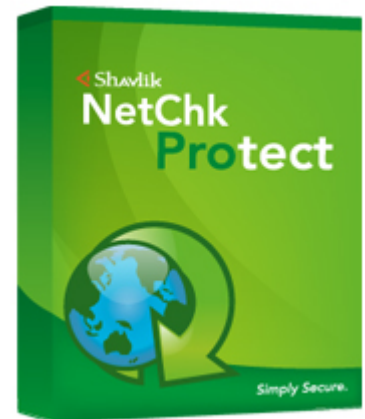




Quick Start Guide

**Shavlik NetChk[®] Protect
7.1 or later**

Virtual Machine



Copyright

© 2008 – 2009 Shavlik Technologies. All rights reserved.

No part of this document may be reproduced or retransmitted in any form or by any means electronic, mechanical, or otherwise, including photocopying and recording for any purpose other than the purchaser's personal use without written permission of Shavlik Technologies.

Trademarks

Shavlik NetChk Protect, Shavlik HFNetChkPro Plus, Shavlik NetChk Limited, Shavlik NetChk Configure, and PatchPush Tracker are registered trademarks of Shavlik Technologies. Shavlik Security Intelligence and the Shavlik Technologies logo are trademarks of Shavlik Technologies. VMware is a registered trademark of VMware, Inc. Microsoft, Windows, and Microsoft Baseline Security Analyzer are registered trademarks of Microsoft Corporation.

All other trademarks, tradenames, or images mentioned herein belong to their respective owners.

Document Information and Print History

Document number: N/A

Date	Version	Description
August 2008	Shavlik NetChk Protect 6.5	Initial release of the Offline Virtual Image Quick Start Guide .
June 2009	Shavlik NetChk Protect 7.0	Updated for interface changes in version 7.0.
August 2009	Shavlik NetChk Protect 7.1	Removed "Offline" from document name. Updated for interface changes in version 7.1.

Table Of Contents

VIRTUAL MACHINE OVERVIEW	1
Online Virtual Machines.....	1
Offline Virtual Machines.....	1
System Requirements	2
Notes About Virtual Machines	2
Roadmap of Tasks.....	5
Patch Tasks	5
Asset Management Tasks	5
ADDING VIRTUAL MACHINES TO A MACHINE GROUP	6
Adding Servers and Virtual Machines Hosted by a Server	6
Adding Offline Virtual Machines That Reside on Workstations.....	7
Adding a Virtual Machine Residing on a Workstation	8
Add a Directory of Virtual Machines	9
Viewing Servers and Virtual Machines in a Machine Group	9
HOW TO SCAN VIRTUAL MACHINES.....	10
REVIEWING PATCH SCAN RESULTS.....	11
DEPLOYING PATCHES TO OFFLINE VIRTUAL MACHINES	12
What Happens After You Deploy Patches to Offline Virtual Machines	12
When Deployments to Virtual Machines May Fail.....	12

**This page intentionally left blank.
The document is designed for duplex printing.**

VIRTUAL MACHINE OVERVIEW

A virtual machine is not actually a physical machine but rather a software environment (usually an operating system) designed to emulate a physical machine. A virtual machine can run programs just like a physical machine. The physical machine used to host the virtual machine can often support multiple virtual machines.


Shavlik NetChk Protect can scan for and deploy patches to the virtual machines on your network regardless of whether they are online or offline. It can also perform an asset inventory scan of your online and offline virtual machines.

Online Virtual Machines

A virtual machine that is online and running is treated by NetChk Protect exactly the same as a physical machine. Patch scans and asset inventory scans will be performed in exactly the same manner as on a physical machine. Any patches that may be missing can also be deployed in the same manner to both your physical machines and your online virtual machines. This means your online virtual machines are protected by the latest software patches just like your physical machines.

Offline Virtual Machines

NetChk Protect also enables you to scan and patch offline virtual machines. Offline virtual machines are those that aren't powered on when a patch scan or an asset inventory scan is performed. These virtual machines may be powered on for only a few hours or days a month and then powered off until they are needed again the next month. It's important to ensure that these systems are patched so that when they are brought online they don't place your network at risk.

NetChk Protect makes it easy to scan these offline virtual machines. When you initiate a scan of a machine group that contains offline virtual machines, NetChk Protect will perform a full assessment of the offline virtual machines and display the scan results alongside the results for running systems. Offline virtual machines will be differentiated in the patch scan results by a unique icon (). The scan results may even identify offline virtual machines that you don't even know about. When viewing machines in Machine View the **Offline Scan** column in the top pane will indicate if a virtual machine was offline at the time of the scan.

Patching offline virtual machines is similarly simple. You simply highlight the machines and patches you'd like to install and then select **Deploy** from the NetChk Protect menu. The patches will be copied to the offline virtual machines and will be installed the moment that the virtual machine is started (or according to the scheduled patch deployment time).



System Requirements

Shavlik NetChk Protect supports offline virtual machines created by any of the following:

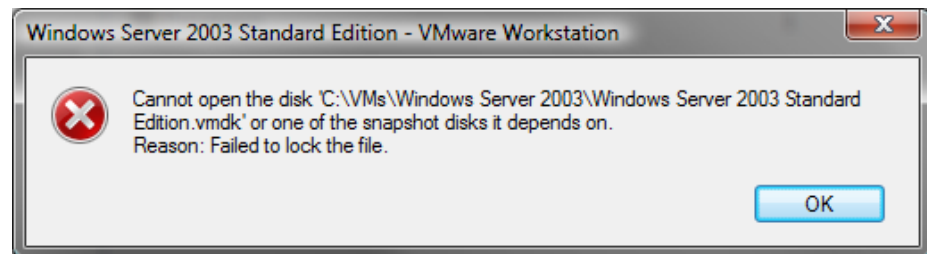
- VMware ESX Server 3.0 or later
 - VMware VirtualCenter 2.0 or later
 - VMware Server
 - VMware Workstation 4.0 or later
 - VMware Player
-

Notes About Virtual Machines

Before using Shavlik NetChk Protect to scan virtual machines, please review the following notes:

- Only the current state of the offline virtual machine will be scanned and patched. Snapshots of virtual machines are not supported.
- A virtual machine is counted only once against the total number of license seats available, even if it is scanned both in online (powered on) mode and offline (powered off) mode.
- In the patch scan results, a special icon will distinguish an offline virtual machine () from a physical machine or an online virtual machine () .
- Avoid using network drive letters when defining offline virtual machines in a machine group. The recommended practice is to instead specify the Uniform Naming Convention (UNC) path. This comes into play when performing a scheduled scan on an offline virtual machine. Network drive mappings are session-specific, so it is very possible that a specified mapping will no longer exist when the scheduled scan process is run.
- Within a machine group, the **Scan only** filters do not apply to offline virtual machines.
- Dual boot systems (for example, a virtual machine with two partitions, each containing a different operating system) are not supported.
- Virtual machines that are offline (powered off) will be mounted before they are scanned. Virtual machines that are online (powered on) do not need to be mounted as they are treated no differently than a regular machine.
 - When performing a patch scan, a virtual machine that was added to a machine group as an offline virtual machine but that is powered on at the time of a scan will fail to mount and will not be scanned.
 - When performing an asset scan, a virtual machine that was added to a machine group as an offline virtual machine but that is powered on at the time of a scan may still be scanned if group or default credentials are set.
- In order to mount a VMware ESX Server through a virtual infrastructure server, you must be running VMware Infrastructure 2.5 or later.

- When scanning virtual machines that are supported by VMware, please keep in mind the following:
 - You cannot mount encrypted virtual disks.
 - You cannot mount a virtual machine if any of its .vmdk files are compressed or have read-only permissions.
 - You cannot mount a virtual machine that is currently being used by a running or suspended virtual machine.
 - Linked clones, template images, and compressed images are not supported.
- In very rare cases, Shavlik NetChk Protect may inadvertently leave the hard drive in a mounted state after scanning an offline virtual machine. One clue that this has happened is if you get an error message similar to the following when trying to power on a virtual machine:



If this should occur, here's how you can unmount the hard drive:

1. Open a command prompt on a Windows machine.
2. Change to the **C:\Program Files\VMware\VMware Virtual Disk Development Kit\bin** directory.

For example:

```

C:\WINDOWS\system32\cmd.exe
C:\>cd \Program Files\VMware\VMware Virtual Disk Development Kit\bin
C:\Program Files\VMware\VMware Virtual Disk Development Kit\bin>
  
```

3. Type the `vmware-mount .exe` command.

A list of all currently mounted hard drives is displayed. For example:

```
Z:\ => [SAN8-Devastator] liriano-4/liriano-4-000001.vmdk
```

4. Type the following command:

```
vmware-mount.exe Z: /f /d
```

where `Z:` = the drive letter of the hard drive you want to unmount.

- When deploying patches to an offline virtual machine, the new deployment job will overwrite any older deployment jobs that have not yet been performed. For this reason you should deploy an accumulative collection of patches rather than only the most recent patches.

Example: You deploy Patch A to an offline virtual machine. The virtual machine is still offline a month later when you deploy Patches B and C. Because the first deployment job was never executed it gets overwritten and only Patches B and C are now scheduled for deployment. To avoid this you simply include Patch A along with Patches B and C in the second deployment job.

One way to manage this is to use a patch group to define the patches you want deployed to your virtual machines. When new patches are identified you simply add them to the list of patches in the patch group. This is particularly useful when specifying a patch group and enabling the **Automatically deploy with** check box on a patch scan template. See *Creating a New Patch Scan Template* in the Help file for more details about these options.

- Shavlik NetChk Agent operations are not supported on offline virtual machines.
- If you install Shavlik NetChk Agent on an online virtual machine and then later scan the virtual machine while it is in an offline state, Shavlik NetChk Protect may report the wrong agent status for that image. For example, it may show that the agent is not installed, or it may let you attempt to uninstall the agent. This occurs because Shavlik NetChk Agent operations are not supported on offline virtual machines. The correct status will be reported once the virtual machine is brought back online and rescanned by Shavlik NetChk Protect.
- Offline virtual machines running on Windows NT systems are not supported.

Roadmap of Tasks

Patch Tasks

Shavlik NetChk Protect can scan and deploy patches to online and offline virtual machines. You do this by performing the following tasks:

1. Create one or more machine groups that contain the virtual machines you want to scan and patch.

See *Adding Virtual Machines to a Machine Group* on page 6 for details.

2. Use the machine group in a scan.

See *How to Scan Virtual Machines* on page 10 for details.

3. Review the scan results.

See *Reviewing Patch Scan Results* on page 11 for details.

4. Deploy the desired patches to the desired virtual machines.

See *Deploying Patches to Offline Virtual Machines* on page 12 for details.

Asset Management Tasks

NetChk Protect can perform asset management scans of online and offline virtual machines. You do this by performing the following tasks:

1. Create one or more machine groups that contain the virtual machines you want to scan.

See *Adding Virtual Machines to a Machine Group* on page 6 for details.

2. Use the machine group in an asset scan.

See *How to Scan Virtual Machines* on page 10.

3. Review the asset scan results.

See **Viewing Virtual Asset Summaries** in the Help system for details.

When viewing machines in Machine View the **Offline Scan** column in the top pane will indicate if a virtual machine was online or offline at the time of the scan.

ADDING VIRTUAL MACHINES TO A MACHINE GROUP

Virtual machines can be added to a machine group. A typical implementation is to create a machine group consisting of nothing but virtual machines. You can, however, add both physical machines and virtual machines to the same machine group if you wish.

There are four different ways to add virtual machines to a machine group:

- Virtual machines that are online are treated the same as physical machines. They should be added using the **Machine Name** tab, the **Domain Name** tab, or the **IP Address/Range** tab.
- If offline virtual machines are hosted by a server you can add the server to the machine group. This effectively adds all virtual machines hosted by the server to the machine group. See *Adding Servers and Virtual Machines Hosted by a Server* for details.
- If offline virtual machines are hosted by a server you can add individual virtual machines to the machine group. See *Adding Servers and Virtual Machines Hosted by a Server* on page 6 for details.
- If offline virtual machines reside on individual workstations you can add the full path names or directory names of the offline virtual machines to the machine group. See *Adding Offline Virtual Machines That Reside on Workstations* on page 7 for details.

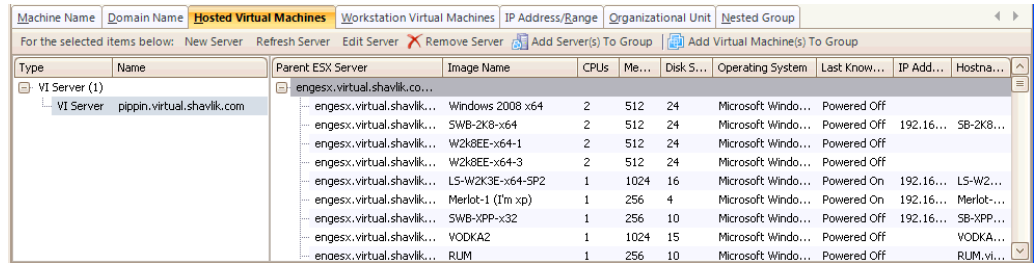
Adding Servers and Virtual Machines Hosted by a Server

Many organizations will host their virtual machines on one or more VMware servers. Doing so provides the means to manage the virtual machines in an organized fashion. There are two main types of VMware servers:

- **VMware ESX Servers:** A server dedicated to hosting and managing multiple virtual machines. VMware ESX servers are typically used in medium-sized organizations that want to control multiple virtual machines from one location. The server often runs on a dedicated blade computer that is using a VMware operating system.
- **Virtual Infrastructure Servers:** A virtual infrastructure server is typically used by large organizations that need to manage multiple VMware ESX servers, each of which may be running multiple VMware images. For example, you can quickly move a highly-utilized virtual machine from a busy ESX server to another less busy ESX server.

You can use the **Hosted Virtual Machines** tab to log on to these servers and select the virtual machines you want to include in your machine group.

Note: The virtual machines that are added to the group from this tab are intended to be scanned in offline mode. If a virtual machine that is added from this tab is online when a scan is initiated, the scan of that machine may or may not succeed. It depends on whether the default credentials or the optionally assigned group credentials are adequate for the program to make a connection to the online virtual machine.



1. Log on to the desired server by clicking **New Server** and then specifying the server name and the proper credentials.

After a connection is made the server is displayed in the left-hand table. The virtual machines hosted by the server are displayed in the right-hand table.

2. At this point you can either add the server itself to the group or you can add individual virtual machines.

- To add a server: Select the server and then click **Add Server(s) to Group**.
- To add individual virtual machines: In the right-hand table, select the virtual machines you want to add to the machine group and then click **Add Virtual Machine(s) To Group**.

The server or virtual machines are added to the bottom pane of the machine group.

You can log on to multiple servers at the same time. All virtual machines found on the servers are displayed in the right-hand table.

Adding Offline Virtual Machines That Reside on Workstations

Some virtual machines may reside on individual workstations. Any machine using VMware Workstation software is capable of supporting a virtual machine. The virtual machines may reside almost anywhere, including hard drives, network drives, jump drives, etc. You use the **Workstation Virtual Machines** tab to add these stand-alone offline virtual machines to a machine group.


Note: This tab is used to specify the offline identity of each virtual machine. If a virtual machine added here is online when a scan is performed, a mounting error will occur and the scan of that machine will fail. Online virtual machines must instead be added using the **Machine Name** tab, the **Domain Name** tab, or the **IP Address/Range** tab.

Tip: If you want to be absolutely sure that all your virtual machines are successfully scanned, simply add the same machines to the group a second time using one of the other tabs (**Machine Name**, **Domain Name**, or **IP Address/Range**). This duplication assures that each virtual machine will be successfully scanned regardless of its power state (online or offline).

Note: The virtual machines specified here are the actual images and you must therefore specify the full path name. Once the virtual machine is added to a machine group you should also specify the credentials used to connect to that virtual machine. This is different from virtual machines hosted by a server. Credentials for those machines are provided at the server level.

Adding a Virtual Machine Residing on a Workstation

There are two ways to add an offline virtual machine that is hosted on a workstation:

- In the **Click here to enter the full path to a virtual system image file** box, type the full path name of the virtual machine. You must specify the full path name and not just the name of the virtual machine. The name must contain a valid image extension (such as .vmx) and must not contain any illegal characters (such as @, ", etc.). When possible, avoid using network drive letters; the recommended practice is to instead specify the Uniform Naming Convention (UNC) path. For example: `C:\virtual\directory\machine.vmx`.
- OR -
- Click the Browse button () and locate the virtual machine by browsing your local machine and your network for the desired file.


Once the virtual machine is defined, click **Add Image** to add it to the machine group list.

Add a Directory of Virtual Machines

There are two ways to add a directory of offline virtual machines:

- In the **Click here to enter the path to a directory of virtual system image files** box, type the full path name of the directory. When possible, avoid using network drive letters. The recommended practice is to specify the Uniform Naming Convention (UNC) path. For example: `\\virtual\directory`.

- OR -

- Click the Browse button () and locate the directory by browsing your local machine and your network for the desired directory.

If you want the program to recursively search all subdirectories for virtual images when performing a scan, enable the **Include all images in all subdirectories** check box.

Once the directory is defined, click **Add Directory** to add it to the machine group list.

Viewing Servers and Virtual Machines in a Machine Group

When servers and virtual machines are added to a machine group, the new entries are displayed within the bottom section of the machine group pane. For example:

Type	Name	Credentials A...	E-Mail Options...	When Scan...
Virtual Server (1)				
Virtual Server	engesx.virtual.shavlik.com	Yes	No	Include
Offline VM Image (1)				
Offline VM Image	\\mydevhp\VMImages\QATesting\EN-2000\WinXPPro.vmx	No	No	Include
Hosted Image (2)				
Hosted Image	W2k8EE-x86-3	No	No	Include
Hosted Image	LS-2K-SP4	No	No	Include

The recommended best practice is to always supply credentials for the servers and the offline VM images (the virtual machines hosted by workstations). See *Supplying Credentials* in the Help system for details. Be careful if you have multiple console administrators, as different administrators are likely to provide different server credentials.

Note: Credentials cannot be applied to hosted images (virtual machines hosted by a server), they are instead provided at the server level. Hosted images are intended to be scanned in offline mode. If a hosted image is online at the time of a patch or asset scan, the scan of that machine may or may not succeed. It depends on whether the default credentials or the optionally assigned machine group credentials are adequate for the program to make a connection to the online virtual machine.

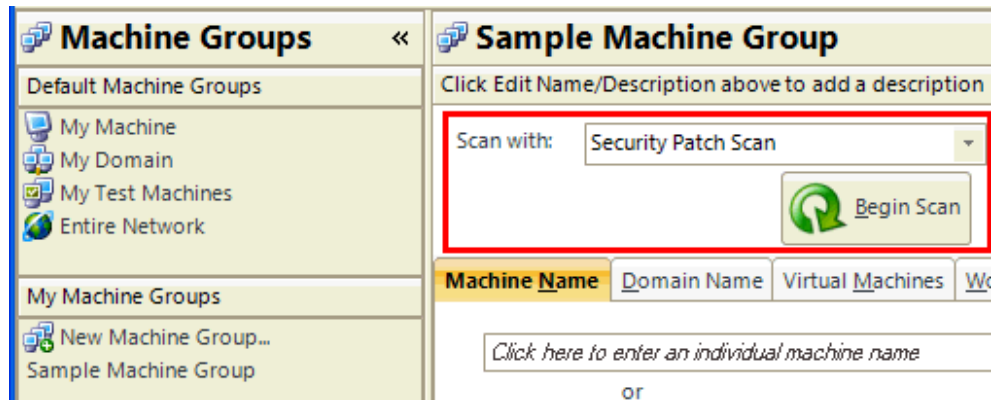
HOW TO SCAN VIRTUAL MACHINES

After defining your virtual machines in a machine group, you initiate a scan in the exact same manner as any other machine group.

1. In the **Machine Groups** pane select the machine group that contains your virtual machines.
2. Verify the desired virtual machines are contained within the group.
3. Apply any credentials that are needed to connect to the virtual machines.

Before performing the scan, the recommended best practice is to always supply credentials for the servers and the offline VM images (the virtual machines hosted by workstations). Credentials cannot be applied to individual hosted images (virtual machines hosted by a server). If a hosted image is online at the time of a scan, the program will attempt to use the machine group credentials and then the default credentials in an attempt to scan the image in an online mode.

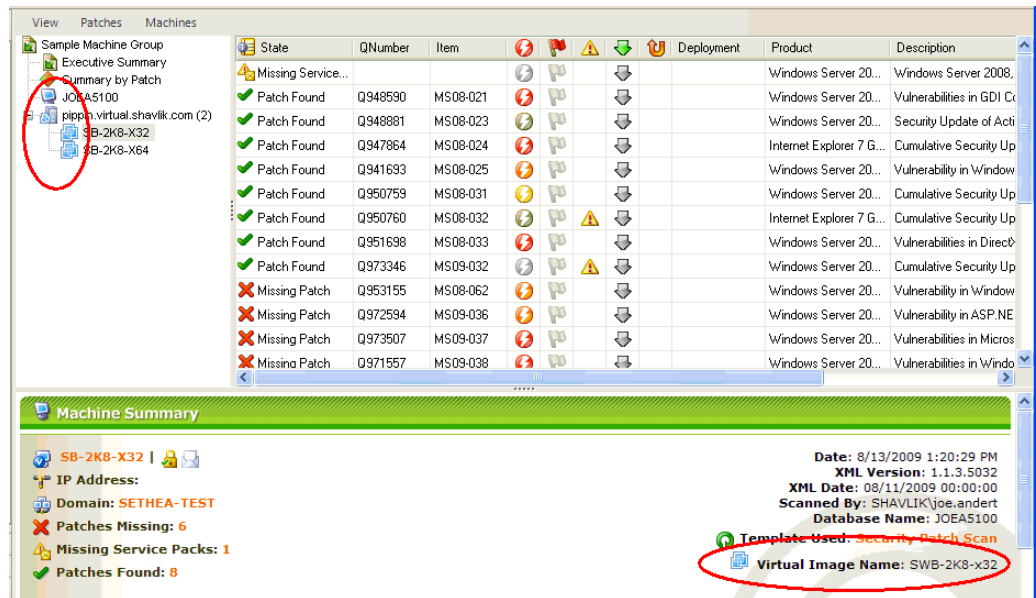
4. In the **Scan with** box select the desired scan template (either a patch scan template or an asset scan template).
5. Click **Begin Scan**.



Shavlik NetChk Protect will perform a full assessment of each virtual machine. In the patch scan results, a special icon will distinguish a virtual image (🖥️) from a physical machine.

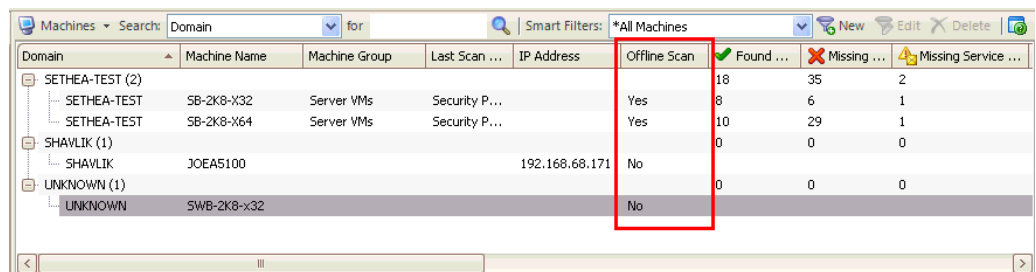
REVIEWING PATCH SCAN RESULTS

When reviewing your patch scan results, a special icon will distinguish an offline virtual machine (🖥️) from a physical machine or an online virtual machine (💻). For example:



Other than displaying the unique icon, Shavlik NetChk Protect will treat an offline virtual machine no different than a physical machine. If an offline machine is brought online and is rescanned, the offline virtual machine icon will be replaced by a regular machine icon.

Within Machine View, the **Offline Scan** column in the top pane will indicate if a virtual machine was online or offline at the time of the scan. For example:



DEPLOYING PATCHES TO OFFLINE VIRTUAL MACHINES

The method for initiating a patch deployment is the same regardless of whether you are deploying to a physical machine, to an online virtual machine, or to an offline virtual machine. See **Deploying Patches** in the Help file for details. It's what happens after you deploy a patch, however, that is slightly different for offline virtual machines.

What Happens After You Deploy Patches to Offline Virtual Machines

If you specify that you want the patches installed immediately, the patches, the scheduler, and all other required files are copied to the offline virtual machine. The installation won't actually occur, however, until the virtual machine is powered on. At that point NetChk Protect will recognize that there is a deployment task outstanding and it will initiate the task.

If you specify that the patch deployment should occur at some later time, and if the virtual machine is powered on before that time, nothing will happen. The deployment will not occur until both of the following criteria are met:

- The scheduled date/time arrives
- The virtual machine is online

Note: During deployment the virtual network will need to remain connected. Also, the patch deployment will be run under the Local System account so any credentials that are provided are ignored.

When Deployments to Virtual Machines May Fail

When you perform the deployment you will not know if a particular virtual machine is currently online or offline, and it doesn't matter as long as the power state of the machine has not changed since it was scanned. Patches must be deployed to virtual machines in the same manner that they were scanned. This means the deployment may fail under certain circumstances. For example:

Virtual Machine Was	Virtual Machine Is	The Deployment Will
Online when scanned	Online during deployment	Succeed
Online when scanned	Offline during deployment	Fail
Offline when scanned	Online during deployment	Fail
Offline when scanned	Offline during deployment	Succeed