VMware Department of Defense (DoD) Security Technical Implementation Guide (STIG) vSphere Installation Bundle (VIB) Overview and Installation Guide

Prepared by

Ryan Lakey
VMware Professional Services
rlakey@vmware.com

Version History

Date	Ver.	Author	Description	Reviewers
11/3/2015	1.0	Ryan Lakey	Initial Release	
8/27/2016	2.0	Ryan Lakey	Updated for ESXi 5.0 version 9 and ESXi 6.0 version 2 of the STIG. Removed GEN002140-ESXI5-000046 as it was listed in error. Added vulnerability IDs to items remediated tables.	

VMware, Inc.
3401 Hillview Ave
Palo Alto, CA 94304
www.vmware.com

Contents

List of Figures

1. Overview

1.1 Summary

The DoD Security Technical Implementation Guide (STIG) ESXi VIB is a fling that provides a custom VMware signed ESXi VIB to assist in remediating Defense Information Systems Agency (DISA) STIG controls for ESXi.

This VIB has been developed to help customers rapidly implement the more challenging aspects of the vSphere STIG that must be done in a manual time consuming effort directly on the ESXi hosts, or required complex scripting, or even development of a VIB in house that was not officially signed by VMware and therefore could not be deployed as normal patches would.

The need for a VMware signed VIB is due to the “system” level files that are replaced which cannot be replaced at a “community supported” acceptance level.

1.2 Benefits

The use of the VMware signed STIG VIBs provides customers the following benefits:

- The ability to use vSphere Update Manager (VUM) to quickly deploy the VIB to ESXi hosts where you cannot do this with a customer created VIB.
- The ability to use VUM to quickly check if all ESXi hosts have the STIG VIB installed and therefore also compliance.
- No need to manually replace and copy files directly on each ESXi host in your environment.
- No need to create complex shell scripts that run each time ESXi boots to re-apply settings.

1.3 System Requirements

ESXi 5.x and 6.0 are supported but each have a different set of VIBs as the vSphere 5.0 and 6.0 STIGs have different requirements.

The following VIBs are provided for each ESXi version as follows:

ESXi 5.x

- dod-esxi5-stig-rd
- dod-esxi5-stig-re

ESXi 6.0

- dod-esxi6-stig-rd
- dod-esxi6-stig-re

1.4 Why two VIBs?

Multiple versions of each VIB were created as marked by the “rd” and “re” in the filename. This designation is for root SSH enabled and root SSH disabled. Depending on your organizational policies and whether or not it is possible to join ESXi to Active Directory will dictate which VIB fits your needs.

STIG ID SRG-OS-000109-ESXI5 for 5.0 and STIG ID ESXI-06-000014 for 6.0 requires root logins be disabled via SSH.

1.5 Support

Since these VIBs are released as a fling they are not officially supported by VMware. However they have gone through basic functionality and installation testing.

1.6 What this STIG VIB does NOT do

Installing this STIG VIB will NOT completely remediate your ESXi hosts against the vSphere STIG. Installation only addresses a subset of items found in the STIG that would normally require manual remediation.

1.7 Versioning

The version of the STIG VIB will follow the DISA STIG versioning. For example the current vSphere 5.0 ESXi STIG is release 1 version 8 so the VIB would be version 1.0.8 to match. Any updates to the STIG that warrant a change in the VIB will have its version updated accordingly.

2. VIB Contents

2.1 What's in the 5.x STIG VIB?

The 5.x STIG VIB will replace the following files on the ESXi host:

- /etc/issue
    - Updated to contain the DoD login banner
- /etc/pam.d/passwd
    - Updated to meet STIG password complexity requirements and policies
- /etc/ssh/sshd_config
    - Updated to add necessary SSH daemon settings from the STIG

The 5.x STIG VIB remediates the following STIG IDs:

STIG ID	Vuln ID	Severity
GEN000585-ESXI5-000080	V-39263	CAT II
GEN000790-ESXI5-000085	V-39246,V-39418	CAT II
GEN005515-ESXI5-000100	V-39248	CAT III
GEN005517-ESXI5-000101	V-39250	CAT III
GEN005519-ESXI5-000102	V-39265	CAT II
GEN005528-ESXI5-000106	V-39266	CAT II
GEN005530-ESXI5-000107	V-39267	CAT II
GEN005531-ESXI5-000108	V-39268	CAT II
GEN005536-ESXI5-000110	V-39420	CAT II
GEN005539-ESXI5-000113	V-39285	CAT II
SRG-OS-000023-ESXI5	V-39394	CAT II
SRG-OS-000027-ESXI5	V-39253	CAT II
SRG-OS-000033-ESXI5	V-39411	CAT I
SRG-OS-000069-ESXI5	V-39255	CAT II
SRG-OS-000070-ESXI5	V-39256,V-39257	CAT II
SRG-OS-000071-ESXI5	V-39258	CAT II
SRG-OS-000072-ESXI5	V-39259	CAT II
SRG-OS-000077-ESXI5	V-39261	CAT II
SRG-OS-000078-ESXI5	V-39262	CAT II
SRG-OS-000109-ESXI5	V-39391	CAT II
SRG-OS-000112-ESXI5	V-39412	CAT I
SRG-OS-000120-ESXI5	V-39260	CAT II
SRG-OS-000250-ESXI5	V-39415	CAT I
SRG-OS-000266-ESXI5	V-39416	CAT II

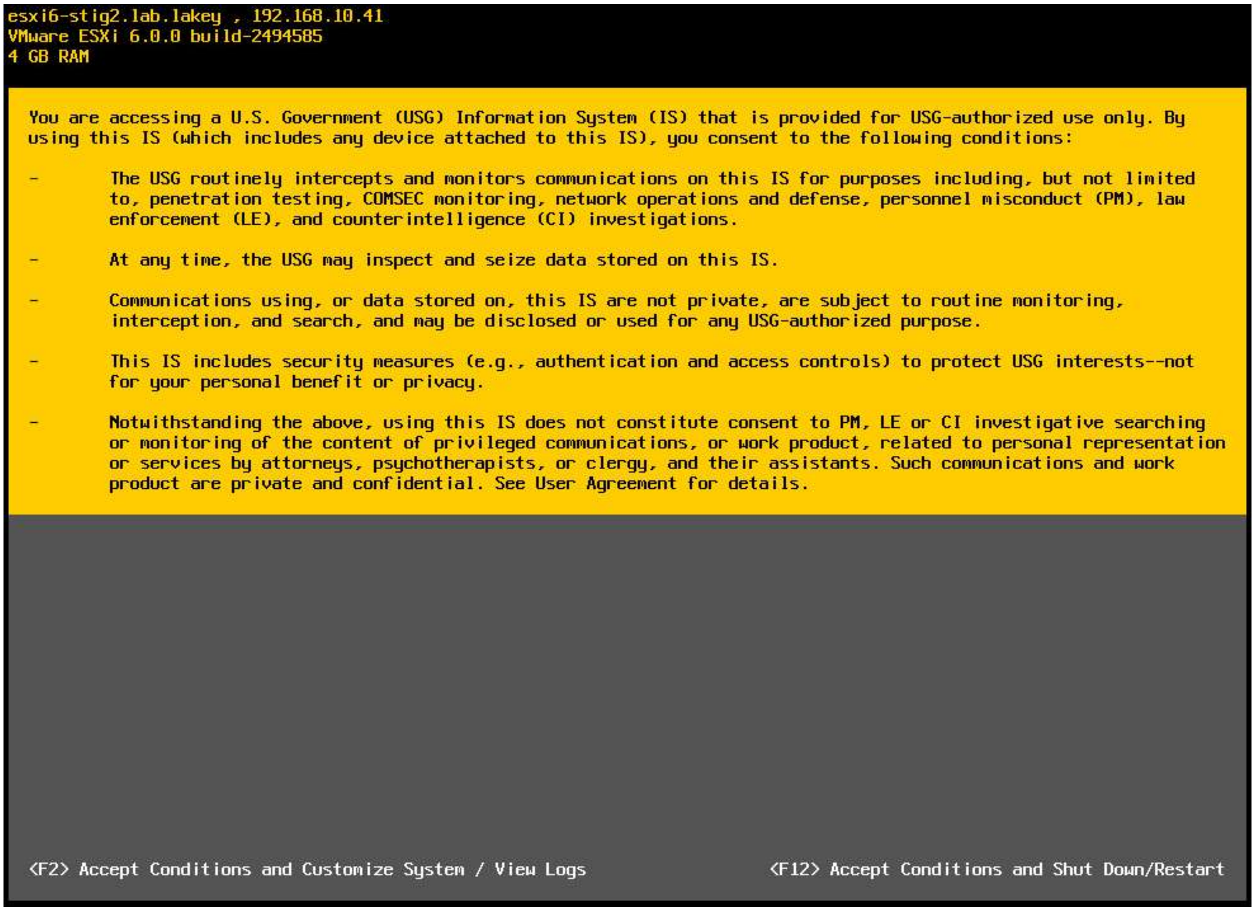
Note – Creation of the /etc/ssh/ssh_config file is no longer required as of the vSphere ESXi 5.0 Version 1 Release 5 STIG so this file is not included in the VIB as it does not exist by default. If this file does exist in your environment then it must be configured according to the STIG.

2.2 What's in the 6.0 STIG VIB?

The 6.0 STIG VIB will replace the following files on the ESXi host:

- /etc/issue
  - Updated to contain the DoD login banner
- /etc/pam.d/passwd
  - Updated to meet STIG password complexity requirements and policies
- /etc/ssh/sshd_config
  - Updated to add necessary SSH daemon settings from the STIG
- /etc/vmware/welcome
  - Updated to add the DoD login banner to the Direct Console UI (DCUI) login screen

Figure 1. DCUI Login screen with DoD Login Banner



```
esxi6-stig2.lab.lakey , 192.168.10.41
VMware ESXi 6.0.0 build-2494585
4 GB RAM

  You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By
  using this IS (which includes any device attached to this IS), you consent to the following conditions:

  -       The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited
          to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law
          enforcement (LE), and counterintelligence (CI) investigations.

  -       At any time, the USG may inspect and seize data stored on this IS.

  -       Communications using, or data stored on, this IS are not private, are subject to routine monitoring,
          interception, and search, and may be disclosed or used for any USG-authorized purpose.

  -       This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not
          for your personal benefit or privacy.

  -       Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching
          or monitoring of the content of privileged communications, or work product, related to personal representation
          or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work
          product are private and confidential. See User Agreement for details.

  <F2> Accept Conditions and Customize System / View Logs                 <F12> Accept Conditions and Shut Down/Restart
```

The 6.0 STIG VIB remediates the following STIG IDs:

STIG ID	Vuln ID	Severity
ESXI-06-000007	V-63183	CAT II
ESXI-06-000008	V-63185	CAT II
ESXI-06-000009	V-63187	CAT II
ESXI-06-000010	V-63189	CAT II

STIG ID	Vuln ID	Severity
ESXI-06-000011	V-63191	CAT I
ESXI-06-000012	V-63193	CAT II
ESXI-06-000013	V-63195	CAT II
ESXI-06-000014	V-63197	CAT III
ESXI-06-000015	V-63199	CAT I
ESXI-06-000016	V-63201	CAT II
ESXI-06-000017	V-63203	CAT II
ESXI-06-000018	V-63205	CAT III
ESXI-06-000019	V-63207	CAT III
ESXI-06-000020	V-63209	CAT II
ESXI-06-000021	V-63211	CAT II
ESXI-06-000022	V-63213	CAT III
ESXI-06-000023	V-63215	CAT II
ESXI-06-000024	V-63217	CAT II
ESXI-06-000025	V-63219	CAT II
ESXI-06-000026	V-63221	CAT III
ESXI-06-000027	V-63223	CAT III
ESXI-06-000028	V-63225	CAT II
ESXI-06-000031	V-63231	CAT II
ESXI-06-000032	V-63233	CAT II
ESXI-06-000033	V-63235	CAT II
ESXI-06-100007	V-63485	CAT II
ESXI-06-100010	V-63501	CAT II
ESXI-06-100031	V-63531	CAT II
ESXI-06-200031	V-63867	CAT II
ESXI-06-300031	V-63905	CAT II
ESXI-06-400031	V-63919	CAT II
ESXI-06-500031	V-63923	CAT II

3. Installation procedures

3.1 Installing the DoD STIG VIB for 5.x or 6.0

3.1.1 Manual Installation

To install a VIB manually you will have to copy the installation file locally to the host or to a datastore which the host has access too. You can do this via the datastore browser or with a scp client like WinSCP.

Once you have the file copied, follow these steps:

1. Enable SSH or the local shell on your ESXi host.
2. Login to the host as root or equivalent.
3. Execute the following command to install:

```
esxcli software vib install -v <path to VIB>
```

Note – Maintenance mode and a reboot is not required to complete the installation.

4. To verify the installation you can execute the following command:

```
esxcli software vib list | more
```

3.1.2 Installation with vSphere Update Manager

The STIG VIB can also be deployed through VUM to make installation and compliance checking easier in large environments.

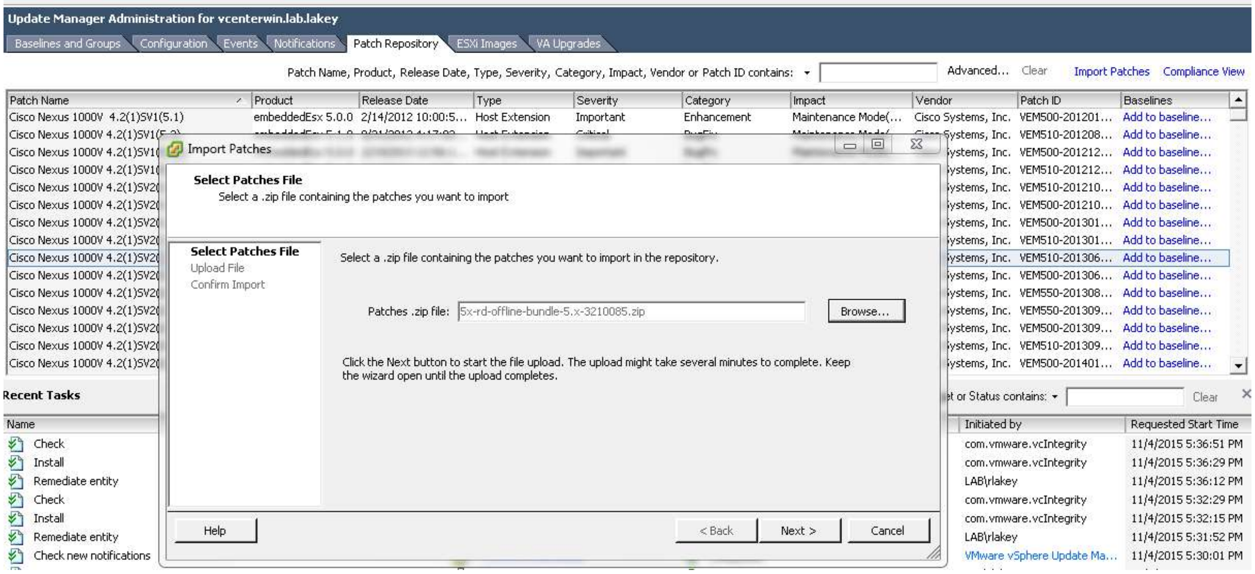
To deploy through VUM, follow these steps:

1. Login to the vSphere client and navigate to Update Manager.

Note – These steps can be performed through the vSphere Web Client as of 6.0 Update 1.

2. Go to the patch repository tab and select Import Patches.
3. Browse to the offline bundle zip file of the STIG VIB and click next to import.

Figure 2. Import Patch through VUM



Update Manager Administration for vcenterwin.lab.lakey

Patch Name	Product	Release Date	Type	Severity	Category	Impact	Vendor	Patch ID	Baselines
Cisco Nexus 1000V 4.2(1)SV1(5.1)	embeddedEsx 5.0.0	2/14/2012 10:00:5...	Host Extension	Important	Enhancement	Maintenance Mode(...	Cisco Systems, Inc.	VEM500-201201...	Add to baseline...
Cisco Nexus 1000V 4.2(1)SV1(							Systems, Inc.	VEM510-201208...	Add to baseline...
Cisco Nexus 1000V 4.2(1)SV1(							ystems, Inc.	VEM500-201212...	Add to baseline...
Cisco Nexus 1000V 4.2(1)SV1(							ystems, Inc.	VEM510-201212...	Add to baseline...
Cisco Nexus 1000V 4.2(1)SV2(							ystems, Inc.	VEM510-201210...	Add to baseline...
Cisco Nexus 1000V 4.2(1)SV2(							ystems, Inc.	VEM500-201210...	Add to baseline...
Cisco Nexus 1000V 4.2(1)SV2(							ystems, Inc.	VEM500-201301...	Add to baseline...
Cisco Nexus 1000V 4.2(1)SV2(							ystems, Inc.	VEM510-201301...	Add to baseline...
Cisco Nexus 1000V 4.2(1)SV2(							ystems, Inc.	VEM510-201306...	Add to baseline...
Cisco Nexus 1000V 4.2(1)SV2(							ystems, Inc.	VEM500-201306...	Add to baseline...
Cisco Nexus 1000V 4.2(1)SV2(							ystems, Inc.	VEM550-201308...	Add to baseline...
Cisco Nexus 1000V 4.2(1)SV2(							ystems, Inc.	VEM550-201309...	Add to baseline...
Cisco Nexus 1000V 4.2(1)SV2(							ystems, Inc.	VEM500-201309...	Add to baseline...
Cisco Nexus 1000V 4.2(1)SV2(							ystems, Inc.	VEM510-201309...	Add to baseline...
Cisco Nexus 1000V 4.2(1)SV2(							ystems, Inc.	VEM500-201401...	Add to baseline...

Import Patches

Select Patches File

Select a .zip file containing the patches you want to import

Select a .zip file containing the patches you want to import in the repository.

Patches .zip file: 5x-rd-offline-bundle-5.x-3210085.zip

Click the Next button to start the file upload. The upload might take several minutes to complete. Keep the wizard open until the upload completes.

Name	Initiated by	Requested Start Time
Check	com.vmware.vcIntegrity	11/4/2015 5:36:51 PM
Install	com.vmware.vcIntegrity	11/4/2015 5:36:29 PM
Remediate entity	LAB\rlakey	11/4/2015 5:36:12 PM
Check	com.vmware.vcIntegrity	11/4/2015 5:32:29 PM
Install	com.vmware.vcIntegrity	11/4/2015 5:32:15 PM
Remediate entity	LAB\rlakey	11/4/2015 5:31:52 PM
Check new notifications	VMware vSphere Update Ma...	11/4/2015 5:30:01 PM

4. Next create a baseline that will include the patch that can then be attached to hosts.

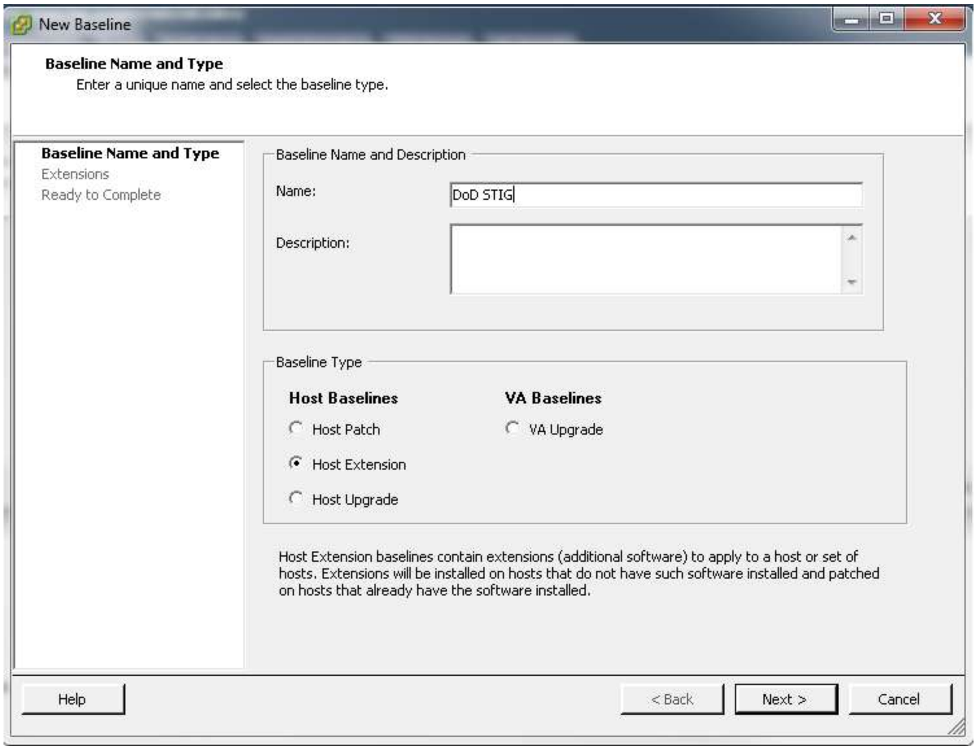
5. Go to the Baselines and Groups tab and under Baselines click create.

6. Enter a name and select Host Extension for the type and click next.

7. Add the DoD ESXi STIG VIB to the baseline and click next to finish.

8. You can then attach the baseline to hosts and perform a scan to check compliance and then perform installations. Alternatively you can create a baseline group to include the newly created baseline in.

Figure 3. New Baseline creation in VUM Name and Type



New Baseline

Baseline Name and Type

Enter a unique name and select the baseline type.

Baseline Name and Description

Name: DoD STIG

Description:

Baseline Type

Host Baselines

○ Host Patch

● Host Extension

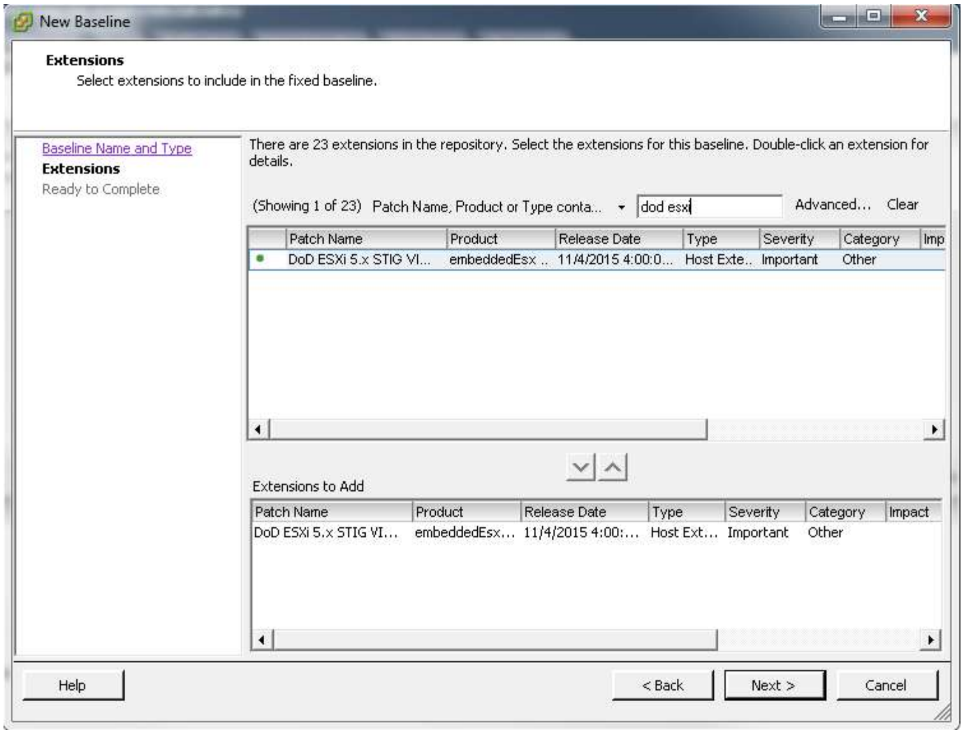
○ Host Upgrade

VA Baselines

○ VA Upgrade

Host Extension baselines contain extensions (additional software) to apply to a host or set of hosts. Extensions will be installed on hosts that do not have such software installed and patched on hosts that already have the software installed.

Figure 4. New Baseline create in VUM Add Extension



Extensions

Select extensions to include in the fixed baseline.

There are 23 extensions in the repository. Select the extensions for this baseline. Double-click an extension for details.

(Showing 1 of 23) Patch Name, Product or Type conta... dod esxi

Patch Name	Product	Release Date	Type	Severity	Category	Imp
● DoD ESXi 5.x STIG VI...	embeddedEsx ..	11/4/2015 4:00:0...	Host Exte..	Important	Other	

Extensions to Add

Patch Name	Product	Release Date	Type	Severity	Category	Impact
DoD ESXi 5.x STIG VI...	embeddedEsx...	11/4/2015 4:00:...	Host Ext...	Important	Other	

3.1.3 Installation with PowerCLI

Another alternative for installation is through PowerCLI. Although outside the scope of this document use of the Get-ESXCli command could be used for installation through scripting.

3.2 Updating the DoD STIG VIB for 5.x or 6.0

3.2.1 Manual updates

Should an updated version of the STIG VIB be released as DISA updates the STIGs you may need to update your ESXi hosts. To update a VIB manually you will have to copy the installation file locally to the host or to a datastore which the host has access too. You can do this via the datastore browser or with a scp client like WinSCP.

Once you have the file copied, follow these steps:

1. Enable SSH or the local shell on your ESXi host.
2. Login to the host as root or equivalent.
3. Execute the following command to update:

```
esxcli software vib update -v <path to VIB>
```

3.2.2 Updates with VUM

Updates with VUM will follow the same procedures as a new install. VUM will detect the newly imported patch as a newer version once it is added to a baseline and hosts are scanned.

3.3 Removing the DoD STIG VIB for 5.x or 6.0

3.3.1 Manual removal

If removal of the STIG VIB is needed it can be done by following these steps:

1. Enable SSH or the local shell on your ESXi host.
2. Login to the host as root or equivalent.
3. Execute the following command to update:

```
esxcli software vib remove –n <name to VIB>
```

4. Reboot the host to complete the removal.

Appendix A: Glossary

DoD – Department of Defense

DISA – Defense Information Systems Agency

STIG – Security Technical Implementation Guide

VIB – vSphere Installation Bundle

VUM – vSphere Update Manager

Appendix B: References

DISA vSphere STIGs - http://iase.disa.mil/stigs/os/virtualization/Pages/index.aspx

VMware DoD STIG VIB Fling – https://labs.vmware.com/flings/dod-security-technical-implementation-guidestig-esxi-vib

Appendix C: VIB Details

5.x File Contents

/etc/issue

```
You are accessing a U.S. Government (USG) Information System (IS) that is
provided for USG-authorized use only. By using this IS (which includes any
device attached to this IS), you consent to the following conditions: -The
USG routinely intercepts and monitors communications on this IS for purposes
including, but not limited to, penetration testing, COMSEC monitoring,
network operations and defense, personnel misconduct (PM), law enforcement
(LE), and counterintelligence (CI) investigations. -At any time, the USG may
inspect and seize data stored on this IS. -Communications using, or data
stored on, this IS are not private, are subject to routine monitoring,
interception, and search, and may be disclosed or used for any USG-authorized
purpose. -This IS includes security measures (e.g., authentication and access
controls) to protect USG interests--not for your personal benefit or privacy.
-Notwithstanding the above, using this IS does not constitute consent to PM,
LE or CI investigative searching or monitoring of the content of privileged
communications, or work product, related to personal representation or
services by attorneys, psychotherapists, or clergy, and their assistants.
Such communications and work product are private and confidential. See User
Agreement for details.
```

/etc/pam.d/passwd

```
#%PAM-1.0

password   requisite    /lib/security/$ISA/pam_passwdqc.so similar=deny
retry=3 min=disabled,disabled,disabled,disabled,14

password   sufficient   /lib/security/$ISA/pam_unix.so use_authtok nullok
shadow sha512 remember=5

password   required     /lib/security/$ISA/pam_deny.so
```

/etc/ssh/sshd_config

Note – Root disabled VIB will have PermitRootLogin no instead of yes

```
# running from inetd
# Port 2200
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key

UsePrivilegeSeparation no

SyslogFacility auth
LogLevel info

PrintMotd yes
PrintLastLog no

TCPKeepAlive yes

Ciphers aes128-ctr,aes192-ctr,aes256-ctr

UsePAM yes
# only use PAM challenge-response (keyboard-interactive)
PasswordAuthentication no

Subsystem sftp /usr/lib/vmware/openssh/bin/sftp-server -f LOCAL5 -l INFO

AuthorizedKeysFile /etc/ssh/keys-%u/authorized_keys

# Timeout value of 10 mins. The default value of ClientAliveCountMax is 3.
# Hence, we get a  3 * 200 = 600 seconds timeout if the client has been
# unresponsive.
ClientAliveInterval 200

# sshd(8) will refuse connection attempts with a probability of "rate/100"
# (30%) if there are currently "start" (10) unauthenticated connections.  The
# probability increases linearly and all connection attempts are refused if
the
# number of unauthenticated connections reaches "full" (100)
MaxStartups 10:30:100

# STIG Customization

#SRG-OS-000109-ESXI5
PermitRootLogin yes

#SRG-OS-000023-ESXI5
Banner /etc/issue

#SRG-OS-000033-ESXI5, SRG-OS-000112-ESXI5
Protocol 2

#GEN005515-ESXI5-000100
AllowTcpForwarding no
```

```
#GEN005517-ESXI5-000101

GatewayPorts no


#GEN005519-ESXI5-000102

X11Forwarding no


#GEN005528-ESXI5-000106

AcceptEnv LOCALE


#GEN005530-ESXI5-000107

PermitUserEnvironment no


#GEN005531-ESXI5-000108

PermitTunnel no


#GEN005536-ESXI5-000110

StrictModes yes


#GEN005539-ESXI5-000113

Compression no


#SRG-OS-000027-ESXI5

MaxSessions 1


#SRG-OS-000250-ESXI5
```

```
MACs hmac-sha1,hmac-sha1-96
```

6.0 File Contents

/etc/issue

```
You are accessing a U.S. Government (USG) Information System (IS) that is
provided for USG-authorized use only. By using this IS (which includes any
device attached to this IS), you consent to the following conditions: -The
USG routinely intercepts and monitors communications on this IS for purposes
including, but not limited to, penetration testing, COMSEC monitoring,
network operations and defense, personnel misconduct (PM), law enforcement
(LE), and counterintelligence (CI) investigations. -At any time, the USG may
inspect and seize data stored on this IS. -Communications using, or data
stored on, this IS are not private, are subject to routine monitoring,
interception, and search, and may be disclosed or used for any USG-authorized
purpose. -This IS includes security measures (e.g., authentication and access
controls) to protect USG interests--not for your personal benefit or privacy.
-Notwithstanding the above, using this IS does not constitute consent to PM,
LE or CI investigative searching or monitoring of the content of privileged
communications, or work product, related to personal representation or
services by attorneys, psychotherapists, or clergy, and their assistants.
Such communications and work product are private and confidential. See User
Agreement for details.
```

/etc/pam.d/passwd

```
#%PAM-1.0



# Change only through host advanced option "Security.PasswordQualityControl".

password   requisite    /lib/security/$ISA/pam_passwdqc.so similar=deny
retry=3 min=disabled,disabled,disabled,disabled,15

password   sufficient   /lib/security/$ISA/pam_unix.so use_authtok nullok
shadow sha512 remember=5
```

```
password   required     /lib/security/$ISA/pam_deny.so
```

/etc/ssh/sshd_config

Note – Root disabled VIB will have PermitRootLogin no instead of yes

```
# running from inetd
# Port 2200

## VMware Default Settings not part of the STIG ##

HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key

UsePrivilegeSeparation no

SyslogFacility auth
LogLevel info

PrintMotd yes
PrintLastLog no

TCPKeepAlive yes

UsePAM yes
# only use PAM challenge-response (keyboard-interactive)
PasswordAuthentication no
```

```
Subsystem sftp /usr/lib/vmware/openssh/bin/sftp-server

AuthorizedKeysFile /etc/ssh/keys-%u/authorized_keys

# sshd(8) will refuse connection attempts with a probability of “rate/100”
# (30%) if there are currently “start” (10) unauthenticated connections.  The
# probability increases linearly and all connection attempts are refused if the
# number of unauthenticated connections reaches “full” (100)
MaxStartups 10:30:100

## DoD STIG Items Below ##
Banner /etc/issue
Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,aes192-cbc,aes256-cbc
Protocol 2
IgnoreRhosts yes
HostbasedAuthentication no
PermitRootLogin yes
PermitEmptyPasswords no
PermitUserEnvironment no
MACs hmac-sha1,hmac-sha2-256,hmac-sha2-512
GSSAPIAuthentication no
KerberosAuthentication no
StrictModes yes
```

```
Compression no

GatewayPorts no

X11Forwarding no

AcceptEnv

PermitTunnel no

ClientAliveCountMax 3

ClientAliveInterval 200

MaxSessions 1
```

/etc/vmware/welcome

```
{bgcolor:black} {/color}{align:left}{bgcolor:black}{color:yellow}{hostname} ,
{ip}{/color}{/bgcolor}{/align}

{bgcolor:black} {/color}{align:left}{bgcolor:black}{color:yellow}{esxproduct}
{esxversion}{/color}{/bgcolor}{/align}

{bgcolor:black} {/color}{align:left}{bgcolor:black}{color:yellow}{memory}
RAM{/color}{/bgcolor}{/align}

{bgcolor:black} {/color}{align:left}{bgcolor:black}{color:white}   {/color}{/bgcolor}{/align}

{bgcolor:black} {/color}{align:left}{bgcolor:yellow}{color:black}
{/color}{/bgcolor}{/align}

{bgcolor:black} {/color}{align:left}{bgcolor:yellow}{color:black}  You are accessing a U.S.
Government (USG) Information System (IS) that is provided for USG-authorized use only. By
{/color}{/bgcolor}{/align}

{bgcolor:black} {/color}{align:left}{bgcolor:yellow}{color:black}  using this IS (which includes
any device attached to this IS), you consent to the following conditions:
{/color}{/bgcolor}{/align}

{bgcolor:black} {/color}{align:left}{bgcolor:yellow}{color:black}
{/color}{/bgcolor}{/align}

{bgcolor:black} {/color}{align:left}{bgcolor:yellow}{color:black}  -       The USG routinely
intercepts and monitors communications on this IS for purposes including, but not limited
{/color}{/bgcolor}{/align}
```

```
{bgcolor:black} {/color}{align:left}{bgcolor:yellow}{color:black}          to, penetration
testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law
{/color}{/bgcolor}{/align}

{bgcolor:black} {/color}{align:left}{bgcolor:yellow}{color:black}          enforcement (LE), and
counterintelligence (CI) investigations.
{/color}{/bgcolor}{/align}

{bgcolor:black} {/color}{align:left}{bgcolor:yellow}{color:black}
{/color}{/bgcolor}{/align}

{bgcolor:black} {/color}{align:left}{bgcolor:yellow}{color:black}  -       At any time, the USG
may inspect and seize data stored on this IS.
{/color}{/bgcolor}{/align}

{bgcolor:black} {/color}{align:left}{bgcolor:yellow}{color:black}
{/color}{/bgcolor}{/align}

{bgcolor:black} {/color}{align:left}{bgcolor:yellow}{color:black}  -       Communications using,
or data stored on, this IS are not private, are subject to routine monitoring,
{/color}{/bgcolor}{/align}

{bgcolor:black} {/color}{align:left}{bgcolor:yellow}{color:black}          interception, and
search, and may be disclosed or used for any USG-authorized purpose.
{/color}{/bgcolor}{/align}

{bgcolor:black} {/color}{align:left}{bgcolor:yellow}{color:black}
{/color}{/bgcolor}{/align}

{bgcolor:black} {/color}{align:left}{bgcolor:yellow}{color:black}  -       This IS includes
security measures (e.g., authentication and access controls) to protect USG interests--not
{/color}{/bgcolor}{/align}

{bgcolor:black} {/color}{align:left}{bgcolor:yellow}{color:black}          for your personal
benefit or privacy.
{/color}{/bgcolor}{/align}

{bgcolor:black} {/color}{align:left}{bgcolor:yellow}{color:black}
{/color}{/bgcolor}{/align}

{bgcolor:black} {/color}{align:left}{bgcolor:yellow}{color:black}  -       Notwithstanding the
above, using this IS does not constitute consent to PM, LE or CI investigative searching
{/color}{/bgcolor}{/align}

{bgcolor:black} {/color}{align:left}{bgcolor:yellow}{color:black}          or monitoring of the
content of privileged communications, or work product, related to personal representation
{/color}{/bgcolor}{/align}
```

```
{bgcolor:black} {/color}{align:left}{bgcolor:yellow}{color:black}          or services by
attorneys, psychotherapists, or clergy, and their assistants. Such communications and work
{/color}{/bgcolor}{/align}

{bgcolor:black} {/color}{align:left}{bgcolor:yellow}{color:black}          product are private
and confidential. See User Agreement for details.
{/color}{/bgcolor}{/align}

{bgcolor:black} {/color}{align:left}{bgcolor:yellow}{color:black}
{/color}{/bgcolor}{/align}

{bgcolor:black} {/color}{bgcolor:dark-grey}{color:black}
{/color}{/bgcolor}

{bgcolor:black} {/color}{bgcolor:dark-grey}{color:black}
{/color}{/bgcolor}

{bgcolor:black} {/color}{bgcolor:dark-grey}{color:black}
{/color}{/bgcolor}

{bgcolor:black} {/color}{bgcolor:dark-grey}{color:black}
{/color}{/bgcolor}

{bgcolor:black} {/color}{bgcolor:dark-grey}{color:black}
{/color}{/bgcolor}

{bgcolor:black} {/color}{bgcolor:dark-grey}{color:black}
{/color}{/bgcolor}

{bgcolor:black} {/color}{bgcolor:dark-grey}{color:black}
{/color}{/bgcolor}

{bgcolor:black} {/color}{bgcolor:dark-grey}{color:black}
{/color}{/bgcolor}

{bgcolor:black} {/color}{bgcolor:dark-grey}{color:black}
{/color}{/bgcolor}

{bgcolor:black} {/color}{bgcolor:dark-grey}{color:black}
{/color}{/bgcolor}

{bgcolor:black} {/color}{bgcolor:dark-grey}{color:black}
{/color}{/bgcolor}

{bgcolor:black} {/color}{bgcolor:dark-grey}{color:black}
{/color}{/bgcolor}

{bgcolor:black} {/color}{bgcolor:dark-grey}{color:black}
{/color}{/bgcolor}
```

```
{bgcolor:black} {/color}{bgcolor:dark-grey}{color:black}
{/color}{/bgcolor}

{bgcolor:black} {/color}{bgcolor:dark-grey}{color:black}
{/color}{/bgcolor}

{bgcolor:black} {/color}{bgcolor:dark-grey}{color:black}
{/color}{/bgcolor}

{bgcolor:black} {/color}{bgcolor:dark-grey}{color:black}
{/color}{/bgcolor}

{bgcolor:black} {/color}{align:left}{bgcolor:dark-grey}{color:white}  <F2> Accept Conditions and
Customize System / View Logs{/align}{align:right}<F12> Accept Conditions and Shut Down/Restart
{bgcolor:black} {/color}{/color}{/bgcolor}{/align}

{bgcolor:black} {/color}{bgcolor:dark-grey}{color:black}
{/color}{/bgcolor}
```