule, select **McAfee Agent** as the Product.
  - Select the Task Type as **Product Update**.
  - Under Task Name click **Create New Task**.
  - Name the task, select the **Package selection** as all packages, then click **Save**.

**Image 5-46. Task Catalog**

<table>
<thead>
<tr>
<th>Client Task Catalog : New Task - McAfee Agent: Product Update</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Task Name</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>&quot;Update in Progress&quot; dialog box (Windows systems only):</td>
</tr>
<tr>
<td>Show &quot;Update in Progress&quot; dialog box on managed systems</td>
</tr>
<tr>
<td>Allow end users to postpone this update</td>
</tr>
<tr>
<td>Maximum number of postpones allowed: 1</td>
</tr>
<tr>
<td>Option to postpone expires after (seconds): 20</td>
</tr>
<tr>
<td>Display this text:</td>
</tr>
<tr>
<td><strong>Package selection:</strong></td>
</tr>
<tr>
<td>all packages</td>
</tr>
<tr>
<td>Selected packages</td>
</tr>
<tr>
<td><strong>Package types:</strong></td>
</tr>
<tr>
<td>Patches and service packs:</td>
</tr>
<tr>
<td>VirusScan Enterprise 8.5.0</td>
</tr>
<tr>
<td>ePO Agent Key Updater 5.3.1</td>
</tr>
<tr>
<td>MagBus Cert Updater 5.3.1</td>
</tr>
</tbody>
</table>
• Click Next to schedule the task immediately or as required, and then click Next to view the Summary of the product update task.
• Click Save.

Send an agent wake-up call, for the MOVE SVA machines.

**NOTE**

Use the Honeywell Qualified exclusions list, which is available at "Exclusion list for McAfee users" under section 6.1.1 in SUIT Anti Virus Guidelines for configuring the McAfee MOVE exclusions list.

Link:
6 Install/Upgrade VMware Tools on the Guest Virtual Machines
VMware Tools include the Thin Agent that must be installed on each guest virtual machine to be protected. Virtual machines with VMware Tools installed are automatically protected whenever they are started up on an ESXi host that has the security solution installed. That is, protected virtual machines retain the security protection through shut downs and restarts, and even after a vMotion move to another ESXi host with the security solution installed.

6.1 Install VMware Tools on the New Guest Virtual Machines
If you are installing VMware Tools onto a VM for the first time, then follow the instructions in this section. Otherwise, skip to section 7.2 to upgrade your existing VMware Tools install.

1. Go to the VM in the console right click and select Install/Upgrade VMware Tools

Image 6-1. Install VMware Tools

2. Click OK in the Install VMware Tools information screen.

Image 6-2. Install

3. Log in to VM Console and run the D: VMware Tools Installation.
Click **Next** and select **Custom** option.

### Image 6-4. Custom Type

5. **Click Next.**

6. Navigate to **VMCI Driver > NSX File Introspection Driver** and then right-click to select **Entire feature will be installed on local hard drive.**
Image 6-5. Select **NSX File Introspection Driver**.

![VMware Tools Setup](image)

NOTE: Ensure that the other components are not selected as per the following image. **Image 6-6**

![VMware Tools Setup](image)

7. Follow the on-screen instructions to complete the installation.
8. After successful installation, click **Yes**.
Image 6-7. Complete VMware tools

6.2 Upgrade VMware Tools on the Guest Virtual Machines

Note: If the VM already has VMware Tools installed you will need to ensure that it has the correct components installed to allow MOVE to work, by default these components are not installed, so follow these instructions to enable the additional features.

1. Go to the VM in the console right click and select Install/Upgrade VMware Tools
2. Select Interactive tools upgrade option and click

OK.

Image 6-8. Select Interactive Tools
3. Log in to VM Console and run the D: VMware Tools Installation

**Image 6-9**
- Hard Disk Drives (1)
  - Local Disk (C:)
    - 29.6 GB free of 69.8 GB

- Devices with Removable Storage (2)
  - Floppy Disk Drive (A:)
  - DVD Drive (D:) VMware Tools
    - 0 bytes free of 87.3 MB
    - CDFS

- Network Location (4)

4. Click Next and select Modify option
5. Install the Entire feature on local disk and click Next – Change

**Image 6-10.** Select entire drivers

**Image 6-11.** De-select NSX Network Introspection Driver
6. Select yes, once the setup is successful.

**Image 6-12**

You must restart your system for the configuration changes made to VMware Tools to take effect. Click Yes to restart now or No if you plan to manually restart later.

Note: Once VMware tools are installed in the VMs than thin agents should be enabled on the virtual machine.

- Login into the VSphere web client as an administrator
- Select Host, and navigate to **Monitor | Guest Introspection** Tab to see the Thin Agent enabled VM’s.

**Image 6-13. Thin Agent view**

Note: Network introspection captures networking events such as AD login/logout and all other normal networking traffic. This driver can be safely removed and does not affect AV if the AV is not configured to use network introspection. Follow the below link procedure to uninstall the NSX Network introspection driver.

Link:  [https://kb.vmware.com/s/article/2149764](https://kb.vmware.com/s/article/2149764)
6.3 Disabling Windows Defender

To disable Windows Defender using Registry on each VM that is protected by McAfee MOVE AV, perform the following steps:

1. Use the Windows key + R keyboard shortcut to open the Run command.
2. Type regedit, and click OK to open the Registry.
3. Browse the following path:

   HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender

   **Quick Tip:** You can now copy and paste the path in the new Registry's address bar to quickly jump to the key destination.

4. If you don’t see the DisableAntiSpyware DWORD, right-click the Windows Defender (folder) key, select New, and click on DWORD (32-bit) Value.
5. Name the key “DisableAntiSpyware” and press Enter.

6. Double-click the newly created DWORD and set the value from 0 to 1.
7. Click OK.

After completing the steps, restart your device to apply the settings.

**Result:** Windows Defender is now disabled.
7 Power on Sequence

Use the following VMware NSX sequence to power-on and communicate successfully. This would be useful, when user have restarted the host, NSX appliance or Service Definitions VM’s like McAfee MOVE AV and Guest Introspection.

1. NSX Virtual Appliance
2. Guest Introspection VM
3. McAfee MOVE VM
4. McAfee MOVE EPO
5. Power on VM’s
8 EICAR Test

To verify that the anti-virus protection is enabled on the MOVE-AV Agents.

Prerequisites

Turn-off Anti- Virus temporally because the EICAR test file gets deleted before moving it to thin client enabled virtual machines.

Use this procedure to test whether the MOVE-AV is installed correctly and can properly scan for malware:

1. Open the following web page http://www.eicar.org/anti_virus_test_file.htm
2. Open a text editor such as Notepad.
3. Copy the following string into the new file:
   X5O!P%@AP[4]
PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
4. Save the file as EICAR-AV-Test.txt
5. Move this file to the Thin Agent enabled virtual machines. Virus test file should just disappear.

After few minutes, you can see the detection of the virus in the EPO interface in the Threat Event Log.

Image 8-1 Threat Event Log
6. The detection of the virus as shown below and the action on the detected files will be as configured in the MOVE policies in section 7.4.

Image 8-2. Threat Report

<table>
<thead>
<tr>
<th>Event Received Time</th>
<th>Event ID</th>
<th>Event Description</th>
<th>Event Category</th>
<th>Threat Target IPv4 Address</th>
<th>Action Taken</th>
<th>Threat Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>6/4/19 8:36:38 AM PST</td>
<td>1234567890</td>
<td>Malware detected access denied</td>
<td>Malware</td>
<td>192.168.0.100</td>
<td>Access denied</td>
<td>Test</td>
</tr>
<tr>
<td>6/4/19 8:36:38 AM PST</td>
<td>2345678901</td>
<td>Malware detected access denied</td>
<td>Malware</td>
<td>192.168.0.101</td>
<td>Access denied</td>
<td>Test</td>
</tr>
<tr>
<td>6/4/19 8:36:38 AM PST</td>
<td>3456789012</td>
<td>Malware detected access denied</td>
<td>Malware</td>
<td>192.168.0.102</td>
<td>Access denied</td>
<td>Test</td>
</tr>
</tbody>
</table>

7. Same can be seen in the web client, the scan discovers infected virtual machines and tags them with the security tag ANTI_VIRUS.VirusFound.threat=high or MCAFEE.MOVE.unprotected=yes.

- Log in to VSphere web client as an administrator.
- Go to Home | Networking & Security | NSX Managers (IP) and click the Manage tab, then click the Security Tags tab

Image 8-3. Security tags
9  Uninstall McAfee MOVE Antivirus

1. Logon to vCenter Web client and then navigate to NSX Manager “Networking & Security” → “Installation and Upgrade” → Select McAfee MOVE AV under Service Deployment page and click DELETE.

   A confirmation dialog box appears.

   Image 9-1

2. Click DELETE.

   Image 9-2

   Wait for the uninstallation of the service to complete.

   Image 9-3

3. Repeat the deletion steps for the Guest Introspection service.
Choose the schedule of your choice and then click **DELETE**.

Wait for the uninstallation of the service to complete.

Select MOVE Policy created under **Security Policies** in **Service Composer**.

Click **DELETE**.
Note: Delete all security policies created for McAfee MOVE.

7. Repeat the deletion steps for **Security Groups** under **Service Composer**.

8. Click **DELETE** to delete the Security Group for McAfee MOVE.
9.1 McAfee MOVE – Un-install Extensions

1. Log on to the McAfee MOVE EPO as an administrator privileges
2. Select Menu → Software → Extensions
3. Under McAfee Group, select Data Center Security and click Remove for the following extensions.
   a. MOVE AntiVirus
   b. MOVE AntiVirus Common
   c. vSphere Connector
   d. MDCC
4. Select Help Content under McAfee Group and click Remove for mvav_help extension.

9.2 Uninstall VMware NSX extensions from the vSphere Web Client

A complete uninstall of NSX removes host VIBs, the NSX Manager, controllers, all VXLAN configuration, logical switches, logical routers, NSX firewall, and the vCenter NSX plug in. Make sure to follow the steps for all hosts in the cluster. VMware recommends that you uninstall the network virtualization components from a cluster before removing the NSX plug-in from vCenter Server.

Removing of VMware NSX completely requires 2 host reboots as follows:
   a. First reboot is after successful removing of VMware NSX VIB’s.
   b. Second reboot is after successful removing the host VTEPs and vcPortgroups used for VTEPs (if the user is not using these NSX components, ignore the second reboot).

Note:
   a. VMware recommends that you uninstall the network virtualization components from a cluster before removing the NSX plug-in from vCenter Server.
   b. Do not remove NSX appliances from vCenter directly. Always manage and remove NSX appliances using the Networking and Security tab of the vSphere Web Client.

Pre-requisites:
   a. Logon to the vSphere Web client using an Administrator privileges.
   b. Make sure McAfee MOVE services is un-registered and successfully removed.

9.2.1 Remove NSX from vSphere Web Client

1. In the vCenter Web Client, go to Administration → vCenter Server Extensions → vSphere ESX Agent Manager. On the Configure tab, right-click the NSX agency and click Delete Agency.

   ![Image 9-11]

2. Reboot the hosts manually.
3. Delete the NSX Manager appliance VMs from the disk.
4. For the vCenter on which you want to remove the NSX Manager plug-in, log in to the managed object browser at https://your_vc_server/mb.
5. Click **Content**.
   Image 9-12

6. Click **ExtensionManager**.
   Image 9-12

7. Click **UnregisterExtension**.
8. Enter the string “com.vmware.vShieldManager” and click **Invoke Method**.

9. Enter the string “com.vmware.nsx.ui.h5” and click **Invoke Method**.
10. If you are running the vSphere 6 vCenter Appliance, launch the console and enable the BASH shell under Troubleshooting Mode Options.

11. Delete the vSphere Web Client directories for NSX and then restart the Web Client service.

**vCenter Server 5.x:**
- Windows 2008/2012 Path: “%ALLUSERSPROFILE%VMware\vSphere Web Client\vc-packages\vsphere-client-serenity\”
- VMware vCenter Server Appliance – “/var/lib/vmware/vsphere-client/vc-packages/vsphere-client-serenity/”

**vCenter Server 6.0.x:**
- Windows 2008/2012 Path – “C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity\”
- VMware vCenter Server Appliance – “/etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity/”

**Restarting the services:**
- a. For vCenter Server Appliance, run the service “vsphere-client restart” command in the appliance shell.
- b. For Windows-based vCenter, run services.msc, right-click vSphere Web Client, and click Start.
9.2.2 Verify that MOVE has been successfully uninstalled

After successful un-installation, verify the following conditions are removed from the following locations.

1. McAfee MOVE AV and Guest Introspection VM’s should be removed successfully in Service Definitions.
2. Security Groups and Security policies should be successfully removed from the Service Composers.
3. Verify that the VMware vCenter Server Appliance is removed from the NSX cluster.
4. Verify that the MOVE plugin is not listed under Automation in McAfee EPO.

Image 9-17

5. Logon to vSphere web client and verify that the Networking & Security icon no longer appears on the Home screen in the vCenter Web Client.

9.3 Remove an individual host from NSX Prepared Cluster

Perform the following procedure to remove a host from the NSX Prepared Cluster.

1. Power off all the VMs and place the ESXi host in the Maintenance mode before proceeding to remove the NSX.
2. Place the individual ESXi host, outside the NSX prepared cluster. NSX uninstalls the network virtualization components and service virtual machines from the host.
3. Reboot the ESXi host, after successfully moved out of the NSX prepared cluster.
4. Verify NSX VIBs to the host are successfully removed, by SSH into the ESXi host.
   a. Use command “esxcli software vib list | grep esx” and verify it does not contain the strings with “esx-vsip” and “esx-vxlan”.
   b. If the VIBs remain on the host, you might want to view the logs to determine why automated VIB removal did not work or user can remove the VIB manually by using the following commands.
      i. esxcli software vib remove --vibname=esx-vxlan
      ii. esxcli software vib remove --vibname=esx-vsip
10 Known issues & References

10.1 Known issues

1) VMware NSX-based deployment of MOVE Agentless Security Virtual Machines fails on vSphere 6.0. Refer KB85930 article for more information and workaround.
   https://kc.mcafee.com/corporate/index?page=content&id=KB85930

2) Virtual machines are stuck at 0% or 35% when powering on.
   Refer KB 2150904 article for more information and workaround
   https://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&docType=kc&externalId=2150904&slicId=1&docTypeID=DT_KB_1_1&dialogID=456900774&stateId=1%200%204569%16319

3) When McAfee MOVE is powered off, it takes multiple attempts to login to vCenter server via vSphere Client.

4) Error: The vSphere client could not connect to vCenter Server. The server vCenter Server took too long to respond. (The command has timed out as the remote server is taking too long to respond)

Document References McAfee
McAfee Move 4.8.0 Installation Guide:

McAfee MOVE 4.8.0 Product Guide:

VMware

https://docs.vmware.com/en/VMware-vSphere/index.html


10.2 References

Reference Links:
