July 2014

Tips and Tricks on Building Agentless Antivirus Scanners for VMware View Virtual Desktops

Yury Magalif, vExpert 2014, VCP

Principal Architect – Cloud Computing

okzebra@gmail.com

yury.magalif@cdillc.com

CDI COMPUTER DESIGN & INTEGRATION LLC

Agenda

I. Design Decisions – Current AV or Agentless
II. How to Configure the Parent VM
III. vShield Manager
IV. Trend Micro Deep Security Manager
V. Trend Micro - Deploy Filter Driver and Appliance
VI. Trend Micro – Protect VMs
VII. Build McAfee MOVE
VIII. Trend Deep Security Tips
IX. McAfee MOVE Agentless Tips

I. Design Decisions – Current AV or Agentless

- Goal: Minimize I/O

Design – current AV or Agentless?

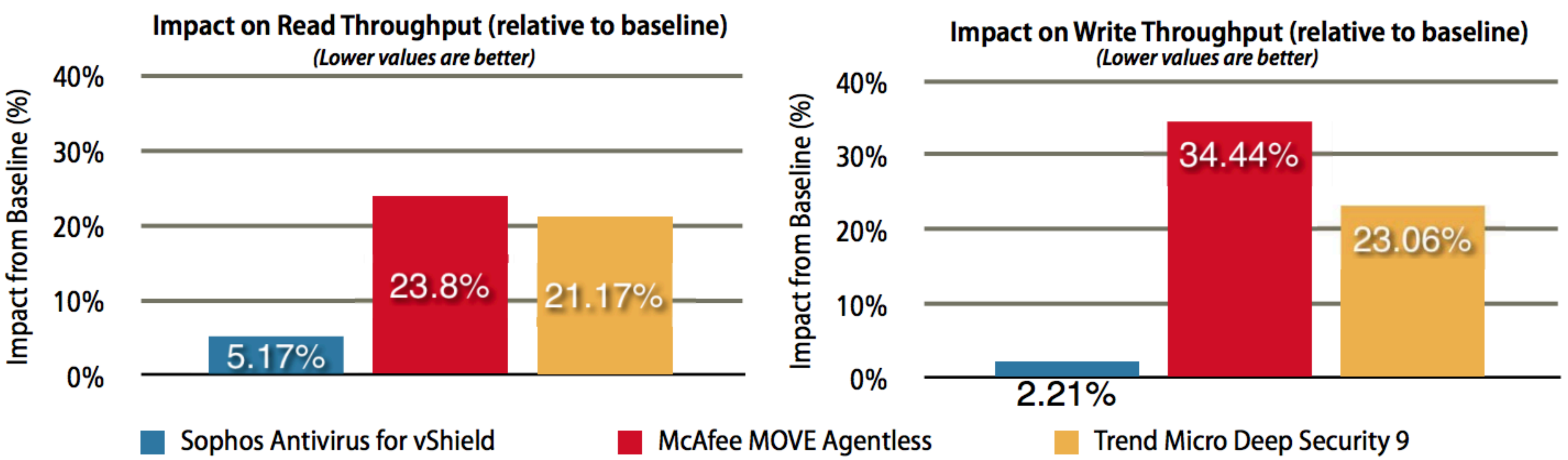
- ProjectVRC.com Whitepaper
- MCAFEE VIRUSSCAN ENTERPRISE 8.8.0
  - Scan within the VM.
  - I/O overhead at 50%
- MCAFEE MOVE MULTIPLATFORM 2.0
  - Offloading AV scanning to a separate VM.
  - I/O overhead at 16%

Design – current AV or Agentless? Continued.

- MCAFEE MOVE AGENTLESS 2.5
- Scanning offloaded to VM, very light VMware agent inside
- IO overhead at most 10%. -- all write, no read at all.

- **Conclusion:** Using Agentless makes sense.

Sophos wins in 1 report, but Sophos ordered report



VMware ESXi 5.5 vShield-Enabled Server Workload Performance

Windows Server 2008 R2 CIFS File Server Performance

as reported by Load DynamiX Test Development Environment 3.2

Note: A nested 72.4GB file set was used for read transactions. Client load emulated by Load DynamiX TDE 3.2, requesting approximately 9:1 read/write transactions. Tests run for a period of 1 hour. Lower impact from baseline is better. Baseline read throughput 43.77MB/s, write throughput, 4.9MB/s.

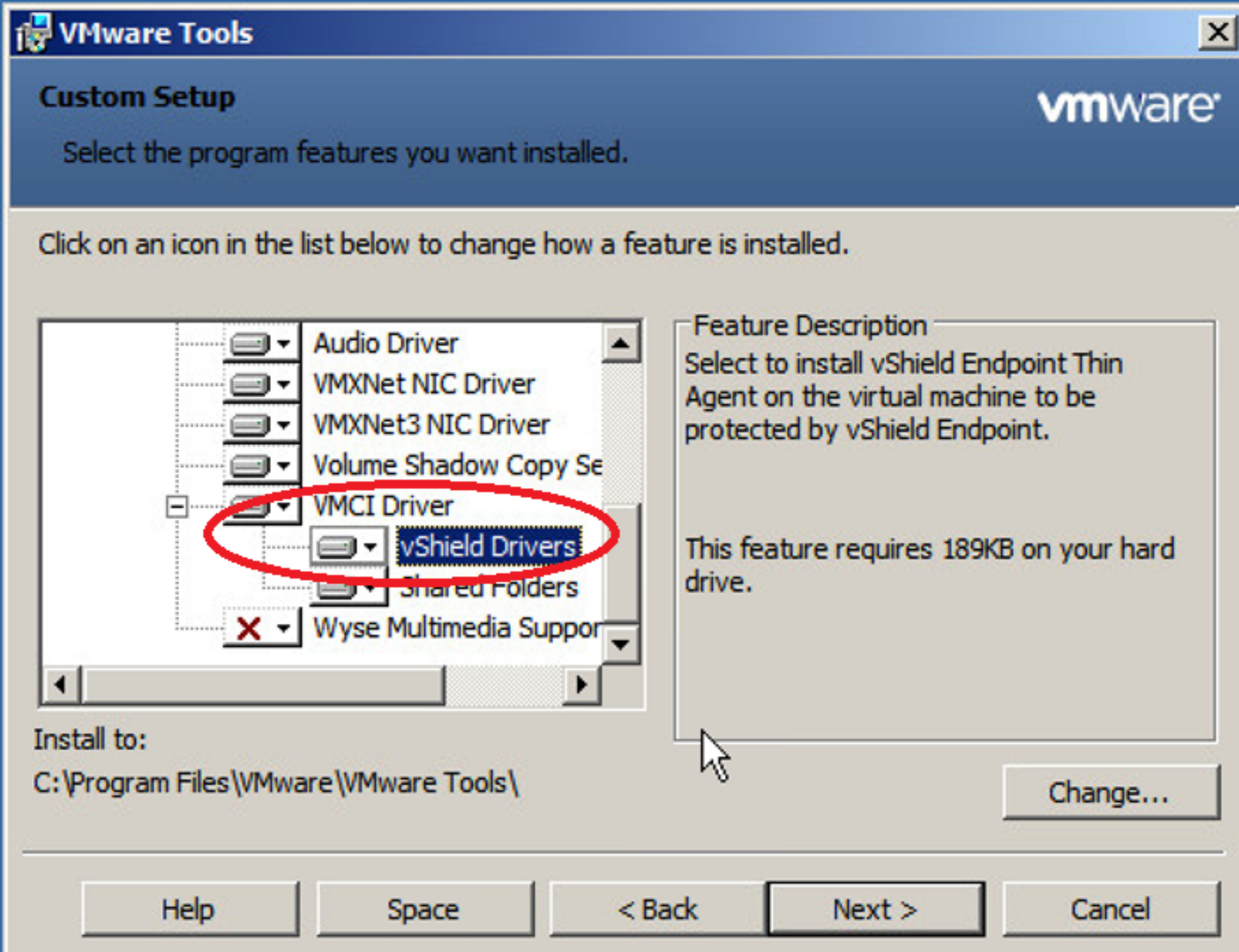
Source: Tolly, February 2014

Figure 1

II. Trend – How to Configure the Parent VM

- »Goal: Make it easier

VMCI – what VM uses to talk outside the bubble



VMware Tools

Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

- Audio Driver
- VMXNet NIC Driver
- VMXNet3 NIC Driver
- Volume Shadow Copy Se
- VMCI Driver
  - vShield Drivers
  - Shared Folders
- ☒ Wyse Multimedia Suppor

Feature Description

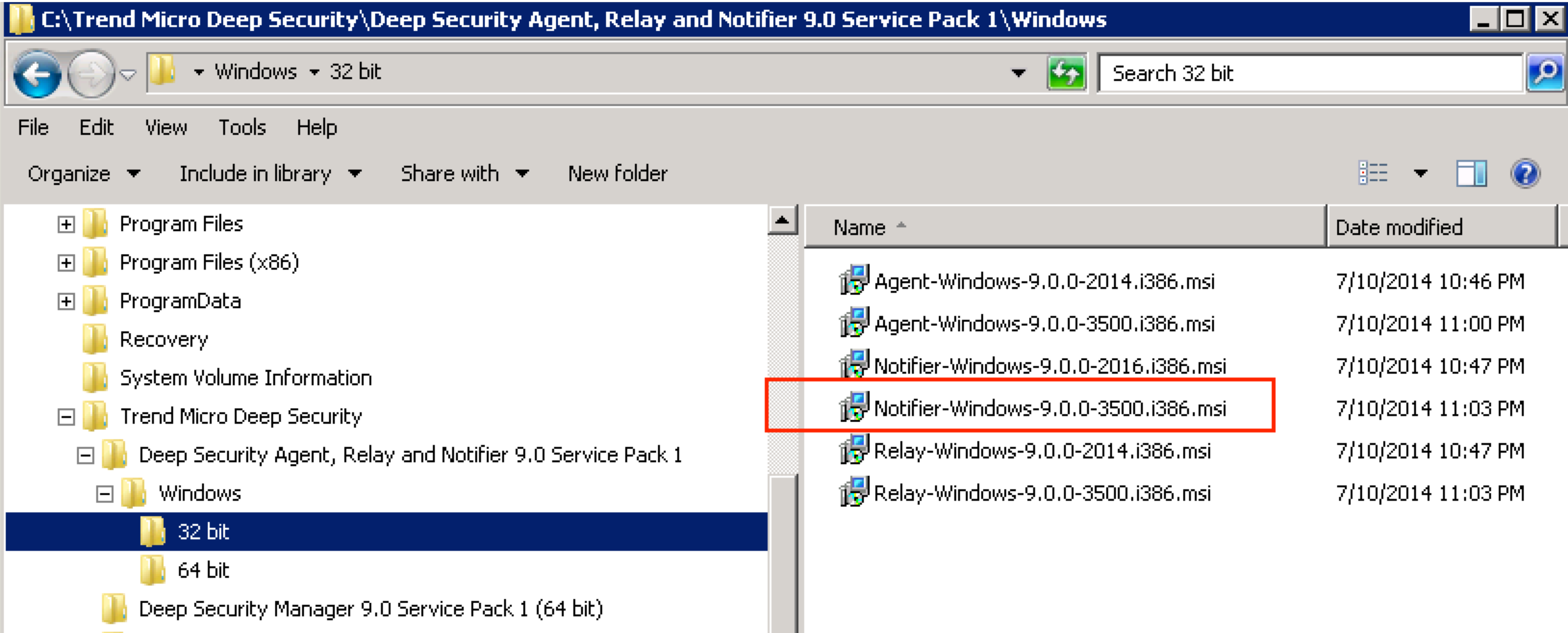
Select to install vShield Endpoint Thin Agent on the virtual machine to be protected by vShield Endpoint.

This feature requires 189KB on your hard drive.

Install to:

C:\Program Files\VMware\VMware Tools\

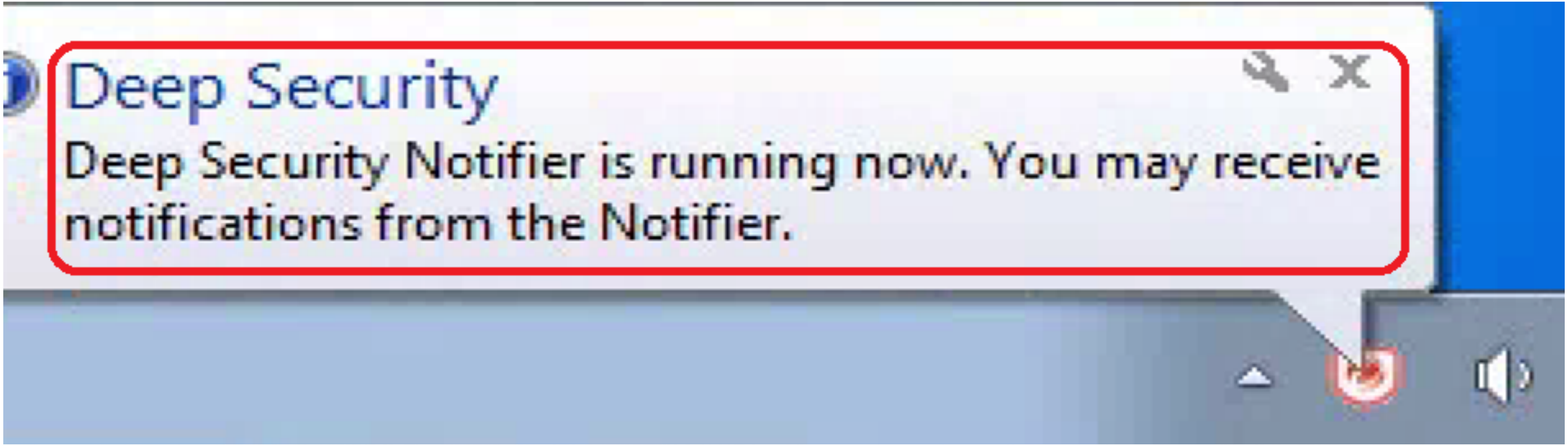
Download Notifier installation file from the Trend Website and run install. Choose all defaults.



C:\Trend Micro Deep Security\Deep Security Agent, Relay and Notifier 9.0 Service Pack 1\Windows

Name	Date modified
Agent-Windows-9.0.0-2014.i386.msi	7/10/2014 10:46 PM
Agent-Windows-9.0.0-3500.i386.msi	7/10/2014 11:00 PM
Notifier-Windows-9.0.0-2016.i386.msi	7/10/2014 10:47 PM
Notifier-Windows-9.0.0-3500.i386.msi	7/10/2014 11:03 PM
Relay-Windows-9.0.0-2014.i386.msi	7/10/2014 10:47 PM
Relay-Windows-9.0.0-3500.i386.msi	7/10/2014 11:03 PM

Once installed, the Notifier displays a bubble upon first login. Some admins don't like any popups in their Parent VM. You can opt not to install Notifier then.

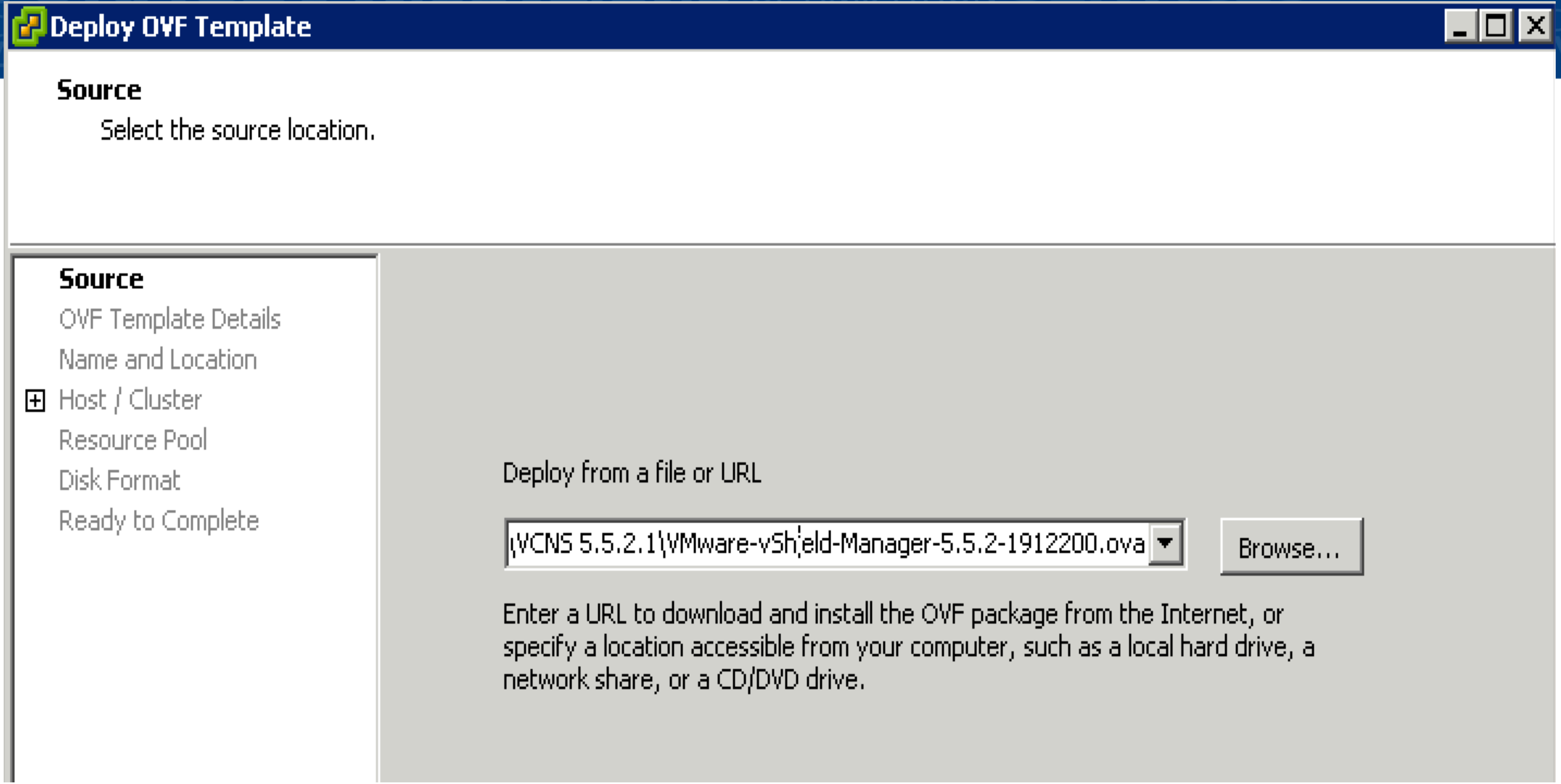


Deep Security

Deep Security Notifier is running now. You may receive notifications from the Notifier.

III. vShield Manager

- Goal: Follow the Antivirus Manufacturer manual



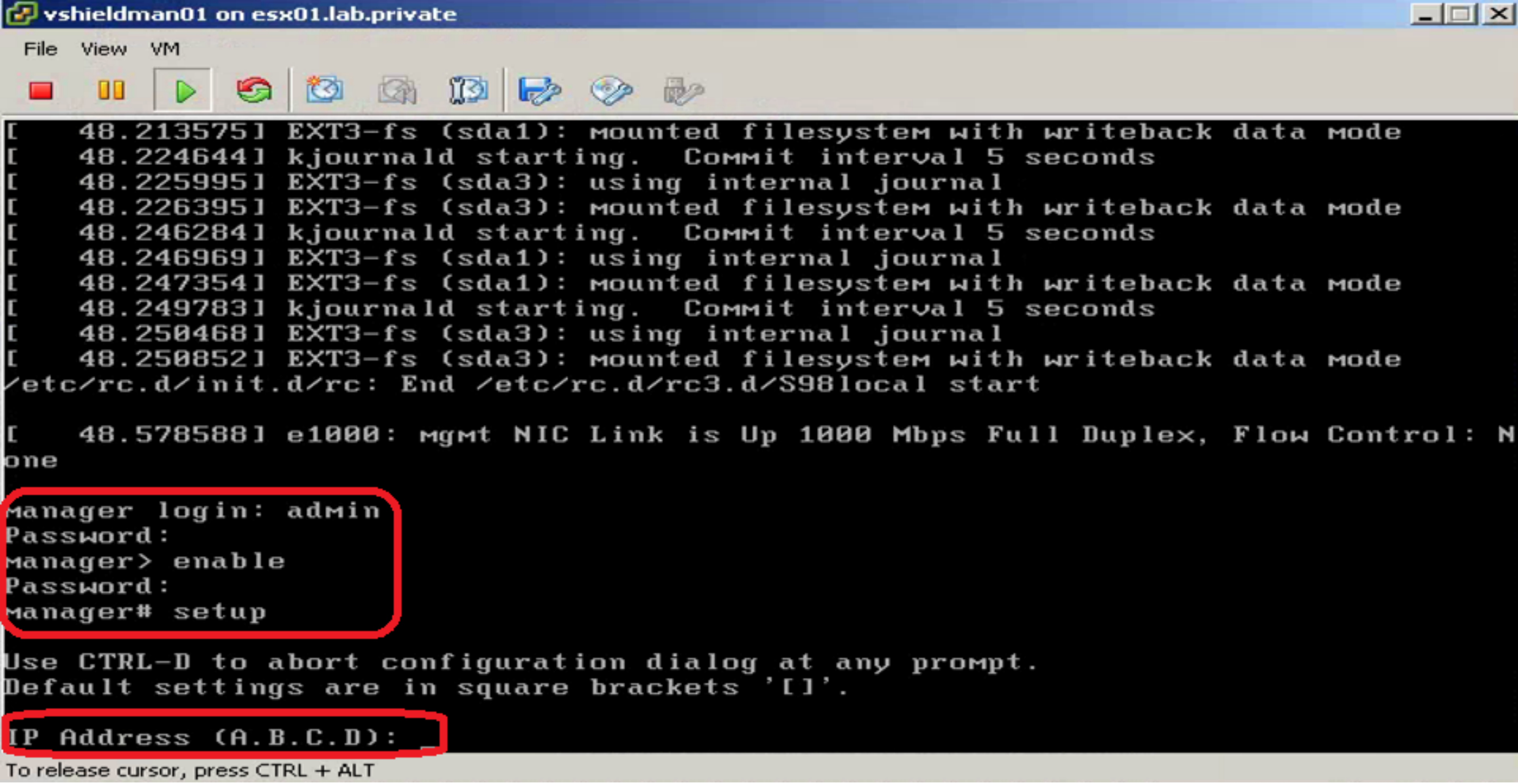
Source

Select the source location.

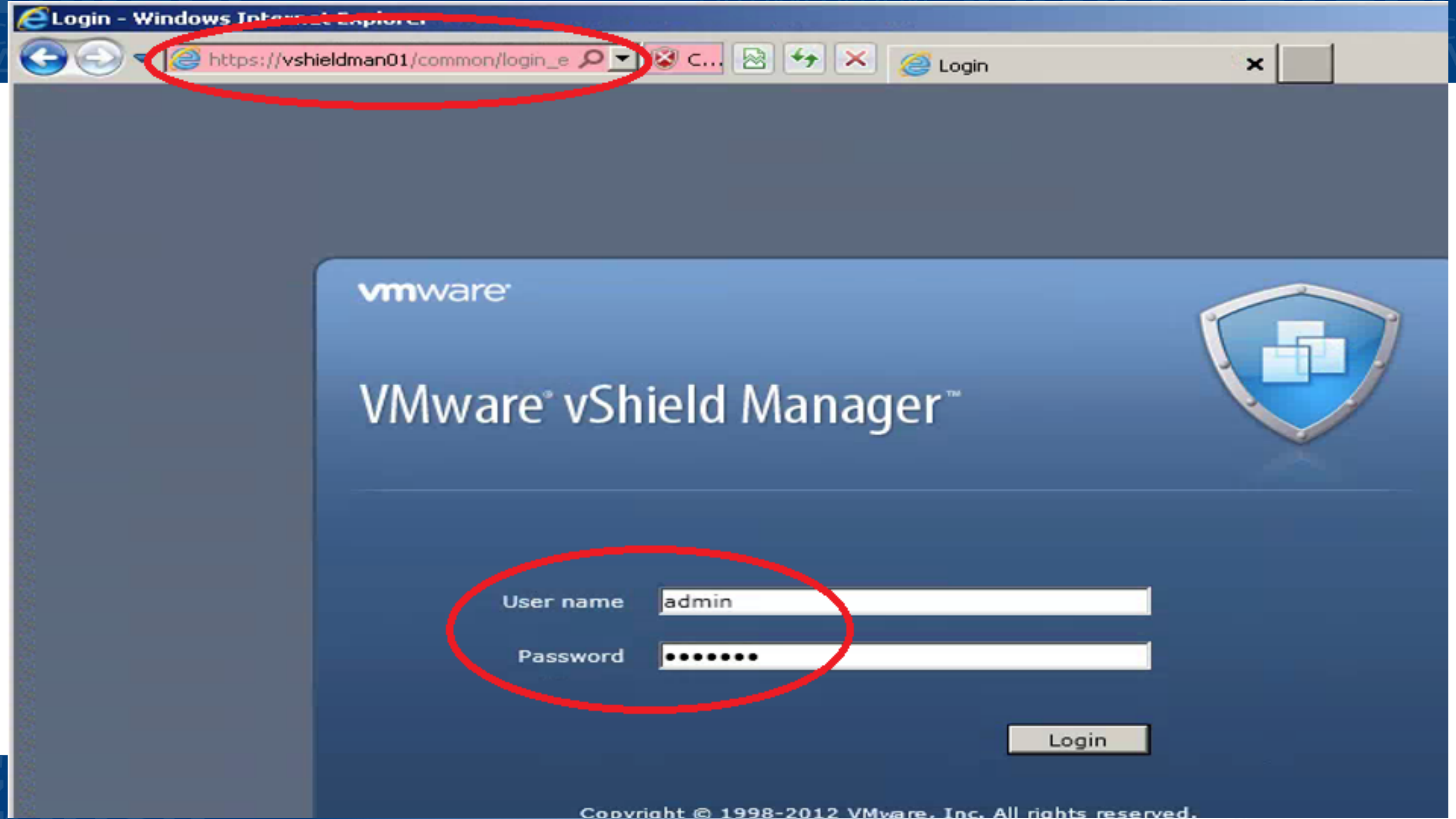
Deploy from a file or URL

\VCNS 5.5.2.1\VMware-vShield-Manager-5.5.2-1912200.ova

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.


vshieldman01 on esx01.lab.private
File
View
VM
To release cursor, press CTRL + ALT

```
[    48.213575] EXT3-fs (sda1): mounted filesystem with writeback data mode
[    48.224644] kjournald starting.  Commit interval 5 seconds
[    48.225995] EXT3-fs (sda3): using internal journal
[    48.226395] EXT3-fs (sda3): mounted filesystem with writeback data mode
[    48.246284] kjournald starting.  Commit interval 5 seconds
[    48.246969] EXT3-fs (sda1): using internal journal
[    48.247354] EXT3-fs (sda1): mounted filesystem with writeback data mode
[    48.249783] kjournald starting.  Commit interval 5 seconds
[    48.250468] EXT3-fs (sda3): using internal journal
[    48.250852] EXT3-fs (sda3): mounted filesystem with writeback data mode
/etc/rc.d/init.d/rc: End /etc/rc.d/rc3.d/S98local start

[    48.578588] e1000: mgmt NIC Link is Up 1000 Mbps Full Duplex, Flow Control: N
one

manager login: admin
Password:
manager> enable
Password:
manager# setup

Use CTRL-D to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

IP Address (A.B.C.D):
```



Login - Windows Internet Explorer

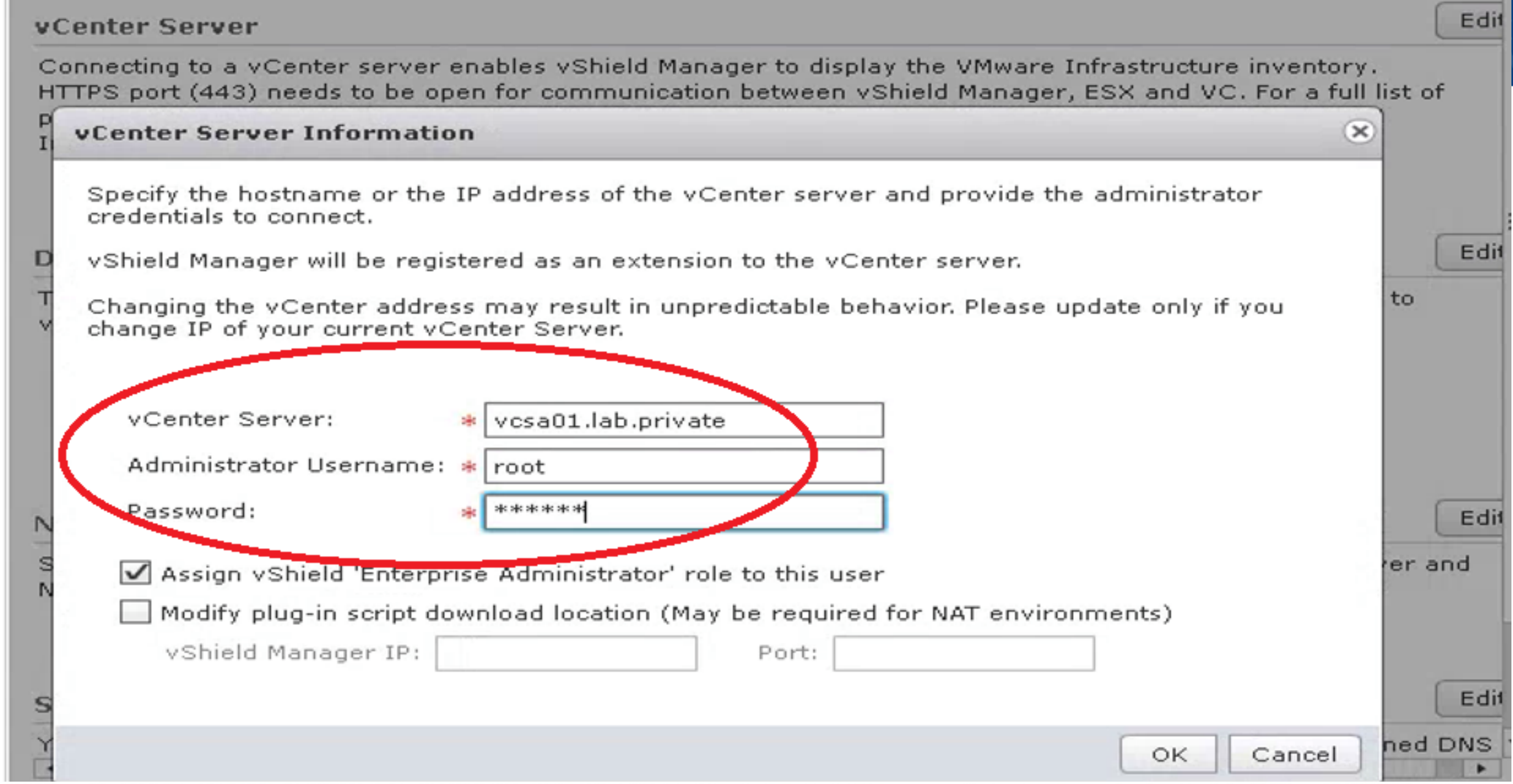
https://vshieldman01/common/login_e

VMware® vShield Manager™

User name: admin

Password: ••••••••

Copyright © 1998-2012 VMware, Inc. All rights reserved.



vCenter Server

Connecting to a vCenter server enables vShield Manager to display the VMware Infrastructure inventory. HTTPS port (443) needs to be open for communication between vShield Manager, ESX and VC. For a full list of

vCenter Server Information

Specify the hostname or the IP address of the vCenter server and provide the administrator credentials to connect.

vShield Manager will be registered as an extension to the vCenter server.

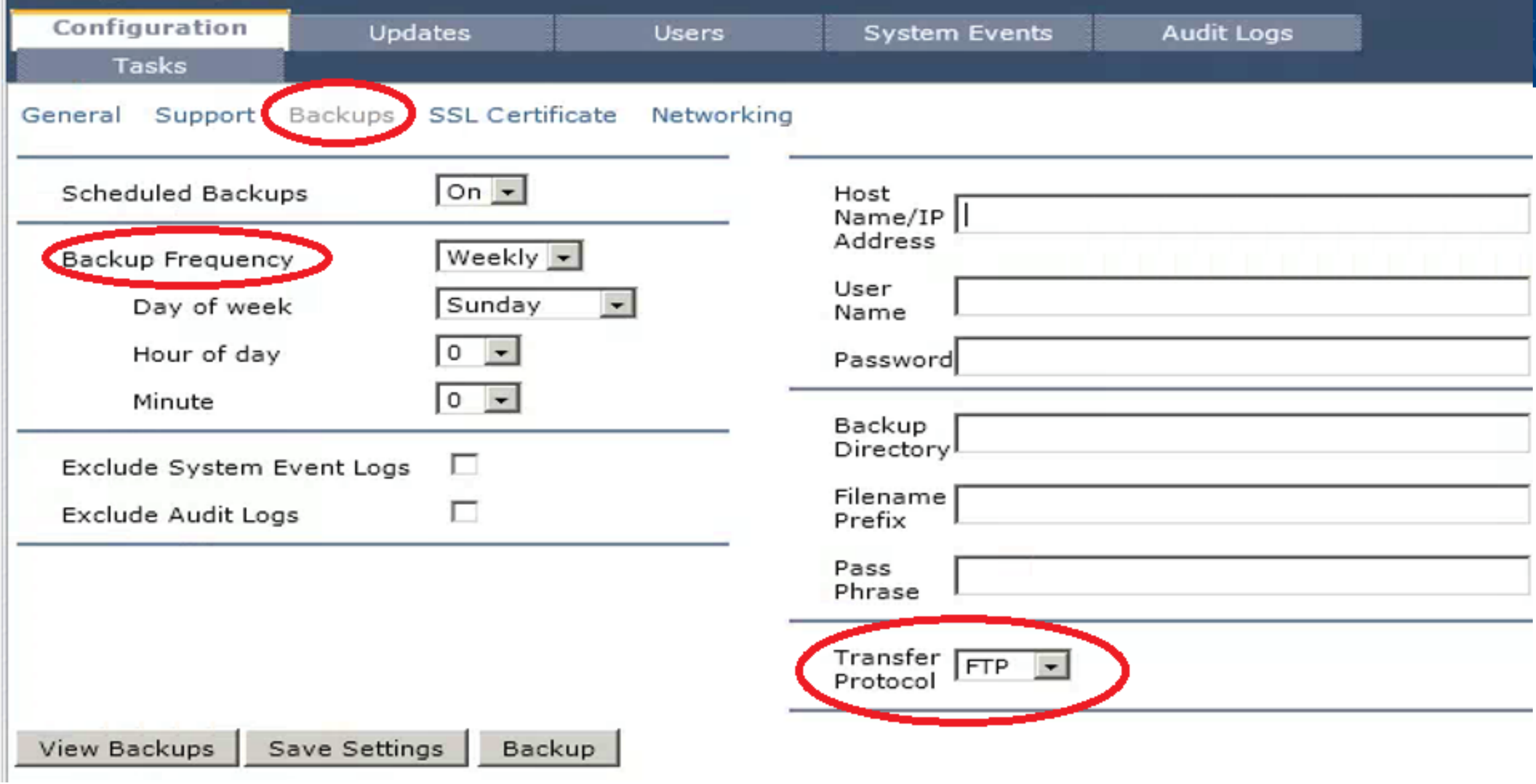
Changing the vCenter address may result in unpredictable behavior. Please update only if you change IP of your current vCenter Server.

vCenter Server: *	vcsa01.lab.private
Administrator Username: *	root
Password: *	******

☑ Assign vShield 'Enterprise Administrator' role to this user

□ Modify plug-in script download location (May be required for NAT environments)

vShield Manager IP: Port:



Scheduled Backups: On

Backup Frequency: Weekly

Day of week: Sunday

Hour of day: 0

Minute: 0

Exclude System Event Logs ☐

Exclude Audit Logs ☐

Host Name/IP Address:

User Name:

Password:

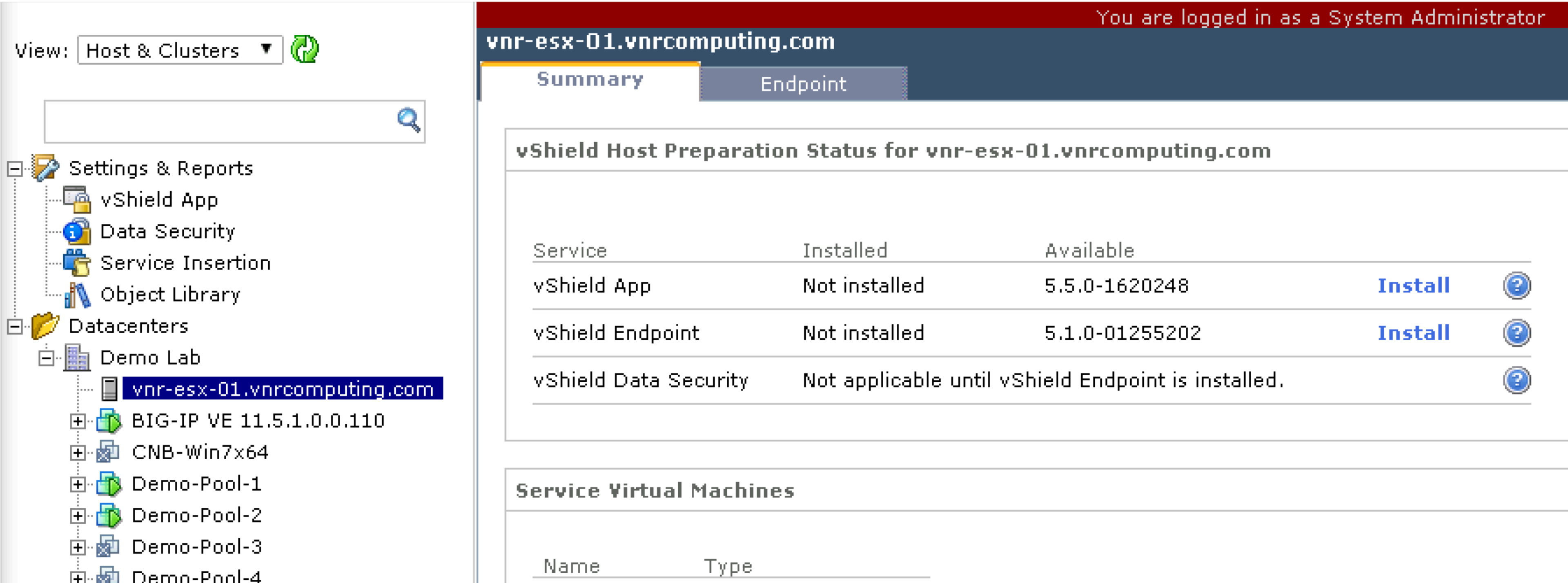
Backup Directory:

Filename Prefix:

Pass Phrase:

Transfer Protocol: FTP

Select host, then look for vShield tab to the right. Click the Install button next to vShield Endpoint.



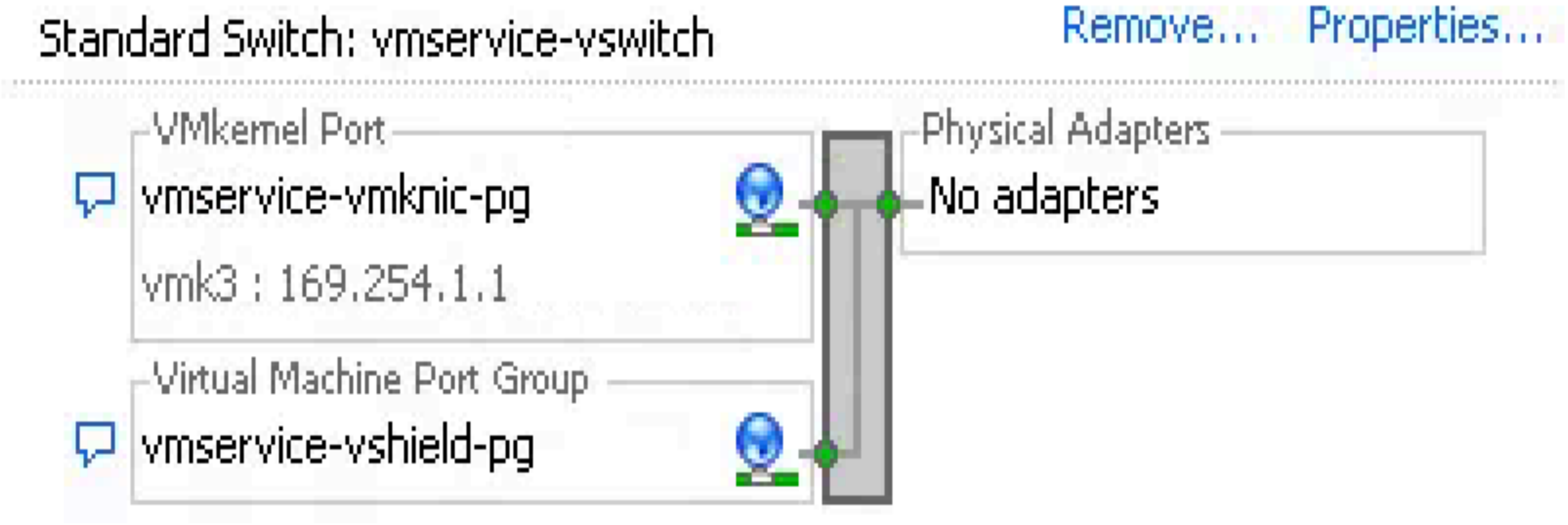
vnr-esx-01.vnrcomputing.com

vShield Host Preparation Status for vnr-esx-01.vnrcomputing.com

Service	Installed	Available		
vShield App	Not installed	5.5.0-1620248	**Install**	?
vShield Endpoint	Not installed	5.1.0-01255202	**Install**	?
vShield Data Security	Not applicable until vShield Endpoint is installed.			?

Service Virtual Machines

Name	Type



Standard Switch: vmservice-vswitch

VMkernel Port

vmservice-vmknic-pg

vmk3 : 169.254.1.1

Virtual Machine Port Group

vmservice-vshield-pg

Physical Adapters

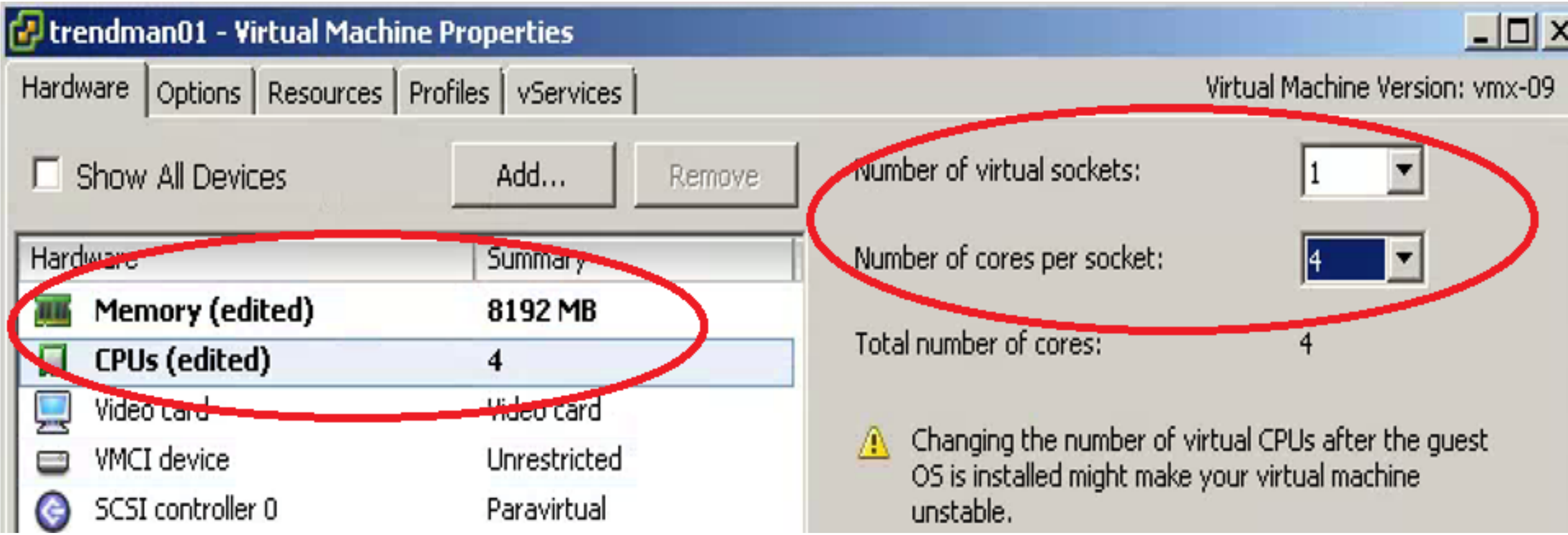
No adapters

On the Networking configuration tab for the host, look for a new Standard Switch. Do NOT delete it.

IV. Trend Micro Deep Security Manager

- »Goal: Install management

Create a VM for Trend Micro Deep Security Manager with 8GB of RAM, 1 socket and 4 cores.



trendman01 - Virtual Machine Properties

Virtual Machine Version: vmx-09

□ Show All Devices

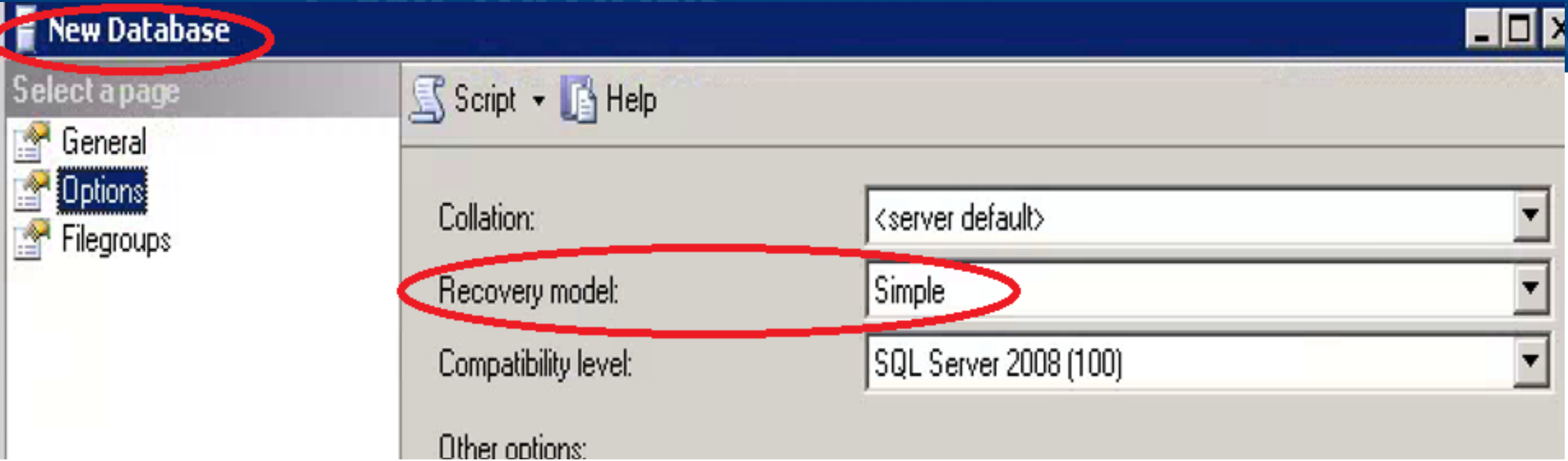
Hardware	Summary
Memory (edited)	8192 MB
CPUs (edited)	4
Video card	Video card
VMCI device	Unrestricted
SCSI controller 0	Paravirtual

Number of virtual sockets: 1

Number of cores per socket: 4

Total number of cores: 4

⚠ Changing the number of virtual CPUs after the guest OS is installed might make your virtual machine unstable.



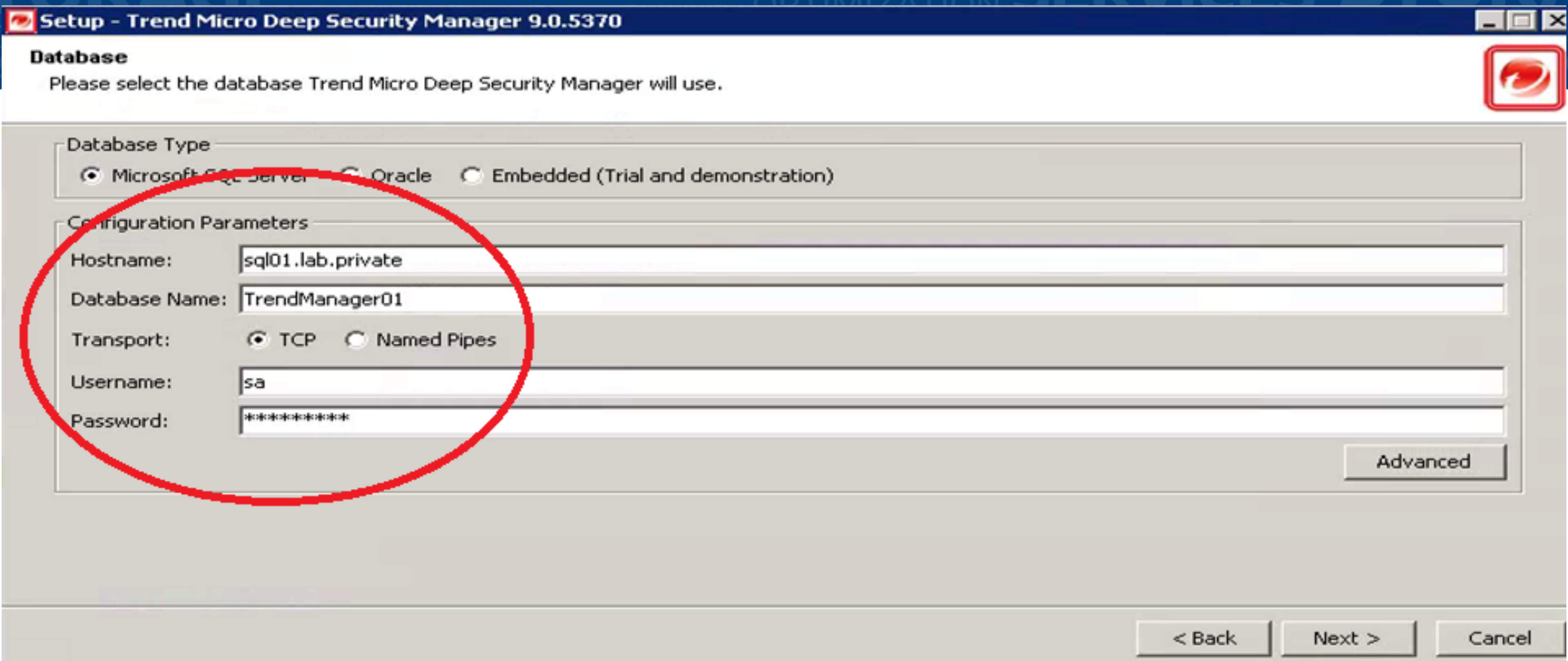
Collation: <server default>

Recovery model: Simple

Compatibility level: SQL Server 2008 (100)

Other options:

In SQL Server Management Studio, create a new database, and make sure to specify Recovery model as Simple – no need for up to date logs here.



Setup - Trend Micro Deep Security Manager 9.0.5370

Database

Please select the database Trend Micro Deep Security Manager will use.

Database Type

● Microsoft SQL Server ○ Oracle ○ Embedded (Trial and demonstration)

Configuration Parameters

Hostname: sql01.lab.private

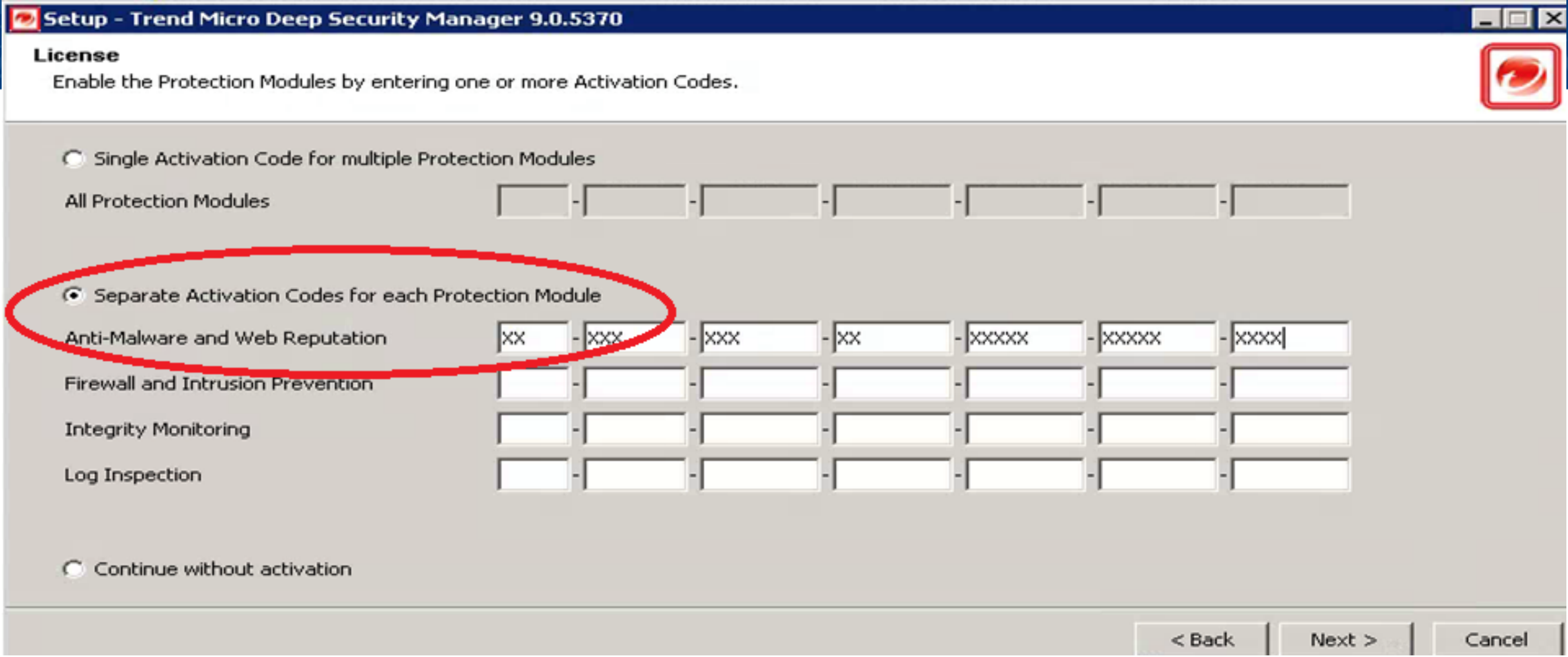
Database Name: TrendManager01

Transport: ● TCP ○ Named Pipes

Username: sa

Password: **********

Specify SQL database name. Use SA account or the one given by your SQL Admins.



Setup - Trend Micro Deep Security Manager 9.0.5370

License

Enable the Protection Modules by entering one or more Activation Codes.

○ Single Activation Code for multiple Protection Modules

All Protection Modules ____-____-____-____-____-____-____

● Separate Activation Codes for each Protection Module

Anti-Malware and Web Reputation XX-XXX-XXX-XX-XXXXX-XXXXX-XXXX

Firewall and Intrusion Prevention ____-____-____-____-____-____-____

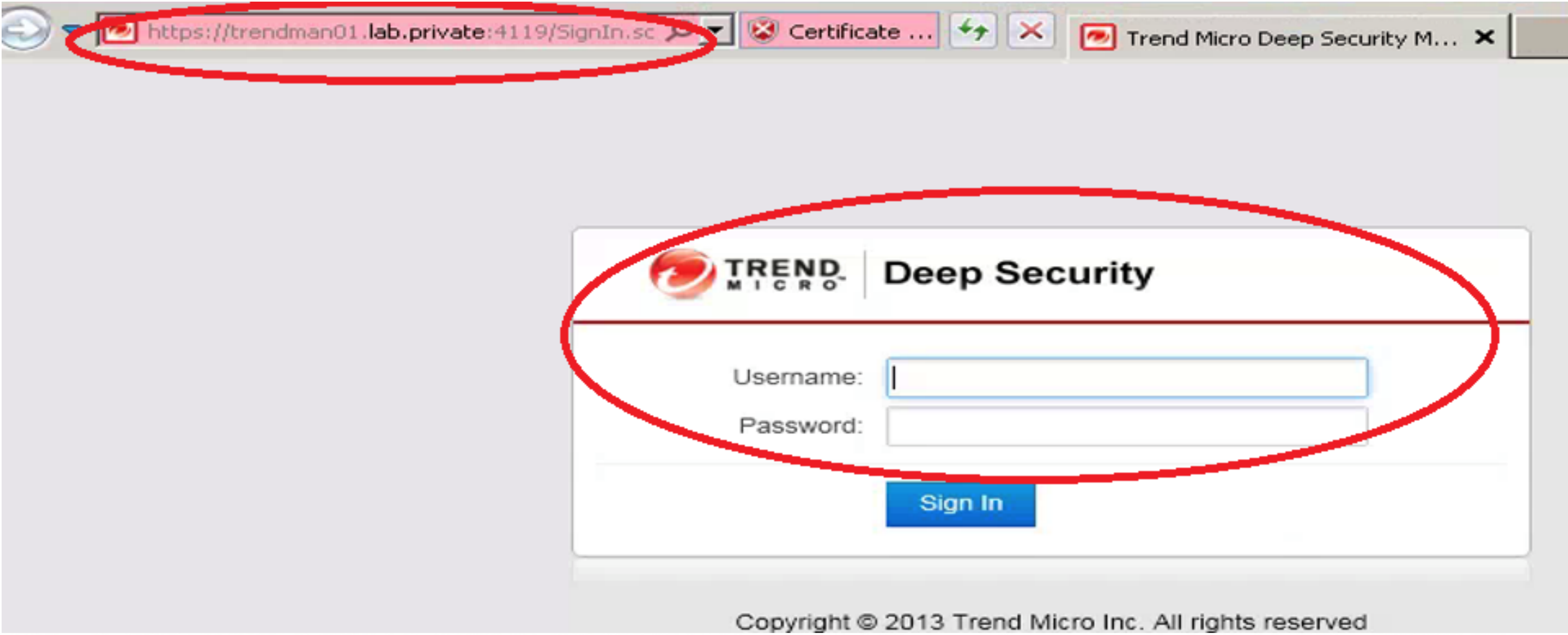
Integrity Monitoring ____-____-____-____-____-____-____

Log Inspection ____-____-____-____-____-____-____

○ Continue without activation

For Antivirus, you only need to enter “Anti-Malware and Web Reputation” Activation Codes. No need to buy others.

Go to URL of the https://TrendManagerFQDN:4119 to manage

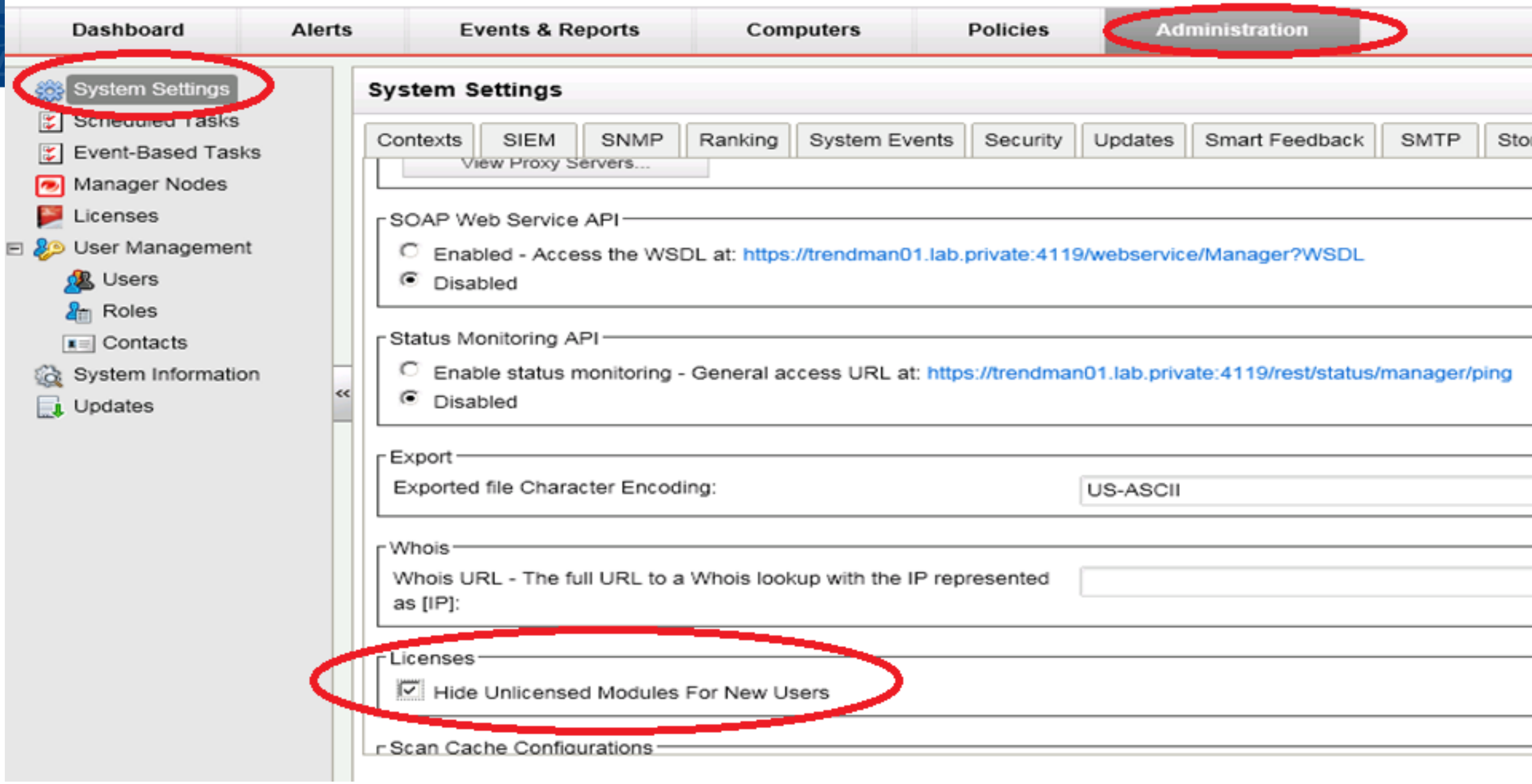


https://trendman01.lab.private:4119/SignIn.sc

Username:

Password:

Copyright © 2013 Trend Micro Inc. All rights reserved



System Settings

SOAP Web Service API

○ Enabled - Access the WSDL at: https://trendman01.lab.private:4119/webservice/Manager?WSDL

● Disabled

Status Monitoring API

○ Enable status monitoring - General access URL at: https://trendman01.lab.private:4119/rest/status/manager/ping

● Disabled

Export

Exported file Character Encoding: US-ASCII

Whois

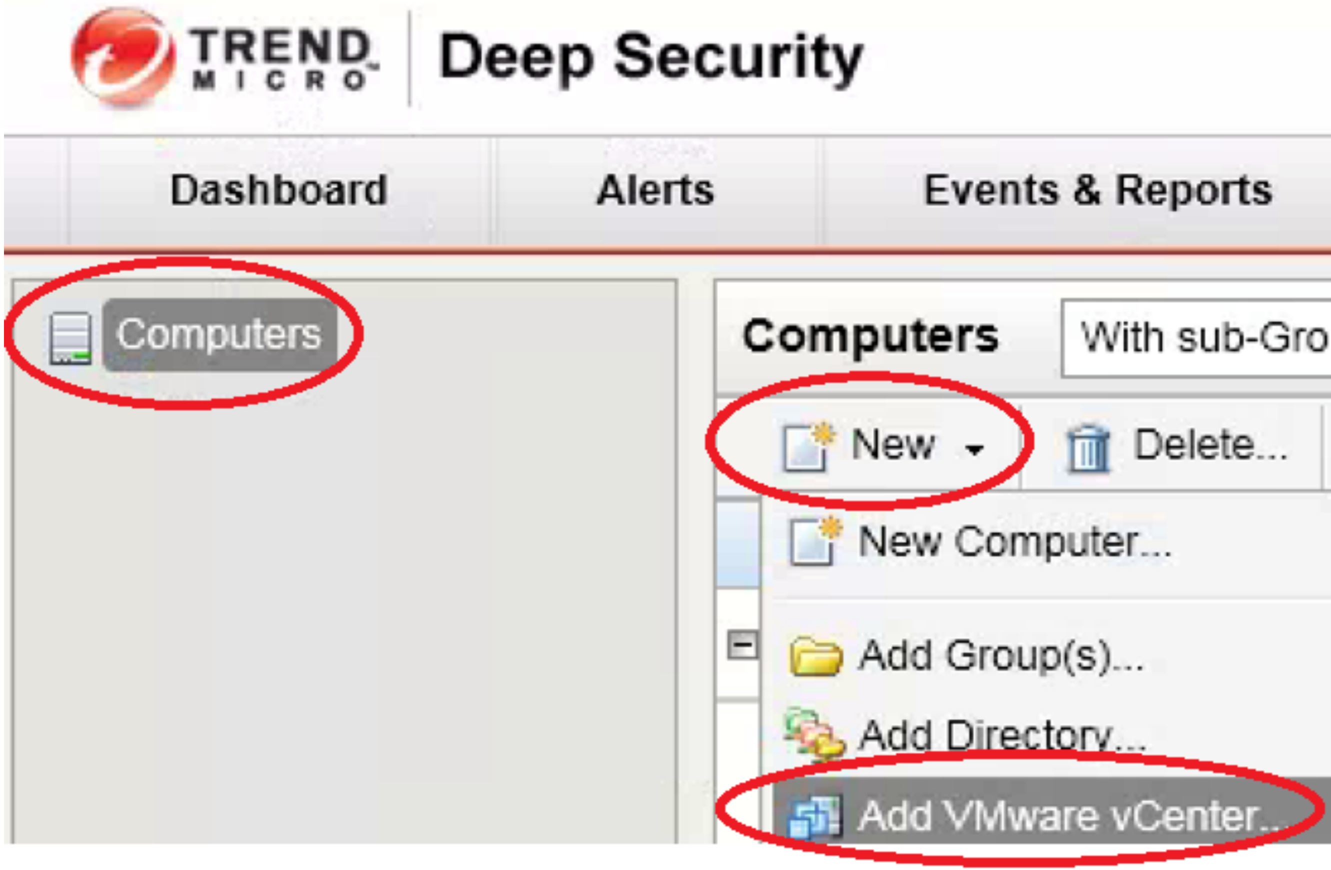
Whois URL - The full URL to a Whois lookup with the IP represented as [IP]:

Licenses

☑ Hide Unlicensed Modules For New Users

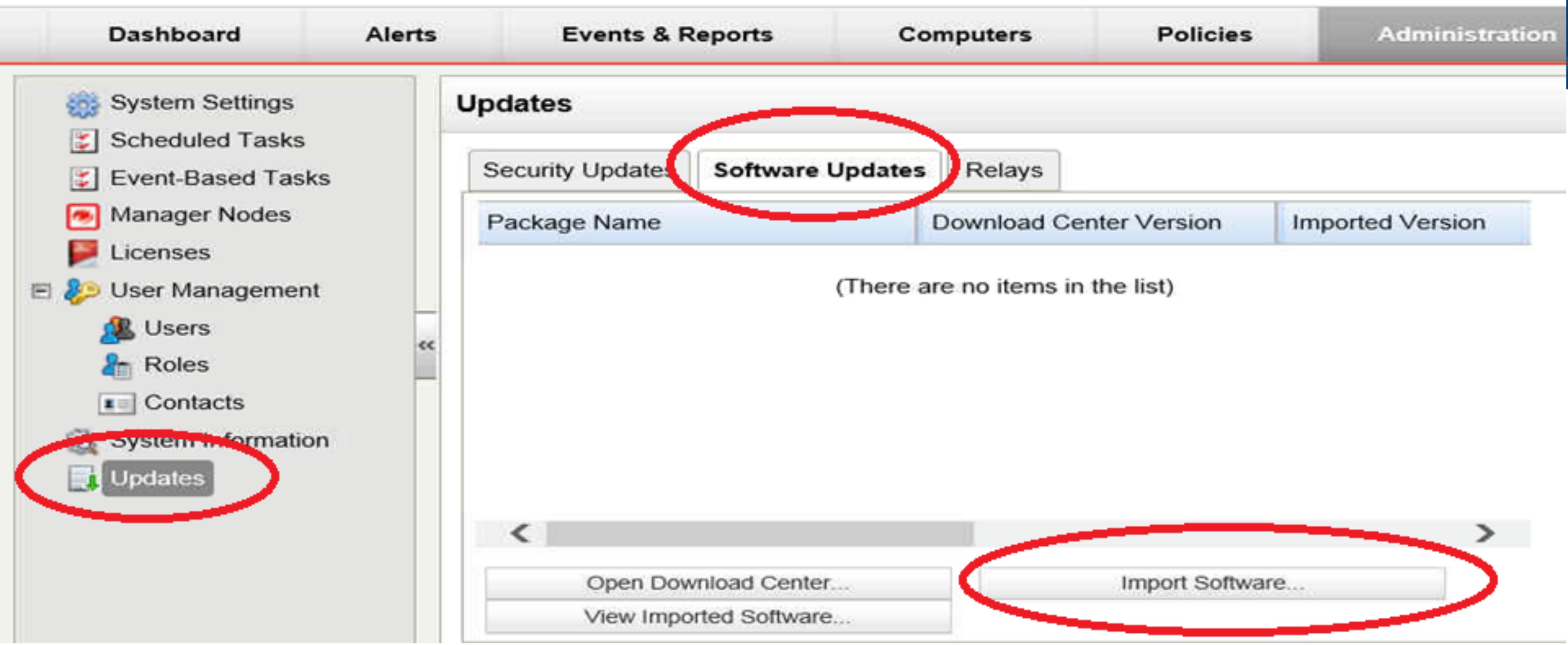
Scan Cache Configurations

Go to Computers, New, then "Add VMware vCenter"

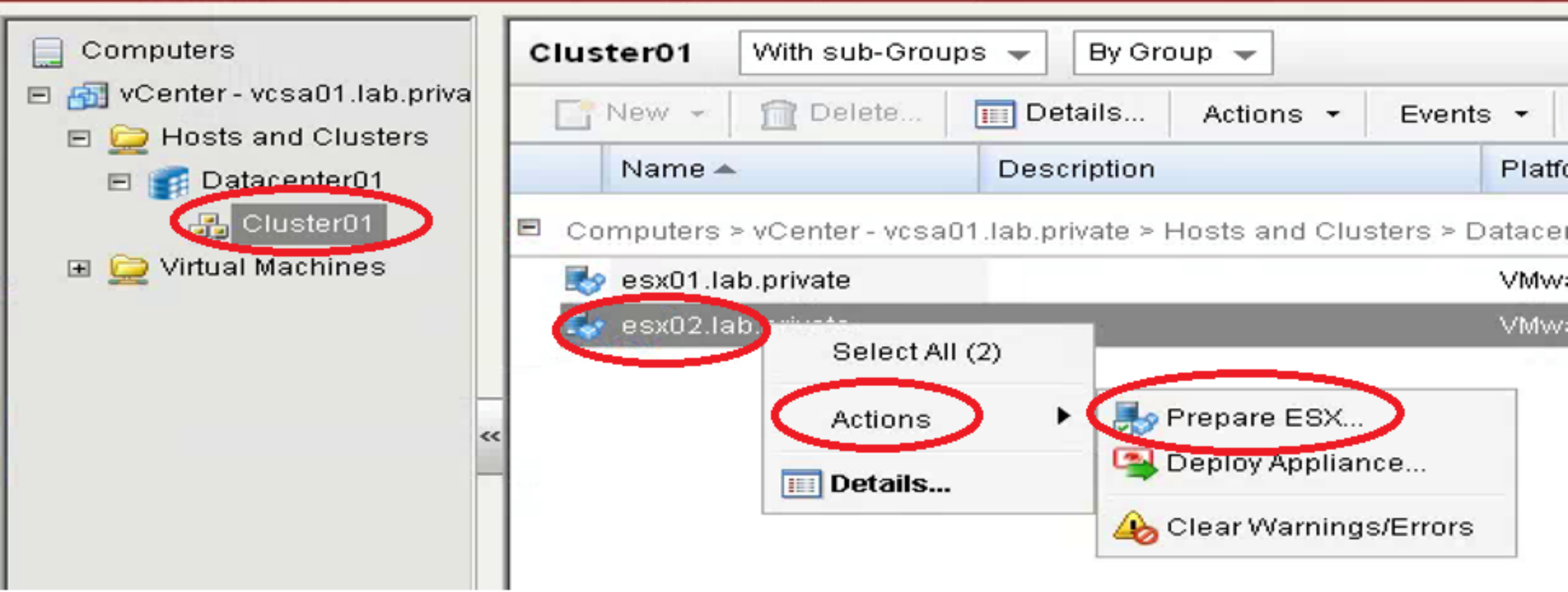


V. Trend Micro - Deploy Filter Driver and Appliance

- Goal: Install mechanics

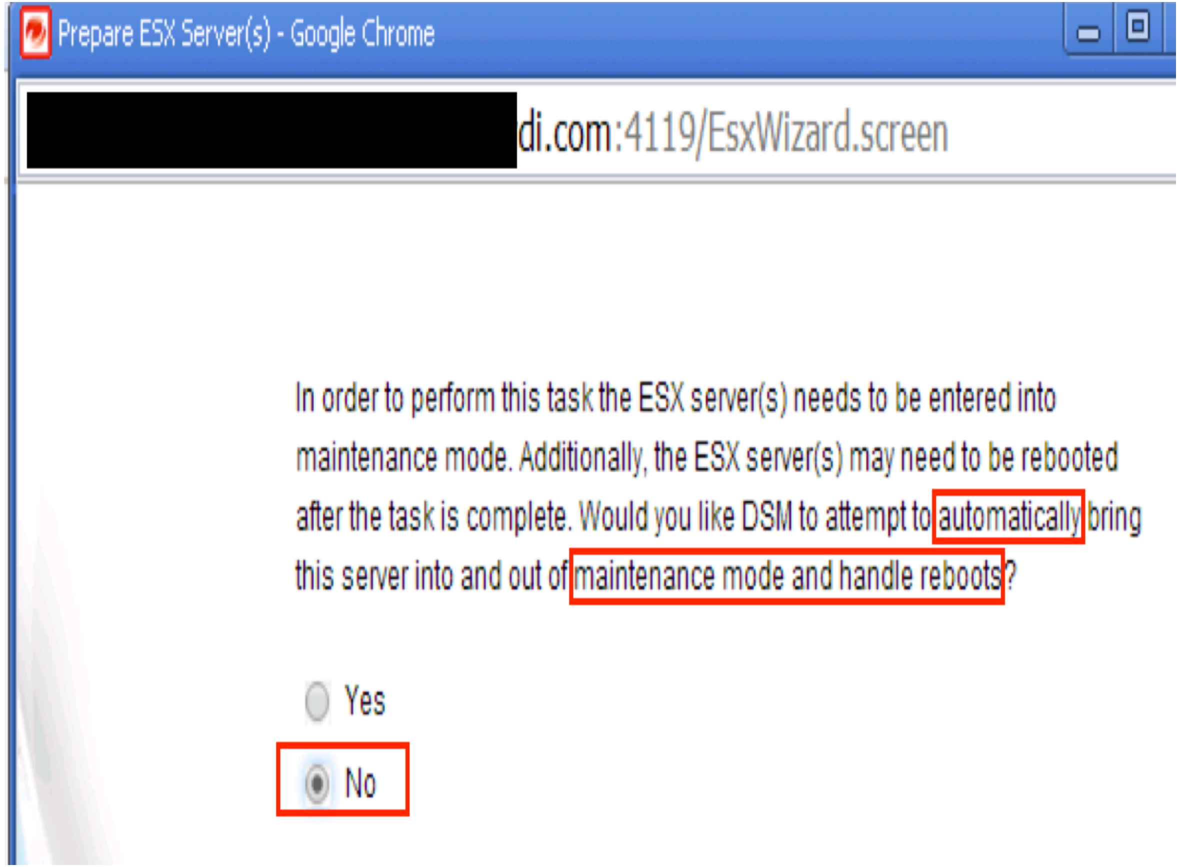


Add Trend modules you downloaded previously. Go to Updates, Software Updates and click “Import Software”



Select the Cluster in the tree, then select each ESX host, choose Actions, then "Prepare ESX..." to deploy the Filter Driver. You must do this on each host separately.

Vmotion VMs manually off the target ESX host, then manually put into Maintenance Mode. Choose No to let Trend deploy ONLY the Filter driver automatically. Then wait – it is slow. Monitor in vCenter.



Prepare ESX Server(s) - Google Chrome

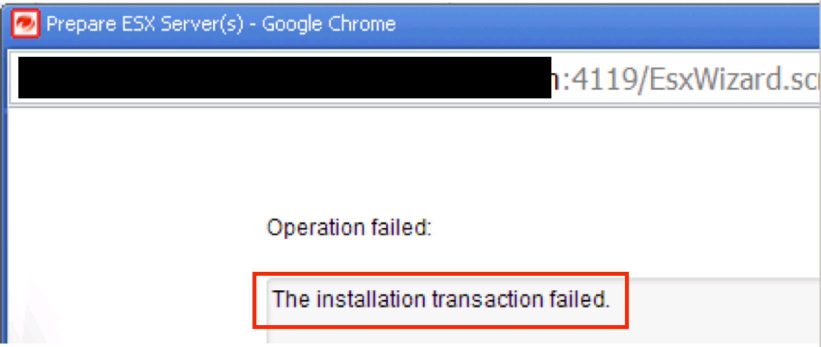
[redacted]di.com:4119/EsxWizard.screen

In order to perform this task the ESX server(s) needs to be entered into maintenance mode. Additionally, the ESX server(s) may need to be rebooted after the task is complete. Would you like DSM to attempt to automatically bring this server into and out of maintenance mode and handle reboots?

○ Yes

● No

If “Installation transaction”error w vSphere 5.5



Prepare ESX Server(s) - Google Chrome

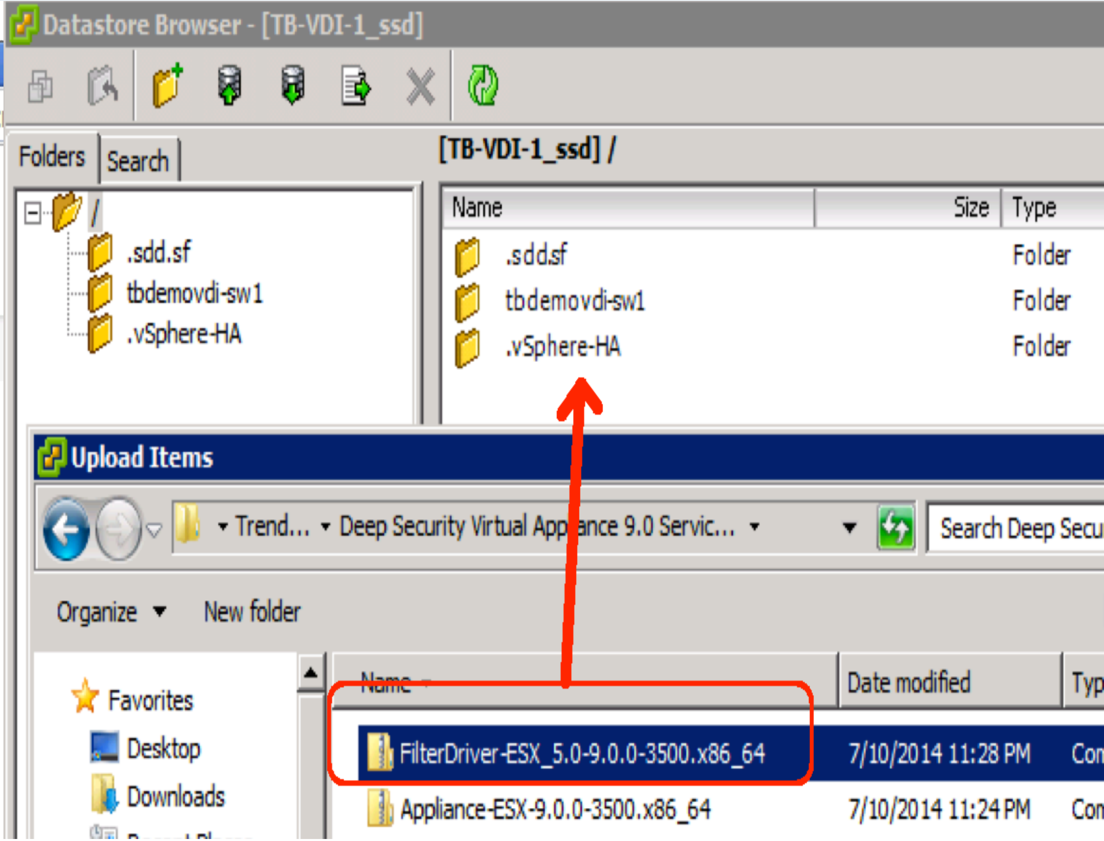
[redacted]:4119/EsxWizard.sc

Operation failed:

The installation transaction failed.

Copy Filter driver to ESXi local drive, follow VMware KB article 2077265 at the link below:

http://ow.ly/zBgS3



Datastore Browser - [TB-VDI-1_ssd]

[TB-VDI-1_ssd] /

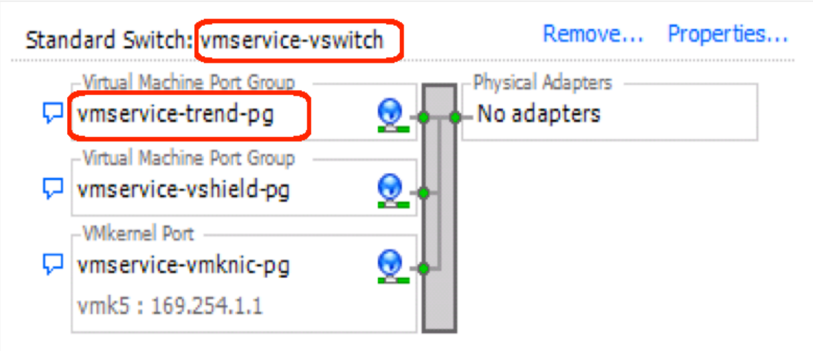
Name	Size	Type
.sdd.sf		Folder
tbdemovdi-sw1		Folder
.vSphere-HA		Folder

Upload Items

Name	Date modified	Typ
FilterDriver-ESX_5.0-9.0.0-3500.x86_64	7/10/2014 11:28 PM	Com
Appliance-ESX-9.0.0-3500.x86_64	7/10/2014 11:24 PM	Con

Error remediation, page 2

Put host into Maintenance Mode, add **vmservice-trend-pg** portgroup to *vmservice-vswitch*, install Filter driver manually, reboot server.



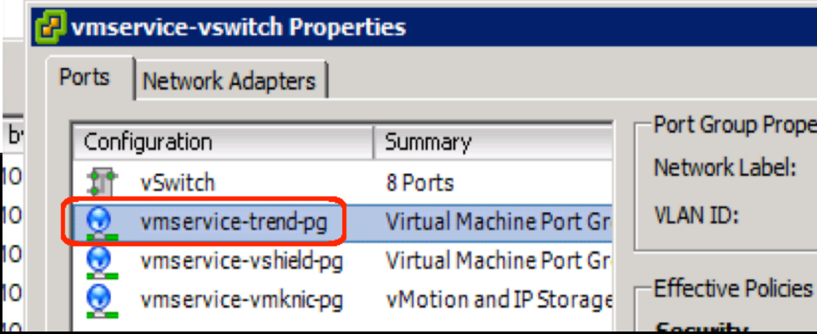
Standard Switch: vmservice-vswitch

Virtual Machine Port Group
vmservice-trend-pg

Virtual Machine Port Group
vmservice-vshield-pg

VMkernel Port
vmservice-vmknic-pg
vmk5 : 169.254.1.1

Physical Adapters
No adapters

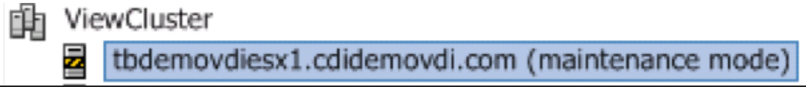


vmservice-vswitch Properties

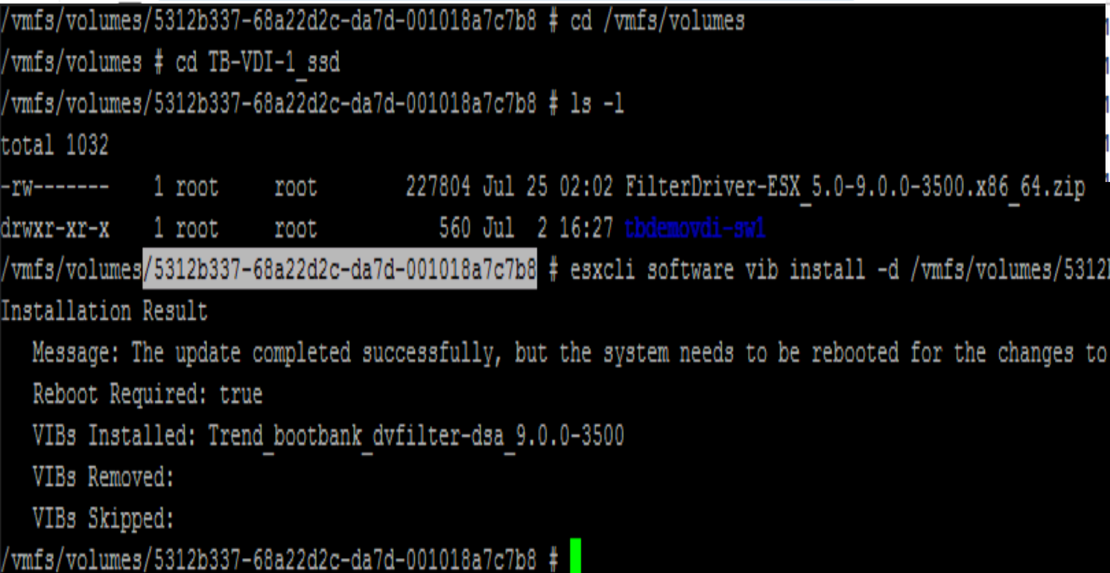
Configuration	Summary
vSwitch	8 Ports
vmservice-trend-pg	Virtual Machine Port Gr
vmservice-vshield-pg	Virtual Machine Port Gr
vmservice-vmknic-pg	vMotion and IP Storage

Port Group Prope
Network Label:
VLAN ID:

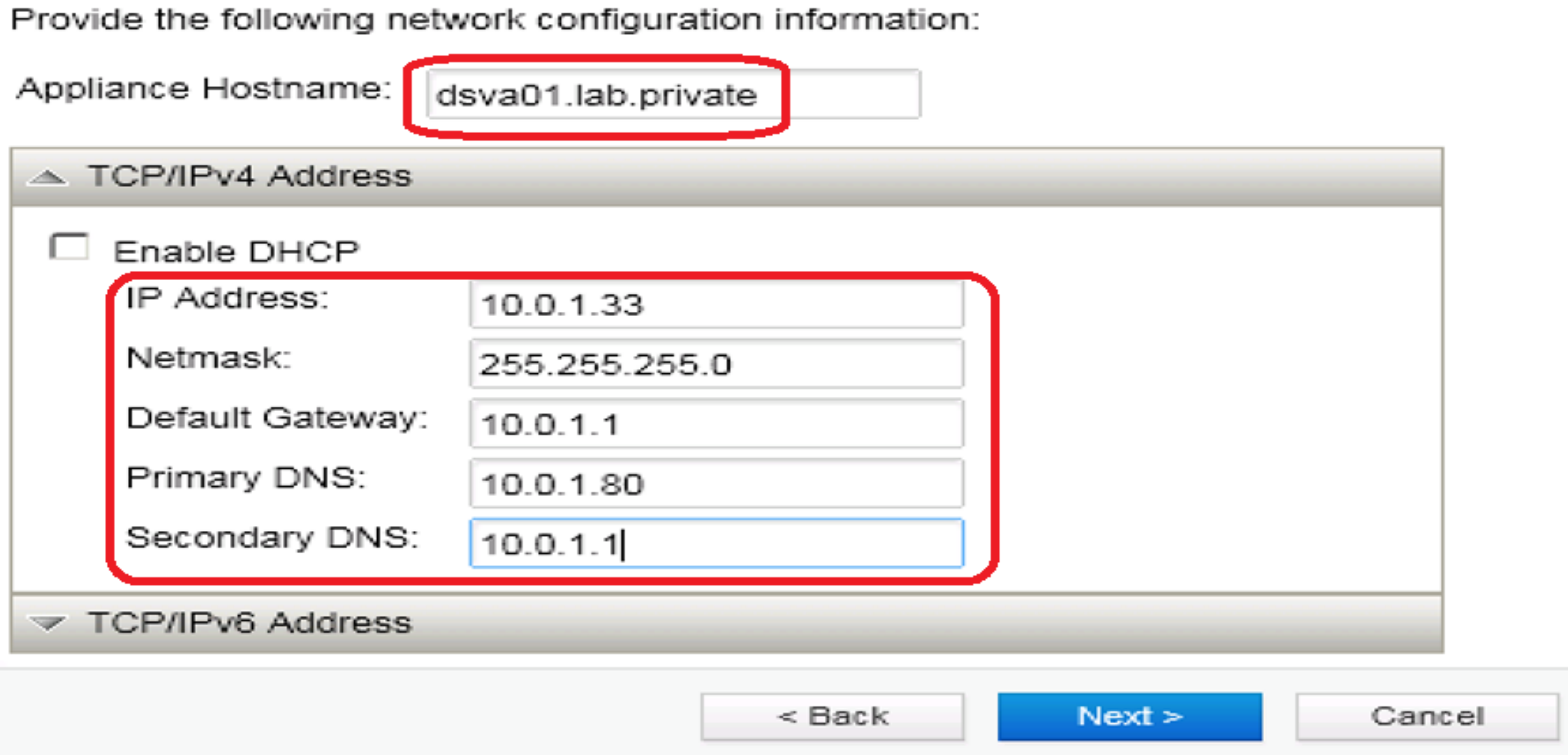
Effective Policies
Security



ViewCluster
tbdemovdiesx1.cdidemovdi.com (maintenance mode)



```
/vmfs/volumes/5312b337-68a22d2c-da7d-001018a7c7b8 # cd /vmfs/volumes
/vmfs/volumes # cd TB-VDI-1_ssd
/vmfs/volumes/5312b337-68a22d2c-da7d-001018a7c7b8 # ls -l
total 1032
-rw-------    1 root     root        227804 Jul 25 02:02 FilterDriver-ESX_5.0-9.0.0-3500.x86_64.zip
drwxr-xr-x    1 root     root           560 Jul  2 16:27 tbdemovdi-sw1
/vmfs/volumes/5312b337-68a22d2c-da7d-001018a7c7b8 # esxcli software vib install -d /vmfs/volumes/5312b337-68a22d2c-da7d-001018a7c7b8/FilterDriver-ESX_5.0-9.0.0-3500.x86_64.zip
Installation Result
   Message: The update completed successfully, but the system needs to be rebooted for the changes to be effective.
   Reboot Required: true
   VIBs Installed: Trend_bootbank_dvfilter-dsa_9.0.0-3500
   VIBs Removed:
   VIBs Skipped:
/vmfs/volumes/5312b337-68a22d2c-da7d-001018a7c7b8 #
```



Provide the following network configuration information:

Appliance Hostname: dsva01.lab.private

TCP/IPv4 Address

□ Enable DHCP

IP Address: 10.0.1.33

Netmask: 255.255.255.0

Default Gateway: 10.0.1.1

Primary DNS: 10.0.1.80

Secondary DNS: 10.0.1.1

TCP/IPv6 Address

Provide FQDN and Static IP address.

Cluster01 Settings

- Cluster Features
- vSphere DRS
  - DRS Groups Manager
  - Rules
  - Virtual Machine Options
  - Power Management
    - Host Options
- VMware EVC
- Swapfile Location

☑ Enable individual virtual machine automation levels.

Set individual automation level options for virtual machines in the cluster.

Virtual Machine or Automation Level contains:

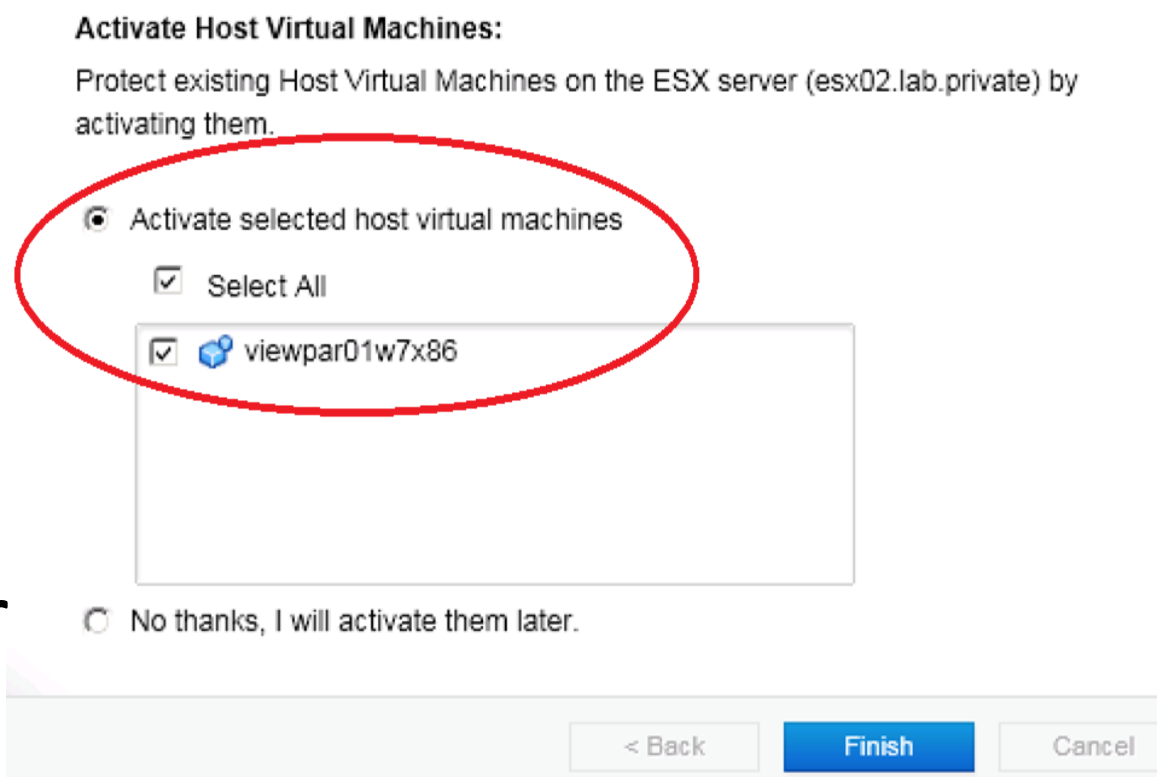
Virtual Machine	Automation Level
sql01a	Default (Manual)
vshieldman01	Default (Manual)
vcsa01	Default (Manual)
viewpar01w7x86	Default (Manual)
vdesktop-20	Default (Manual)
DSVA02	Disabled
viewcon01a	Default (Manual)
trendman01	Default (Manual)

Ensure appliance is Disabled from DRS automatic VMotion

VI. Trend Micro – Protect VMs

- Goal: Protection

Activate all VMs on the host for protection. You can also activate them later through the Trend Manager interface.



Activate Host Virtual Machines:

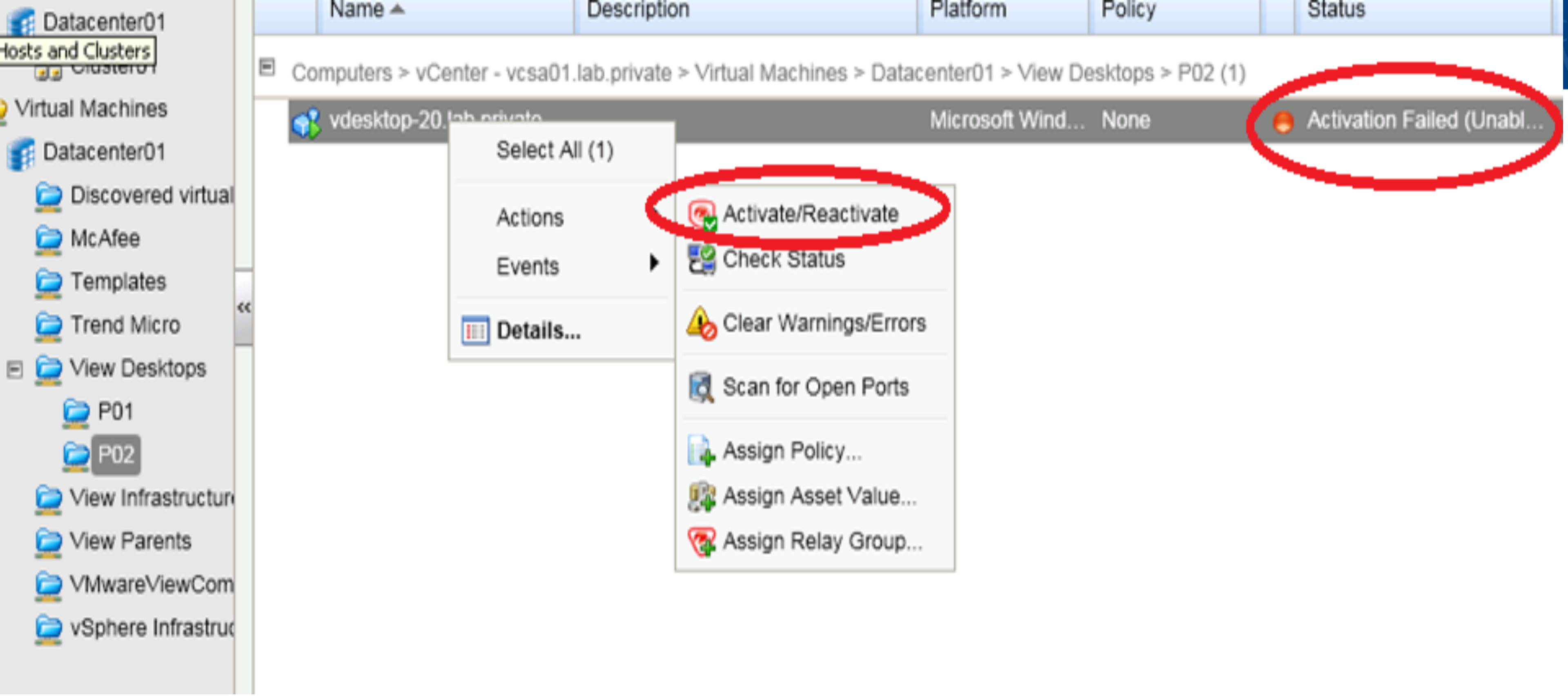
Protect existing Host Virtual Machines on the ESX server (esx02.lab.private) by activating them.

● Activate selected host virtual machines

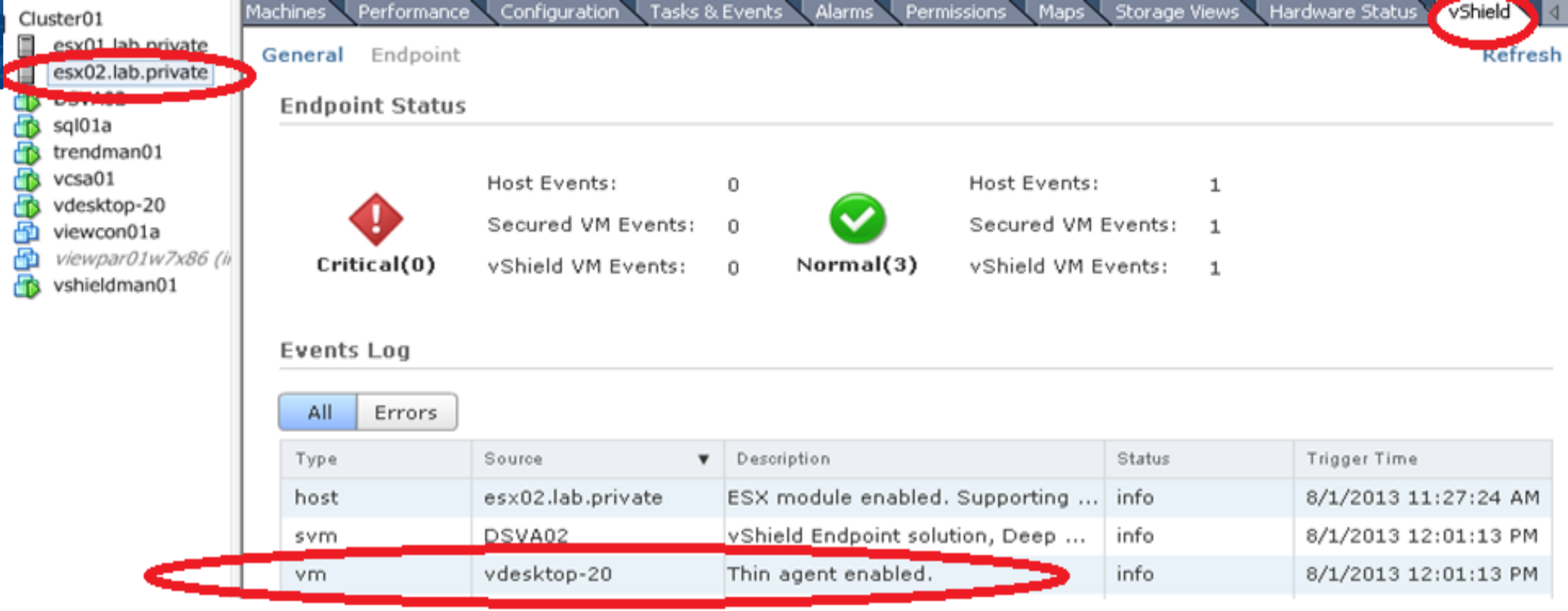
☑ Select All

☑ viewpar01w7x86

○ No thanks, I will activate them later.



If activation fails, you can reactivate the VM manually



Endpoint Status

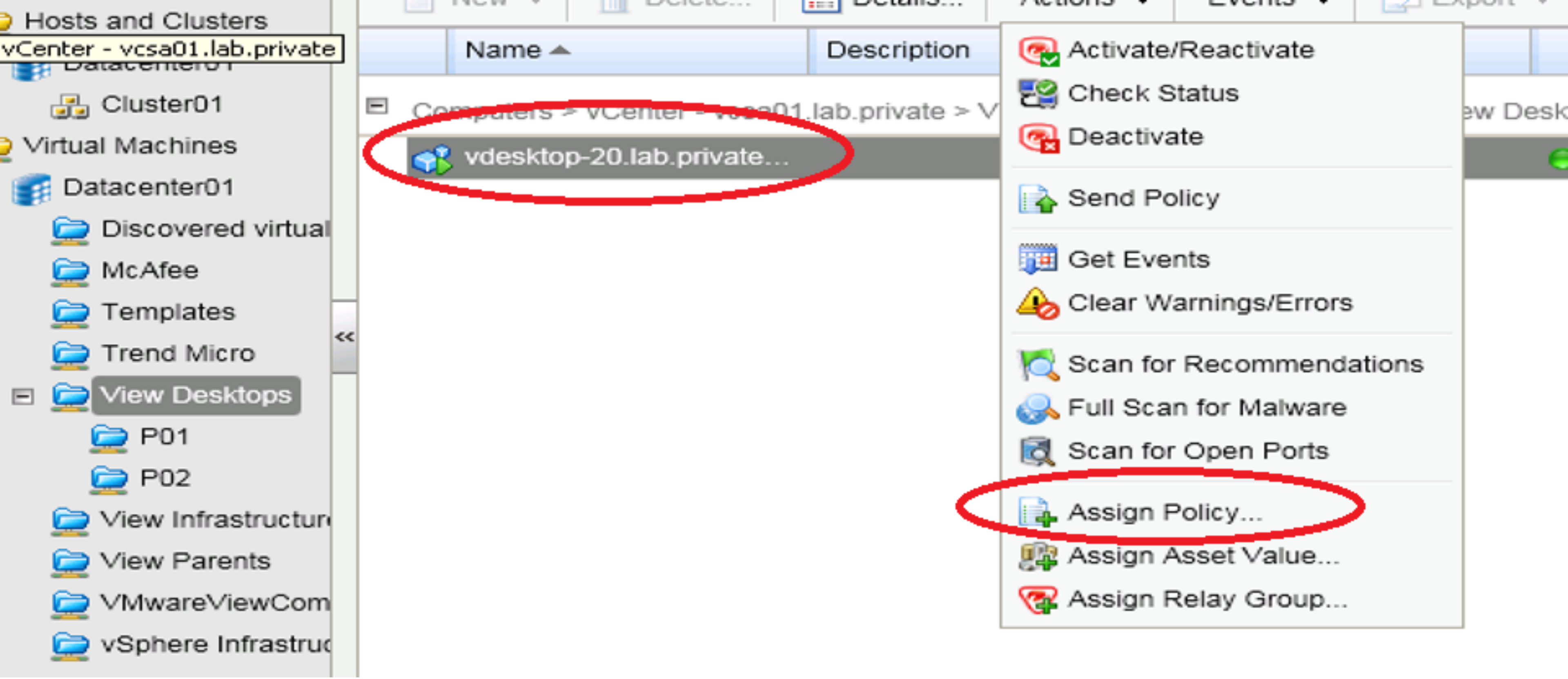
Critical(0)
Host Events: 0
Secured VM Events: 0
vShield VM Events: 0

Normal(3)
Host Events: 1
Secured VM Events: 1
vShield VM Events: 1

Events Log

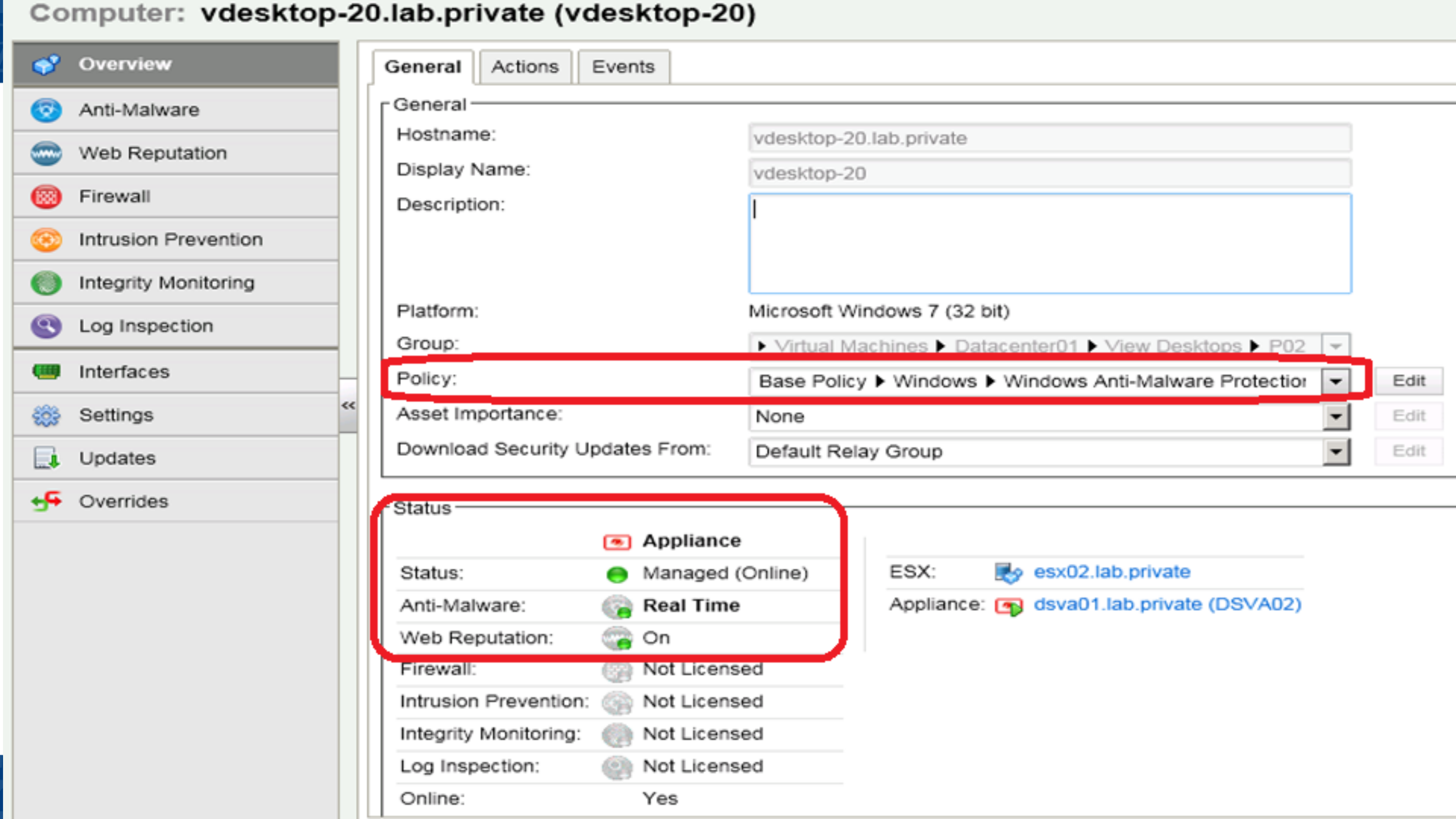
Type	Source	Description	Status	Trigger Time
host	esx02.lab.private	ESX module enabled. Supporting ...	info	8/1/2013 11:27:24 AM
svm	DSVA02	vShield Endpoint solution, Deep ...	info	8/1/2013 12:01:13 PM
vm	vdesktop-20	Thin agent enabled.	info	8/1/2013 12:01:13 PM

After activation is successful, go to ESX vShield tab & look for the name of the VM with the status of “Thin agent enabled”



Next, right click on VM in Trend Manager and Assign Policy.

Choose Base>Windows>Windows Anti-Malware Protection



Computer: vdesktop-20.lab.private (vdesktop-20)

General

Hostname:	vdesktop-20.lab.private
Display Name:	vdesktop-20
Description:	
Platform:	Microsoft Windows 7 (32 bit)
Group:	▸ Virtual Machines ▸ Datacenter01 ▸ View Desktops ▸ P02
Policy:	Base Policy ▸ Windows ▸ Windows Anti-Malware Protectior
Asset Importance:	None
Download Security Updates From:	Default Relay Group

Status

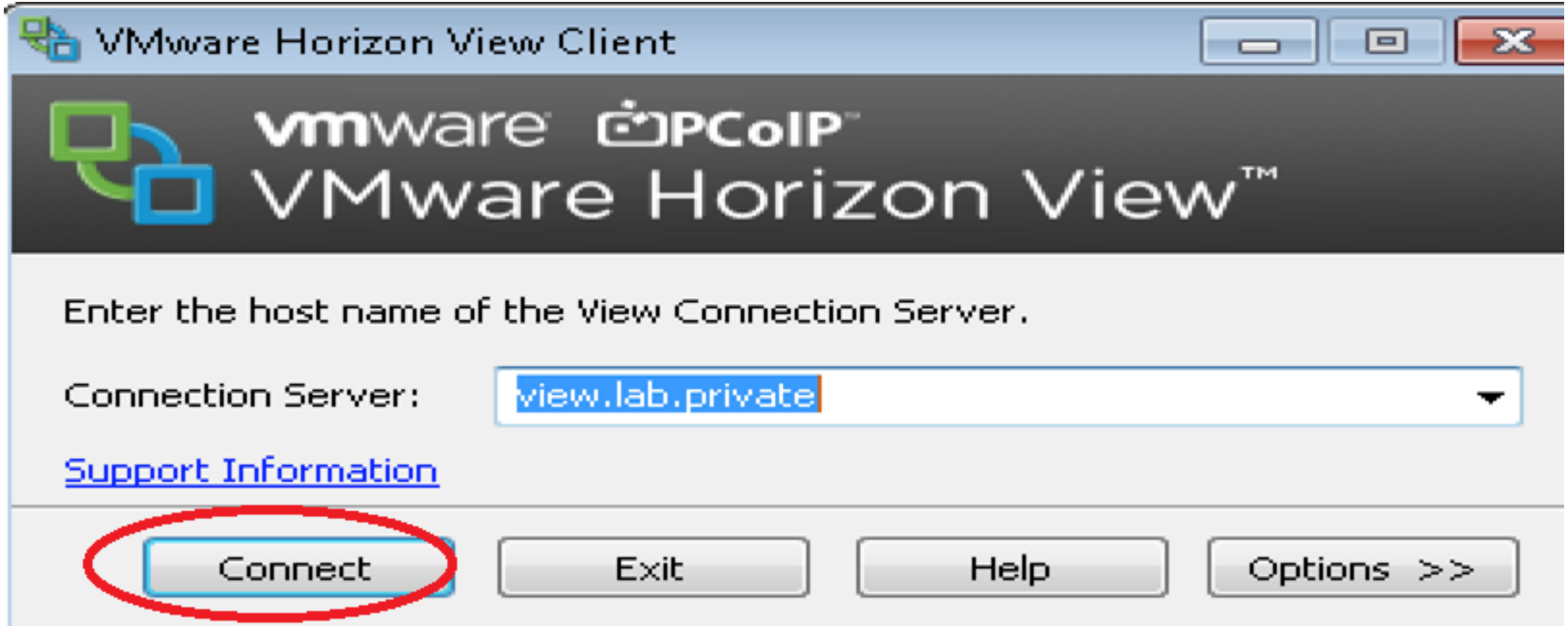
	Appliance
Status:	Managed (Online)
Anti-Malware:	**Real Time**
Web Reputation:	On
Firewall:	Not Licensed
Intrusion Prevention:	Not Licensed
Integrity Monitoring:	Not Licensed
Log Inspection:	Not Licensed
Online:	Yes

ESX:	esx02.lab.private
Appliance:	dsva01.lab.private (DSVA02)

VII. Connect View Desktop

- Goal: Test catching viruses

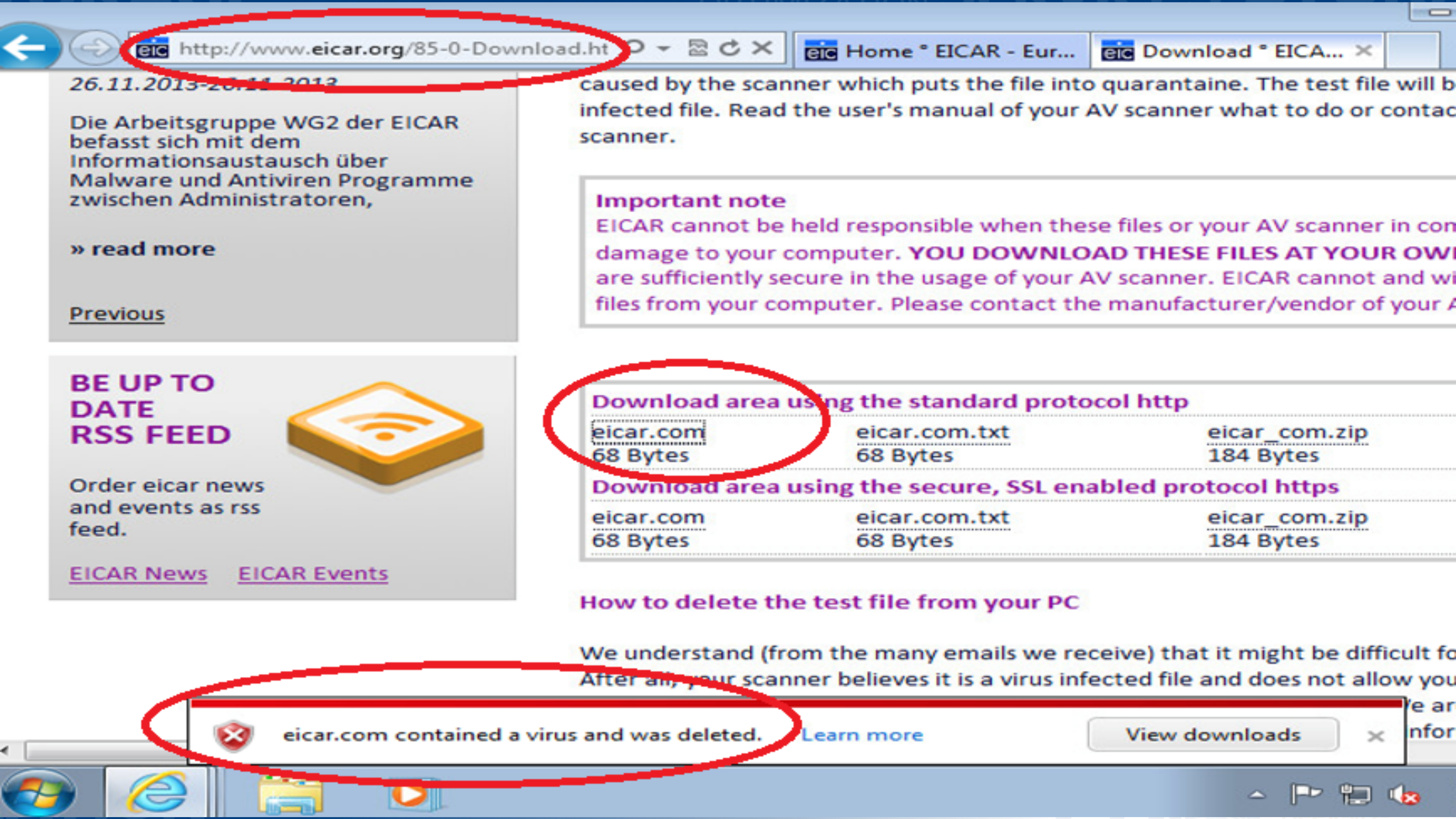
Connect to your Virtual Desktop, in this case VMware View 5.3



VMware Horizon View Client

Enter the host name of the View Connection Server.

Connection Server: view.lab.private



26.11.2013-26.11.2013

Die Arbeitsgruppe WG2 der EICAR befasst sich mit dem Informationsaustausch über Malware und Antiviren Programme zwischen Administratoren,

» read more

Previous

BE UP TO DATE RSS FEED

Order eicar news and events as rss feed.

EICAR News EICAR Events

caused by the scanner which puts the file into quarantaine. The test file will b
infected file. Read the user's manual of your AV scanner what to do or contac
scanner.

Important note
EICAR cannot be held responsible when these files or your AV scanner in con
damage to your computer. **YOU DOWNLOAD THESE FILES AT YOUR OWI**
are sufficiently secure in the usage of your AV scanner. EICAR cannot and wi
files from your computer. Please contact the manufacturer/vendor of your A

Download area using the standard protocol http

eicar.com 68 Bytes	eicar.com.txt 68 Bytes	eicar_com.zip 184 Bytes

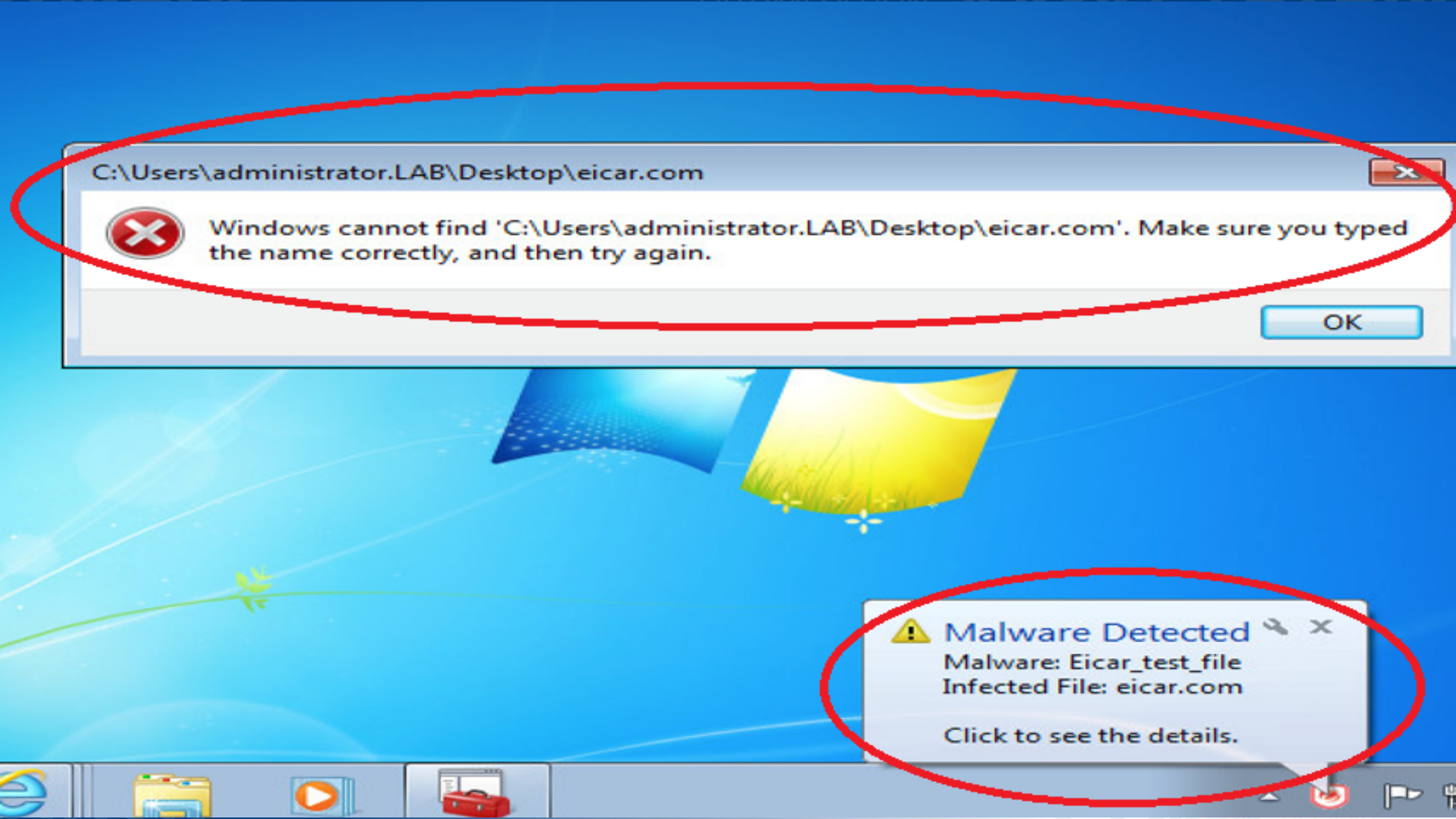
Download area using the secure, SSL enabled protocol https

eicar.com 68 Bytes	eicar.com.txt 68 Bytes	eicar_com.zip 184 Bytes

How to delete the test file from your PC

We understand (from the many emails we receive) that it might be difficult fo
After all, your scanner believes it is a virus infected file and does not allow you
'e ar
nfor

eicar.com contained a virus and was deleted.



C:\Users\administrator.LAB\Desktop\eicar.com

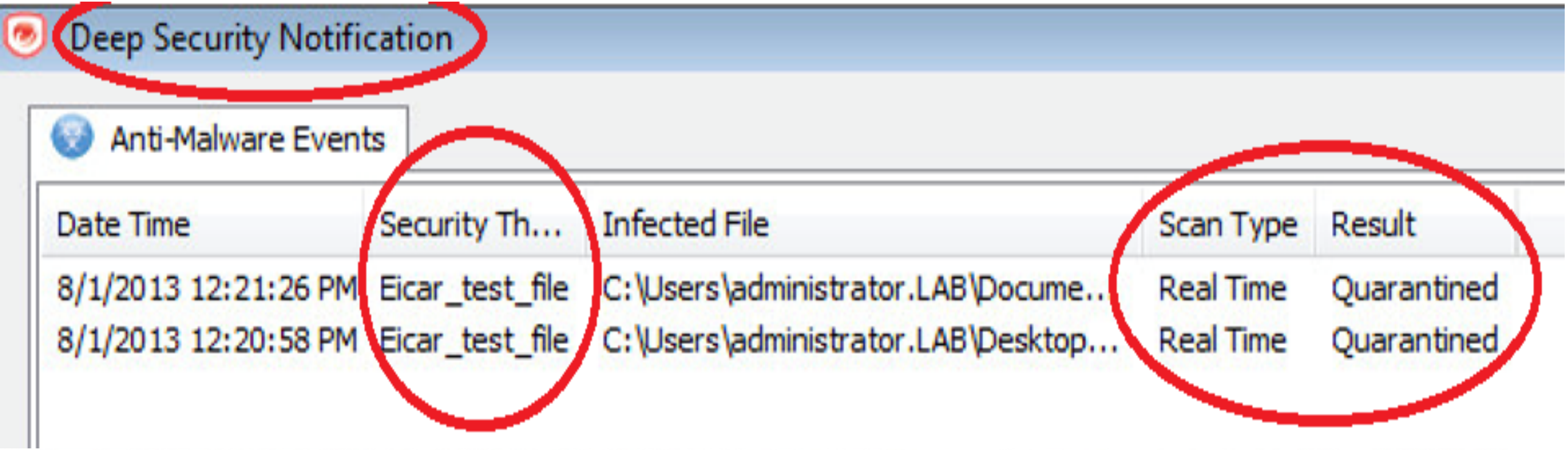
Windows cannot find 'C:\Users\administrator.LAB\Desktop\eicar.com'. Make sure you typed the name correctly, and then try again.

Malware Detected

Malware: Eicar_test_file
Infected File: eicar.com

Click to see the details.

If you click to see the details of the caught virus, you will see that it was Quarantined



Deep Security Notification

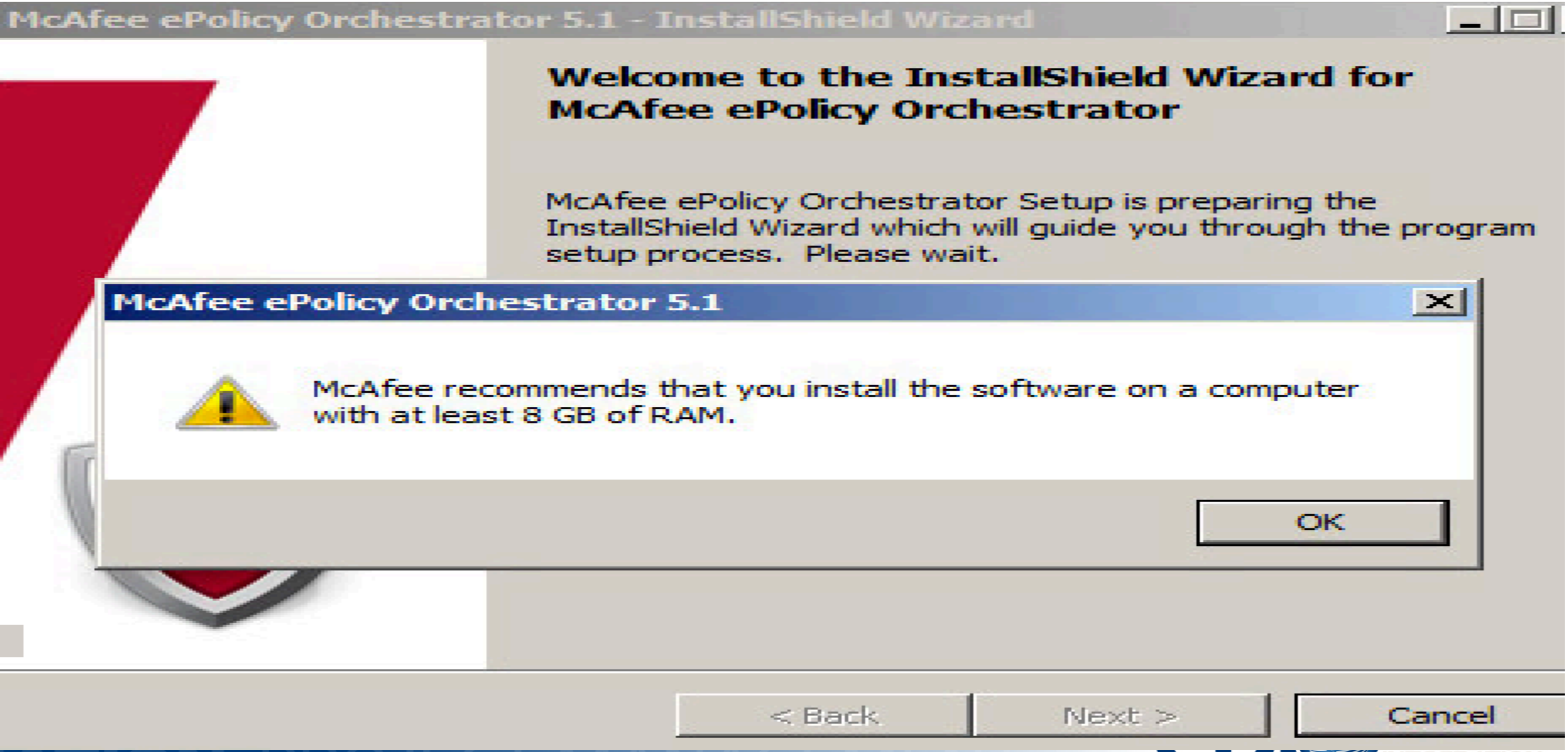
Anti-Malware Events

Date Time	Security Th...	Infected File	Scan Type	Result
8/1/2013 12:21:26 PM	Eicar_test_file	C:\Users\administrator.LAB\Docume...	Real Time	Quarantined
8/1/2013 12:20:58 PM	Eicar_test_file	C:\Users\administrator.LAB\Desktop...	Real Time	Quarantined

VIII. McAfee Mechanics

- Build McAfee MOVE

Initial install



McAfee ePolicy Orchestrator 5.1 - InstallShield Wizard

Welcome to the InstallShield Wizard for McAfee ePolicy Orchestrator

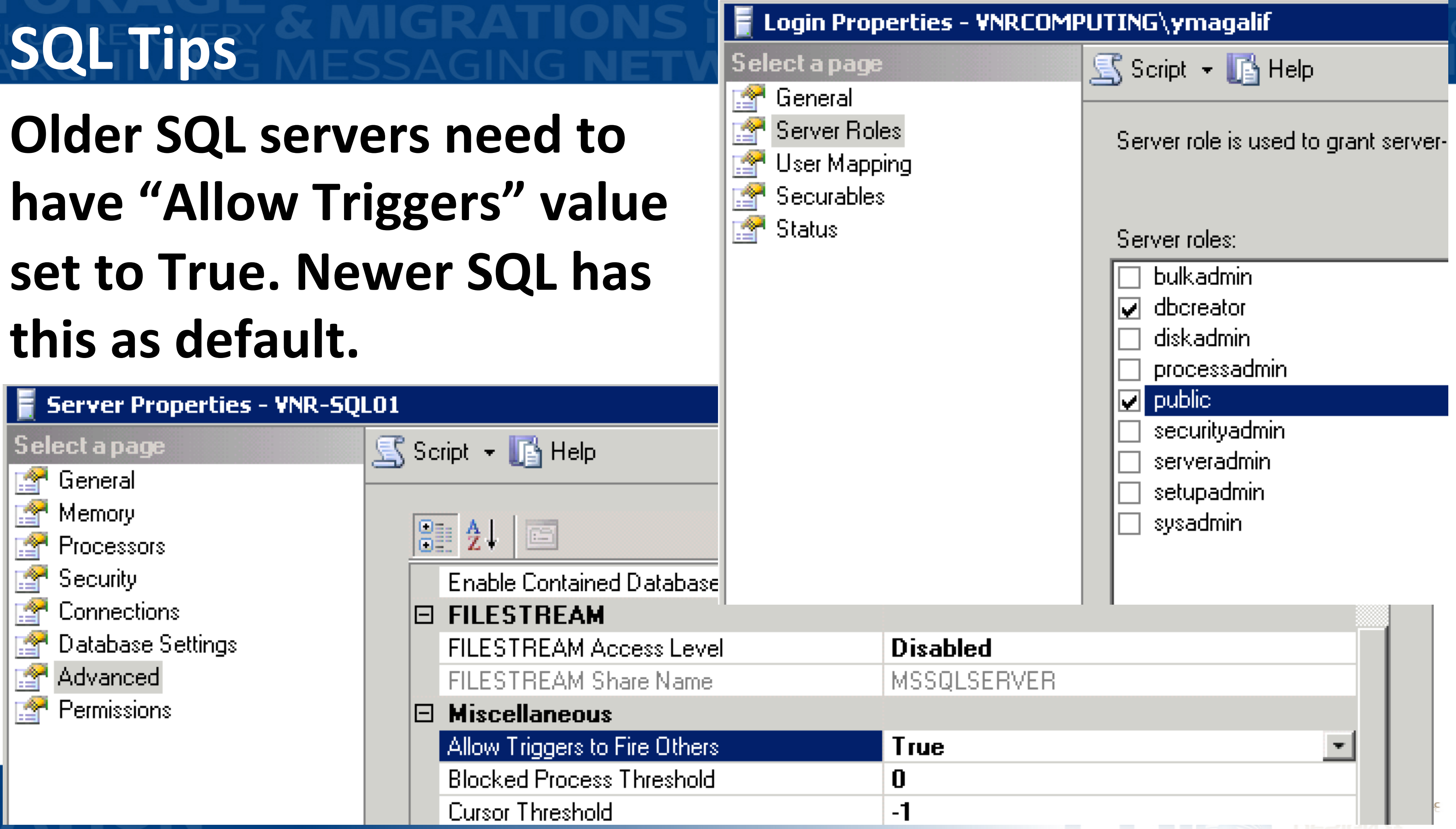
McAfee ePolicy Orchestrator Setup is preparing the InstallShield Wizard which will guide you through the program setup process. Please wait.

McAfee ePolicy Orchestrator 5.1

McAfee recommends that you install the software on a computer with at least 8 GB of RAM.

SQL Tips

Older SQL servers need to have “Allow Triggers” value set to True. Newer SQL has this as default.



Login Properties - VNRCOMPUTING\ymagalif

Server role is used to grant server-

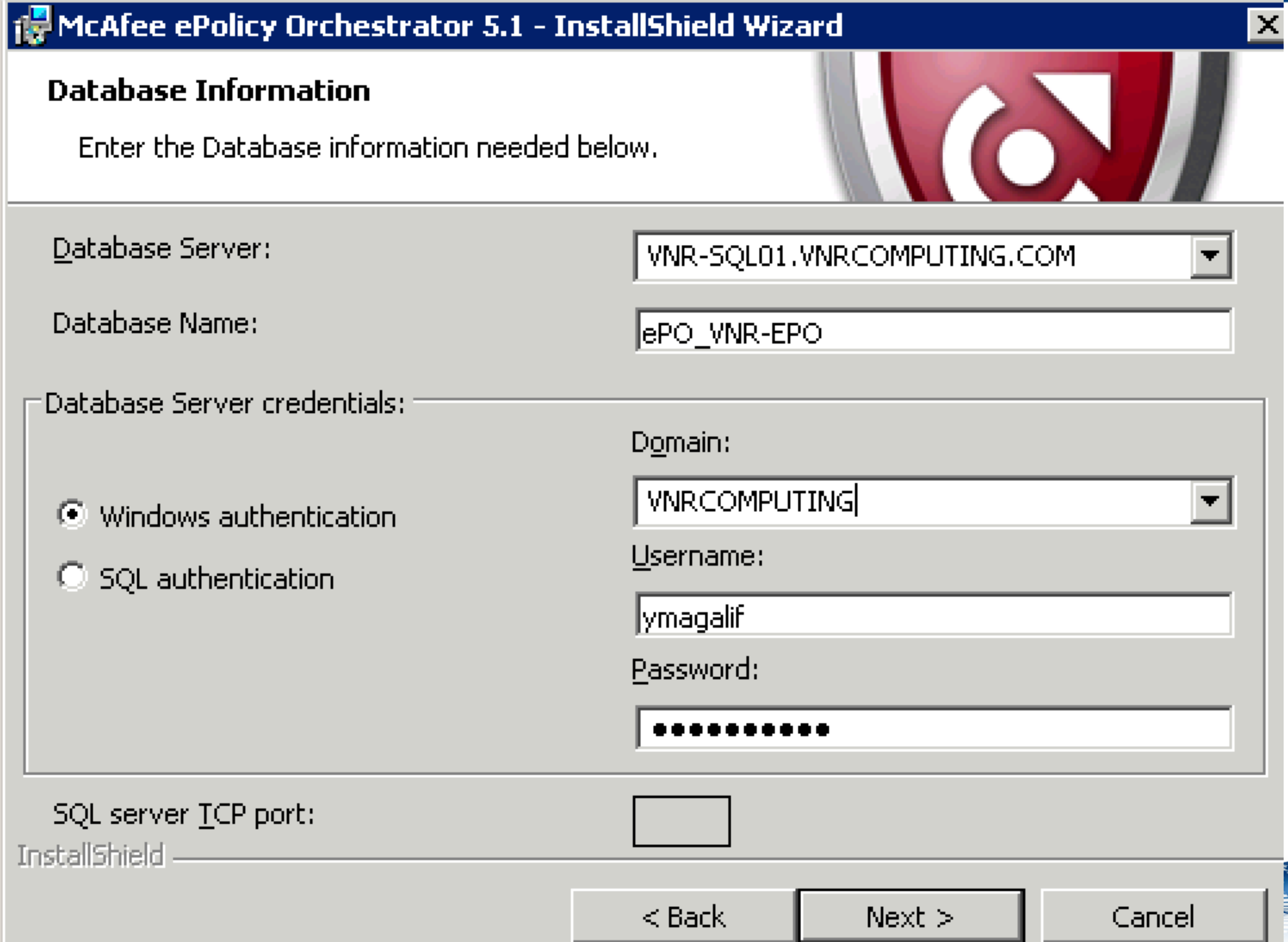
Server roles:

- ☐ bulkadmin
- ☑ dbcreator
- ☐ diskadmin
- ☐ processadmin
- ☑ public
- ☐ securityadmin
- ☐ serveradmin
- ☐ setupadmin
- ☐ sysadmin

Server Properties - VNR-SQL01

Enable Contained Database	
⊟ **FILESTREAM**	
FILESTREAM Access Level	**Disabled**
FILESTREAM Share Name	MSSQLSERVER
⊟ **Miscellaneous**	
Allow Triggers to Fire Others	**True**
Blocked Process Threshold	**0**
Cursor Threshold	-1

Database will be created



Database Information

Enter the Database information needed below.

Database Server: VNR-SQL01.VNRCOMPUTING.COM

Database Name: ePO_VNR-EPO

Database Server credentials:

● Windows authentication

○ SQL authentication

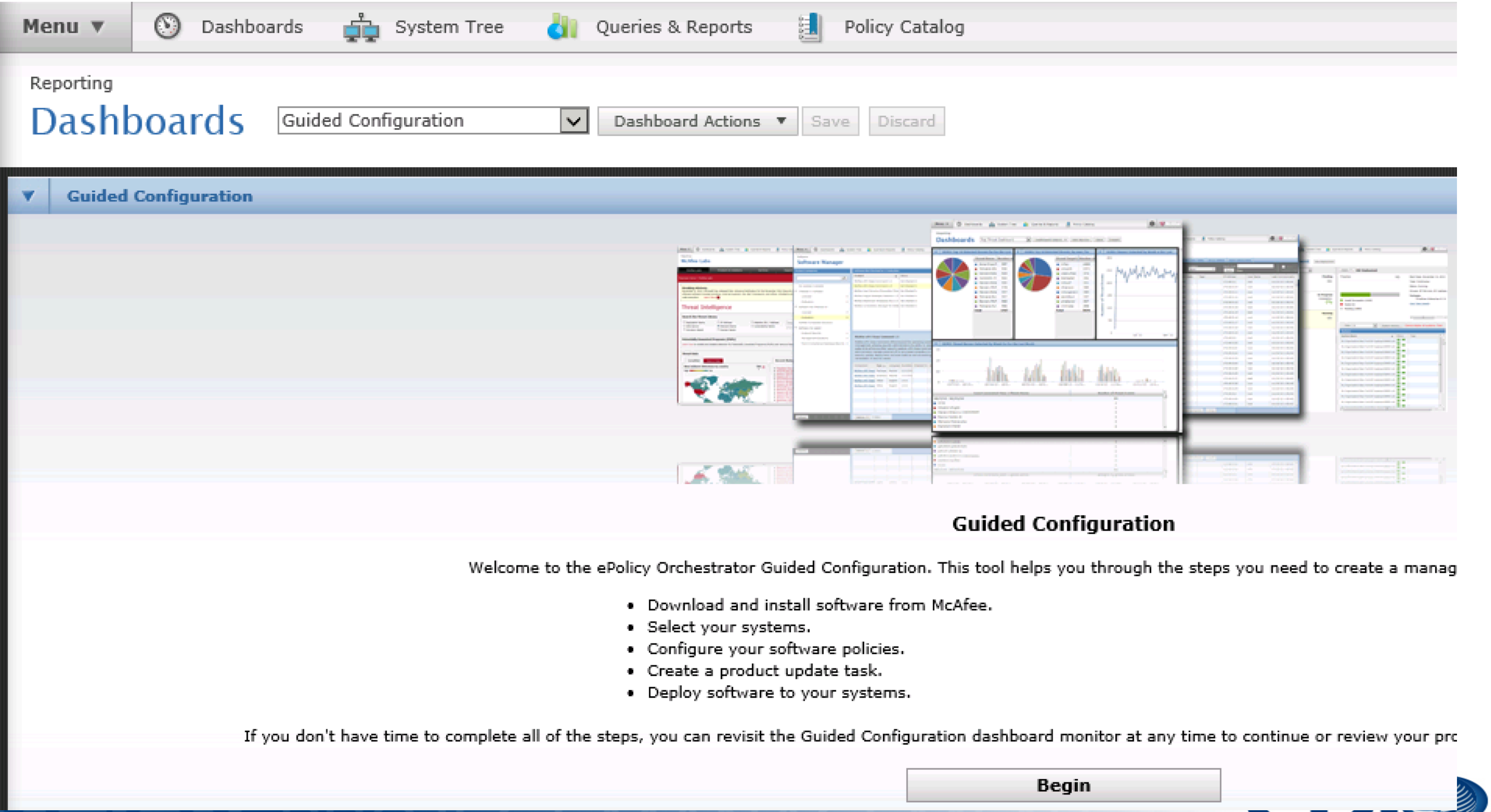
Domain: VNRCOMPUTING

Username: ymagalif

Password: ●●●●●●●●●●●●

SQL server TCP port:

Use Guided configuration for initial basic setup



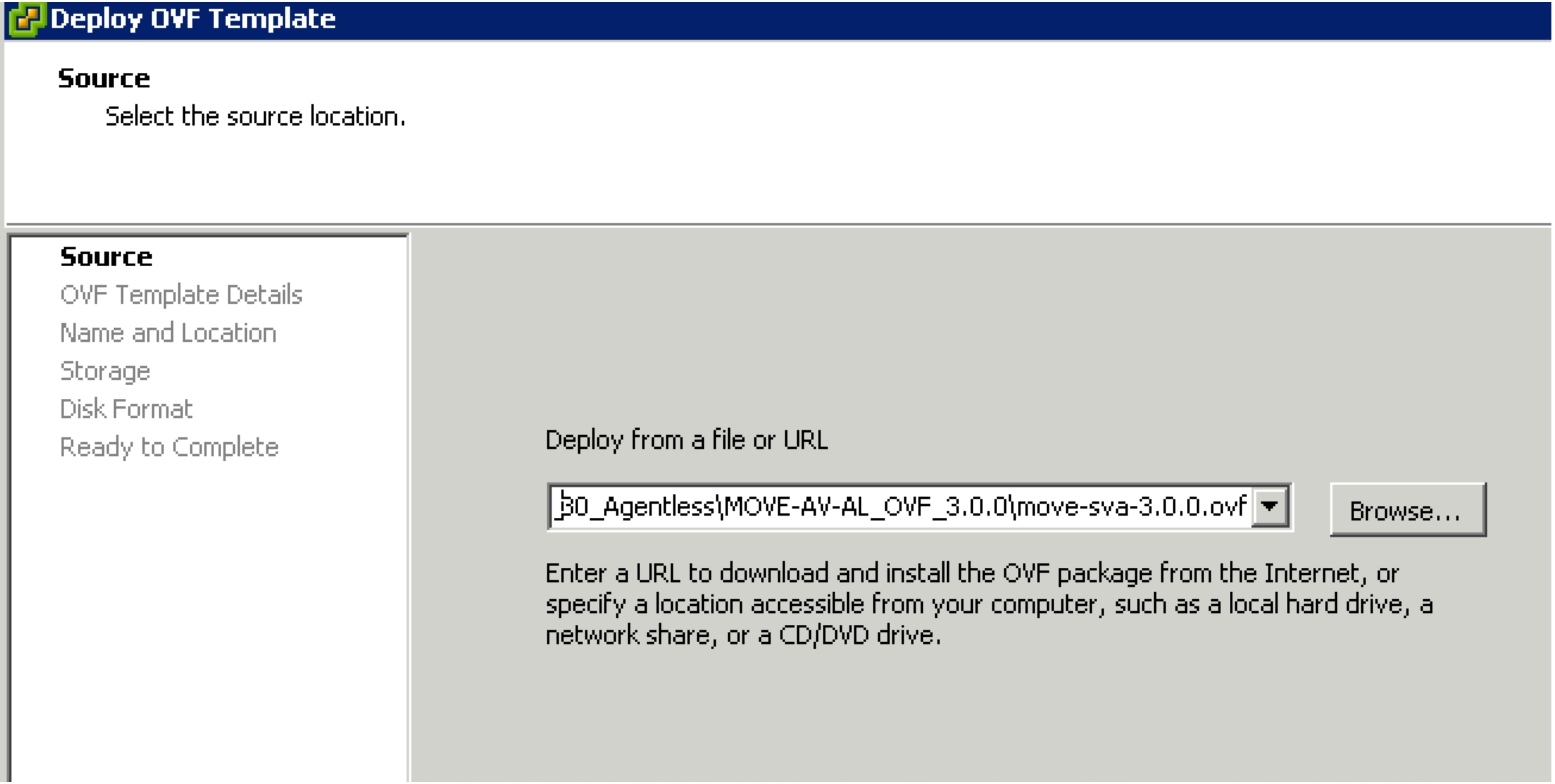
Guided Configuration

Welcome to the ePolicy Orchestrator Guided Configuration. This tool helps you through the steps you need to create a manag

- Download and install software from McAfee.
- Select your systems.
- Configure your software policies.
- Create a product update task.
- Deploy software to your systems.

If you don't have time to complete all of the steps, you can revisit the Guided Configuration dashboard monitor at any time to continue or review your pro

Deploy appliance yourself, manually



Source

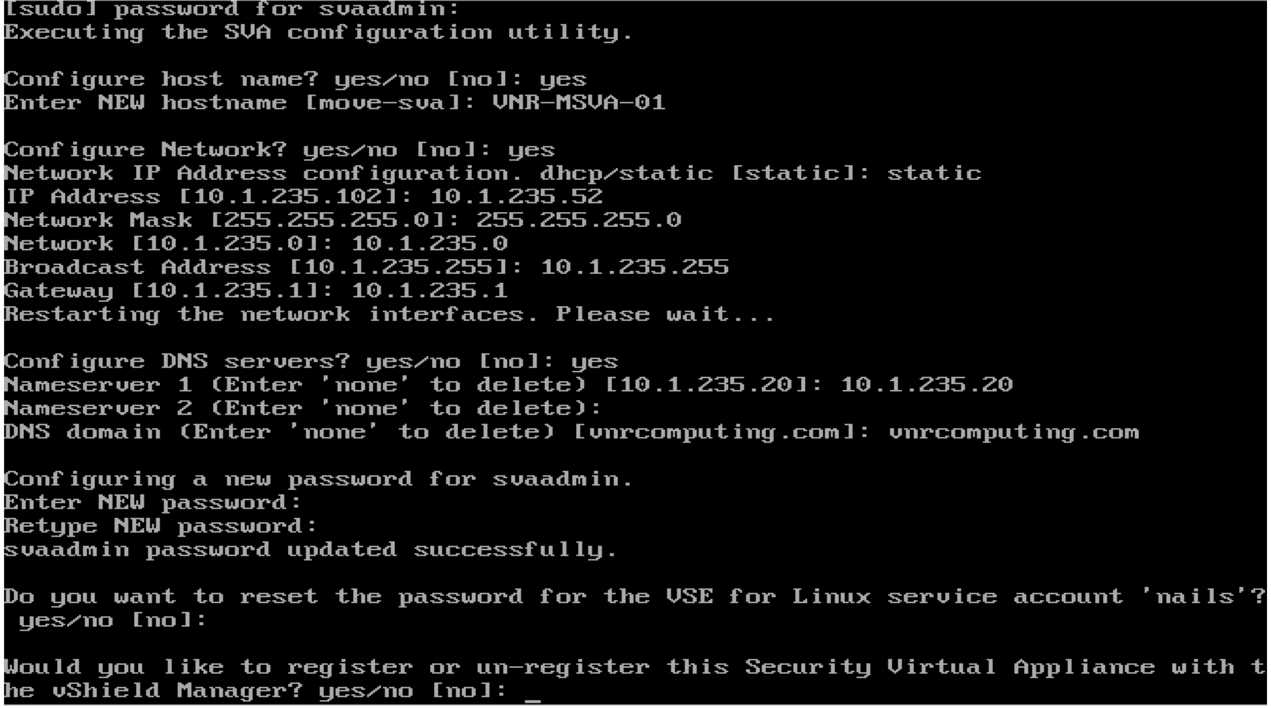
Select the source location.

Deploy from a file or URL

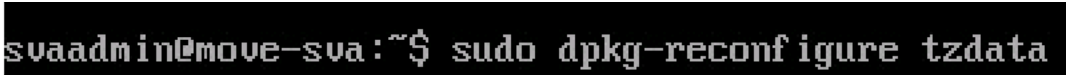
30_Agentless\MOVE-AV-AL_OVF_3.0.0\move-sva-3.0.0.ovf

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

Better configure appliance manually – don't set OVF settings

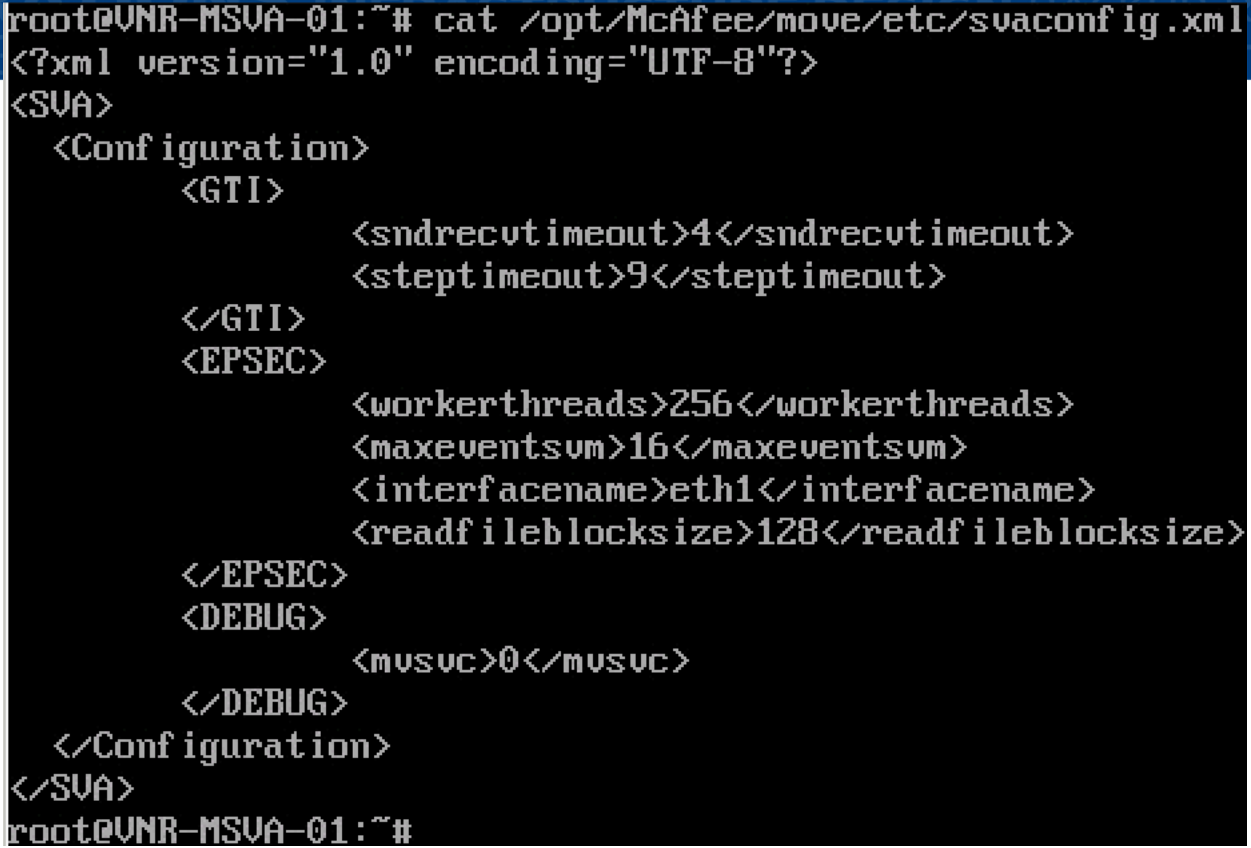


```
[sudo] password for svaadmin:
Executing the SVA configuration utility.

Configure host name? yes/no [no]: yes
Enter NEW hostname [move-sva]: VNR-MSVA-01

Configure Network? yes/no [no]: yes
Network IP Address configuration. dhcp/static [static]: static
IP Address [10.1.235.102]: 10.1.235.52
Network Mask [255.255.255.0]: 255.255.255.0
Network [10.1.235.0]: 10.1.235.0
Broadcast Address [10.1.235.255]: 10.1.235.255
Gateway [10.1.235.1]: 10.1.235.1
Restarting the network interfaces. Please wait...

Configure DNS servers? yes/no [no]: yes
Nameserver 1 (Enter 'none' to delete) [10.1.235.20]: 10.1.235.20
Nameserver 2 (Enter 'none' to delete):
DNS domain (Enter 'none' to delete) [vnrcomputing.com]: vnrcomputing.com

Configuring a new password for svaadmin.
Enter NEW password:
Retype NEW password:
svaadmin password updated successfully.

Do you want to reset the password for the VSE for Linux service account 'nails'?
 yes/no [no]:

Would you like to register or un-register this Security Virtual Appliance with t
he vShield Manager? yes/no [no]: _
```



```
svaadmin@move-sva:~$ sudo dpkg-reconfigure tzdata
```

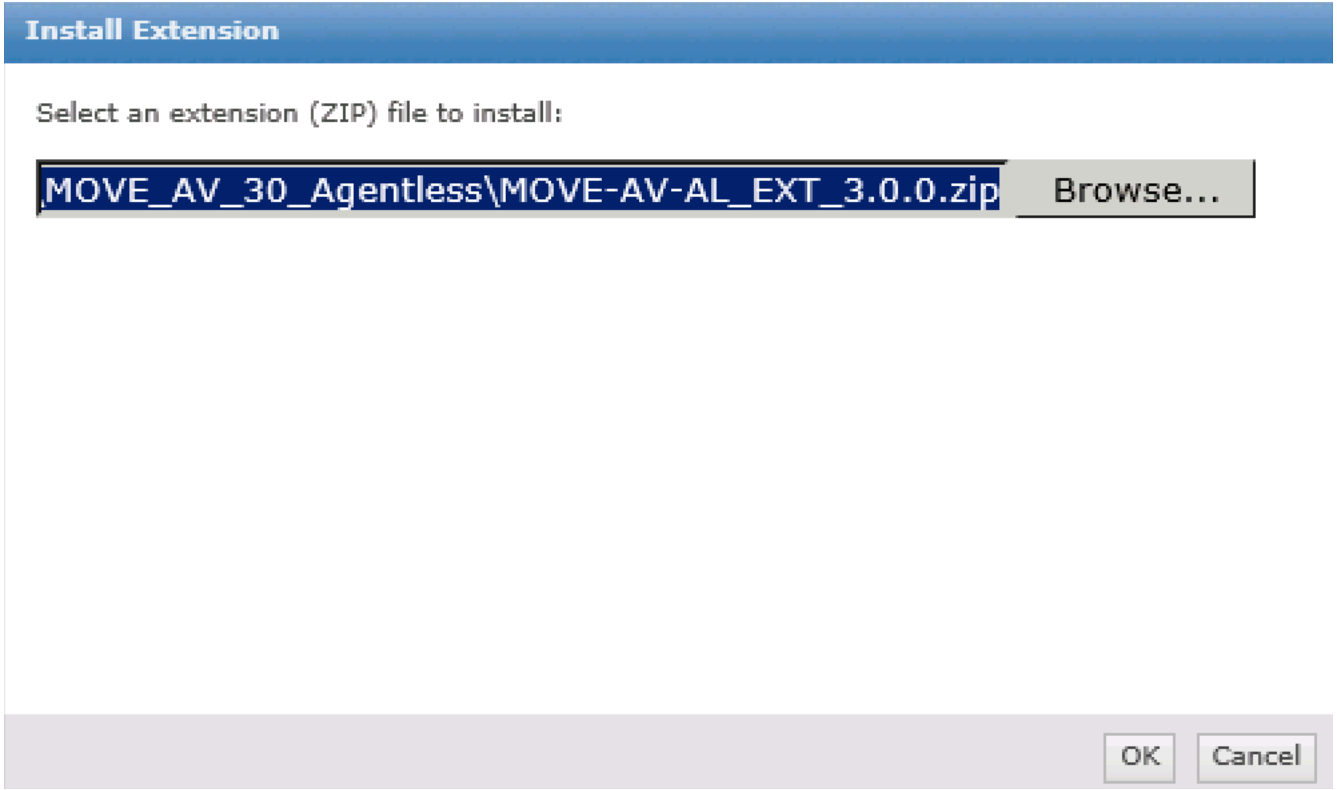
Increase threads



```
root@VNR-MSVA-01:~# cat /opt/McAfee/move/etc/svaconfig.xml
<?xml version="1.0" encoding="UTF-8"?>
<SVA>
  <Configuration>
        <GTI>
                <sndrecvtimeout>4</sndrecvtimeout>
                <steptimeout>9</steptimeout>
        </GTI>
        <EPSEC>
                <workerthreads>256</workerthreads>
                <maxeventsvm>16</maxeventsvm>
                <interfacename>eth1</interfacename>
                <readfileblocksize>128</readfileblocksize>
        </EPSEC>
        <DEBUG>
                <mvsvc>0</mvsvc>
        </DEBUG>
  </Configuration>
</SVA>
root@VNR-MSVA-01:~#
```

https://kc.mcafee.com/corporate/index?page=content&id=KB78947

Install extensions, Including Data Center Connector 3

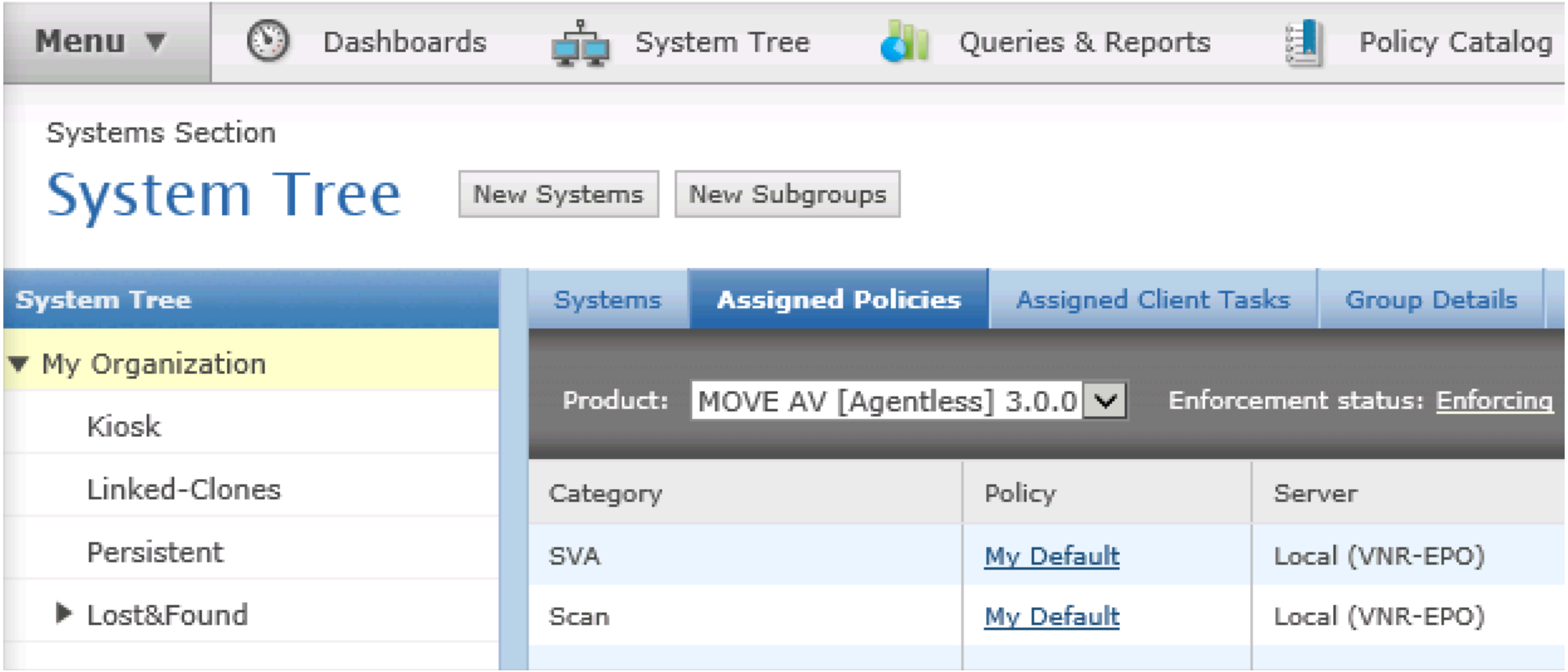


Install Extension

Select an extension (ZIP) file to install:

MOVE_AV_30_Agentless\MOVE-AV-AL_EXT_3.0.0.zip

Create 2 policies and assign to objects

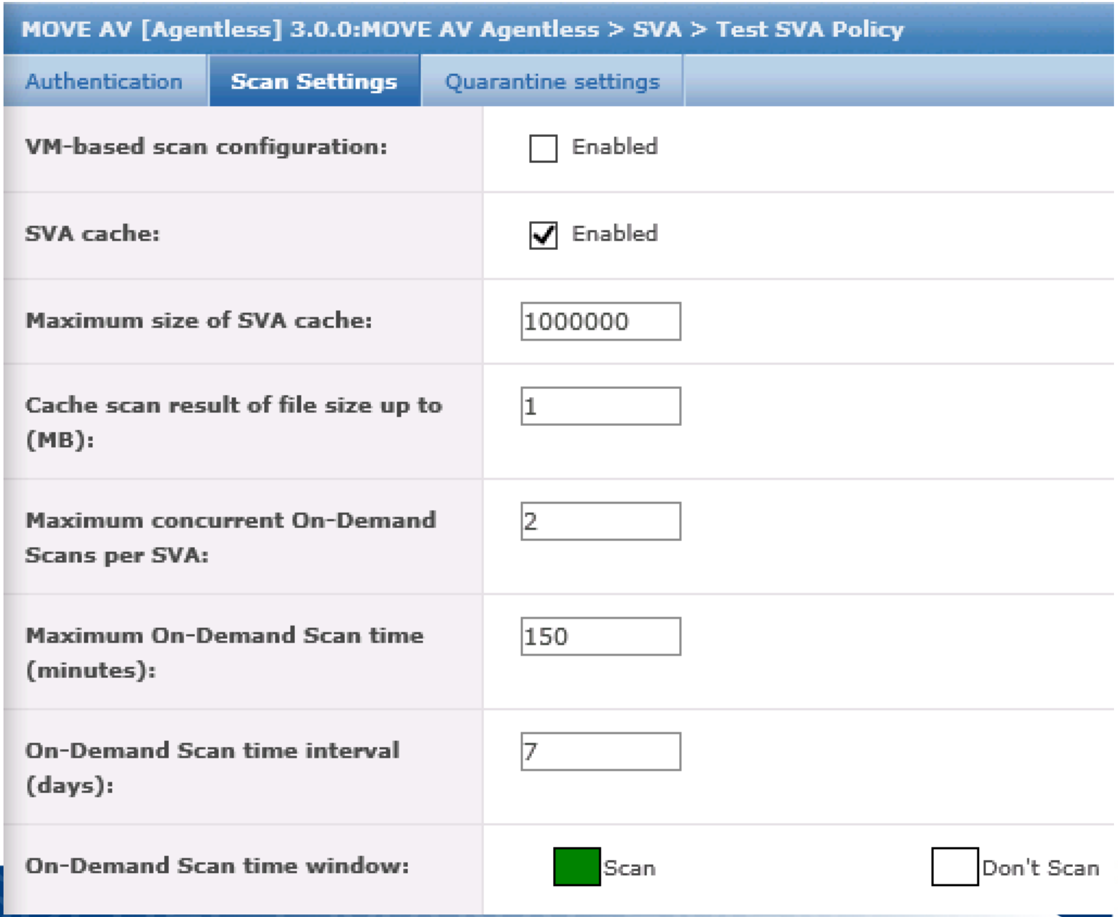


Product: MOVE AV [Agentless] 3.0.0

Enforcement status: Enforcing

Category	Policy	Server
SVA	My Default	Local (VNR-EPO)
Scan	My Default	Local (VNR-EPO)

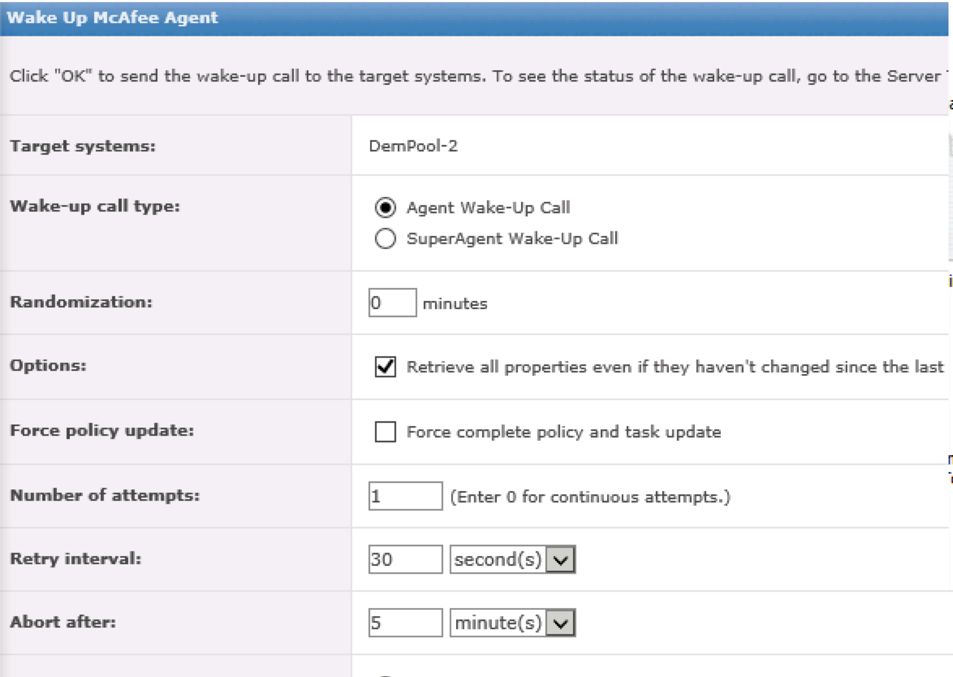
Enable VM based scan, install Data Center Connector 3!



MOVE AV [Agentless] 3.0.0:MOVE AV Agentless > SVA > Test SVA Policy

VM-based scan configuration:	□ Enabled
SVA cache:	☑ Enabled
Maximum size of SVA cache:	1000000
Cache scan result of file size up to (MB):	1
Maximum concurrent On-Demand Scans per SVA:	2
Maximum On-Demand Scan time (minutes):	150
On-Demand Scan time interval (days):	7
On-Demand Scan time window:	🟩 Scan □ Don't Scan

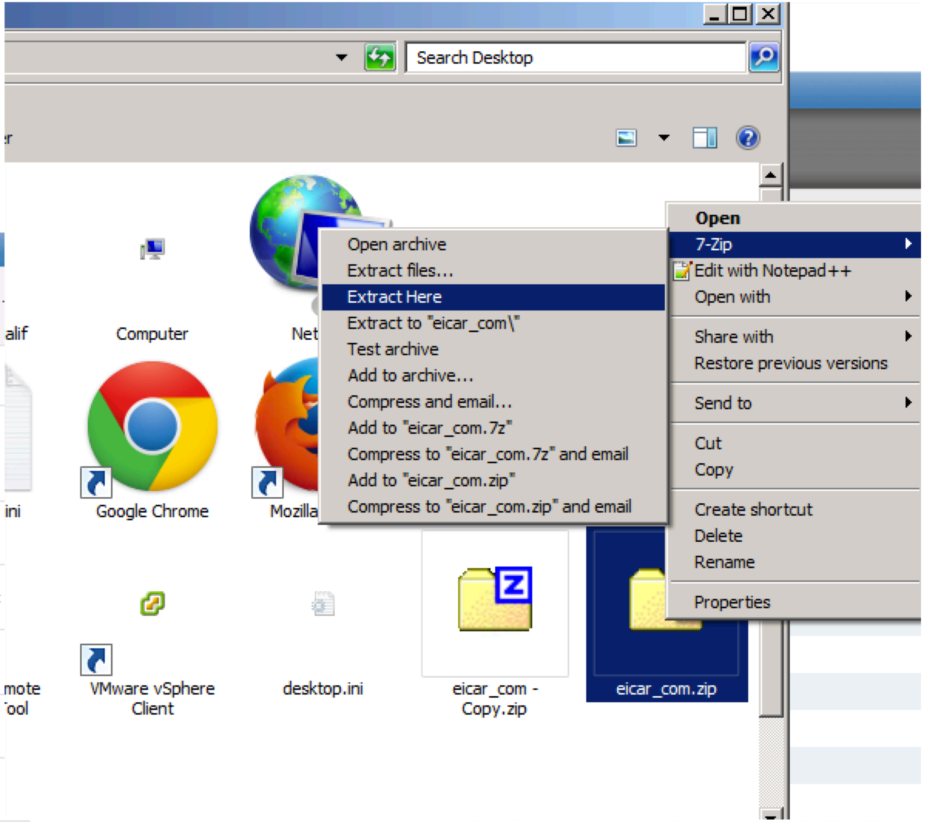
Wake up SVA and VM, then test with EICAR



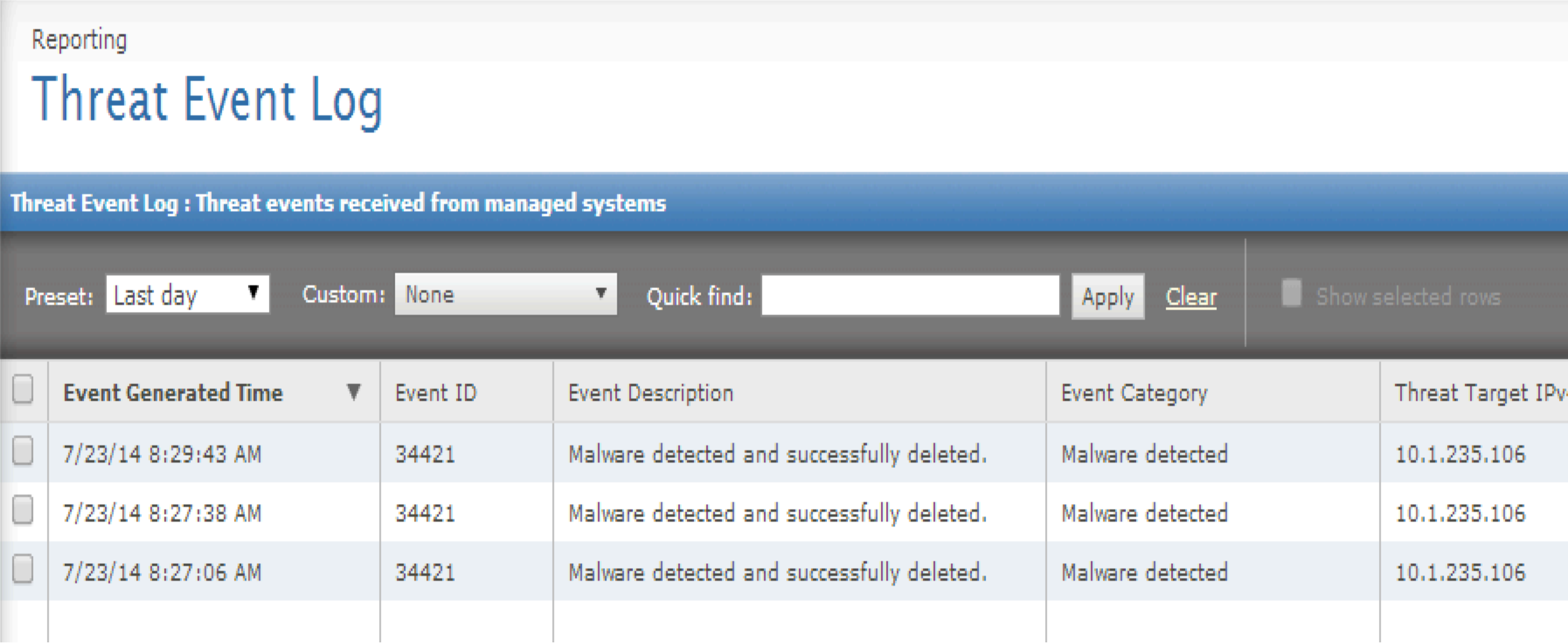
Wake Up McAfee Agent

Click "OK" to send the wake-up call to the target systems. To see the status of the wake-up call, go to the Server

Target systems:	DemPool-2
Wake-up call type:	● Agent Wake-Up Call ○ SuperAgent Wake-Up Call
Randomization:	0 minutes
Options:	☑ Retrieve all properties even if they haven't changed since the last
Force policy update:	□ Force complete policy and task update
Number of attempts:	1 (Enter 0 for continuous attempts.)
Retry interval:	30 second(s)
Abort after:	5 minute(s)



If successful, in 5-30 min will see messages in log



Reporting

Threat Event Log

Threat Event Log : Threat events received from managed systems

Preset: Last day ▼ Custom: None ▼ Quick find: Apply Clear □ Show selected rows

□	Event Generated Time ▼	Event ID	Event Description	Event Category	Threat Target IPv
□	7/23/14 8:29:43 AM	34421	Malware detected and successfully deleted.	Malware detected	10.1.235.106
□	7/23/14 8:27:38 AM	34421	Malware detected and successfully deleted.	Malware detected	10.1.235.106
□	7/23/14 8:27:06 AM	34421	Malware detected and successfully deleted.	Malware detected	10.1.235.106

IV. Trend Deep Security Tips

- Before installing vShield service on each ESX host, make sure the vCenter VM is NOT on that host. Install, then move vCenter back. Same w/Filter driver.
- Do NOT assign a Security Profile to the Deep Security Manager VM itself (even though there IS one). Otherwise, you will get “Anti-Malware Driver Offline”
- You CAN apply the DP Virtual Appliance Profile to each VA
- Shut down Manager first, then SVAs. Start SVAs first, then manager.
- vShield modifies the VMX file – be aware if you move VM to non-vShield environment.

IX. McAfee MOVE Agentless Tips

- No filter driver – no reboot of ESX is necessary to deploy!
- To deploy the SVA to a hypervisor with a distributed switch (vDS), at least two ESX servers must be connected to the vDS
- Manually disable VMotion on SVAs.
- Only do Script based deployment for Clustered installs and installs with many ESXi servers.
- From the ePolicy Orchestrator console, deploy a policy with a category of Scan – real time. SVA category (scheduled scan) is less important, but still necessary to configure.

Thank you!

- I would like to thank Chris Ruotolo, Will Chin, Jose Restrepo, Richard Agnew, Jeroen van de Kamp, Ryan Bijkerk, Ruben Spruijt & ProjectVRC for help with this presentation.

Contact Info & Questions

Please give feedback – it helps me come back.

Get the slides in on my work blog:

www.cdillc.com/newsroom/cloud-giraffe

Connect with me on LinkedIn: Yury Magalif

Twitter:

@YuryMagalif

@CDILLC

Personal Blog: cloud-zebra.com

E-Mail Questions:

okzebra@gmail.com

yury.magalif@cdillc.com

YouTube:

www.youtube.com/user/ym640

CDI COMPUTER DESIGN & INTEGRATION LLC