



Security Health Check Report

16 July 2010 02:51

Assessment Overview

Environment: VMware vCenter Server 4.1.0 build-258902

Version: 4.1.0

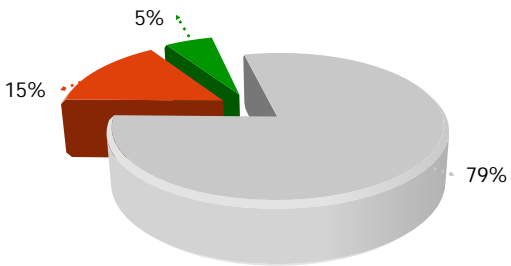
Duration: 00:01:45

Policy: VMinformer Database Policy, VMinformer Recommended Policy

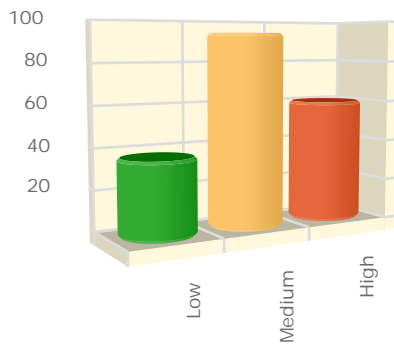
ESX Hosts: 2

VM Guests: 8

Assessment Summary



Risk Summary



ESX Host Summary for vmidw-vm01.vmidemo.com

Name: [vmidw-vm01](#)

IP Address: [10.18.2.80](#)

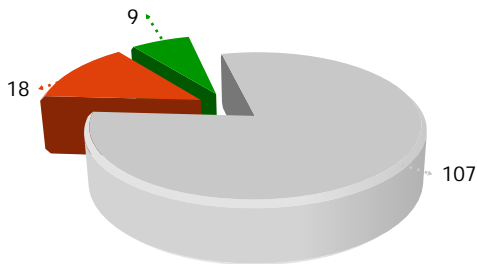
State: [green](#)

Firewall: [Incoming ports blocked by default](#),
[Outgoing ports blocked by default](#)

VM Guests: [7](#)

Rules: [57](#)

Assessment Summary



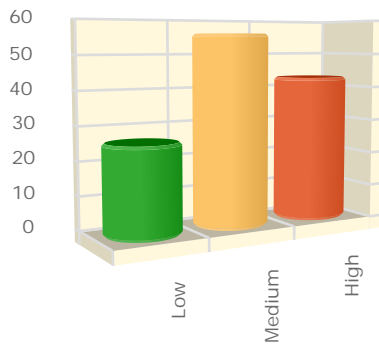
 Pass

 Warning

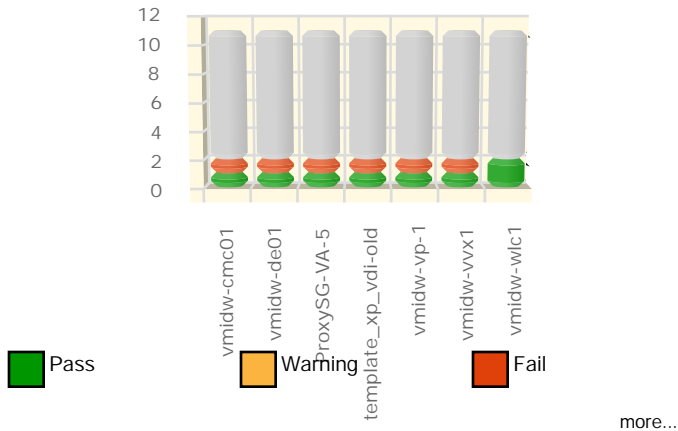
 Fail

[more...](#)

Risk Summary



Guest Summary



Results

Ungrouped Results

NotSet (44)

- Account lockout after 3 failed login attempts
- Allow NTP to resolve hostnames over the loopback interface
- Check if using sudo aliases
- Check that NTP has Access Control Methods in place
- Check the NTP drift file
- Set appropriate permissions and ownership on esxcfg-auth
- Verify the /etc/grub.conf settings
- Verify that the system 'hosts' file contains entries for NTP Servers
- Limit Access to the su command
- Display different log level messages on different screens
- Prevent automatic mounting of USB devices on the ESX Host
- Ensure that NTP is running
- Verify NTP Step-ticker settings
- Verify PASS_MAX_DAYS parameter in /etc/login.defs
- Verify the PASS_MIN_DAYS parameter in /etc/login.defs
- Permissions of failed log
- Setting appropriate permissions and ownership of all /usr/sbin/esxcfg-* files
- Verify the /etc/grub.conf permissions
- Change the permissions of the snmpd.conf file
- Setting appropriate permissions and ownership on the virtual machine log files
- Prevent Direct Root Login Using SSH

- Use remote syslog logging
- Protect against the root file system filling up
- Prevent Root Login at the Physical Console
- Do not change mode from read only for SNMP
- Configure SNMP to use Version 3
- Verify that syslog configured for sudo
- Verify that sudo contains settings for logging sudo activity remotely
- Verify That Failed root Logins Increment Deny Counter
- Verify that the NOPASSWD entry does not exist in the /etc/sudoers file
- Verify PASS_WARN_AGE param in /etc/login.defs
- Verify that the rootpw entry does not exist in /etc/sudoers files
- Verify the size of the vmksummary log file is less than or equal to 4096k
- Verify all VMDK files permissions
- Verify the /etc/logrotate.d/vmkernel file uses the compress option
- Verify the size of the /etc/logrotate.d/vmkernel log file is less than or equal to 4096k
- Verify the the vmksummary file uses the 'compress' option
- Verify that the VMKwarning file uses the compress option
- Verify the size of the vmkwarning log file is less than or equal to 4096k
- Verify all vmx files permissions
- Set appropriate permissions and ownership on the webAccess directory
- Limit Software and Services Running in the Service Console
- Configure the firewall for maximum security
- Do not use a port group with a vlan id equal to 1

✘ Fail (12)

- Check that your NTP Config has at least 3 ntp servers defined
- Verify the log rotation history for the vmksummary file
- Verify the log rotation history for /etc/logrotate.d/vmkernel
- Verify the min age of passwords in /etc/shadow
- Verify password expiration warning age in /etc/shadow
- Setting appropriate permissions and ownership on Service Console and Authentication log files
- Setting appropriate permissions and ownership on VirtualCenter agent and ESX host agent log files
- Setting appropriate permissions and ownership on vmkernel log files
- Setting appropriate ownership and configuring the setuid bit for the required setuid programs
- Verify the max age of passwords in /etc/shadow
- Protect against Forged Transmits
- Protect against MAC address spoofing

✔ Pass (1)

- Do not use promiscuous mode on network interfaces

Guest Summary for vmidw-cmc01

Name: [vmidw-cmc01](#)

IP Address:

State: [green](#)

Power State: [poweredOff](#)

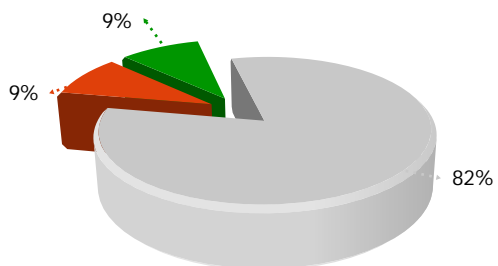
Template: [No](#)

Rules: [11](#)

Disk Name: [MSServer](#)

Disk Volume: [sanfs://vmfs_uuid:4a268660-7a553fb2-1860-001b2119c2b9/](#)

Assessment Summary



Pass



Warning



Fail

[more...](#)