



VMware ACE

Extending Your Patch Management Framework

This document explains how to use the custom quarantine feature of VMware® ACE to enforce the patch management policies that have been adopted by your company.

This document contains the following topics:

- [About Patch Management on page 1](#)
- [About VMware ACE on page 2](#)
- [Implementing A Solution with VMware ACE on page 3](#)
- [Getting Started on page 6](#)
- [Installing the Scripts and Tools on page 8](#)
- [Setting up Scripts on the Virtual Machine on page 9](#)
- [Setting up the Host Machine on page 14](#)
- [Testing the Update Script on page 17](#)
- [Deploying the Virtual Machine Package on page 19](#)
- [The Update File Contents on page 19](#)

About Patch Management

Managing updates and patches is an essential function in any enterprise environment. Patch management includes issues such as:

- Enforcing anti-virus updates
- Making sure that users are running the most current version of applications
- Making sure that users are running the current version of your corporate image

You can use VMware ACE to ensure that IT policies regarding updates and patches are applied across the enterprise by taking advantage of the network quarantine features to restrict the network access of non-compliant machines — for example, allowing them to connect only to an update server of your choosing. VMware ACE integrates easily with whatever patch management system you are using, such as Altiris, LANDesk, Microsoft® Systems Management Server (SMS) or your own custom solution.



About VMware ACE

VMware ACE extends virtual machine technology to address security issues in a networked computing environment. VMware ACE enables you to apply corporate IT policies to a virtual machine containing an operating system, enterprise applications and data to create a secure, isolated PC environment known as an “assured computing environment”.

A primary of advantage of using VMware ACE is that you create a standard, self-policing PC environment for your user. This means:

- Users can run standard PC applications without modification.
- Users can connect to the corporate network with standard networking protocols.
- Users can work whether connected to the corporate network or not; when users are not connected, IT policies, such as authentication and access to devices and networks, are still enforced.

With VMware ACE, you create a virtual machine and apply a set of Virtual Rights Management policies to it. Policies include:

- **Encryption and authentication** — Protect data on the virtual machine through encryption and control access through password and directory service authentication.
- **Life cycle control** — Set an expiration date, after which the virtual machine is disabled. For example, you can limit guest workers to the length of a contract, or reclaim licenses that have expired.
- **Network quarantine** — Restrict the networks that the virtual machine or host can access. For example, you can require that the virtual machine connect to the corporate network through a VPN server only and restrict the host machine from any access to the corporate network.
- **Device access** — Restrict the virtual machine access to some or all of the host’s devices, such as CD-ROM/DVD, floppy and USB drives, to create a totally isolated environment.

After you create a virtual machine, set desired policies and install any software on the virtual machine, you create an installable package. You can easily supply the newly created virtual machine to employees, contractors or business partners as needed.

If IT policies change, or if particular users need to change policies, you can easily create a new set of policies and distribute an update package with the new policies to your end users.

Basic Terminology

The following terms are important in the context of this document:

Guest operating system — An operating system that runs inside a virtual machine.

Host computer (or machine) — The physical computer on which the VMware ACE software is installed. It hosts VMware ACE virtual machines. The operating system on a host machine is referred to as the host operating system.

Virtual Rights Management policies — Policies control the capabilities of a virtual machine. You set policies by using the policy editor in VMware ACE Manager.

Network quarantine policy — A policy that controls the access of a virtual machine to networks and machines. Network quarantine policies can be either static or dynamic. A static policy is installed with the virtual machine and cannot be updated except by updating the entire virtual machine. A dynamic policy resides on a Web server or on an Active Directory server, and can be updated as necessary without updating the virtual machine.



Policy server — A Web server or Active Directory server you set up that is accessible to host machines. You place your dynamic network quarantine policies on this server. Host machines check the policy server at regular intervals to determine which policies to apply to their installed virtual machines. You can update dynamic policies by editing the policies in the policy editor; then post the new policies to the policy server.

Update or patch server — A server containing update patches that you set up and manage with patch management software. Virtual machines can access this server to update their operating environments.

Implementing A Solution with VMware ACE

VMware ACE provides two methods for enforcing patch management: custom network quarantine and version-based quarantine. This document describes custom quarantine. For information about version-based quarantine, see “Enforcing Patch Management” at www.vmware.com/support/resources/ace_resources.html.

Custom network quarantine enables you to define two different network quarantine policies based on whether the virtual machine is up-to-date:

- Normal access — For up-to-date virtual machines. You can specify any access — from no restrictions, to access (or denial of access) to specific networks and machines.
- Restricted access — For out-of-date virtual machines. Typically, you restrict network access to the update server, to force out-of-date machines to install updates.

Custom quarantine works in tandem with your patch management system and provides a very fine-grained approach to enforcing patch management policies. You can apply restricted network quarantine whenever any specific product or patch is missing from the virtual machine.

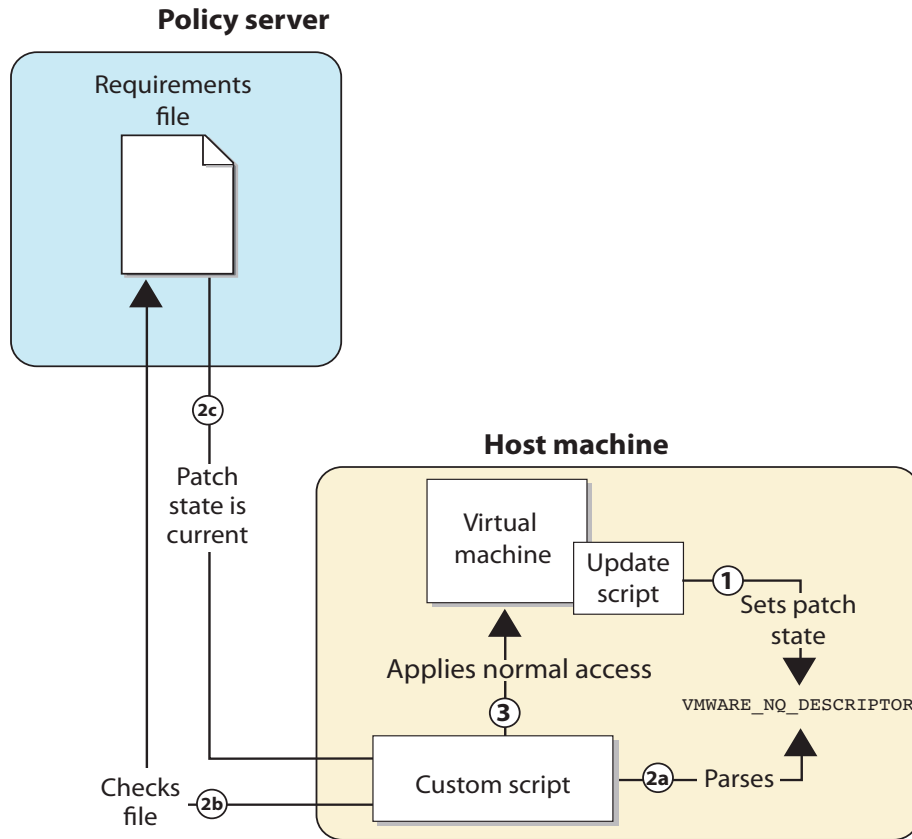
You set up custom quarantine as follows:

- You define normal and restricted access policies by using VMware ACE Manager.
- On the installed virtual machine, you write a script that:
 - Runs tools and scripts to enumerate the patch state of the virtual machine.
 - Runs the VMware ACE `nq-set` command to write the patch state to the ACE environment variable `VMWARE_NQ_DESCRIPTOR`.
- On the host machine, you write a custom script that:
 - Reads the patch state from the `VMWARE_NQ_DESCRIPTOR` variable and compares the results to a patch requirements file (hosted locally or on a policy server).
 - Sets the access to normal or restricted depending on the result of the comparison.

In practice, custom network quarantine works as described in the following paragraphs and figures. Numbers in the paragraphs correlate to callouts in the figures.



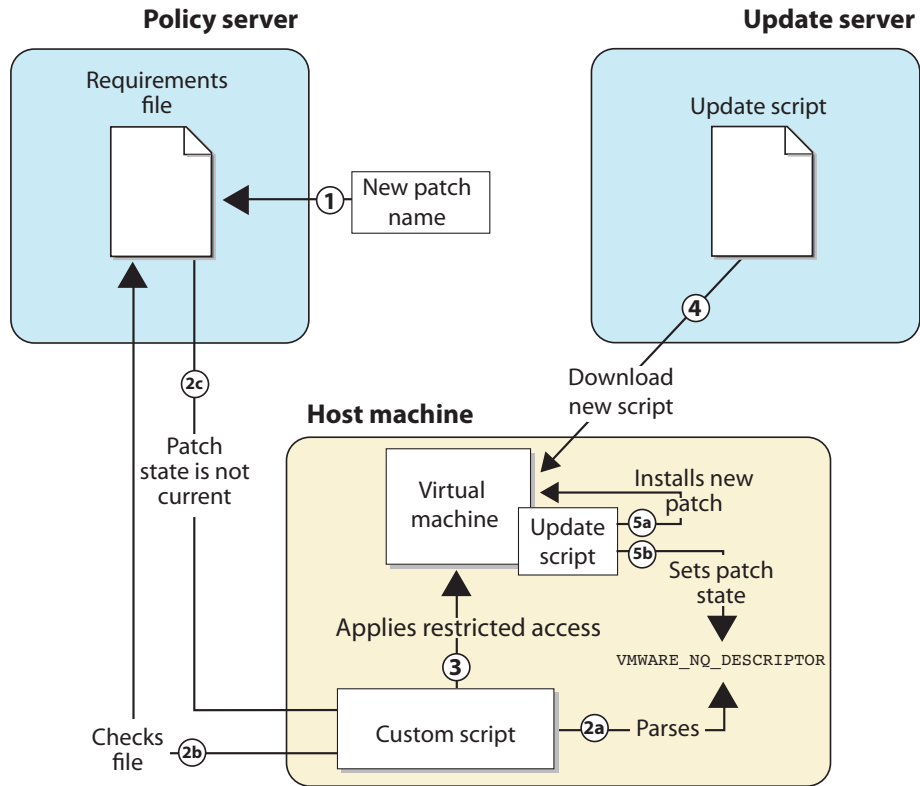
The first figure shows how the custom script works initially.



1. The update script on the virtual machine writes the patch state to the VMware ACE environment variable `VMWARE_NQ_DESCRIPTOR`.
2. Setting `VMWARE_NQ_DESCRIPTOR` triggers the custom script to run on the host. The custom script does the following:
 - a. Parses `VMWARE_NQ_DESCRIPTOR` to determine the patch state of the virtual machine.
 - b. Parses the requirements file, which resides on the policy server.
 - c. Compares the patch state to the requirements and determines that the patch state matches the current requirements.
3. The custom script sets normal access because the patch state is up-to-date.



The next figure shows what happens when you have an update patch for your virtual machines to install.



1. You add a new patch requirement to the requirements file.
2. The custom script, which is set up to run at periodic intervals does the following:
 - a. Parses VMWARE_NQ_DESCRIPTOR to determine the patch state of the virtual machine.
 - b. Parses the updated requirements file.
 - c. Compares the patch state to the requirements and determines that the patch state does not match the current requirements.
3. The custom script applies restricted access to the virtual machine because the patch state is out-of-date.
4. The virtual machine user downloads a new version of the update script from the update server.
 Be certain that you have added the patch installer to the update server and that the update script contains a call to the proper patch installer.
5. The virtual machine user runs the new update script, which does the following:
 - a. Installs the new patch.
 - b. Writes the patch state to the VMware ACE environment variable VMWARE_NQ_DESCRIPTOR.



Setting `VMWARE_NQ_DESCRIPTOR` triggers the custom script to run again on the host. The patch state and the patch requirements now match, so VMware ACE restores normal access.

Getting Started

This document describes a set of simple scripts and tools you can use to implement custom network quarantine for a virtual machine. You can download all the scripts and tools from the VMware Web site and third-party Web sites.

In most cases, you can implement a custom quarantine solution with no or slight modifications to the existing scripts. The scripts are Windows® batch files so you can edit them with any text editor. In addition, source files are included for all the VMware-provided tools so you can see in detail how they work and modify them if you wish.

Note: The VMware provided script that runs on the virtual machine calls a free tool from Shavlik Technologies, `HFNetChk`, to enumerate the patch state of the virtual machine. VMware does not endorse the use of `HFNetChk` over any other tools that provide the same functionality. You can use any tool you wish to extract the patch state, for example, a tool provided by your patch management software or one that integrates easily with that software.

Before you can set the custom quarantine policies described in this document, you must use VMware ACE Manager to create a project, add a virtual machine and apply other policies to the virtual machine. This section provides a high-level view of the process you must follow before setting network quarantine policies. It assumes you are familiar with using VMware ACE Manager and that you have read the technical note, "VMware ACE: Best Practices Setup," available at: www.vmware.com/support/resources/ace_resources.html. That document describes in detail the process that this section covers at a high level.

What You Need

To complete the procedures in this document requires the following:

- VMware ACE Manager.
- System software to install on the virtual machine.
- The sample scripts and files from VMware, which are contained in the `CustomPatch` folder. You can download this folder from: www.vmware.com/support/resources/ace_resources.html. `Custom-build` includes source files, executables and any library files needed to build the executables.
- The `HFNetChk` tool from Shavlik Technologies. You can download a free version of `HFNetChk` from www.shavlik.com/hfn_exe.aspx.
- A C compiler to compile the sample scripts if you plan to modify any of them.
- Patch management software, such as Altiris, LANDesk, Microsoft Systems Management Server (SMS)
- A policy server
- An update server

Before starting the step-by-step procedures in this document, make certain you have the *VMware ACE Administrator's Manual* available. You should also photocopy and fill out the two checklists in that manual:

- Checklist: Creating a Project
- Checklist: Adding a Virtual Machine



Creating a Project and Adding a Virtual Machine

A project contains one or more virtual machines and the VMware ACE application to run the virtual machines. In the project you create a package to install a virtual machine and the application on a user's machine.

To create a project, run VMware ACE Manager and click the New Project icon or click **File > New Project** to start the New Project Wizard. Enter a name for the project and a location in which to store project files. When you are finished, select **Open the Add Virtual Machine Wizard** to go directly to the wizard for adding a virtual machine to the project.

Note: When you create a project, the New Project Wizard automatically adds the VMware ACE application to the project. End users use this application to run and manage the virtual machine. You can set preferences for this application if you wish, although this document does not show you how to do so.

When the Add Virtual Machine Wizard starts, take the following steps to add a virtual machine to the project:

1. Click **Next** to enter the wizard. The Add New or Existing Virtual Machine panel appears.

Note: This document assumes you have already created a corporate virtual machine image that contains your supported operating system and applications.

Select **Existing virtual machines** and click **Next**.

2. The Select Virtual Machines panel appears.

Click **Browse** and navigate to the configuration (`.vmtx`) file for the virtual machine you want to add to the project.

3. The Ready to Complete panel appears.

When you are ready to finish the Add Virtual Machine Wizard, select **Set policies after the wizard closes** to go directly to the policy settings editor after the wizard creates the virtual machine.

Click **Finish** to exit the wizard.

Creating Policies for the Virtual Machine

Policies are at the heart of managing a virtual machine. You set policies using the policy editor in VMware ACE Manager. At a minimum, you should set the following policies:

- **Encryption and Authentication** enable you to secure the data and the virtual machine itself through encryption and password protection. When you password-protect a virtual machine, you should also enable a recovery key and hot fixes in case the end user forgets the password.
- **Copy Protection** ensures that the virtual machine can be run only from the location in which you install it.
- **Device policies** restrict access for the virtual machine to the host's devices such as DVD/CD-ROM, floppy and so on. This prevents data on the virtual machine from being exposed when the host machine is outside the corporate network.

You can set other policies as well, such as an expiration date when the virtual machine can no longer be used. But the policies just described ensure that the virtual machine is secure and isolated from the host on which it runs.

For detailed information about why and how to set these policies, see the technical paper Best Practices for Setting Up VMware ACE, available at: www.vmware.com/support/resources/



[ace_resources.html](#). The remainder of this document describes in detail how to use custom quarantine policies with your patch management system.

Installing the Scripts and Tools

This section describes how to obtain the different scripts and tools that you need to implement custom quarantine. All of these tools are free. Some are available from VMware and some are from third-party vendors.

Scripts from VMware

You can obtain the scripts from VMware at the following URL: www.vmware.com/support/resources/ace_resources.html. Download the `CustomSource` folder to your host machine.

The `CustomPatch` folder contains the following folders: `Guest`, `Helper` and `Host`. Copy the `Guest` folder to the virtual machine and leave the `Host` and `Helper` folders on your host machine.

To copy the `Guest` folder, run VMware ACE Manager, select the tab for the virtual machine and start the virtual machine by clicking **Start this virtual machine** in the Commands panel. Then drag the `Guest` folder from the host machine to the virtual machine.

Guest Folder

The `Guest` folder contains the following files and folders:

- `nqsetcmd` — A folder that contains the `nqsetcmd` source and executable files. This application builds an `nq-set` command line so `nq-set` can be executed from the `update.bat` file.
- `PatchEnumerator` — A folder that contains the `PatchEnumerator` source and executable files. `PatchEnumerator` is a C application that parses the XML patch state information output from `HFNetChk` and reduces it to a concise format.

Note: `PatchEnumerator` uses an open source XML parser that is not included in this sample script. You may use a parser of your choice or download one at ezxml.sourceforge.net.
- `Update.bat` — Batch file that runs the tools in this folder to install patches, and obtain and pass the patch state to the host machine.
- `temp1.xml` — Sample output from `HFNetChk`.
- `temp2.xml` — Sample output from `PatchEnumerator`.

Helper Folder

The `Helper` folder contains the `stringlist` folder which contain C libraries for use by `PatchEnumerator` and `NQ-sample`. You only need the helper files if you modify and recompile the source for either application.

Host Folder

The host folder contains a single folder, `nqsamples`, which contains the source and executable files for the `NQ-sample` application. It also contains the `patches.xml` requirements file which is used as input to `NQ-sample`.

Third-Party Software

The implementation described in this document uses the `HFNetChk` tool from Shavlik Technologies to obtain the patch state of the virtual machine. You can download a free version



of HFNetChk from www.shavlik.com/hfn_exe.aspx. You install HFNetChk on the virtual machine. For information on installing HFNetChk on the virtual machine, see [Obtaining the Patch State with HFNetChk on page 10](#).

Note: VMware does not endorse the use of HFNetChk over any other tools that provide the same functionality. You can use any tool you wish to extract the patch state, for example, a tool provided by your patch management software or one that integrates easily with that software.

Setting up Scripts on the Virtual Machine

The following sections describe the tools that you install and run on the virtual machine to determine the virtual machine's patch state and communicate that state to the network quarantine script running on the host machine:

- [About the Update Script on page 9](#) describes the update.bat script. The update script is the master script that runs on the virtual machine. It calls other tools and scripts to install patches, obtain the patch state of the virtual machine and set the patch state in the VMWARE_NQ_DESCRIPTOR variable.
- [Obtaining the Patch State with HFNetChk on page 10](#) describes how to use the HFNetChk tool to assess the patch state of the virtual machine.
- [Compacting the Patch State with PatchEnumerator on page 11](#) describes how to use the PatchEnumerator utility to parse the XML output from HFNetChk and create concise XML output that is small enough to be passed on the command line.
- [Using nq-set to Save the Patch State to VMWARE_NQ_DESCRIPTOR on page 12](#) describes how to call the VMware Tools nq-set command from within a batch file to set the value of the VMWARE_NQ_DESCRIPTOR variable.
- [Testing the Update Script on page 17](#) describes how to run the update script after all the other tools and scripts are in place.

About the Update Script

The update.bat script, which is included in the Guest folder, does the following:

- Downloads patches from the update server.
 - Note:** The sample update script has a place holder comment for installing patches but no code to actually do so. The actual code you write depends on the patch management system you are using.
- Obtains the current patch state and updates the VMware ACE environment variable, VMWARE_NQ_DESCRIPTOR, with this information.

To obtain the patch state and set VMWARE_NQ_DESCRIPTOR, update calls the following tools:

- HFNetChk to obtain the patch state.
- PatchEnumerator to reduce the patch state information to a size that can be passed on the command line.
- nqsetcmd to build a command line that executes commands to set VMWARE_NQ_DESCRIPTOR.

The following sections describe these tools in detail.

Note: For simplicity, the sample update script assumes all the tools it calls are in the current directory. You do not know where users will put the update script when they download it from



the update server. To make matters easier for your end users, you could modify this script and specify full paths for each tool. Alternately, you could specify additional paths in the `Path` variable for these tools.

In a production environment, you put a copy of the update script on your update server. The network quarantine message that users receive when their virtual machines are put in quarantine must direct them to download the update script from the update server. [Setting Network Quarantine Policies on page 15](#) includes information about specifying a network quarantine message.

See [The Update File Contents on page 19](#) to see the contents of `update.bat`.

Obtaining the Patch State with HFNetChk

HFNetChk is a free command-line tool from Shavlik Technologies that assesses the patch status of a computer running Windows NT 4.0, Windows 2000 or Windows XP. HFNetChk is the first tool called by the update script after new patches are installed.

Installing HFNetChk

To install HFNetChk on the virtual machine, run VMware ACE Manager and take the following steps:

1. Select the project and the virtual machine.
2. From the **Commands** list on the virtual machine details page click **Start this virtual machine**.
After the operating system boots, open an Internet browser.
3. Copy the address of the HFNetChk download page into the browser and press the Enter key.
www.shavlik.com/hfn_exe.aspx
4. Click the **Download** link and save `hfnetchk_<version>.exe` to a location in the virtual machine.
5. Double-click `hfnetchk_<version>` from the location in which you installed it to launch the setup program for HFNetChk.

Follow the instructions in the Setup program to install HFNetChk in the virtual machine. By default, Setup installs HFNetChk in the following directory:

```
C:\Program Files\Shavlik Technologies\HFNetChk>
```

You can accept the default location or choose a different location.

Note: The update script, which executes HFNetChk, assumes all the tools and scripts it calls are in the current directory. You can install HFNetChk in the same directory as the other tools, or modify the script and specify a complete path for HFNetChk.

Running HFNetChk

Ultimately, end users run HFNetChk when they download and run the update script. You can run HFNetChk independently to see what it does by entering the following command line in a Command Prompt window:

```
HFNetChk -o xml2 -history -f templ.xml
```

HFNetChk first downloads a compressed XML file, `mssecure.cab`, from the Shavlik Technologies Web site. After decompressing the XML file, HFNetChk scans the virtual machine to identify the operating system, service packs, and programs that are running. It then parses the



XML file to determine which security patches are available for your combination of installed software.

The command line options do the following:

- o `xml2` specifies detailed XML format for the output.
- history displays hot fixes that are explicitly installed and non-superseded hot fixes that are missing.
- f `temp1.xml` specifies the filename for the output.

For each found and missing patch, HFNetChk provides detailed information, including a URL for downloading the patch as well as a complete description. The following shows a small section of sample output from HFNetChk:

```
- <ScanResults>
  <ScanDateTime>Thu Feb 17 13:52:58 2005</ScanDateTime>
  <XMLDataVersion>1.1.2.359</XMLDataVersion>
  <ScannedBy>MICHAEL-LTK17DQ \ Administrator</ScannedBy>
- <ScannerDetails>
  <Version>HFNetChk(Pro) version 3.86</Version>
  <DevelopedBy>Shavlik Technologies, LLC</DevelopedBy>
  <Website>http://www.shavlik.com</Website>
  <Information>info@shavlik.com</Information>
  <Phone>(651)-426-6624</Phone>
</ScannerDetails>
- <Machine>
  <MachineName>MICHAEL-LTK17DQ</MachineName>
  <Domain>WORKGROUP</Domain>
- <Product>
  <ProductName>WINDOWS 2000 SP4</ProductName>
- <PatchFound>
  <BulletinID>MS03-023</BulletinID>
  <BulletinTitle>Buffer Overrun In HTML Converter Could Allow Code Execution (823559)</BulletinTitle>
  <SQNumber>Q823559</SQNumber>
  <BulletinUrl>http://www.microsoft.com/technet/security/bulletin/MS03-023.asp</BulletinUrl>
  <Reason />
  <DownloadURL>http://www.microsoft.com/downloads/details.aspx?FamilyId=FF84E1A58CF5-23DA3AB296B4</DownloadURL>
  <PatchName>Windows2000-KB823559-x86-ENU.exe</PatchName>
  <Description>All versions of Microsoft Windows contain support for file conversion within t
system. This functionality allows users of Microsoft Windows to convert file formats fro
In particular, Microsoft Windows contains support for HTML conversion within the oper
functionality allows users to view, import, or save files as HTML. There is a flaw in the v
converter for Microsoft Windows handles a conversion request during a cut-and-paste
flaw causes a security vulnerability to exist. A specially crafted request to the HTML co
cause the converter to fail in such a way that it could execute code in the context of th
logged-in user. Because this functionality is used by Internet Explorer, an attacker cou
specially formed Web page or HTML e-mail that would cause the HTML converter to run
a user's system. A user visiting an attacker's Web site could allow the attacker to expl
vulnerability without any other user action. To exploit this vulnerability, the attacker w
create a specially-formed HTML e-mail and send it to the user. Alternatively, an attack
```

For help with HFNetChk, type the following in a Command Prompt window:

```
hfnetchk ?
```

For more information about HFNetChk, go to: www.shavlik.com/hfn_exe.aspx.

Compacting the Patch State with PatchEnumerator

The output from HFNetChk is clearly too large to pass on the command line to the VMware ACE environment variable, `VMWARE_NQ_DESCRIPTOR`. The command line can accept at most 4096 bytes. VMware provides `PatchEnumerator`, an XML parser, written in C, to extract a concise XML schema from the HFNetChk output file.



You can find `PatchEnumerator.exe` in the Guest folder that you copied to the virtual machine. `PatchEnumerator` extracts the following XML schema from the `HFNetChk` output file:

```
<State>
  <Product>Product Name </Product>
  <PatchFound>Patch Bulletin ID</PatchFound>
  <MissingPatch>Patch Bulletin ID</MissingPatch>
</State>
```

`PatchEnumerator` is run with the following command line from the update script:

```
PatchEnumerator temp1.xml > tempOUT.xml
```

Note: You can run `PatchEnumerator` independently of the update script if you want to see how it works.

The command line options for `PatchEnumerator` are simply the input and output files:

`temp1.xml` is the XML file generated by `HFNetChk`.

`temp2.xml` is the concise XML file generated by `PatchEnumerator`,

The following shows sample output from `PatchEnumerator`:

```
- <State>
  <Product>INTERNET EXPLORER 6 SP1</Product>
  <Product>WINDOWS 2000 SP4</Product>
  <PatchFound>MS04-003</PatchFound>
  <PatchFound>MS03-033</PatchFound>
  <PatchFound>MS04-018</PatchFound>
  <PatchFound>MS04-013</PatchFound>
  <PatchFound>MS04-004</PatchFound>
  <PatchFound>MS03-032</PatchFound>
  <PatchFound>MS03-020</PatchFound>
  <PatchFound>MS03-014</PatchFound>
  <PatchFound>MS04-037</PatchFound>
  <PatchFound>MS04-031</PatchFound>
  <PatchFound>MS04-024</PatchFound>
  <PatchFound>MS04-023</PatchFound>
  <PatchFound>MS04-022</PatchFound>
  <PatchFound>MS03-049</PatchFound>
  <PatchFound>MS03-045</PatchFound>
  <PatchFound>MS03-044</PatchFound>
  <PatchFound>MS03-039</PatchFound>
  <PatchFound>MS03-034</PatchFound>
  <PatchFound>MS03-026</PatchFound>
  <MissingPatch>MS05-009</MissingPatch>
  <MissingPatch>MS05-014</MissingPatch>
  <MissingPatch>MS05-015</MissingPatch>
  <MissingPatch>MS05-011</MissingPatch>
  <MissingPatch>MS05-008</MissingPatch>
  <MissingPatch>MS05-003</MissingPatch>
  <MissingPatch>MS05-002</MissingPatch>
  <MissingPatch>MS05-001</MissingPatch>
  <MissingPatch>MS04-044</MissingPatch>
  <MissingPatch>TOOL03-039</MissingPatch>
  <MissingPatch>MS03-037</MissingPatch>
  <MissingPatch>MS02-050</MissingPatch>
</State>
```

Using `nq-set` to Save the Patch State to `VMWARE_NQ_DESCRIPTOR`

VMware ACE provides several environment variables that you can use to pass information from the virtual machine to the host machine. One of these variables, `VMWARE_NQ_DESCRIPTOR`, contains the string last set by a guest update of the virtual machine. The `nq-set` command, which is included with VMware Tools, performs a guest update of the virtual machine.



The command line for executing `nq-set` is:

```
C:\Program Files\vmware\vmware tools\vmwareservice -cmd "nq-set
<new descriptor>"
```

The string to set for `VMWARE_NQ_DESCRIPTOR` is the XML patch state generated by `PatchEnumerator`. In the `nq-set` command line, you replace `<new descriptor>` with the output of `PatchEnumerator`.

The `Guest` folder contains a C program, `nqsetcmd`, which builds the command line to invoke the `nq-set` tool. The update script calls `nqsetcmd` and passes two parameters:

- The complete path to the `vmwareservice` command.
- The XML output file from `PatchEnumerator`.

The `nqsetcmd` builds an `nq-set` command line and outputs it to the `nq.bat` file. The update script calls `nqsetcmd` as follows:

```
"c:\Program Files\VMware\VMware Tools\VMwareService.exe"
temp2.xml >> nq.bat
```

The following sample shows the contents of `nq.bat` after the update script executes `nqsetcmd.exe`:

```
@echo off

"c:\Program Files\VMware\VMware Tools\VMwareService.exe" -cmd "nq-set
<State><Product>MDAC 2.5 SP3</Product><Product>INTERNET EXPLORER 5.01 SP4</
Product><Product>WINDOWS 2000 SP4</Product><PatchFound>MS03-023</
PatchFound><MissingPatch>MS04-003</MissingPatch><MissingPatch>MS02-065</
MissingPatch><MissingPatch>MS04-038</MissingPatch><MissingPatch>MS04-018</
MissingPatch><MissingPatch>MS04-044</MissingPatch><MissingPatch>MS04-043</
MissingPatch><MissingPatch>MS04-041</MissingPatch><MissingPatch>MS04-037</
MissingPatch><MissingPatch>MS04-032</MissingPatch><MissingPatch>MS04-031</
MissingPatch><MissingPatch>MS04-023</MissingPatch><MissingPatch>MS04-022</
MissingPatch><MissingPatch>MS04-020</MissingPatch><MissingPatch>MS04-019</
MissingPatch><MissingPatch>MS04-014</MissingPatch><MissingPatch>MS04-012</
MissingPatch><MissingPatch>MS04-011</MissingPatch><MissingPatch>TOOL03-039</
MissingPatch><MissingPatch>MS03-049</MissingPatch><MissingPatch>MS03-044</
MissingPatch><MissingPatch>MS03-043</MissingPatch><MissingPatch>MS03-042</
MissingPatch><MissingPatch>MS03-041</MissingPatch><MissingPatch>MS03-034</
MissingPatch><MissingPatch>MS02-050</MissingPatch></State>"
```

The update script then calls `nq.bat` to execute the `nq-set` command line and set the value of `VMWARE_NQ_DESCRIPTOR` to the XML string output from `PatchEnumerator`.

Note: Execution of the `nq-set` command fails unless if you have already set up custom quarantine with VMware ACE Manager. The rest of the discussion in this section assumes that you have set up custom quarantine and specified a script to run on the host machine. [See Setting up the Host Machine on page 14.](#)

When `nq.bat` executes the `nq-set` command, it triggers execution of the `NQ-Sample` script on the host machine. `NQ-Sample` determines if the `VMWARE_NQ_DESCRIPTOR` variable has been set properly and if so, whether to apply normal or restricted access based on the patch state in `VMWARE_NQ_DESCRIPTOR`. You may check the log file on the host machine if network quarantine is not set as you expect. By default, the log file is in the following directory:

```
C:\Documents and Settings\<username>\My Documents\My Virtual
Machines\<machine_name>\vmware.log
```



Setting up the Host Machine

On the host machine, you must do the following:

- Set up a custom script that reads the patch state generated by the update script on the virtual machine, compares it to a requirements list, and sets network quarantine policies accordingly.
- Run VMware ACE Manager to define network quarantine policies.

Setting up the Custom Host-Machine Script

`NQ-sample` is a C program, included in the `Host` folder, that runs on the host machine and determines whether to set normal or restricted network access for the virtual machine. The script takes an XML patch requirements file as input.

`NQ-sample` does the following:

- Examines the `VMWARE_NQ_DESCRIPTOR` variable from the VMware ACE environment and determines if it is valid. As you recall, this variable is set by a script on the virtual machine and contains the current patch state of the virtual machine. If the variable is invalid, the script outputs `REJECT`. Otherwise, the script goes on to the next step.
- Parses `VMWARE_NQ_DESCRIPTOR` and opens and parses the patch requirements file.
- Searches for the required products and patches (from the requirements file) in the list of installed products and patches (from `VMWARE_NQ_DESCRIPTOR`).

If the script finds all required patches and products, it outputs `YES` and VMware ACE sets normal access.

If any required products or patches are missing, the script outputs `NO` and VMware ACE sets restricted access.

Note: You use the VMware ACE Manager policy editor to define the network access that is enforced for normal and restricted access. See [Setting Network Quarantine Policies on page 15](#).

If the script encounters errors, it exits with a value of 1. All output to `StdErr` is written to the VMware ACE log file. For example, the script writes to `StdErr` a list of any required products or patches that are missing.

You must place a copy of `NQ-sample` in the `Project Resources` directory of the main project directory so VMware ACE can execute the script. You must also put a copy of the requirements file, `patches.xml`, in this directory. The default path to the `Project Resources` directory is:

```

... \My Documents \VMware ACE Projects \<project_name> \Project
Resources

```

The script runs automatically whenever the virtual machines powers on, resets or whenever the virtual machine updates the `VMWARE_NQ_DESCRIPTOR` (that is, whenever the virtual machine user downloads and runs an update script). When you define network quarantine policies in VMware ACE Manager, if you store the policy on a Web server or Active Directory server, you can also specify that the script execute at regular intervals. This is a good practice because it guarantees that the script will enforce restricted quarantine if you add new patches or products to the requirements file.

Note: The sample script looks for the requirements file, `patches.xml`, on the host machine. This is done strictly for simplicity. In a production environment, it makes more sense to place the requirements file on the policy server where the custom scripts for all installed virtual machines



can check for new requirements at regular intervals. See the white paper, "Writing a Simple Authentication Script," available at www.vmware.com/support/resources/ace_resources.html for an example of a script that uses a network file as input.

The `Host` folder contains the source code for `NQ-Sample` so you can see how it works and make changes if you wish. In the `Helper` folder, the `stringlist` folder contains helper routines that `NQ-sample` requires.

Setting Network Quarantine Policies

To set custom network quarantine policies you must identify the script to execute on the host machine and the script must reside in the `Project Resources` directory. Before starting this procedure be certain that you have copied the `nqsample.exe` file to the `Project Resources` directory.

To set custom quarantine policies, complete these steps:

1. In VMware ACE Manager, Start the policy editor (click **Project > Policies**; or from the project summary page, select the **Edit virtual machine policies** icon).
Click the + sign beside the name of the virtual machine. The list of policy categories appears below the virtual machine name.
2. Select **Network quarantine**.
Select **Quarantined access to specific networks and machines**, then click the **Initial Setup** link.
3. The Network Quarantine Options panel of the Network Quarantine Wizard appears.
The wizard guides you through the settings. You may rerun the wizard at any time to change the settings.
Select Custom **quarantine using script**.
Click **Next** to go to the Custom Quarantine Script panel.
4. The Custom Quarantine Script panel appears.
Click **Set** to specify the plug-in script you want to use.
5. The Set Custom Script dialog box appears.
Enter the path to `NQ-Sample` or click **Browse** to navigate to the file. The `NQ-Sample` script should be in the `Project Resources` folder under the project folder for the current project.
The `NQ-Sample` script takes the `patches.xml` requirements file as a parameter. Enter the script name and parameter in Command line, as follows:

```
NQ-Sample.exe patches.xml
```


Note: For simplicity's sake, the requirements file is stored in the virtual machine. You need to specify the complete path to `patches.xml`. In a production environment, it makes more sense to put the requirements file on the policy server so you can dynamically update patch requirements.
If you wish, you may specify a timeout interval. If the script has not completed by the end of that interval, VMware ACE terminates the script.
Click **OK**, then click **Next**.
6. The Policy Lookup panel appears.



Select the type of server you want to use to store the list of approved networks and machines. VMware ACE checks the list on this server to determine what network access is approved for the virtual machine.

Note: You can choose to store the policy with the virtual machine by choosing **Static**. However, it is a limitation of the VMware ACE software that when you choose **Static**, the script cannot be set to run at specified intervals. Therefore, it is recommended that you store the policy on a Web server or an Active Directory server and choose to run the script at periodic intervals.

- **Active Directory** — Select this option if you plan to store the network quarantine policy on your Active Directory server. The wizard adds this information to your Active Directory server for you.

Note: In order to use the directory service option, you must choose an Active Directory domain in the project settings editor. If you select **Active Directory** and have not yet chosen an Active Directory domain, the wizard opens a dialog box that gives you the option of setting the domain at this time. Click **Yes** to open the Policies Domain dialog box.

If you store policies on your Active Directory server, they are stored in a container called VMware directly under the top hierarchy of the domain controller container. By default, this container is not visible in the MMC console. To view the container, in Manage Active Directory Users and Computers, enable advanced features (**View > Advanced Features**).

- **Web server** — Select this option if you plan to store the network quarantine policy on a Web server. Enter the URL of the file where you plan to store the list. Be sure to include the filename in the URL. The wizard creates this file for you at the end of the process.

Click **Update Interval** to specify how often VMware ACE should check for changes to the network quarantine policies. You may choose an interval from 5 minutes to 2 days. The default is 5 minutes.

Click **Next**.

7. The Normal Access panel appears.

Select the way you want to specify network access.

- **Full access** — No restrictions are imposed.
- **Allow access to selected networks and machines** — Specify a whitelist of networks and machines with which the virtual machine may communicate.
- **Deny access to selected networks and machines** — Specify a blacklist of networks and machines with which the virtual machine is not allowed to communicate.

You may set up either a whitelist or a blacklist but not both.

For simplicity, this example assumes you select **Full Access**. If you select either of the other options, a panel appears for specifying a whitelist or blacklist.

Click **Next**.

8. The Restricted Access panel appears.

This panel and the next enable you to choose the network access for machines whose version is out of date.

Select **Allow access to selected networks and machines**, which means out of date virtual machines can connect only to the specific server or servers you specify in the next panel.

Click **Next**.



9. The Networks and Machines panel appears.

Enter the IP address or the fully qualified host name (if you are on the same network) of your update server; for example, your SMS, LANDesk or Altiris server.

Click **Add**. The address appears in the **Allowed IP addresses** field.
10. The Additional Network Traffic panel appears.

Accept all defaults and click **Next**.
11. The Messages panel appears.

Enter a custom message that end users see when the virtual machine is out of date and has restricted access. In the message, be certain to include instructions on how to contact the update server for updates. For example, include the URL of the update server.

Click **Next** to continue.
12. The Summary panel appears.

If you are ready to deploy the policy, click **Next** to go to the Deploy Policy panel. Click **Finish** to save the policy without deploying it. For example, if you do not have access to the policy server from the machine on which you are running VMware ACE Manager, you can save the file and copy it later to the policy server.

The Deploy Policy panel is different depending on whether you select **Web server** or **Active Directory**.
13. If you select **Web server**, when the Deploy Policy panel appears, select **Mark this policy as deployed and save it to a network quarantine policy file** to capture your policy changes. You may type the path and filename for the policy file or click **Browse** to navigate to the location where you want to save the file. VMware ACE Manager automatically copies the policy file to the URL shown in this panel. The policies take effect as soon as you make the file available on the Web server.

Click **Finish** to save the policy file.

If you select **Active Directory**, when the Deploy Policy panel appears, select **Deploy the network quarantine policy to your Active Directory server**. When you click **Finish**, the wizard deploys the policies, which take effect immediately.

Testing the Update Script

With all the pieces in place, you should be able to run the `Update.bat` file to update the state of the virtual machine. To start the virtual machine from VMware ACE Manager, click **Run in VMWare ACE**, which runs the virtual machine in preview mode.

Note: If you power on the virtual machine by clicking **Start this virtual machine**, the changes from the `nq-set` command take effect, but changes are not visible because policies are only enforced in preview mode or when a user powers on an installed virtual machine.

Execute the update script from a Windows Command Prompt window, as follows:

```
update
```

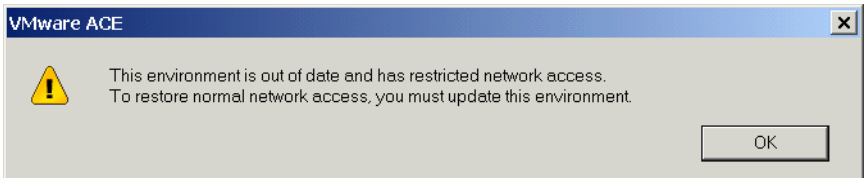
You should see messages similar to the following:

```
Scanning MachineName-0289ED78
.....
Done scanning MachineName-0289ED78
Enumerating products and patches...
Building NQ-SET command line...
```



```
Executing NQ-SET command...
Updating of Guest OS Complete!
```

If the patch state does not match the patches in the requirements file, the out of date message you specified appears in the virtual machine. The following is the default out of date message:



Be certain that the message you specify directs end users to download a new update script and patch from the update server.

When network access is restricted, a red arrow appears next to the network quarantine icon at the bottom of the virtual machine window:



Users can click the network quarantine icon to see the status of network access, including the quarantine message and instructions. They can also click **VMware ACE > Troubleshoot > Update Available** to access the update instructions.

You can also check the check the log file on the host machine for errors and messages. The following shows a portion of a sample log file after running the update script.

```
...
Mar 24 23:56:25: vcpu-0| Policy: Will execute script with command line:
"C:\Documents and Settings\Administrator\My Documents\VMware ACE
Projects\Fun\Project Resources\NQ-Sample1.exe" patches.xml
Mar 24 23:56:25: vcpu-0| POLICY: stderr from script: NQ_DESCRIPTOR: (null)
Mar 24 23:56:25: vcpu-0| Required Product: WINDOWS 2000 SP4
Mar 24 23:56:25: vcpu-0| Required Patch: MS03-023
Mar 24 23:56:25: vcpu-0| Required product "WINDOWS 2000 SP4" was not installed
Mar 24 23:56:25: vcpu-0| Required patch "MS03-023" was not installed
Mar 24 23:56:25: vcpu-0| Policy: Script output: "NO"
```

The requirements file specified one product, WINDOWS 2000 SP4, and one patch, MS03-023, both of which are missing. Therefore the script outputs "NO" and applies restricted access.

In practice, the response to restricted access is to download a new patch and rerun the update script to update the `VMWARE_NQ_DESCRIPTOR` variable with the new patch state.

However, you can easily verify that the script is working without installing new patches by simply changing the requirements file. For example, open the requirements file (`patches.xml` for the sample custom quarantine script) in the `Project Resources` directory. Remove requirements for any products or patches that you know are not installed on the virtual machine. You can remove all requirements if you wish.

Then rerun the update script on the virtual machine. The virtual machine should now have normal access. Because the patch state is current with the requirements file, the restricted arrow does not appear or if it was displayed, it goes away.



Deploying the Virtual Machine Package

For security reasons, you must deploy plug-ins as part of a package to be installed by the package installer. You cannot deploy plug-ins separately to end users' computers and end users cannot modify them.

Note: The plug-in script is the script that runs on the host computer. In this example, it is the `NQ-sample` program that determines whether to assign normal or restricted access. You install the tools that examine the state of the virtual machine in the operating system of the virtual machine.

When you are satisfied with your custom quarantine script and with other aspects of the project you can use the package creation wizard in VMware ACE Manager to create a package. Be certain that the correct version of the script is in the `Project_Resources` directory so the package creation wizard can find it and include it in the package.

For details on creating packages, see the *VMware ACE Administrator's Manual* or the technical note "Best Practices for Setting Up VMware ACE," available at: www.vmware.com/support/resources/ace_resources.html.

The Update File Contents

This section shows the sample `update.bat` file.

```
@echo off
REM ** Take us to the patching directory
c:
cd \patching
REM ** Download patches
REM ** Install patches
REM **
REM ** Run the HFNetChk tool
REM ** The output of HFNetChk is an XML file that describes the
REM ** installed products, found patches, and missing patches
REM **
echo.Checking installed products, and patches...
hfnetchk.exe -o xml2 -history -f temp1.xml
REM **
REM ** Next run the custom program PatchEnumerator
REM ** The output of PatchEnumerator is a concise list of
REM ** installed product names, missing patches, and found patches
REM ** This is also an XML file
REM **
REM ** This list was derived from the xml file output of hfnetchk
REM **
echo.Enumerating products and patches...
PatchEnumerator.exe temp1.xml > temp2.xml
REM **
REM ** Next run the custom program nqsetcmd
REM ** This program combines the path to the vmwareservice tool
REM ** (installed with VMware tools), and the output from
```



```
REM ** PatchEnumerator to create the command line that when
REM ** executed sets the custom Network Quarantine descriptor to
REM ** the output of PatchEnumerator
REM **
REM ** This information is used by the Network Quarantine
REM ** custom script to determine whether to quarantine this host.
REM **

echo.Building NQ-SET command line...
echo @echo off > nq.bat

ngsetcmd.exe "c:\Program Files\VMware\VMware
Tools\VMwareService.exe" temp2.xml >> nq.bat

REM **
REM ** Now execute the command line we built above
REM **

echo.Executing NQ-SET command...
call nq.bat

REM **
REM ** ALL DONE!
REM **

echo.Updating of Guest OS Complete!
```