Hardened Virtual Appliance Operations Guide

Securing the Appliance Base Platform to Meet High Governance Requirements

VMWARE WHITEPAPER

vmware®

Table of Contents

Introduction 3
Purpose 4
Root password 4
Password Expiry 5
Dodscript.sh Script 6
Secure Shell, Administrative Accounts, and Console Access 8
Time Sourcing and Synchronization 10
Log Forwarding – Syslog-ng and Auditd 12
Boot Loader (Grub) Password 15
NFS and NIS 16

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
Copyright © 2010 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

Introduction

The virtual appliance method of deployment for VMware datacenter products provides customers with the ability to rapidly deploy and configure infrastructure components. One of the original challenges with the virtual appliance model was the lack of a standardized security policy across the released product landscape. In 2013, a development effort was launched to standardize the security profile of VMware produced virtual appliances to a technical standard that would meet or exceed current high-governance compliance requirements found in various vertical market segments:

- US Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP)
- Director of Central Intelligence Directive (DCID) 6/3 for US Intelligence Agencies
- FedRAMP
- HIPAA
- PCI-DSS

The two most common references for implementing technical security requirements are the NIST 800.53 and the US Department of Defense Information Systems Agency (DISA) Security Technical Information Guides (STIG). The latest iteration of the STIG, called the Security Requirements Guide (SRG), is an effort by DISA to merge both the NIST 800.53 and the STIG guidance into a single security guide that cross-references both sets of technical requirements. In 2013 VMware commenced the process of the production of the VMware Virtual Appliance OS SRG STIG, to provide customers with the guidance necessary to meet or exceed any high-governance compliance requirement.

In parallel, VMware began an effort to standardize the delivery of the virtual appliance platform by embedding the technical requirements of the STIG in the design. The end result in 2013 is the release of 14 hardened virtual appliances across 9 products that close 91-95% of the identified platform vulnerabilities in code:

- vCenter Server Virtual Appliance 5.5 (VCVA)
- vCenter Orchestrator 5.5 (vCOva)
- vCenter Operations Manager 5.7.1 (vCOPs)
- vCenter Infrastructure Navigator 2.0 (VIN)
- vCloud Automation Center Virtual Appliance 6.0 (vCACva)
- vCenter Management Assistant (vMA)
- VMware Log Insight 1.0
- Horizon Workspace Manager 1.5

Copyright © 2010 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

- vCloud Connector 2.5.1 (vCC)

Purpose

The purpose of the hardened virtual appliance operations guide is to address the remaining technical requirements that are site-specific decisions required to meet the STIG. This document is intended for advanced level administrators, and should be read before deploying hardened virtual appliances in a production environment.

Root password

Most hardened appliances will either allow the modification of the root password during initial setup, or will be pre-installed with the root password set to 'vmware'. It is highly recommended to change the root password for both password complexity and the cryptographic hashing to meet STIG compliance.

NOTE: In some cases like vCVA and vCO, the root user account can be modified in the VMware Appliance Management Infrastructure (VAMI) user interface. vCOPs also provides the ability to modify the root password through a customer admin interface. If deploying one of these appliances, please consult the admin/user guide for the specific product on how to modify the root password.

To change the root password at the command line, use the command 'passwd' at the root shell of the appliance.

```
pgsvr:~ # passwd
Changing password for root.
New password:
Retype new password:
Password changed.
pgsvr:~ #
```

NOTE: the root user bypasses the pam_cracklib module password complexity check (found in /etc/pam.d/common-password). It is imperative to manually ensure that the root password meets the corporate password complexity requirements of your organization.

To check the hash of the root password, as root:

Copyright © 2010 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

more /etc/shadow

```
vcva2013:~ # more /etc/shadow
bin:*:15887:0:60:7:::
daemon:*:15887:0:60:7:::
haldaemon:*:15887:0:60:7:::
ldap:*:15887:0:60:7:::
mail:*:15385::60:::
man:*:15887:0:60:7:::
messagebus:*:15887:0:60:7:::
nobody:*:15385::60:::
ntp:*:15887:0:60:7:::
polkituser:*:15887:0:60:7:::
postfix:*:15887:0:60:7:::
root:$6$KvZ/hiWS$PhOtIUN85TXBgQxc01B3JfrRtPhXxL8n/IwW0fe5XrHETb0Cz9l4bzGlk8gGw9
CXjjbq.PPcCPTFxAJ9M3tgo.:15895:0:1095:7:::
```

The password field is the second field of the shadow file. If account passwords start with "6", then the password is using a sha512 hash. This is the standard hash for all hardened appliances. If the root password does not contain a sha512 hash, run the 'passwd' command to change it.

NOTE: All hardened appliances enable "enforce_for_root" for the pw_history module (found in /etc/pam.d/common-password), so the last five passwords will be remembered by default. Old passwords are stored for each user in the /etc/security/opasswd file. To re-use the same password, delete the entry for the root user in the file. Re-using the same password is not recommended once the system is in production.

Password Expiry

To meet the compliance standard of the STIG, user accounts should be set to 60 days, and service accounts can be set to 365 days. All hardened appliances are set to create accounts with a 60 day password expiry by default. On most hardened appliances, the root account is set to a 365 day password expiry. It is highly recommended to check the expiry on all accounts to meet both security and operation requirements standards.

NOTE: As part of an organization's compliance policies, a procedure should be implemented to ensure that administrators do not forget to change their passwords within the active period. If the root account expires, there will be no method in the appliance to re-instate the root password. It is imperative that site-specific policies are implemented to prevent administrative and root passwords from expiration.

Copyright © 2010 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

As root, run the following command to check the password expiry of all accounts:

more /etc/shadow

```
vcva2013:~ # more /etc/shadow
bin:*:15887:0:60:7:::
daemon:*:15887:0:60:7:::
haldaemon:*:15887:0:60:7:::
ldap:*:15887:0:60:7:::
mail:*:15385::60::::
man:*:15887:0:60:7:::
messagebus:*:15887:0:60:7:::
nobody:*:15385::60::::
ntp:*:15887:0:60:7:::
polkituser:*:15887:0:60:7:::
postfix:*:15887:0:60:7:::
root:$6$KvZ/hiWS$PhOtIUN85TXBgQxc01B3JfrRtPhXxL8n/IwW0fe5XrHETb0Cz9l4bzGlk8gGw9
CXjjbq.PPcCPTFxAJ9M3tgo.:15895:0:1095:7:::
```

The password expiry is the fifth field of the shadow file. In this example, the root expiry is set to 1095 days (3 years).

To modify the expiry of the root account run the following command as root:

passwd –x 365 root

This will change the root password expiry to 365 days. Use the same command to modify any user, substituting 'root' for the specific account, and replacing the number of days to meet the expiry standards of the organization.

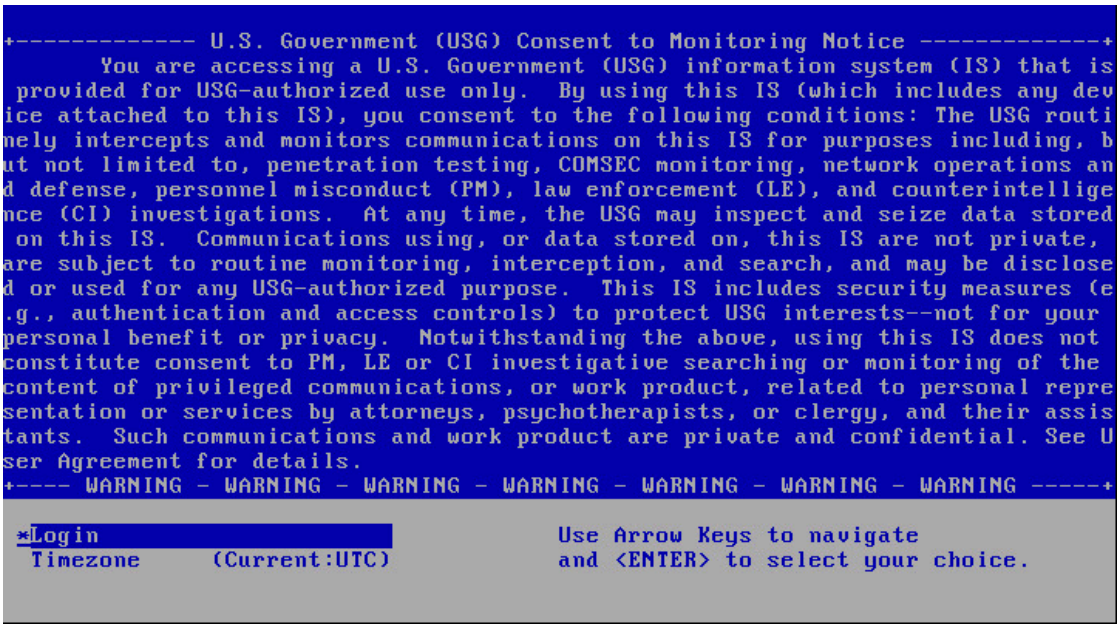
Dodscript.sh Script

To support additional high-governance compliance requirements as documented in the STIG, 4 optional hardening components are enabled with the execution of the dodscript.sh script included in all hardened appliances, which:

- Modifies the password minimum length from 8 to 14 characters.
- Modifies the default audit logs entries to meet the requirements of the STIG (/etc/audit/audit.rules.STIG) and enables syscall logging.
- Modifies all default profile scripts to eliminate console messages (mesg n).

Copyright © 2010 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

- Modifies the default banner for the appliance welcomescreen and SSH to the Department of Defense approved banner (/opt/vmware/etc/isv/welcometextDoD (or welcomtext.template on vCVA) for the console banner and /etc/issue.DoD for the SSH banner).



To enable this configuration, as root, run the following commands:

```
# cd /etc
# ./dodscript.sh
```

NOTE: The banner files can be modified to support non-DoD customer banners. Either edit the above files listed for the console and SSH banners, or create a separate file and use a symbolic link to activate the banner with the following commands (in this example, the new files are welcometext.CUSTOM and issue.CUSTOM):

```
# rm /opt/vmware/etc/isv/welcometext
# ln –s /opt/vmware/etc/isv/welcomtext.CUSTOM /opt/vmware/etc/isv/welcometext

# rm /etc/issue
# ln –s /etc/issue.CUSTOM /etc/issue
```

For vCVA, replace the /opt/vmware/etc/isv/welcometext.template with the preferred console banner text.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
Copyright © 2010 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents.
VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

Secure Shell, Administrative Accounts, and Console Access

For remote connections, all hardened appliances include the Secure Shell (SSH). Because many appliances do not include default user accounts, the root account may still be able to directly login via SSH. To meet the compliance standards for non-repudiation, the SSH server on all hardened appliances comes preconfigured with the "AllowGroups wheel" entry to restrict ssh access to the secondary group wheel.

NOTE: For separation of duties, the "AllowGroups wheel" entry can be modified in /etc/ssh/sshd_config to use another group (such as sshd). The wheel group is enabled with the pam_wheel module for su access, so members of the wheel group are allowed to su – to root (password for root is required). Group separation provides a method for users to ssh to the appliance, but not have the ability to su to root. Do not remove or modify other entries in the AllowGroups field to ensure proper appliance functionality. Any change will require a restart of the ssh daemon (# service sshd restart).

Prior to removing root SSH access, create local administrative accounts that can both use ssh and/or are members of the secondary wheel group. To create a local account on the appliance, run the following command as root:

useradd –g users –G wheel –d /home/*username* –m –s /bin/bash *username*
(Substitute "wheel" for the group specified in AllowGroups for ssh access. To add multiple secondary groups, use –G wheel,sshd)

passwd *username*

Switch to the user to provide a new password so that password complexity checking is enforced:

su – *username*
username@hostname:~> passwd

NOTE: If the password complexity is met, the change of the password will complete successfully. If the password complexity is not met, it will revert back to the original password, so re-run the command to set a compliant password for the user.

Once login accounts are created to allow SSH remote access and wheel access (su – root), the root account can be removed from both SSH direct login direct login.

Copyright © 2010 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

NOTE: Do not modify the PermitRootLogin setting on vCOPs appliance vApp.

Prior to disabling direct root access, thoroughly test to ensure that authorized administrators can access ssh (via AllowGroups) and can su to root (via wheel group). To remove direct root login to ssh, modify the /etc/ssh/sshd_config file with the vi editor, and replace the entry:

(#)PermitRootLogin yes
with:
PermitRootLogin no

Restart the sshd service:
service sshd restart

SSH access should also be restricted with the proper entries to limit access. All VMware virtual appliances include the tcp_wrappers package to allow tcp supported daemons to control the network subnets that can access the libwrapped daemons. By default, the /etc/hosts.allow file contains a generic entry to allow all access to the secure shell:

sshd: ALL : ALLOW

It is recommended that this entry be changed for production environments to include only the localhost entries and the management netwotk subnet for secure operations, such as:

sshd: 127.0.0.1 : ALLOW
sshd: [::1] : ALLOW
sshd: 10.0.0. : ALLOW

This example will allow all localhost connections and connections made by clients on the 10.0.0.0 subnet.

By default, the hardened appliances allow direct login to root via the console. Once administrative accounts have been created for non-repudiation and tested for wheel access (su – root), direct root logins can be disabled by editing the /etc/securetty file as root and replacing the entry:

tty1
with:
console

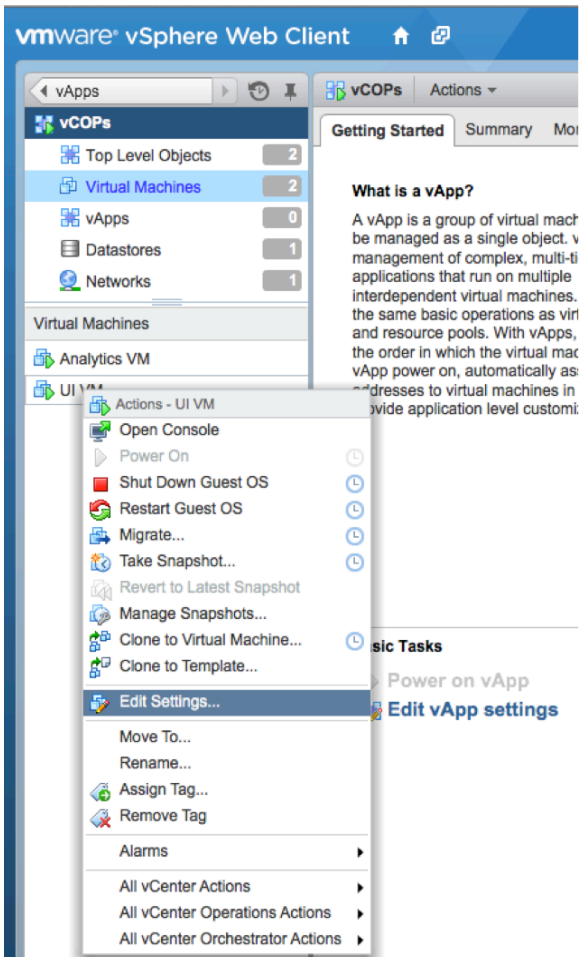
Copyright © 2010 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

Time Sourcing and Synchronization

All hardened appliances include at least two mechanisms for time synchronization: vmtools and the ntp service. It is recommended that virtual appliances use ntp to synchronize for time sensitive environments.

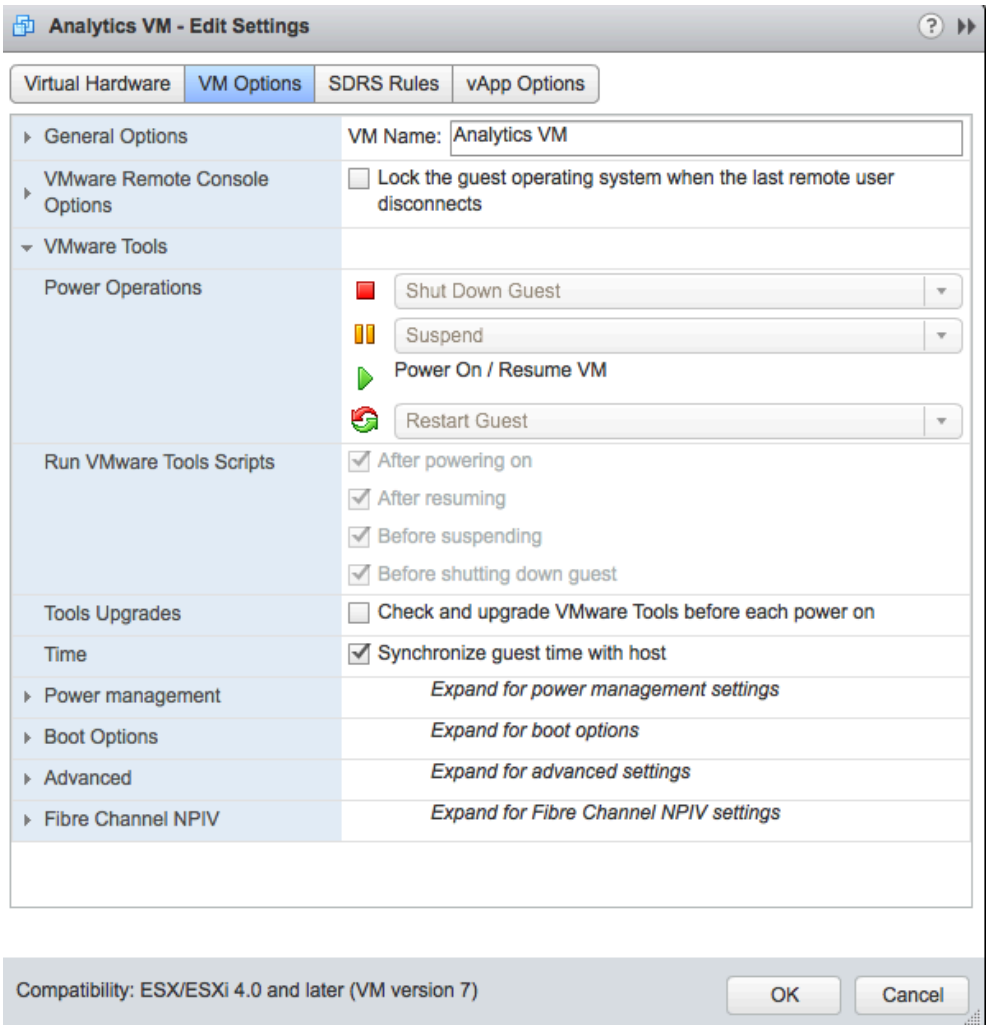
NOTE: The hardened vCenter Server Appliance allows time to be configured with the VAMI user interface. Please refer to the vCenter Server Appliance administration guide on how to configure time services.

VMtools: Time sourcing with vmtools uses the time of the ESXi host for synchronization. To verify vmtools time synchronization, log into the vCenter server web client (https://ip_of_vcenter_server:9443). Under vCenter, navigate to the virtual machine, right click the targeted VM, and select "Edit Settings…"



VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
Copyright © 2010 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

Select the “VM Options” tab, then click on the “VMware Tools” drop down menu to expose the “Time” field. If the “Synchronize guest time with host” box is checked, then the appliance is using vmtools. Uncheck the box if planning to use ntp for time synchronization.



NTP: Time sourcing with ntp leverages the ntp client in the appliance to synchronize time. To configure ntp, first use the above instructions to ensure that vmtools time synchronization is disabled. As root on the appliance, edit the /etc/ntp.conf file to add ntp servers to the list of time sources in the form of:

server *ntpservername options*

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Copyright © 2010 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

For example:

server time.nist gov burst iburst

Add the number of local and centralized time sources as required for the compliance standard of the organization. For trusted time sourcing, the “key” specification can be leveraged to support key based authentication when listing time sources in the form of:

server time.nist.gov burst iburst key 1

Where “1” is the key listed as “1” in /etc/ntp.keys file. For more information on setting up ntp keys, refer to the Linux man page on ntp and key authentication.

Once the /etc/ntp.conf file is properly configured, start the ntp service as root:

chkconfig ntp on
service ntp start

To check the status, run the following command as root:

service ntp status

```
vcva2013:/etc # service ntp status
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*nist1-lv.ustimi .ACTS.           1 u  409 1024  377  100.620    3.043   4.365

Checking for network time protocol daemon (NTPD):                    running
```

Log Forwarding – Syslog-ng and Auditd

All hardened appliances include both comprehensive system and audit logging to support high governance compliance. See the chapter on Dodscript.sh to enable the compliant audit rules.

In 2013, VMware released the VMware Log Insight product to support centralized log services and log analytics. For setup and configuration information, please refer to the product configuration guide.

Copyright © 2010 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

To enable forwarding of system logs, modify the configuration file of the syslog server to specify the protocol, ip address, and port of the central log server. The syslog configuration file is located in /etc/syslog-ng/syslog-ng.conf. Using the vi editor as root, find the following two lines:

```
#destination logserver { udp("10.10.10.10" port(514)); };
#log { source(src); destination(logserver); };
```

Uncomment the two lines, and modify the fields. In this example, using tcp as the transport, 10.10.10.10 as the IP of the central syslog server, and port 514 as the syslog central server port, the entry would be:

```
destination logserver { tcp("10.10.10.10" port(514)); };
log { source(src); destination(logserver); };
```

Restart the service as root to incorporate the change:
service syslog restart

NOTE: Ensure that the firewall allows access to the port specified for the syslog destination log server.

For auditd forwarding, the vCenter Virtual Appliance includes the audisp-remote package to separate audit log forwarding from system log forwarding. If separation of the two logging services is preferred, the audit daemon remote configuration file is located in /etc/audisp/audisp-remote.conf to provide the necessary configuration settings to forward audit logs to a centralized audit server. Using the vi editor as root, edit the following entries:

remote_server = ip_of_remote_audit_server
port = port of auditd central service
transport = protocol for transferring audit logs

In this example, using tcp as the transport, 10.10.10.10 as the IP of the auditd central server, and port 60, the entries would be:

remote_server = 10.10.10.10
port = 60
transport = tcp

Restart the service as root to incorporate the change:
service auditd restart

Copyright © 2010 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

NOTE: Ensure that the firewall allows access to the port specified for the auditd destination log server.

For all other hardened appliances, the syslog remote plugin is provided to forward all audit logs to the syslog-ng service. The configuration file is located in /etc/audisp/plugins.d/syslog.conf. Using the vi editor as root, edit the entry:

active = no
to:
active=yes

This will forward all audit logs to /var/log/messages.

Restart the service as root to incorporate the change:
service auditd restart

NOTE: When using the high governance audit rules, there is an increase in the amount of logging traffic that may warrant reconfiguration of both the q_depth and the priority_boost of the audit dispatcher daemon. The configuration file is located in /etc/audisp/audispd.conf. Using the vi editor as root, edit the following entries:

q_depth = 80 (recommendation for high governance audit logs is at least 1280)
priority_boost = 4 (recommendation for high governance audit logs is at least 8)

Restart the service as root to incorporate the change:
service auditd restart

NOTE: When using the high governance audit rules, there is an increase in the size of log files. To decrease the number of stored logs on the hardened appliances (this assumes log forwarding has been configured), customers can tune the number of daily log files stored by modifying the rotation number. All log rotation configurations are stored in /etc/logrotate.d.

To control the number of stored daily log files for syslog, edit the /etc/logrotate.d/syslog file as root. Modify all of the “rotate 15” entries with the vi editor to the number of days to store local logs. The recommended number of days for centralized log services is at least 7.

To control the number of stored daily log files for the audit daemon, edit the /etc/logrotate.d/audit file as root. Modify the “rotate 15” entry with the vi editor to the

Copyright © 2010 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

number of days to store local audit logs. The recommended number of days for centralized audit log services is at least 7.

Boot Loader (Grub) Password

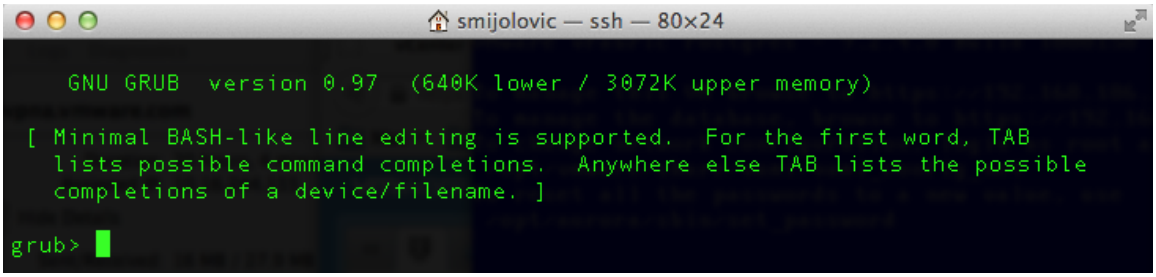
All hardened appliances have the ability to protect the appliance with a password for modification of the default boot settings. To verify it's configuration, read the /boot/grub/menu.lst file. The third line should contain:

password --md5 1(followed by additional characters)

To change or add a password for Grub, run the following procedure as root:

grub

The grub shell will appear.



Run the "md5crypt" command to create the hashed password. Once you type in a password, the hash will be presented. Copy the password. Run the "quit" command to return to the root shell.

Copyright © 2010 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

```
smijolovic — ssh — 80×24

    GNU GRUB  version 0.97  (640K lower / 3072K upper memory)

 [ Minimal BASH-like line editing is supported.  For the first word, TAB
   lists possible command completions.  Anywhere else TAB lists the possible
   completions of a device/filename. ]

grub> md5crypt

Password: ******
Encrypted: $1$28izJ1$0hlx/eUCoGZMGDWgsHz0n0

grub> quit
```

Use the vi editor as root to modify the /boot/grub/menu.lst file. Add the following to the third line of the file:

password --md5 *md5hash*

```
smijolovic — ssh — 80×24
# Modified by YaST2. Last modification on Wed Apr  3 21:02:10 UTC 2013
default 0
timeout 1
password --md5 $1$28izJ1$0hlx/eUCoGZMGDWgsHz0n0
```

Paste the md5 encrypted hash to the end of the entry, and save the file.

NFS and NIS

All hardened appliances come prepackaged with the ability to serve as both a NIS and NFS client. In 2013, NIS service support is depreciated. NFS is included as a non-standard means of supporting syslog shipping. If neither of the two services are required, it is recommended that they are disabled. To disable the services in the hardened virtual appliances, run the following set of commands as root:

chkconfig ypbind off
chkconfg nfs off
chkconfig rpcbind off
service ypbind stop
service nfs stop
service rpcbind stop

Copyright © 2010 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.