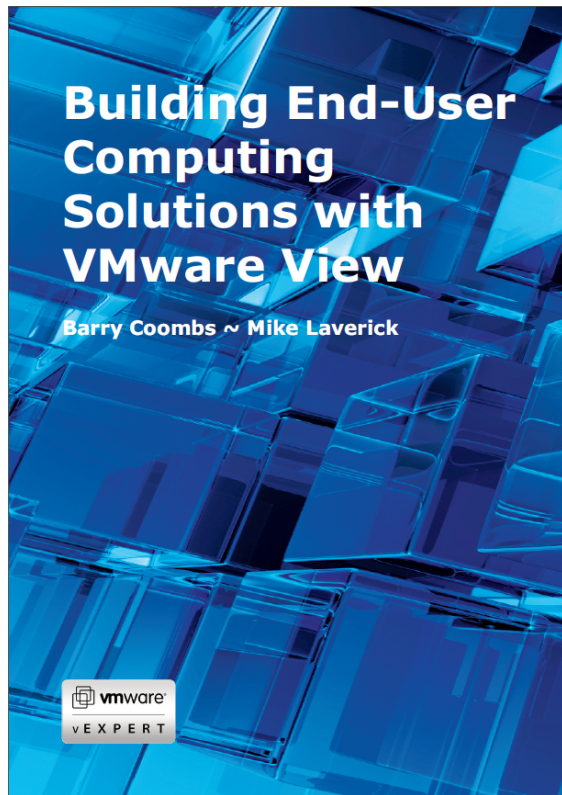


For the complete book please visit:



www.eucbook.com

Chapter 23: VMware vShield End-point

Introduction

There are many security technologies available in the market, and not to be outdone VMware has its own called “vShield”. It’s quite a broad technology that has applications above and beyond the topic of this book – virtual desktops. For example vShield forms a critical part of VMware’s “vCloud Director” their cloud automation platform. In that case vShield allows for vSphere and vCloud Director to support a secure multi-tenancy model where every organization within its boundaries resides in its own network bubble.

In terms of VMware Horizon View, vShield can contribute to improving the user experience and overall scalability of the View Infrastructure by offloading anti-virus workloads to vShield. A good analogy for this resides in the arena of backup. In the early years of virtualization many companies persisted in install backup agents to VMs and treating them the same as physicals – in fact this approach persists to this day. Unfortunately, doing so puts an unnecessary CPU and network load on the ESX host. It’s perhaps more sophisticated and efficient to backup outside of VM – or so-called VM Backup. You could say vShield Endpoint is doing the same for AV that VM Backup pioneered by the likes of VizionCore (now part of Quest Software, now part of Dell!) and Veeam did for backup. Sadly, there’s little in the way of truly independent comparisons between traditional in-guest agent-based AV and vShield – with nearly all the reports being sponsored in some shape or form by the vendors. But if you are looking for good summary the Tolly Group often have this type of compare/contrast data. A good place to start looking is here:

<http://blogs.vmware.com/security/2011/03/security-conference-followup.html>

Some of the performance information is now out of date since the 5.0 and 5.0.1 release of vShield that introduce architectural changes that should improve these base performance figures.

vShield is available in number of formats individually in an “a la carte” fashion or it can be procured as an all-in-one purchase. These are individual components:

- **vShield Manager**
“Installs” as virtual appliance and optionally can be registered with vCenter – it acts the central management point for different functions of vShield App
- **vShield App**
Firewall capabilities with the ability to set policies based on objects within

the inventory of vCenter

- **vShield App with Data Security**

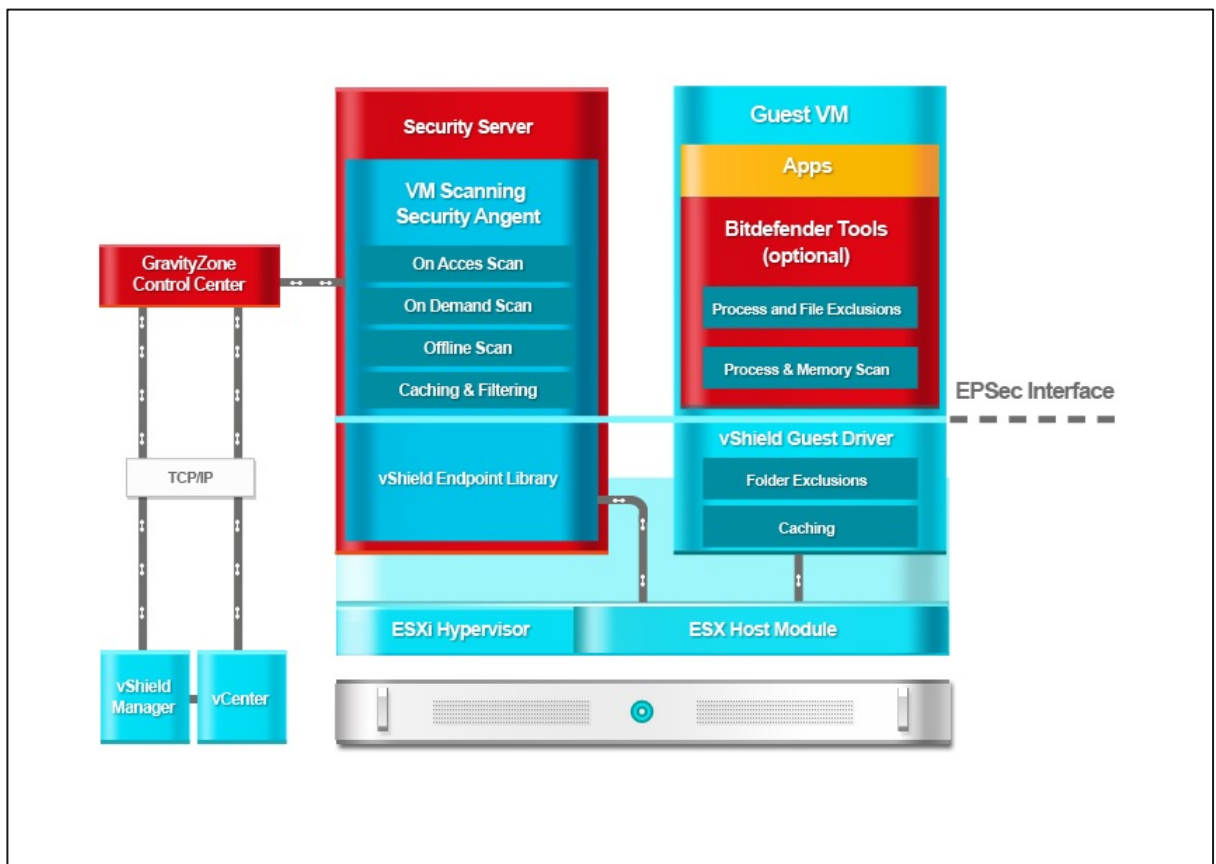
As above but adds inspection of sensitive data based on violations reported by the appliance.

- **vShield Edge**

Provides network security for applications such as vCloud Director and comes with common network components such as DHCP, VPN, NAT and Load-balancing

- **vShield Endpoint**

Offloads anti-virus and anti-malware to dedicate virtual appliance. The appliance is always on updating signatures made available via VMware's 3rd party partners. Protects VMs that are powered on, and automatically updates powered off VMs with new signatures when they powered back on. It ships as a virtual appliance together with a "hypervisor" module that is loaded by the ESX VMkernel. This works in harmony with what's called the "Security Virtual Machine" or SVM. This is provided by third-party to VMware such as Trend Micro or Bitdefender.



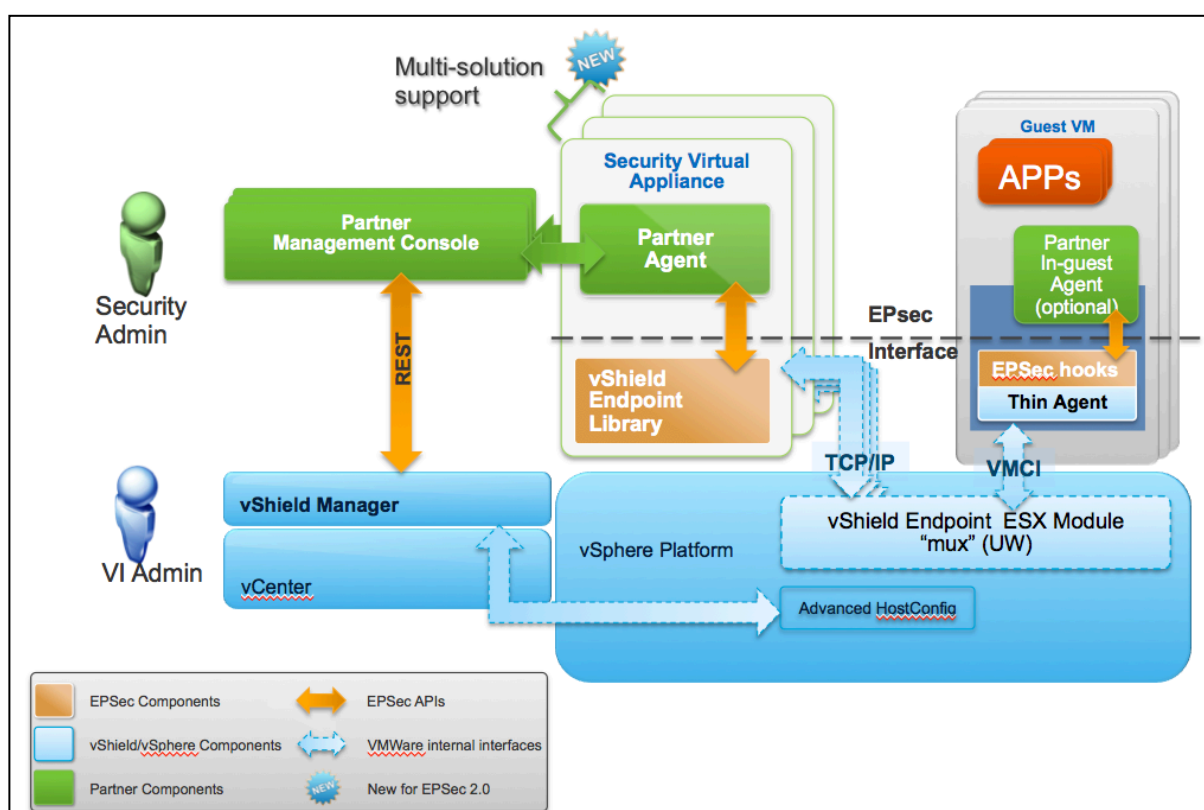
Note: This diagram is taken from Bitdefender's website. Bitdefender "Security for Virtual Environments". It's quite a good graphic because it shows both the VMware and third-party together. So you can see that vShield and the 3rd party management console both speak to vCenter. vShield

Manager assists in installing the “vShield Guest Driver” and VMware Tools includes the “vShield Endpoint Driver” on each VM.

One of the jobs of the third-party Security Console is to aid in the deployment of its Security Virtual Appliance) to each ESX host. The guest operating systems such as virtual desktops can contain optionally a “Bitdefender Silent Agent” that provides the user with an interface to check their protection status. There’s been a little of change in terminology in the recent release with this “silent agent” now merely being referred to as a “client” or “BDTools”.

vShield and its version numbers is how customers reference the product. Between VMware and its partners a separate name is used called “EPSEC” API. vShield 1.0 used EPSEC 1.0 and vShield 5.0 uses EPSEC 2.0. This can be somewhat confusing if the partner your working with refers to the EPSEC version numbering scheme. It’s perhaps best to stick with the vShield numbering, and just confirm that the version of vShield you intend to use is compatible with your version of the vSphere platform you are using.

Below is a more vendor neutral diagram of the EPSEC 2.0 implementation from VMware:



From the guest operating system perspective an endpoint driver is installed into the virtual desktop, which communicates to an “ESX module” on the ESX host called the the “Mux” (Multiplexer). The ESX host moves information from the VMCi layer into the TCP stack, and communicates via an internal vSwitch into the Security Virtual Appliance (SVA). This means that communication is discrete and secure and neither the SVA or the VM needs to be exposed to the internet for virus definition downloads, scans or remediation.

This new structure allows vShield to run with more than one partner on the same ESX host. This is inline with VMware's cloud and multi-tenancy model where multiple tenants in the cloud may prefer to use one AV vendor over another. Additionally, within a partner they may want in future to have separate virtual appliance (VA) for each security function – like a VA for AV, a VA for encryption and so on.

As you might expect most of the AV vendors provide much the same features such as on access and on demand scanning. The biggest variance appears to be what they do if they encounter a virus. This generally reflects their own position on what to do if a virus is encountered. They each have their own ideological view point, and this often reflects how they have handled viruses before virtualization became mainstream.. So some will delete an infected file, whilst some will quarantine it – others might attempt to clean-up the file. They also seem to compete around who has the best caching and filtering algorithms and tools – to reduce the burden of checking files that have been checked before, or files that are to be ignored by the scanning process. Others compete by saying they learn of new viruses quicker than their competitors, and therefore can offer more protection from rapidly spreading dangers.

Hardware and Software Requirements

To get started you need at least one vShield Manager for each vCenter – vShield App and Endpoint require on virtual appliance for each ESX host in the cluster – and one vShield Edge per portgroup on a virtual switch. Our focus will merely be on the configuration of vShield Endpoint – but we've chosen to include the requirements for all the features just in case you decide to adopt vShield in your wider environment.

The other thing you will need is a Security Virtual Appliance (SVA) from a 3rd party anti-virus provider. That can be a little tricky as there isn't a huge number of them – if you are just wanting to evaluate vShield Endpoint, most of the 3rd parties do not allow you to just drop along to their website and download. Most times you will have to register and then be checked out. This is to ensure you get proper support during the evaluation, and ensure you don't get a false impression of the quality of the implementation – that is more a reflection of your ignorance. That's what they say. Hopefully sales people won't harangue you!

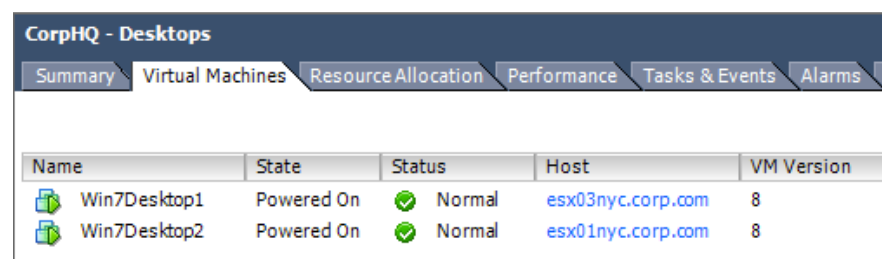
The SVA is a virtual appliance that interfaces with the vShield Virtual Appliance and normally incorporates its own web front-end often referred to as the Security Virtual Console (SVC). This SVC can be used to deploy many SVA's to each ESX host. Many vendors also incorporate an optional "agent" that can be installed into the virtual desktop. Strictly speaking this not required, but some

times end-user like the reassurance of being able to see their security status, as they would with a conventional AV client that has been installed to the guest operating system

All the vShield components need 8GB of memory each – that includes the manger and components like App, Edge and Endpoint. The vShield Manager needs 8GB of disk space, and each vShield App and Edge requires 5GB and 100MB of disk space respectively. VMware recommend at least two 2Gps VMnics teamed together provide network redundancy to the appliances themselves.

The current edition of vShield is compatible with vCenter 4.x Update 2 and ESX 4.0 update 2 – however in the context of this book that has been based on vSphere5, both vShield Endpoint and vShield Data Security require ESXi 5.0 Patch 1. Additionally, both Endpoint and Data Security require the VMs have hardware version 7 or 8, and that VMware Tools is up to date with on version 8.6.0 or higher which was released with ESXi 5.0 Patch 1.

You can confirm the VM hardware level by adding the “VM Version” column to the virtual machine tab in vCenter, or by editing the VM’s settings in vCenter. If you are not using the “Linked Clones” feature you will need to modify you template that is used as the source for deploying new desktops.

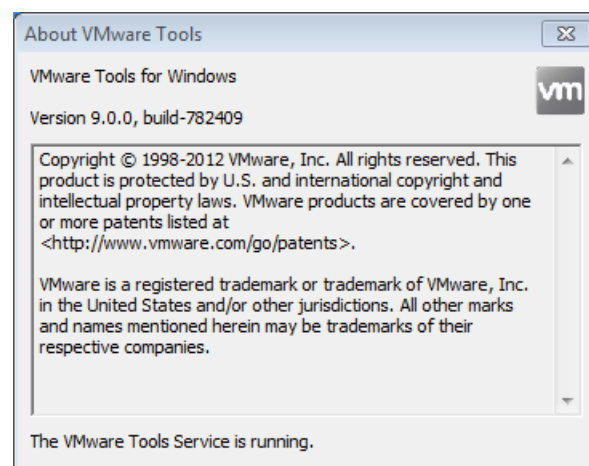


The screenshot shows the vCenter interface for a pool named 'CorphQ - Desktops'. The 'Virtual Machines' tab is selected. A table lists two VMs: Win7Desktop1 and Win7Desktop2. Both are powered on and running Windows 7 (VM Version 8) on ESX hosts.

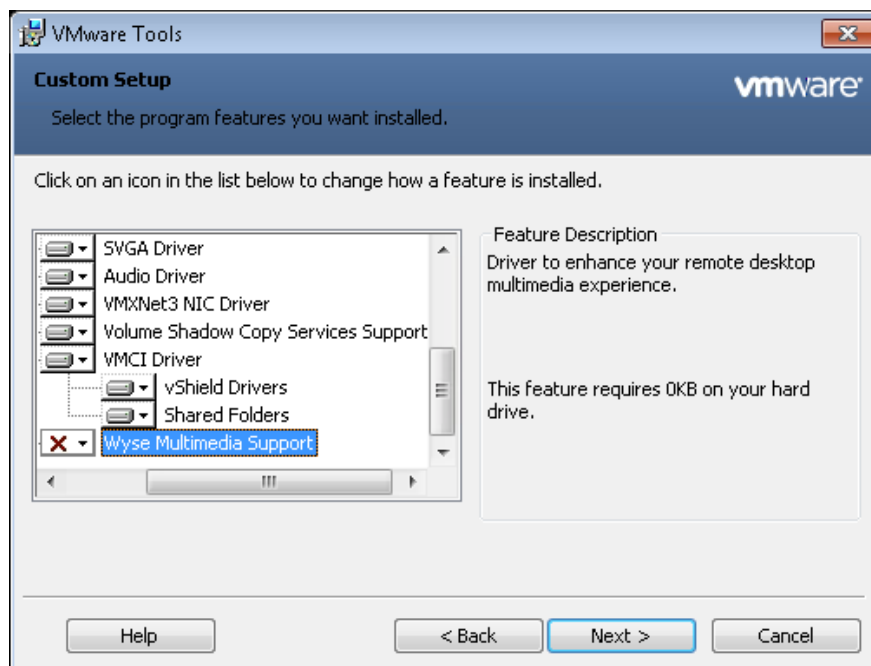
Name	State	Status	Host	VM Version
Win7Desktop1	Powered On	✓ Normal	esx03nyc.corp.com	8
Win7Desktop2	Powered On	✓ Normal	esx01nyc.corp.com	8

Note: As you can see in our case we discovered the Accounts Desktop pool was running Windows 7 under version hardware level 7, rather than vSphere5 native hardware level version 8. We decided to upgrade the “Parent VM”, and the refreshed the linked clone virtual desktop manager.

You can confirm the VMware Tools version the toolbox application that sits in the virtual desktop icon tray in Windows.



Additionally, the vShield Endpoint system requires a driver that's now installed as part of VMware Tools, if you use complete it will be installed and if you use "Custom" you have the option to install under +VMware Device Drivers, + VMCI Driver and "vShield Driver". We would recommend incorporating it into your templates and parent VMs for linked clones. The vShield Driver is often supplemented with what's referred to as vendor's "Silent Agent" and is available to download from the 3rd party vendors website. For example Bitdefender has both 32-bit and 64-bit Silent Agents available for Windows.



Note: The build number shows we are within the requirements within the virtual desktop. Incidentally, the vShield Appliance obviously uses VMware Tools – but VMware's own "Quick Start" guide indicates you should leave those well alone and not attempt to upgrade them. This driver was included in VMware Tools relatively recently – occasionally you will see some vendor documentation that talks about the "Thin Driver" or the "Thin Agent" needing to be installed. That's a little out of date, as since vSphere5 this is now included as part of VMware Tools and is now referred to as the vShield Driver. In previous versions of vShield the driver was SCSI based, and only worked with the LSI Controller inside a VM, and this caused implementation problems with guest operating systems that default to different controller types such as Windows 2000 defaults to using a BusLogic Driver. Starting with vShield 5.0, VMware switched to using their Virtual Machine Communication Interface (VMCI) model. Initially, VMCI was meant to allow for direct VM to VM communication without the need for conventional TCP networking. In new versions of VMCI the intention is just to allow for secure communication between the host and the VM. The main purpose of this driver is to allow for scanning of the VM's virtual disk via the third-party vendors appliance. This driver is no longer distributed alongside the download for vShield (as it was in vShield 1.0) as it is now included in VMware Tools.

The end-point driver is called vsepflt.sys is a File System Filter Driver (FSFD) and does not run as a service. If you want to check that it is installed and present you can use "fltmc" to confirm it is loaded. This FSFD uses VMCI to speak to the ESX module inside the hypervisor – and the ESX module is silently installed in turn by using the vShield Management Console to all the hosts that will support vShield Endpoint functionality.

```
ca. Administrator: Command Prompt

C:\Users\Administrator.CORP>fltmc

Filter Name                               Num Instances  Altitude  Frame
-----
UMWUpfsd                                5             386200    0
vsepflt                                 8             328200    0
bdsum                                    8             320830    0
luafo                                    1             135000    0
FileInfo                                8             45000     0

C:\Users\Administrator.CORP>
```

Note: fltmc shows that the vsepflt.sys drive has been loaded into the guest operating system.

Importing the vShield OVA File

The setup of vShield begins with downloading the single .OVA file that contains the appliance itself. Once download it can be imported into vCenter, and set to run on your chosen VMware Cluster.

Each component of vShield needs to be installed – and sadly there is not a “bulk method” to do this at a cluster level which is a shame. It is possible to automate a great deal of the vShield configuration. That’s something we have chosen not to document in this instance. However, if its matter that’s of interest to you we would recommend checking out two blog post from PowerCLI supremo and VMware employee, Alan Renaud:

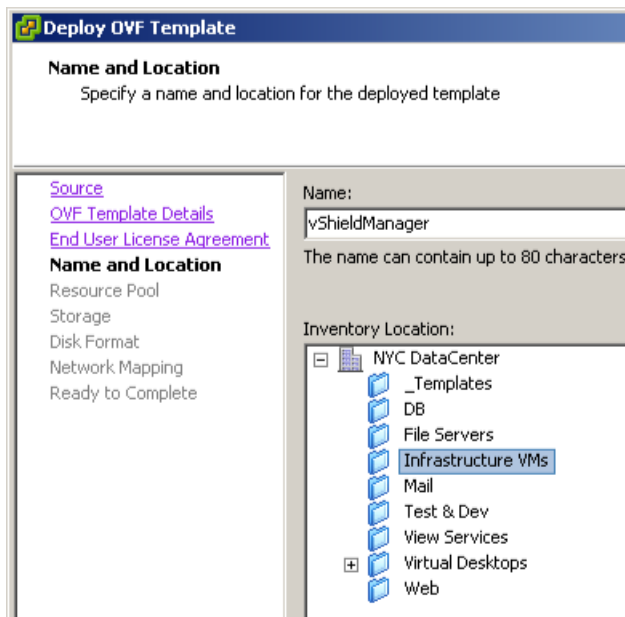
<http://www.virtu-al.net/2012/01/04/vmware-vshield-powershell-module/>

This introductory post to separate posts:

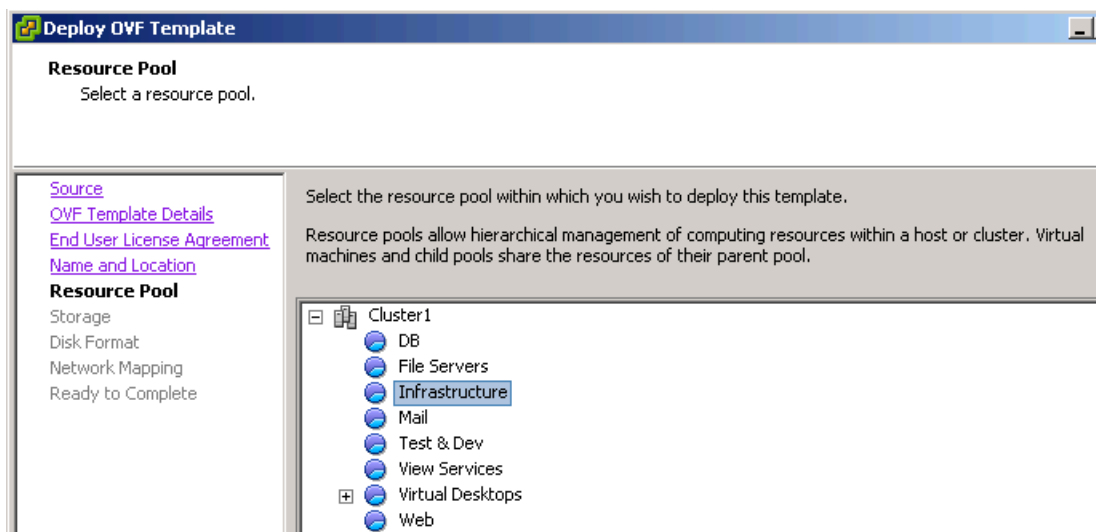
<http://www.virtu-al.net/2011/09/14/powershell-automated-install-of-vshield-5/>

<http://www.virtu-al.net/2011/09/30/automated-install-of-vshield-services/>

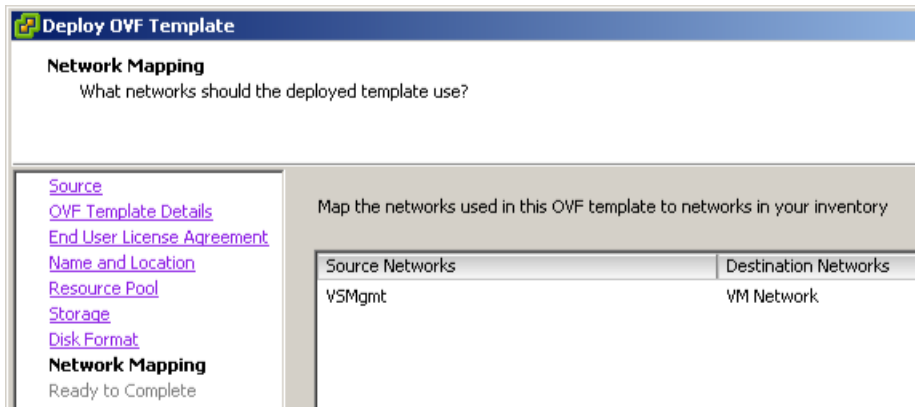
1. From within vCenter, select **File** and **Deploy OVF template**
2. **Browse to locate the OVA file** in our case called “VMware-vShield-Manager-5.0.0-473791.ova”. You build number is likely to vary
3. Click **Next** to accept the description
4. Click **Next** to accept the EULA
5. **Set the vShield Manger name for the vCenter Inventory and folder location** – in our case we place the manager in the “Infrastructure” folder.



6. Next **select a cluster and/or a resource pool** for the appliance to reside



7. Next **select a datastore** to hold the appliances virtual disks
8. Next **select a type of virtual disk**
9. Finally, **select an appropriate portgroup on a virtual switch for the appliance** – remember that the appliance needs to communicate to vCenter and the ESX hosts



Configure IP Settings

Once the appliance has booted you can configure its network settings fit for your environment. After the boot process you will be challenged for the **"admin"** login together with its **default** password. Once authenticated you switch to **"enable"** mode with its **default** password that allows you to run the core setup routine.

1. Open a console window to the vShield Manager, and login as **"admin"** with the password of **"default"**
2. Next type the string **"enable"** and supply the password at the prompt which is **"default"**

```
Manager login: admin
Password:
manager> enable
Password: _
```

Note: If you can't login with the default password chances are you experiencing some latency or keyboard repeat on your console session. This happens particularly when you're connecting remotely to vSphere environment over say a Microsoft RDP link. Consult KB196 for changing the default keyboard repeat values for console sessions.

3. Next type the command **"setup"** to run the network setup wizard
4. Next configure your IP settings relative your management network

```
Manager# setup

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

IP Address (A.B.C.D): 192.168.3.144
Subnet Mask (A.B.C.D): 255.255.255.0
Default gateway (A.B.C.D): 192.168.3.1
Primary DNS IP (A.B.C.D): 192.168.3.130
Secondary DNS IP (A.B.C.D): 192.168.4.130
DNS domain search list (space separated): corp.com
Old configuration will be lost
Do you want to save new configuration (y/[n]): y_
```

5. This will leave you with somewhat odd report that the management NIC is up, and if you press [**ENTER**] will return you to the Manager# prompt. You can logout using the command **"exit"** – and either log back in a ping

the router/default gateway – or better still confirm you can ping the appliance from your management PC.

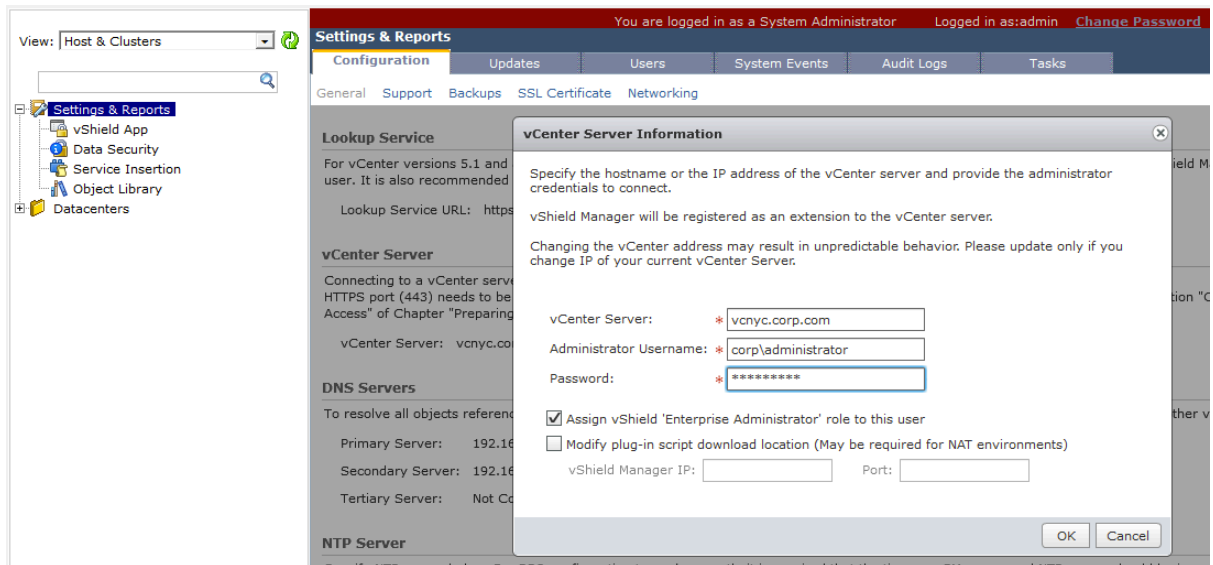
Register with vCenter; Reset Password; License

The next step is using the web-based management front-end of vShield – login as admin and default, and configure vShield to be aware of your vCenter environment.

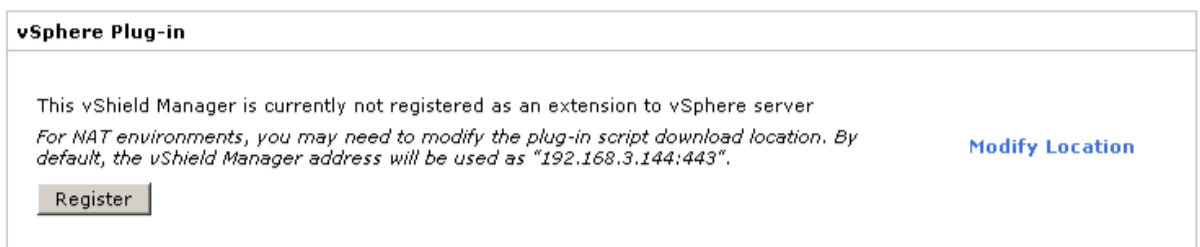
1. Open a web-browser session and type <http://a.b.c.d> where a.b.c.d was the static IP address you configured earlier
2. Login to the vShield using “**admin**” and “**default**” as the username and password respectively



3. After the login you should be transitioned to the “**Settings and Reports**” page, where you input your vCenter credentials. We recommend NOT using the “administrator” account, but instead establish a system of authentication specifically created for vShield itself.



4. Click **Save**, will cause vShield to communicate to vCenter – and you should be confronted with an SSL Thumbprint dialog box, if you are using the built-in certificates from vCenter.
5. You can use the “**Register**” button to add the vShield Plug-in to vCenter – this allows you do 99% of your administration tasks directly from vSphere.



This should generate a plug-in SSL dialog box which is typical of newly enable vSphere Client plug-ins. You can enable the option to “Install this certificate and do not display any security warnings for your IP” and click Ignore. Unless of course, you’re Edward Haletky who never accepts any unsigned or untrusted certificate. ☺

This adds a vShields icon to the “Solutions and Applications” section of the vSphere Client and opens the web-interface of vShield into the vSphere Client. It also enables a tab within vCenter on each cluster and ESX host that allows you to see the status of the vShield components and install the vShield components to the ESX hosts.

Cluster1					
Summary	Virtual Machines	Hosts	DRS	Resource Allocation	Performance
Tasks & Events	Alarms	Permissions	Maps	Profile	
General Endpoint					
Host Information					
Name	User VMs	Service VMs	App Enabled	Endpoint Enabled	Data Security Enabled
esx03nyc.corp.com	12	0	No	No	No
esx02nyc.corp.com	16	0	No	No	No
esx01nyc.corp.com	10	1	No	No	No

Note: Here the "Service VM" is the vShield Manager appliance itself.

- Once configured for vCenter – the web-interface should be able to enumerate your inventory from vCenter like so:

View: Host & Clusters

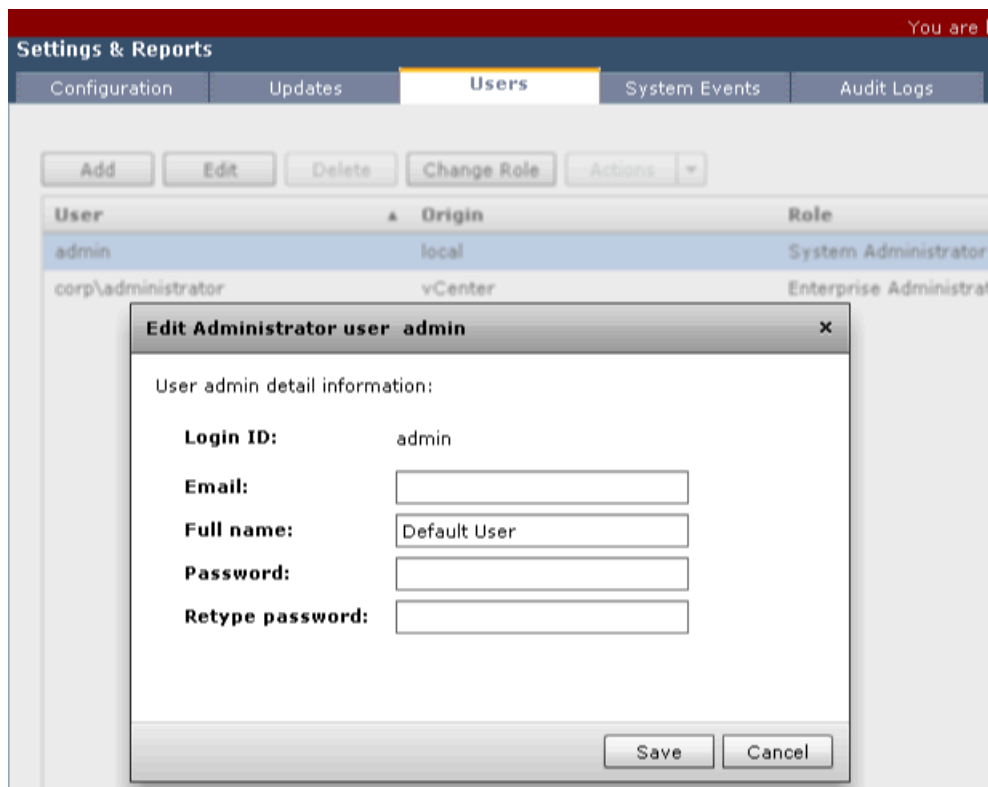
Settings & Reports
vShield App
Data Security
Service Insertion
Object Library
Datacenters
NYC Datacenter
Gold
Silver

You are logged in as a System

Datacenters
Summary

Manager IP Address	Cluster Name	vShields	IP Address
192.168.3.133		TOTAL (for the System)	

- Finally, you can **reset the password for the "admin" account within the "users" tab**. Running a security appliance with a known user accounts with password in the public domain isn't not perhaps a wise management decision – so change the password at the earliest opportunity

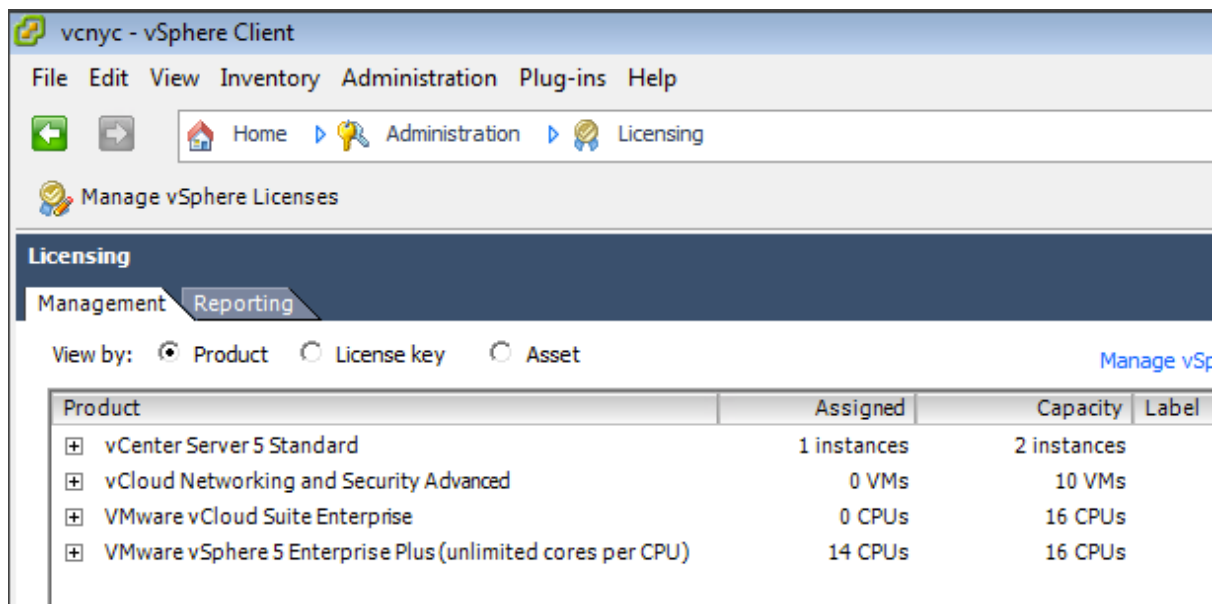


8. By default vShield will run for 60-days in an evaluation mode with some scalability limits imposed (limited to protection 100 VMs). After 60-day period expires the appliance will no longer power on vShield App or Edge appliances or protect VMs. **The licensing of vShield is managed from the very same "licensing" interface in vSphere that is used to license – ESX, vCenter and technologies such as VMware Site Recovery Manager.**

The screenshot shows the 'Licensing' interface with the 'Management' tab selected. The 'View by' dropdown is set to 'Product'. The table below shows the following data:

Product	Assigned	Capacity	Label	Expires
[-] Evaluation Mode	3	Unlimited		
[-] (No License Key)	3	Unlimited		
[-] vShield-App				14/05/2012
[-] vShield-Edge				14/05/2012
[-] vShield-Endpoint				14/05/2012
[+] vCenter Server 5 Standard	2 instances	2 instances		
[+] vCenter Site Recovery Manager Enterprise	0 VMs	100 VMs		
[+] VMware vSphere 5 Enterprise Plus (unlimited co...)	9 CPUs	16 CPUs		

Note: This screen grab shows licensing before the advent of the "vCloud Suite" licensing. With the advent of vSphere 5.5 you will see the new name for vShield as vCloud Network and Security (vCNS)

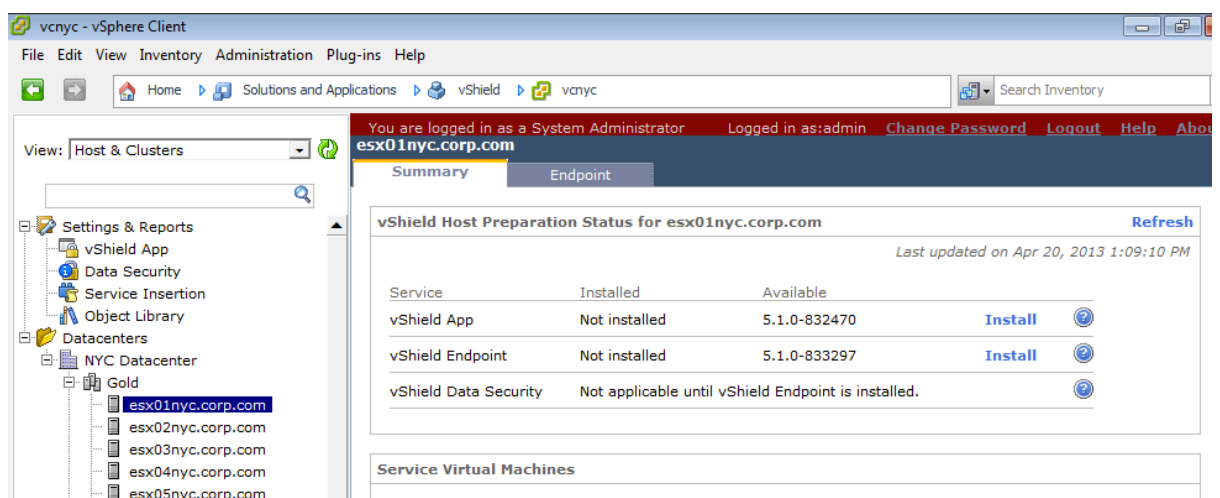


vShield is licensed to protect a certain number of VMs, and most of the third-party vendors have followed suit – although some do still license their technology on a per-CPU basis. vShield is bundled with number of SKUs such as View Premier, and some of the OEM partners have the rights to resell vShield alongside their own components. It really varies from one OEM partner to another.

Installing vShield Endpoint to the ESX host

The next stage is installing the vShield “Host Driver” – this component sits inside the ESX host and interacts with the VMKernel hypervisor.

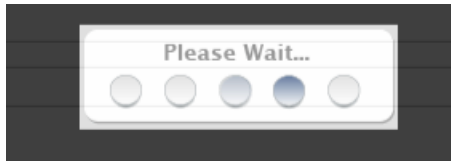
1. You can locate the ESX host in the vShield Inventory, and in the Summary Tab locate the “**Install**” button for the Endpoint Driver.



Note:

When you do this – you will see a number of “Please Wait” messages

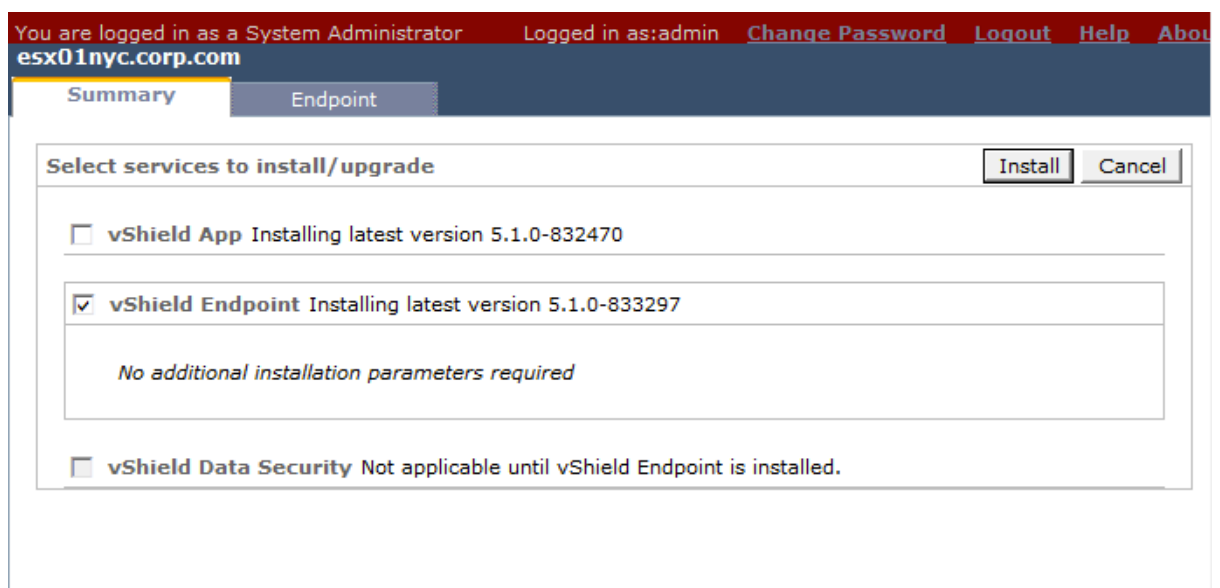
that will come, and go and then come back again. Do not be alarmed. All is well.



And as this happens – you will see events taking place in the Taskbar of the vSphere Client:

	Install		esx04nyc.corp.com
	Open firewall ports		esx04nyc.corp.com
	Add port group		esx04nyc.corp.com
	Add virtual NIC		esx04nyc.corp.com
	Add port group		esx04nyc.corp.com
	Add virtual switch		esx04nyc.corp.com

2. Next click the **Install** button:



3. At the end of the installation this status should change as can be seen below:

You are logged in as a System Administrator Logged in as:admin [Change Passw](#)

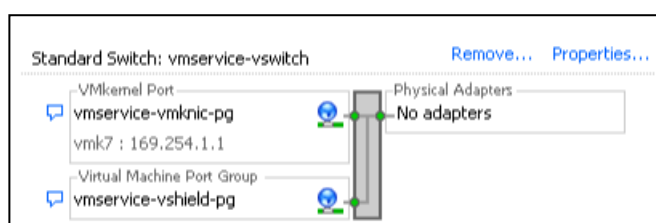
esx01nyc.corp.com

Summary Endpoint

vShield Host Preparation Status for esx01nyc.corp.com Last updated c

Service	Installed	Available	
vShield App	Not installed	5.1.0-832470	Install
vShield Endpoint	5.1.0-833297	-	Uninstall
vShield Data Security	Not installed	5.1.0.0-833296	Install

You should also see that the vShield has created the vmservice-vswitch in the Standard vSwitches view...



This configuration of vShield opens ports 48651 to 48666 on the ESX host firewall. Two rules are created one called "vShield-Endpoint-Mux" which covers these ports and enabled by default, and one called "vShield-Endpoint-Mux-Partners" which is disabled and be enabled by third-parties to install additional components to the ESX host if needed. The internal switch is used by the Partner's SVA to allow it to communicate to the user world components and on to the VMs.

Bitdefender Gravity Zone: Security 1.x for Virtualized Environments

Introduction

Bitdefender Security for Virtualized Environments (or SVE for short) is integrated to VMware vShield. It comes as two components – the management virtual appliance called the "Control Center" and with "Security Virtual Appliance" (SVA). There is one Control Center which manages the system overall and allows you to deploy the SVA to as many ESX hosts as you require. The Control Center includes an "Update Server" component this handles all the upgrade and signature updates. In contrast the SVA handles the scanning and protection of the VMs on each ESX host to which it is deployed.

Bitdefender supports Windows, Linux and Solaris – although at the time of writing support for Solaris has yet to be released. There is also support for an optional Bitdefender "Silent Agent" or "BDTools" that can be installed to any VM or virtual desktop

Import Bitdefender Control Center Virtual Appliance

WARNING:

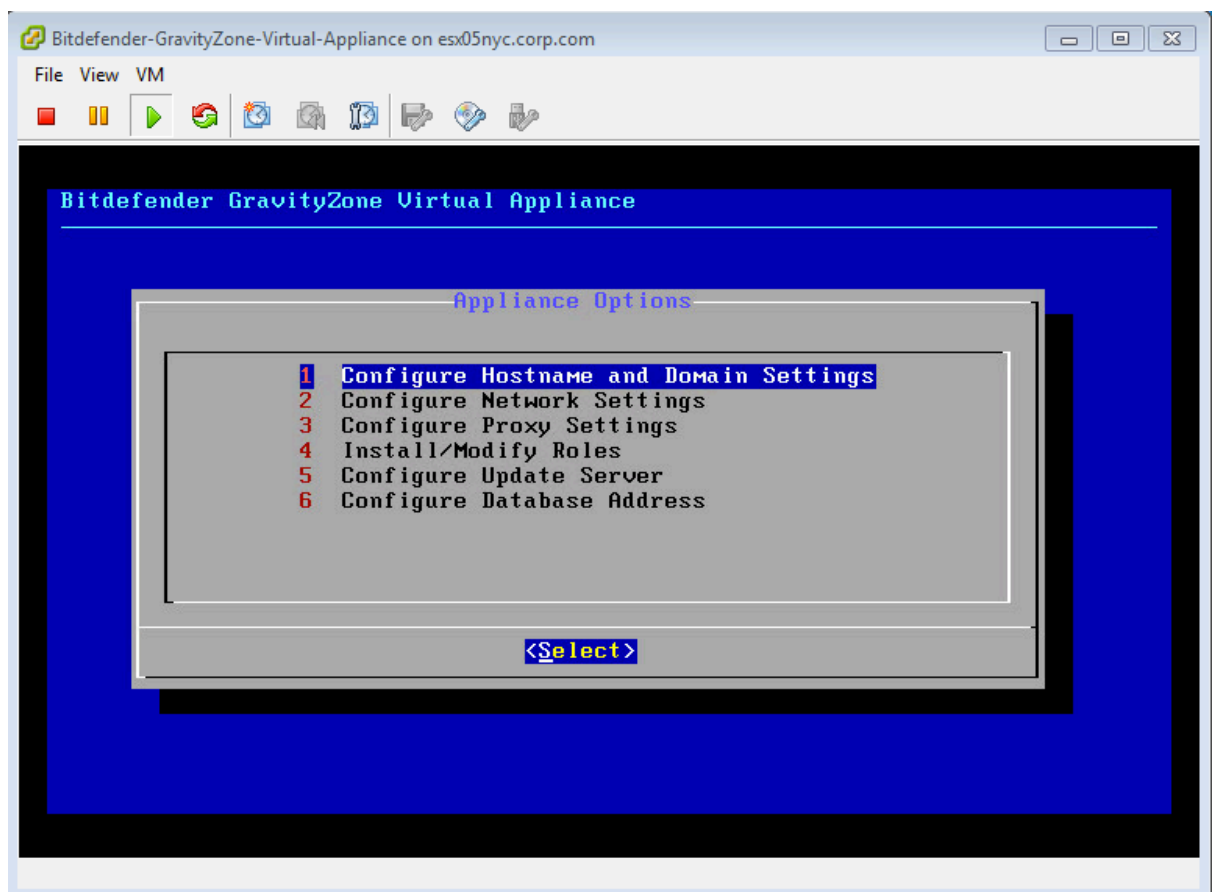
Currently Internet Explorer mishandles .OVA files. The .OVA format is in fact a .TAR zip format. Internet Explorer recognizes that the file is of an archive format, and automatically renames the file extension from .OVA to .TAR. To resolve this issue simply rename the extension. At the time of writing we understand that only Internet Explorer treats .OVA files in this way.

In our case we contacted Bitdefender to gain access to their implementation. We cannot speak for how other vendors work with vShield as this is merely an introduction to the process. With the Bitdefender it ships as an .OVA that needs to be imported into vCenter – and process is very similar to import of the vShield .OVA.

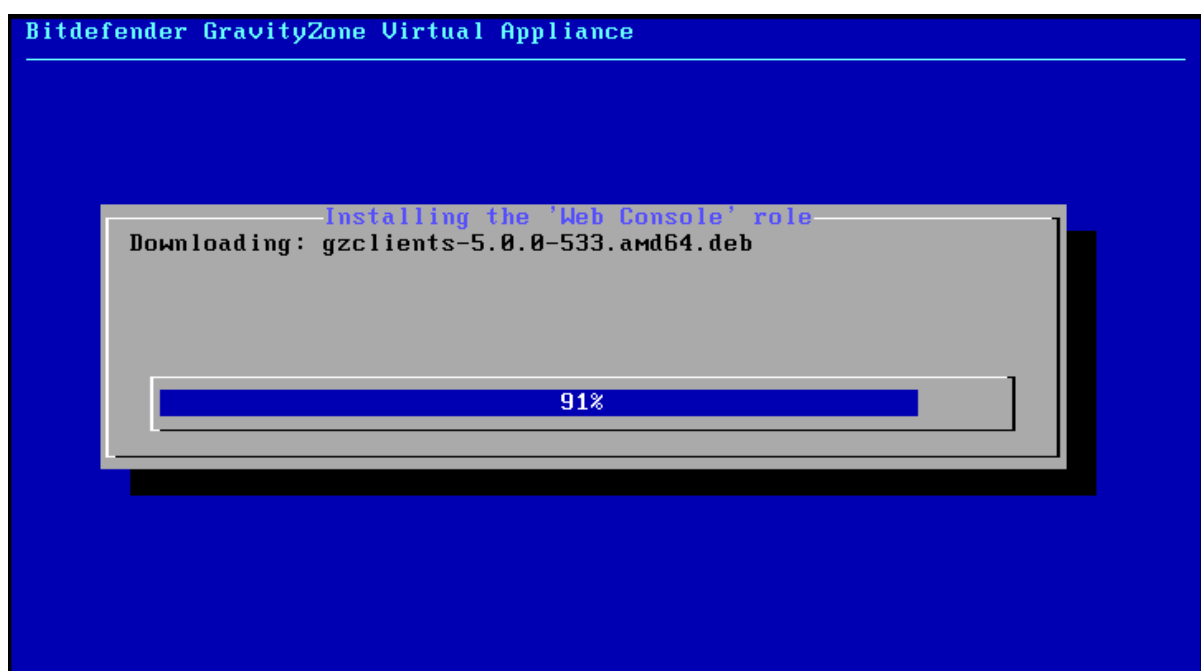
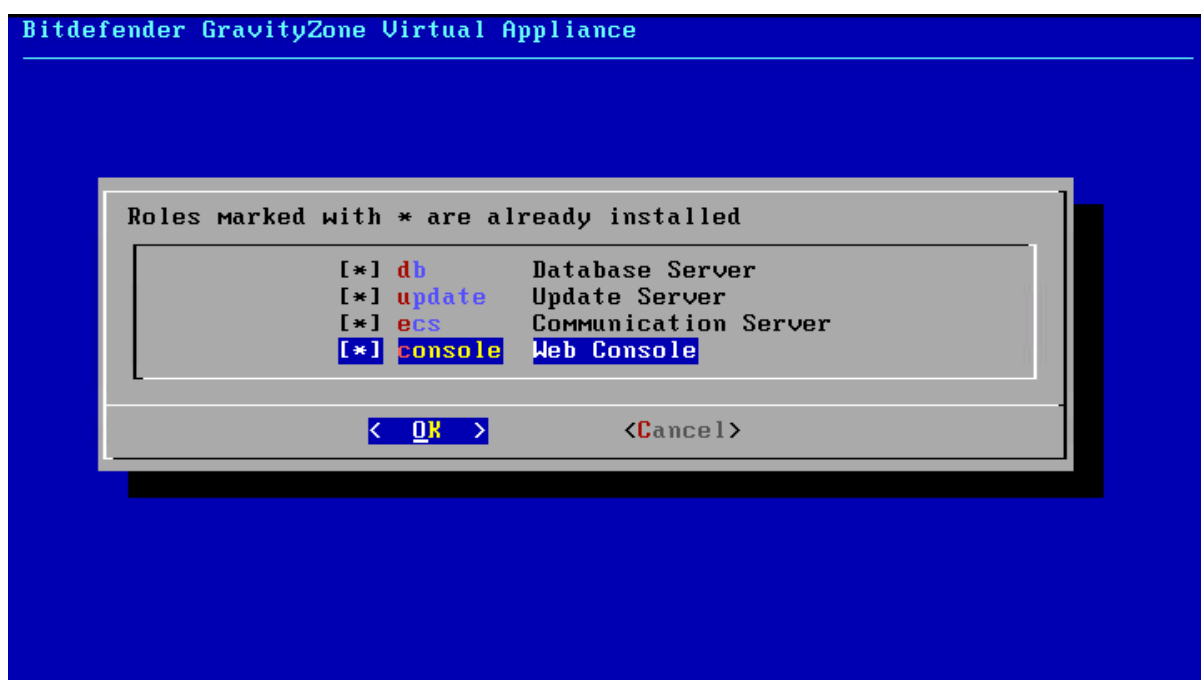
There aren't special requirements to be met during the import process but needless to say it should be on your management network so it can communicate to the vShield environment.

There four roles for the appliance (database server, update server, web console, and communication server) and if you wish you can deploy a virtual appliance allow the appliance to run all four, or configure it to communicate to a dedicated update and database server.

1. **At first boot the appliance** will prompt you to reset the "**bdadmin**" account password.
2. In our case for simplicity will configure the appliance to carry all the roles.

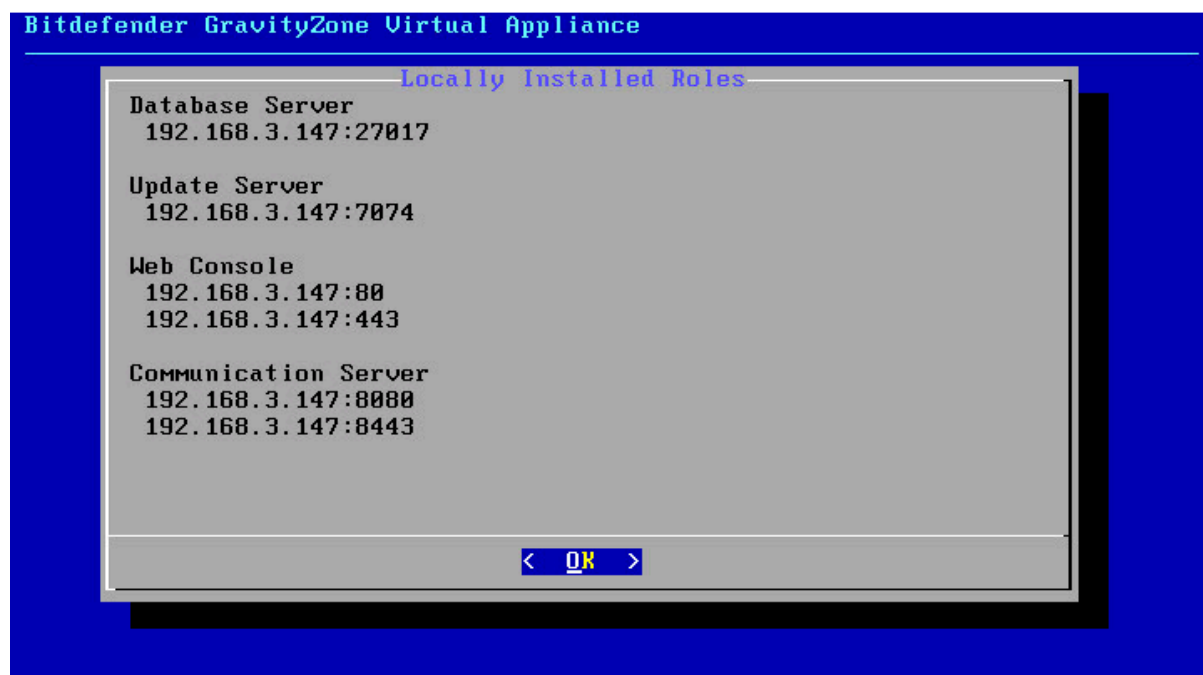


3. After configuring options 1 and 2 as befits your network, select option 4, and install the database. Once complete select option 4 again, to enable the other roles as well. This process downloads from Bitdefender's website the remaining components required for each role – the time this takes will depend on the bandwidth available between the appliance and the Internet



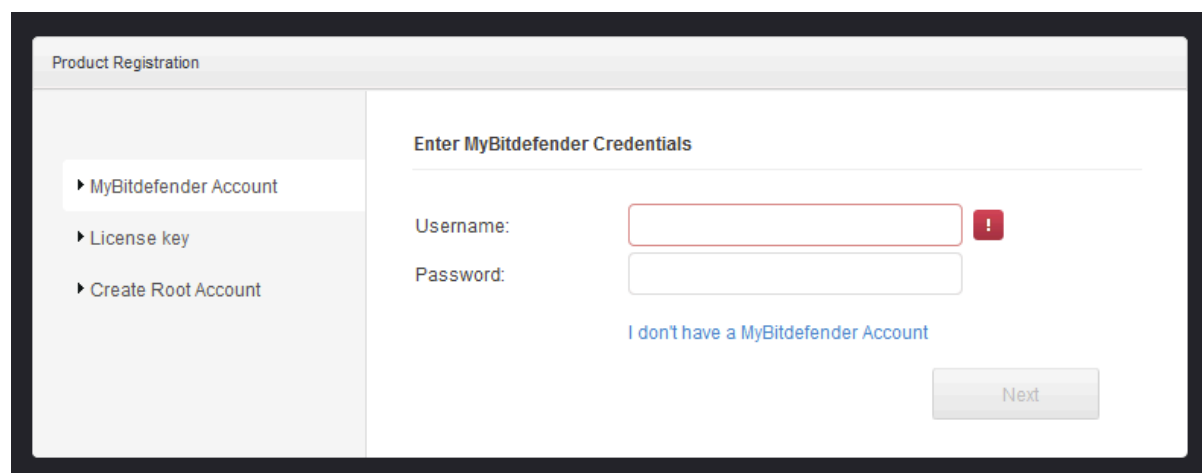
Before proceeding to the next step, its worth checking that all the roles

have been installed correctly. Under menu item 4 "Install/Modify Roles", the sub menu 2 option allows you to "Show locally installed roles"



Post-Configuration at the Bitdefender Control Center

Post-configuration of Bitdefender is carried out at Control Center web-interface – on first run you will be asked to provide your customer credentials and configuring the root account together with your license key – which is provided in email generated for your evaluation.



Once configured the browser will be switched to the "Accounts" page. The main account used to manage the Control Center is the root account. It will need delegate responsibility to another account created to have rights and privileges over the rest of your infrastructure.

Configure Active Directory, vCenter and Create User Account for Network & Security Tasks:

1. Before you begin creating accounts you might find it useful to enable Bitdefender built-in Active Directory support. This can be found under the **"Integration"** tab, and **"Active Directory"**

The screenshot shows the Bitdefender Control Center interface. The top navigation bar includes tabs for Integration, Settings, Update, Infrastructure, Certificates, License, Accounts, and Logs. The 'Integration' tab is selected, and within it, the 'Active Directory' sub-tab is active. A checkbox labeled 'Synchronize with Active Directory' is checked. Below this, there are input fields for 'Synchronization interval (hours)' set to 1, 'Domain' set to corp.com, 'User' set to administrator, and a 'Password' field with a placeholder 'Type here to change the password'. At the bottom right, there are 'Save' and 'Discard' buttons.

2. Next we can setup user for handling network and security tasks. In the **"Accounts"** page of the Control Center. Granting that user rights to manage computers as virtual machines.
3. In the **"Integration Tab"** we can click the plus to adding support for the vCenter server.

The screenshot shows the Bitdefender Control Center interface with the 'Integration' tab selected and the 'Virtualization' sub-tab active. A table is displayed with columns for Name, Hostname, Type, Sync status, and Progress status. The first row shows 'vCenter for New York' as the Name, an empty Hostname field, 'vCenter Server' as the Type, and empty fields for Sync status and Progress status. A plus icon is visible to the right of the table, and a dropdown menu is open showing 'vCenter Server' and 'Xen Server' as options.

4. Provide the necessary **hostname, username and password for the Control Center** to communicate to vCenter and vShield:

Add vCenter Server

vCenter Details

Name: vCenter for New York

Hostname/IP: vcnyc.corp.com

Port: 443

vShield Management

Hostname/IP: vshield.corp.com

Port: 443

Authentication

Use credentials provided for Active Directory synchronization: ☐

User: administrator@corp.com

Password:

Save Cancel

5. Next we need delegate a user account to have control over our VMs, Computers in AD and Mobile Devices. This involves adding an account from the directory service (you can create local custom accounts if you so wish), and then selecting the service and target that the account will control

Bitdefender

CONTROL CENTER

Integration

Settings

Update

Infrastructure

Certificates

License

Accounts

Logs

Accounts

> New Account

Details

Type:

Active Directory User

Force Resync

Username:

Administrator@corp.com

Full Name:

Mike Laverick

Email:

mikelaverick@corp.com

Password:

Click here to change your password

Confirm password:

Click here to retype your password

Note: Password must contain at least one upper case character, at least one lower case character and at least one digit or special character.

Settings and Privileges

Role:

Administrator

Timezone:

(GMT) UTC

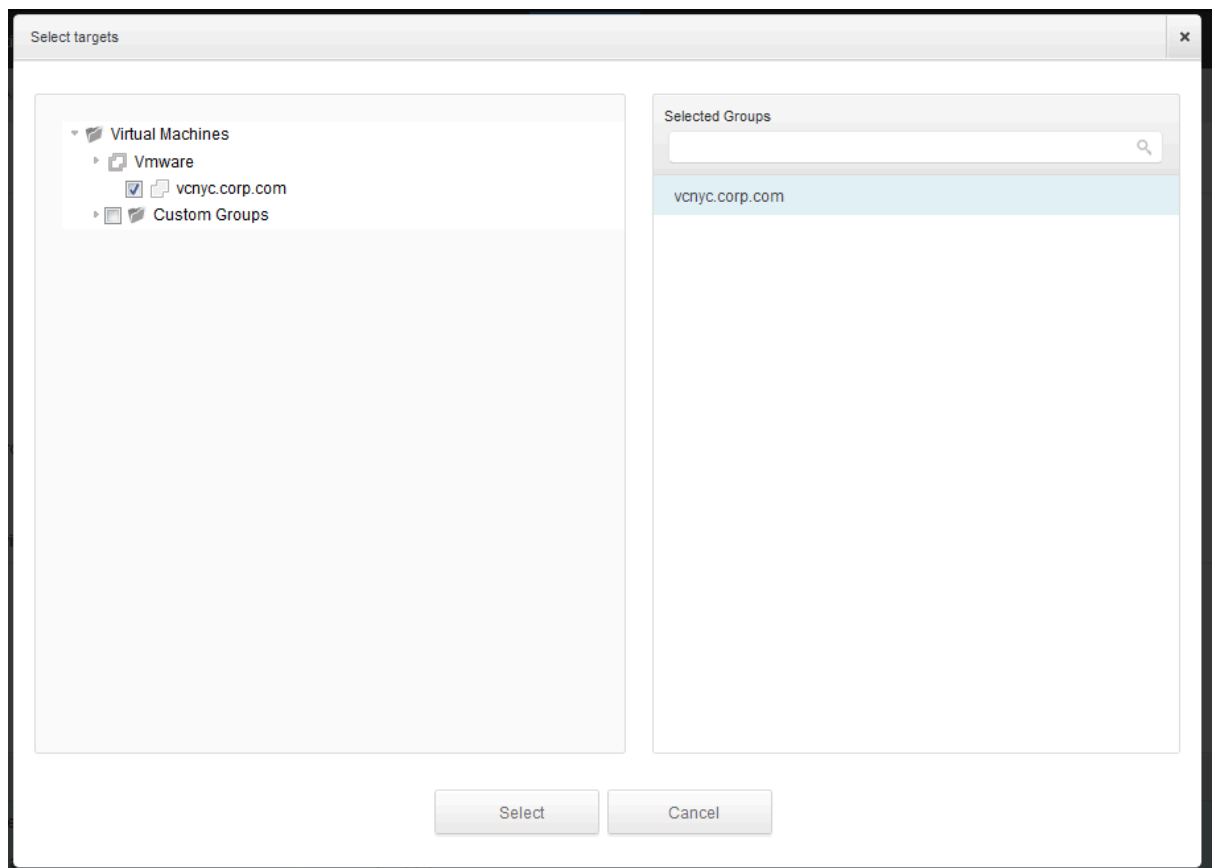
Language:

English

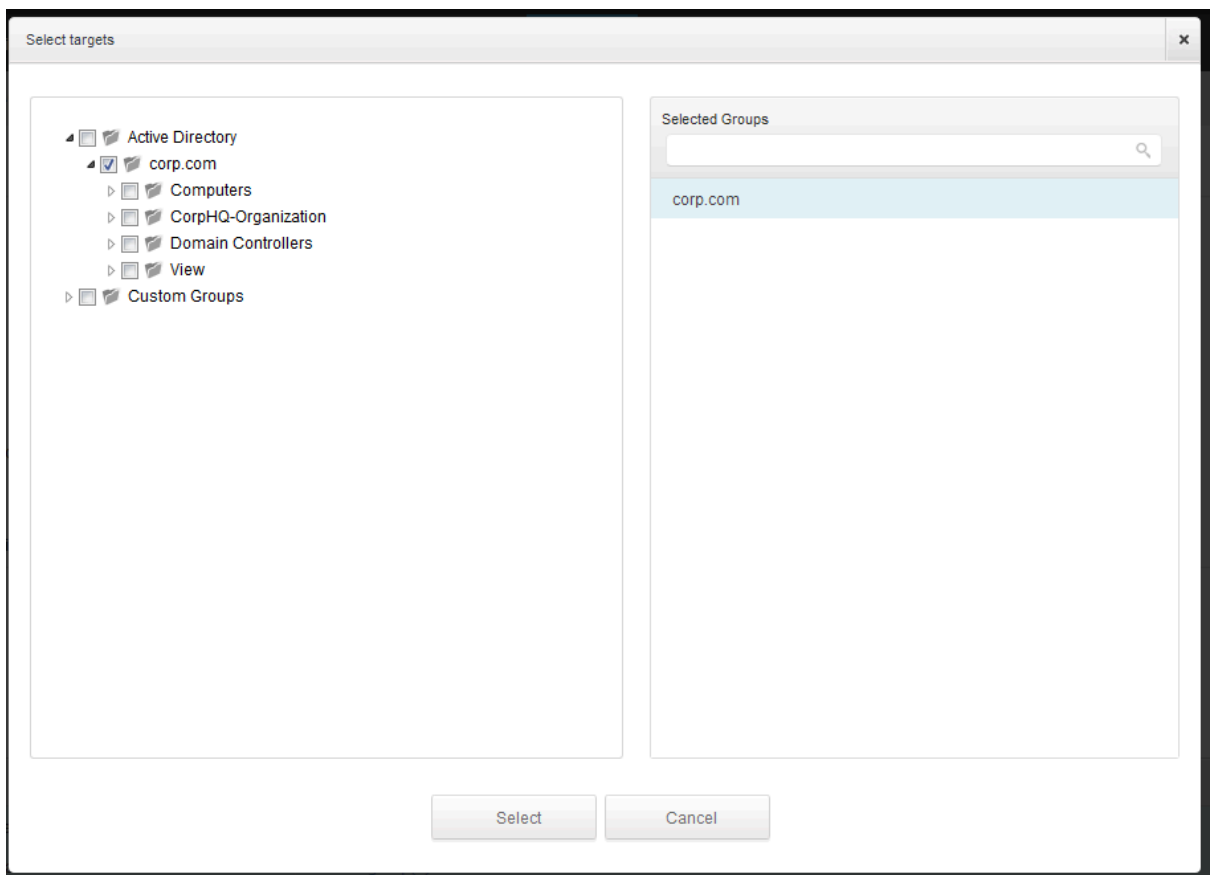
	Service	Target
<input checked="" type="checkbox"/>	Computers	0 group(s) selected
<input checked="" type="checkbox"/>	Virtual Machines	0 server/group(s) selected

Please enable at least 1 service and select at least 1 group from that service.

6. Notice here how the “targets” are in red because they contain no groups that would control this accounts scope of access. **You need to click at these re-lines of text, which will then open a view on the Active Directory and vCenter inventories.** For example, selecting “**0 Server/Groups Selected**” next to “**Virtual Machines**”, opens a dialog box like so:



and for “**Computers**” we see a view of the Active Directory environment:



Once you have selected your service and their respective targets you can add the account into the appliance. In my case I was able to logout and login as administrator@corp.com to properly begin managing the system.

Settings and Privileges

Role: Administrator ⓘ
 Timezone: (GMT) UTC
 Language: English

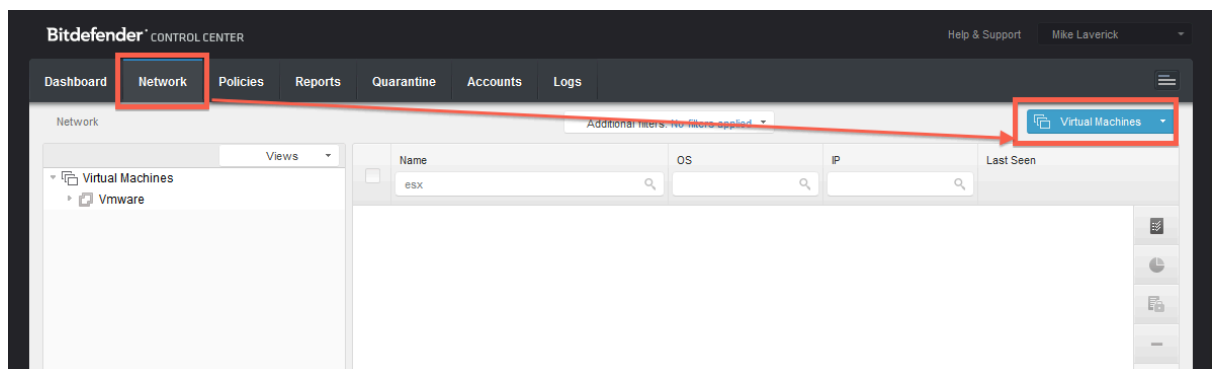
<input type="checkbox"/>	Service	Target
<input checked="" type="checkbox"/>	Computers	1 group(s) selected
<input checked="" type="checkbox"/>	Virtual Machines	1 server/group(s) selected
<input type="checkbox"/>	Mobile Devices	0 group(s) selected

ⓘ Please enable at least 1 service and select at least 1 group from that service.

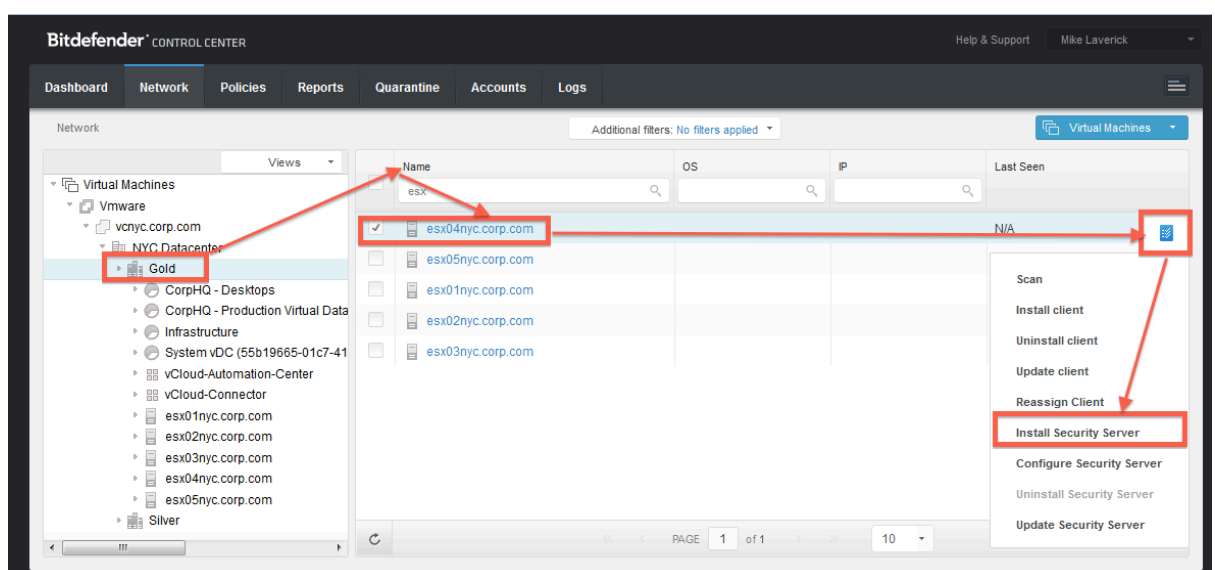
Deploy Bitdefender Security Server to each ESX host

Now we have the management console of Bitdefender configured we can set about deploying the Bitdefender Security Server to the ESX hosts where our VMs reside.

1. Select **Network** menu, and in the far right-hand corner ensure the scope is set to be "Virtual Machines"



2. You should be able navigate through the vSphere/vCenter layers until you can see your ESX hosts. Once there you can **select your first ESX host**, and trigger the **deploy of the Bitdefender Security Server**



3. This should pull up the **"Security Server Installation Page"** – which allows you to control how the service is deployed. There's quite a lot of options in this page, but most of them are common sense we feel:

So "Name" is the VM name of the appliance. I created a folder called "Bitdefender Security Servers" in my "infrastructure" folder so I could keep things nice and tidy.

VM Settings allows you to control the resources assigned to the appliance including which datastore to use and if the appliance will use a thin or thick virtual disk. It controls the amount of memory and CPU allocated to the security server. The guidance indicates that as you have more virtual desktops and general VMs you will need resources. The small (i) icon will give you some ideas on the appropriate settings for your the scale of your environment. The consolidation, memory and CPUs options all control the workload the Security Server expects to take, and virtual resources allocated to deal with them. There are four options under consolidation (Low, Medium, High and Manual). Each option allocates more and more resources to the SVA based on the rate of consolidation you expect in your environment per ESX host. "Low" as assume you have around 0-24 virtual desktops and 0-2 server-based VMs whereas "High" – assumes you have 50 or more virtual desktops, and 8 or more server-based VMs. Obviously "Custom" allows you to manually set your own preferences. Whereas "Low" allocates 2GB of RAM to the appliance, and two vCPUs – the "high" option allocates 4GB of RAM and 6 vCPUs.

You can also set a password for the security server as well as its time zone that can be important for logs and reports.

Pay close attention to the network settings. In our case we placed the appliance on our "management network" and used DHCP to set it up. That was because we have up to 9 servers to deploy to – and we wanted to reduce the per-server settings. It's currently not possible to bulk select many ESX hosts, and just use DHCP. So each host needs to be configured this way. Once completed just click Save, and move on to the next ESX host.

Security Server Installation

Options

Name:

Bitdefender SVE SVA (esx04nyc.corp.cor)

Deploy Container:

BitDefender Security Servers

Virtual Machine Settings

Datastore:

Tier4_Bronze

Provisioning:

Thin

Consolidation:

Low

Memory (MB):

2048

CPUs:

2

☒ Set Administrative Password

Password:

.....

Confirm password:

.....

Timezone:

(GMT) UTC

Network Settings

Name:

Management

Type:

DHCP

vShield Settings

☒ Use user's vCenter credentials

☐ Specify custom credentials

vShield Network:

vmsservice-vshield-pg

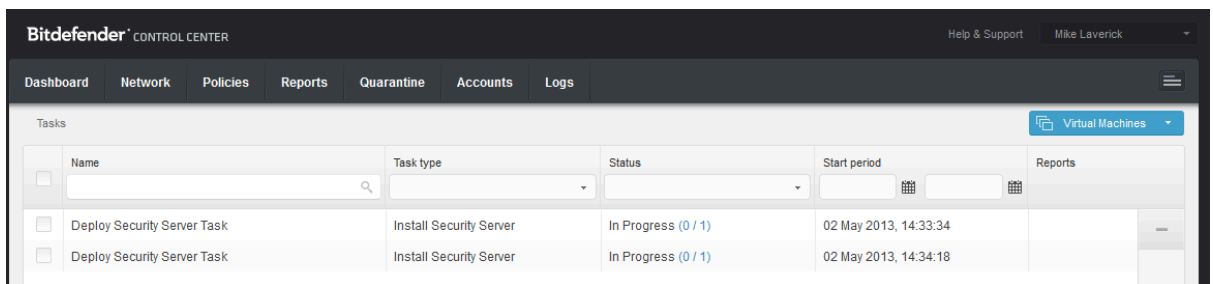
! vShield Mux Component will be also installed if it's missing.

! The Security Server image is not present, it will be downloaded automatically.

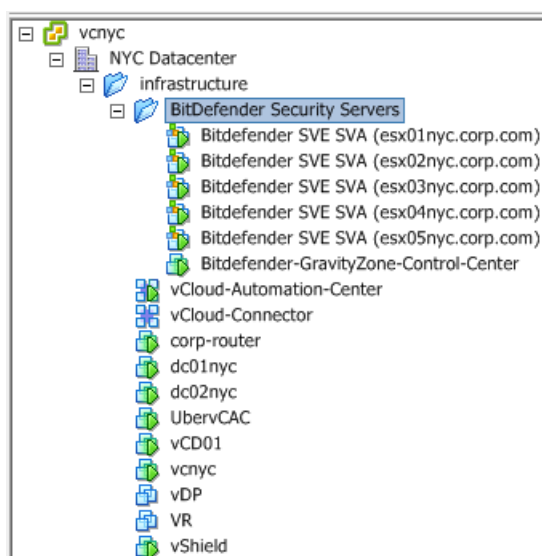
Note: Remember there is no bulk option for deploying the Security Server to every ESX host in the cluster. Also although you can control the VM folder location of the Security Server, the Servers themselves are located on the root of the VMware HA/DRS cluster, and it isn't possible to assign them to a resource pool.

Notice the option "The Security Server image is not present, it will be downloaded automatically". For this reason it can take a little while for the deployment to start the first time – as the Control Center downloads the image.

- As you deploy each appliance "**Task**" page update to show the deployment progress. This accessible from "**Network**" and "**Tasks**"

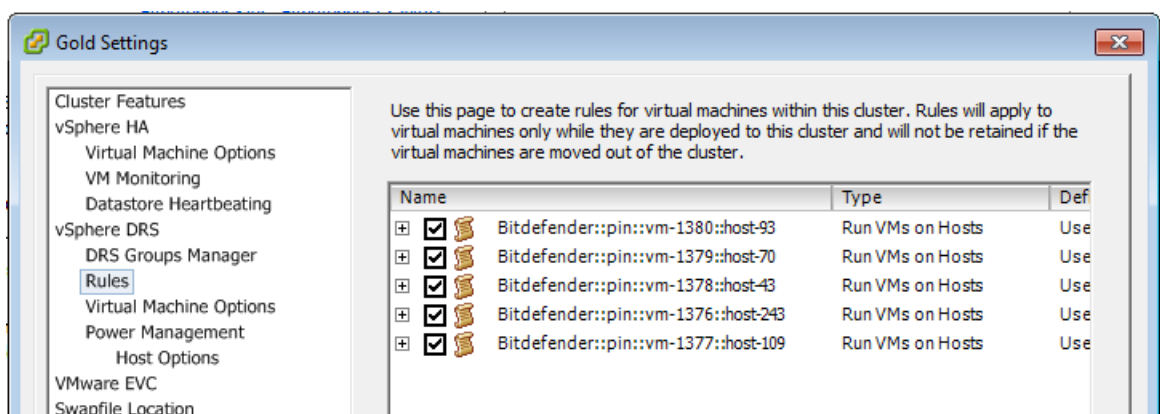


At the end of this deployment phase you should have one Control Center (used to deploy the Security Server and manage the solutions) and what ever number of Security Server dependent on the size and numbers of your vSphere clusters:



Note:

As you can see at the end of the process the result is that we end-up with a Security Server for each ESX host. As part of the deployment process each Security Server is disabled for HA, DRS and VMotion to ensure it remains on the ESX host at all times.



As for maintenance mode – if you do use it VMware will evacuate all the VMs from the ESX host leaving the SVA powered on. If you gracefully shutdown the SVA on the host, maintenance mode will eventually complete.

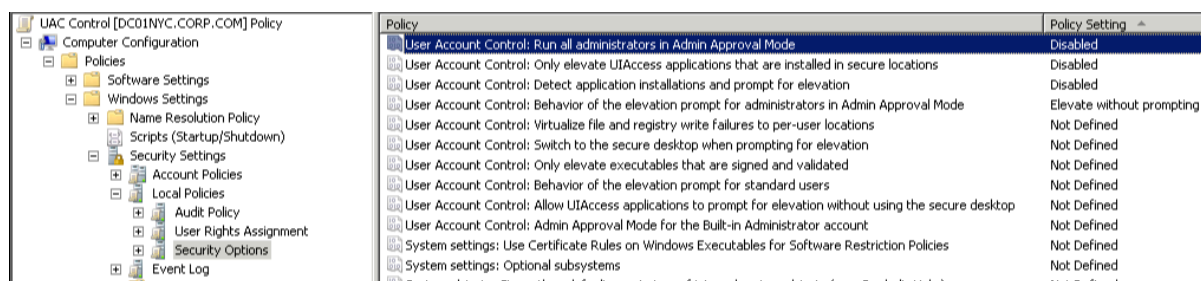
Install the Bitdefender “BDTools” (aka Silent Agent)

In the context of virtual desktops we feel the most efficient way to install or upgrade the “BDTools” (previously referred to in some documentation as the “Silent Agent”) is by incorporating it into your templates or ParentVM. Of course that might not address every requirement. For example if you run dedicated desktops or you want to deploy the agent other systems such as your View Infrastructure servers. For these reason and usage cases you can use the new silent tasks feature in Bitdefender Command Control administration pages to remotely install the agent to the VMs required. There are a number of prerequisite’s that must be met first including:

- You must provide the administrative credentials required for authentication on VMs
- Make sure VMware Tools 8.6.0 build 446312 or newer is installed on VMs (including those running on Linux or Solaris) with the Endpoint Driver installed. If not Bitdefender will report that the “Thin Agent” is not installed. Remember “Thin Agent” is how some vendors refer to the Endpoint Driver
- Windows User Account Control must be disabled

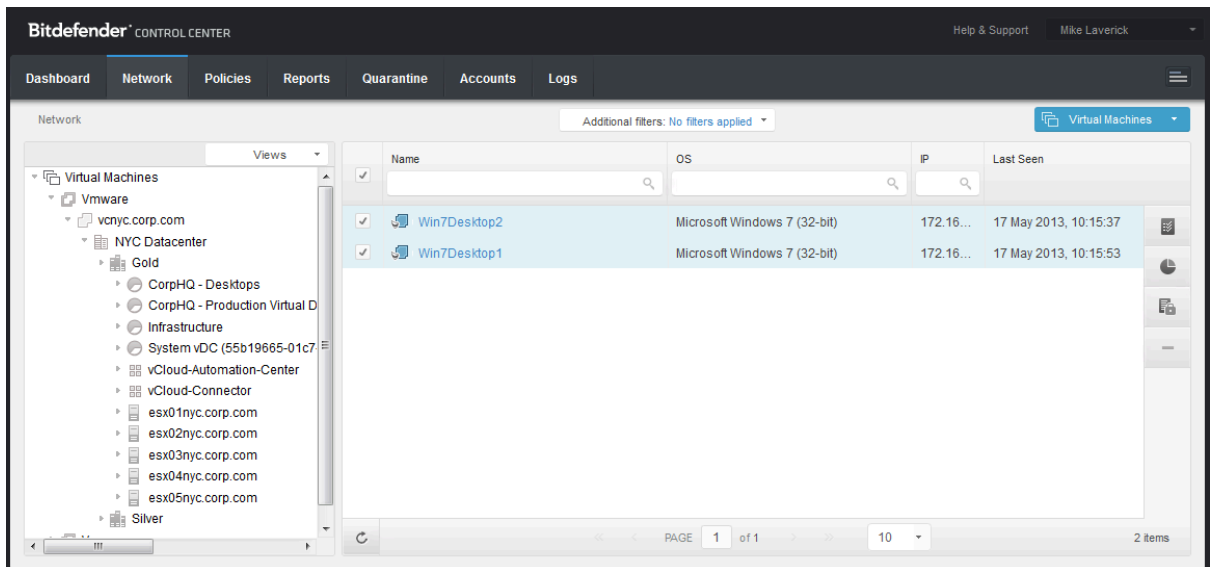
UAC can be disabled via group policy settings. These are located in the Group Policy Editor window, in the **Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options**. To disable UAC you need to disable four policy settings in total:

- User Account Control: Behaviour of the elevation prompt for administrators in Admin Approval Mode - Set its value to **Elevate without prompting**.
- User Account Control: Detect application installations and prompt for elevation - Set its value to **Disabled**.
- User Account Control: Only elevate UIAccess applications that are installed in secure locations - Set its value to **Disabled**.
- User Account Control: Run all administrators in Admin Approval Mode - Set its value to **Disabled**

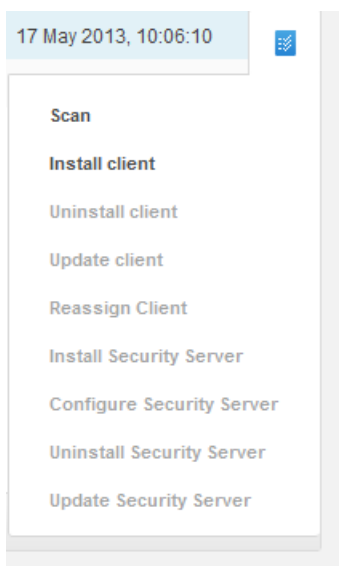


To install the silent agent from the Bitdefender appliance follow these steps:

1. Select **Network** in the main menu, and switch to the **Virtual Machines** view
2. **Navigate to the view that shows the virtual desktops.**



3. If you click the **Task icon** – you should see the option to **Install client**



4. Next we need to **set the credentials used for the installation** – in our case we used the default administrator account for the domain:

BDTools Installation

Options Credentials

No items were selected from credentials manager

Credentials Manager

User should be in DOMAIN\USERNAME form, where DOMAIN is the NetBios name of the domain.

<input type="checkbox"/>	User	Password	Description	Action
<input type="checkbox"/>	corpadministrator	*****	Used To Install Agent	

Save Cancel

Note: Once you click save the deployment will begin and you can monitor the progress under the **Network and Tasks** menu:

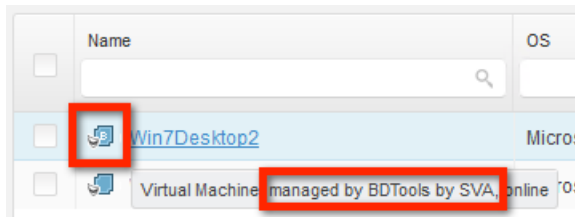
Bitdefender CONTROL CENTER

Dashboard Network Policies Reports Quarantine Accounts Logs

Tasks

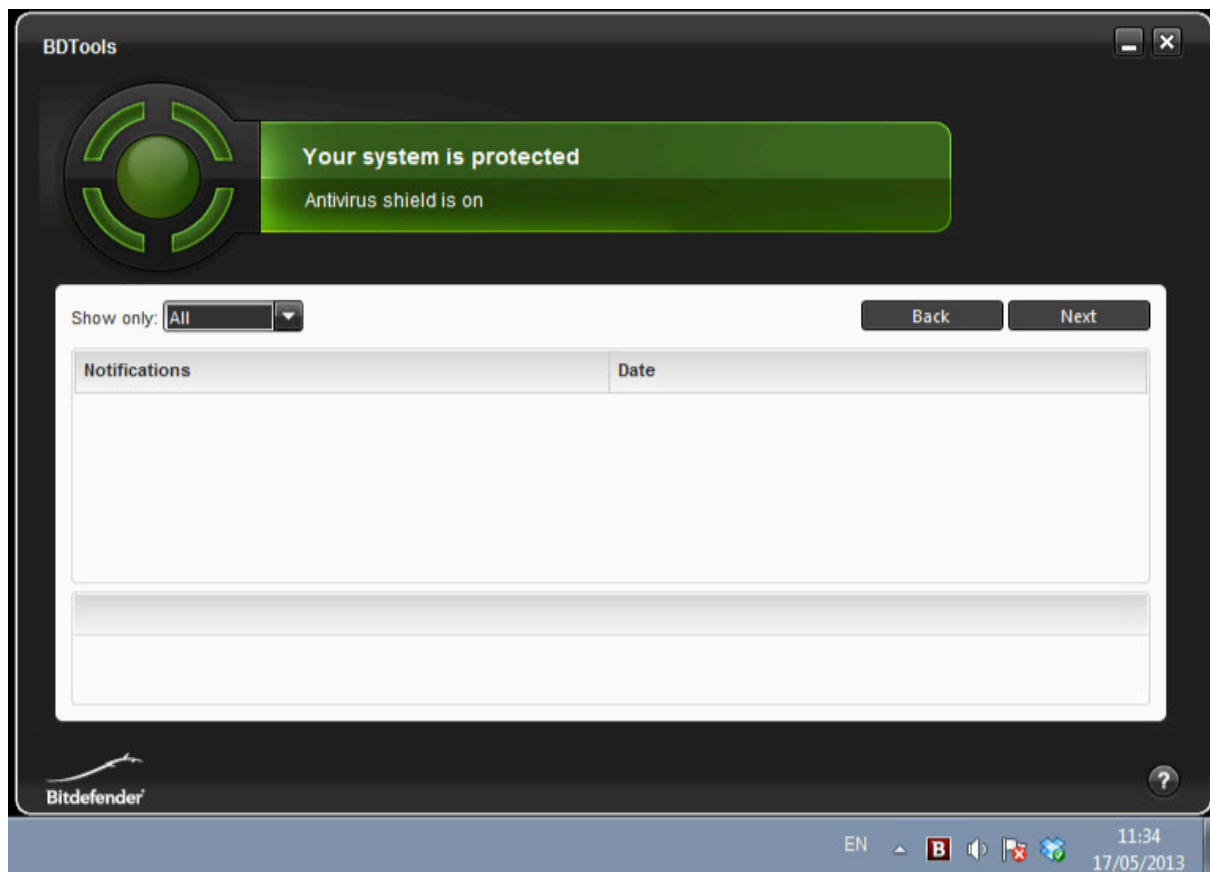
<input type="checkbox"/>	Name	Task type	Status	Start period
<input type="checkbox"/>	Deploy Security Server Task	Install Security Server	Finish (1 / 1)	02 May 2013, 14:34:18
<input type="checkbox"/>	Deploy Security Server Task	Install Security Server	Finish (1 / 1)	02 May 2013, 14:33:34
<input type="checkbox"/>	Deploy Security Server Task	Install Security Server	Finish (1 / 1)	02 May 2013, 14:54:44
<input type="checkbox"/>	Deploy Security Server Task	Install Security Server	Finish (1 / 1)	02 May 2013, 14:51:29
<input type="checkbox"/>	Deploy Security Server Task	Install Security Server	Finish (1 / 1)	02 May 2013, 14:53:42
<input type="checkbox"/>	Install BDTTools Task	Install Client	In Progress (0 / 1)	17 May 2013, 10:20:05

Once the installation has completed the status in the Bitdefender Control Center should indicate that BDTTools has been installed. This is indicated by small "B" in the icon representing the desktop as well as when you mouse over the icon too:



Testing vShield and Bitdefender

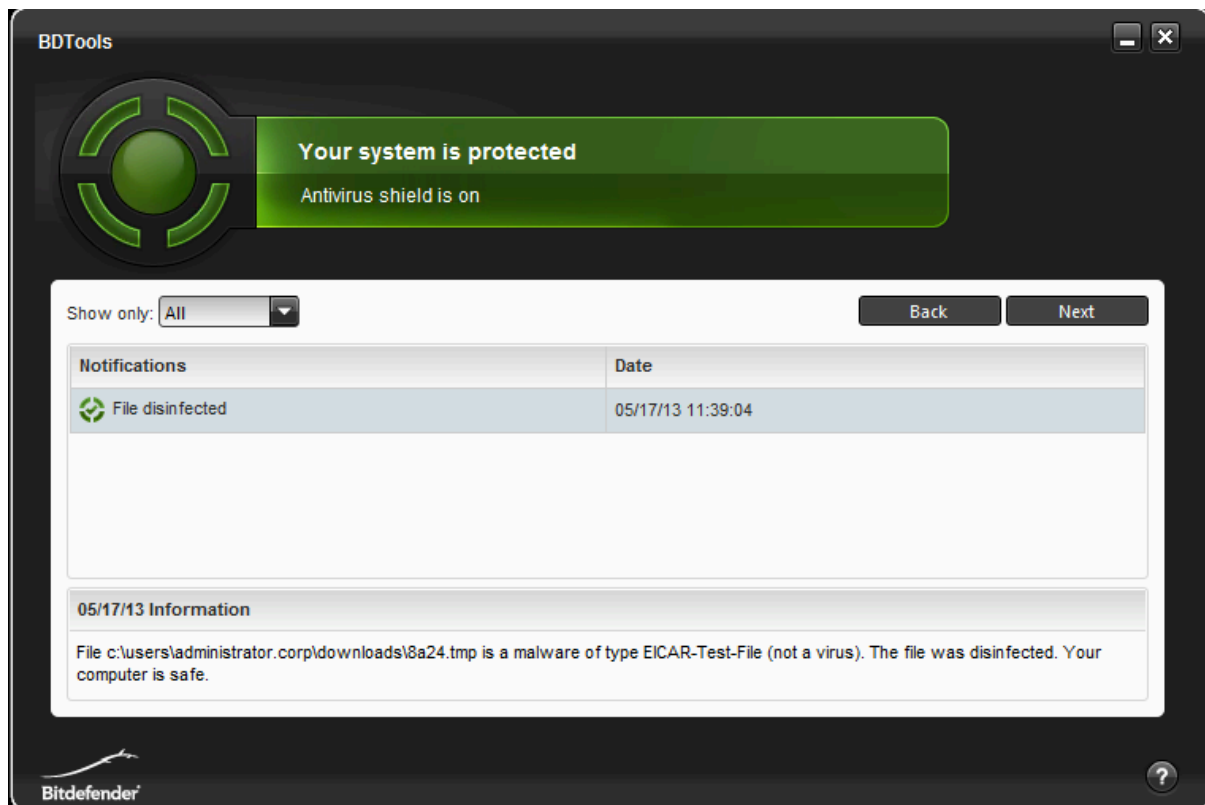
The BDTools installs as .MSI and adds the “B” icon in the taskbar tray. When launched it opens as console that allows the user to confirm they are protected. We found that Internet Explorer reacted negatively to its download and thought it was itself a suspect .EXE. We would recommend downloading it on behalf of the user and incorporating it into your template or parent VM.



Of course you will be keen to test if the anti-virus protection is in place. The easiest way do that is to use the “EICAR Test AV File” – this is a text file that contains a string that identifies itself as a virus AV software. It can be download from the eicar.org website here:

<http://www.eicar.org/85-0-Download.html>

Once downloaded and executed the AV should scan the file and identify it as virus:

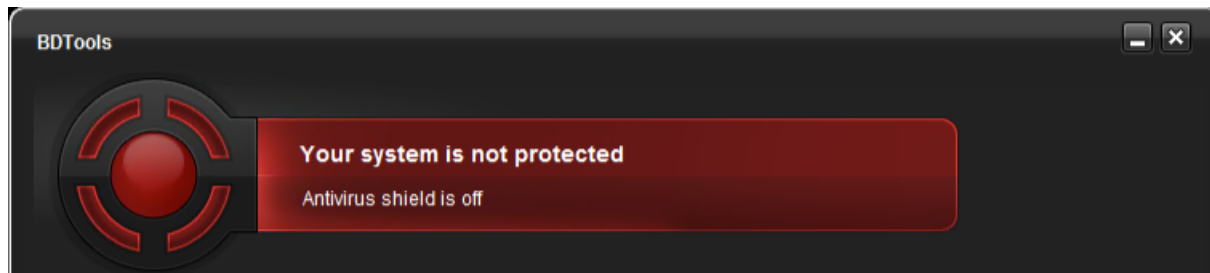


Conclusions

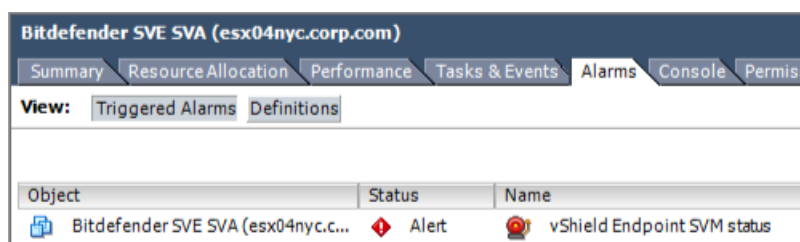
As you can see vShield is very easy to setup and configure – and by relocating the functions of AV out of the guest operating system it affords for great control over the impact of this process. Remember though that vShield itself is not “free”. You need resources to run each of the appliances (SVA) as well as at the two or more management consoles. We estimate that you would need to get significant density of VMs to ESX host to both offset the license and resource costs when compared to traditional methods of managing AV. Consider also that introducing new method of AV is yet another set of changes on what be already a radical departure from the existing model of delivering desktops.

Finally, you might want to review your current methods for patching and updating ESX hosts. As you might recall the virtual appliances that make up a vShield deployment are patch to “internal” standard switches on each hosts. Any VM configured to such a type of vSwitch is not open for vMotion. So if you used to using VMware’s Update Manager to automatically remediate host then maintenance mode with fully automated DRS cluster will not work as expected. You will find maintenance mode will get “stuck” at 2% because vMotion cannot move the SVA to another host. The simplest way to deal with this is shutdown the SVA once all the other VMs have been migrated to other ESX hosts in the cluster. Do not be tempted to power down the SVA prior to carrying out maintenance mode, as this will leave your VMs in an unprotected state. If the SVA is powered down before the VMs it’s protecting then technically they are in

an unprotected state. In the case of Bitdefender the Silent Agent will report the VM is not protected.



and this will trigger a customer Bitdefender SVE SVA Alarm in the vCenter inventory.



So this raises an important dependency issue. Once your AV is dependent on the appliance ensuring this appliance is only powered off in a controlled way is imperative. Additionally, when an ESX host is brought out of maintenance mode the first VM that should be powered on is the SVA before any other VMs are powered on.