Security Hardening vSphere 5.5

Cedric Rajendran
VMware, Inc.

vmware®

Agenda

- Security Hardening vSphere 5.5
  - ESXi Architectural Review
  - ESXi Software Packaging
  - The ESXi Firewall
  - ESXi Local User Security
  - Host Logs and Activity Monitoring
  - Understanding the Hardening Guidelines

vmware

ESXi Architectural Overview

Secure by Design…

vmware®

ESXi Architectural Overview

- **Full-featured hypervisor**
  - Superior consolidation, scalability & reliability
  - Designed from the ground up to run VMs

- **Small, light-weight and secure**
  - OS-Independent, thin architecture
  - Digitally signed software packages

- **Streamlined deployment and configuration**
  - Small code base with minimal configuration
  - Rapid provisioning with stateless support

vmware®

ESXi Architectural Overview

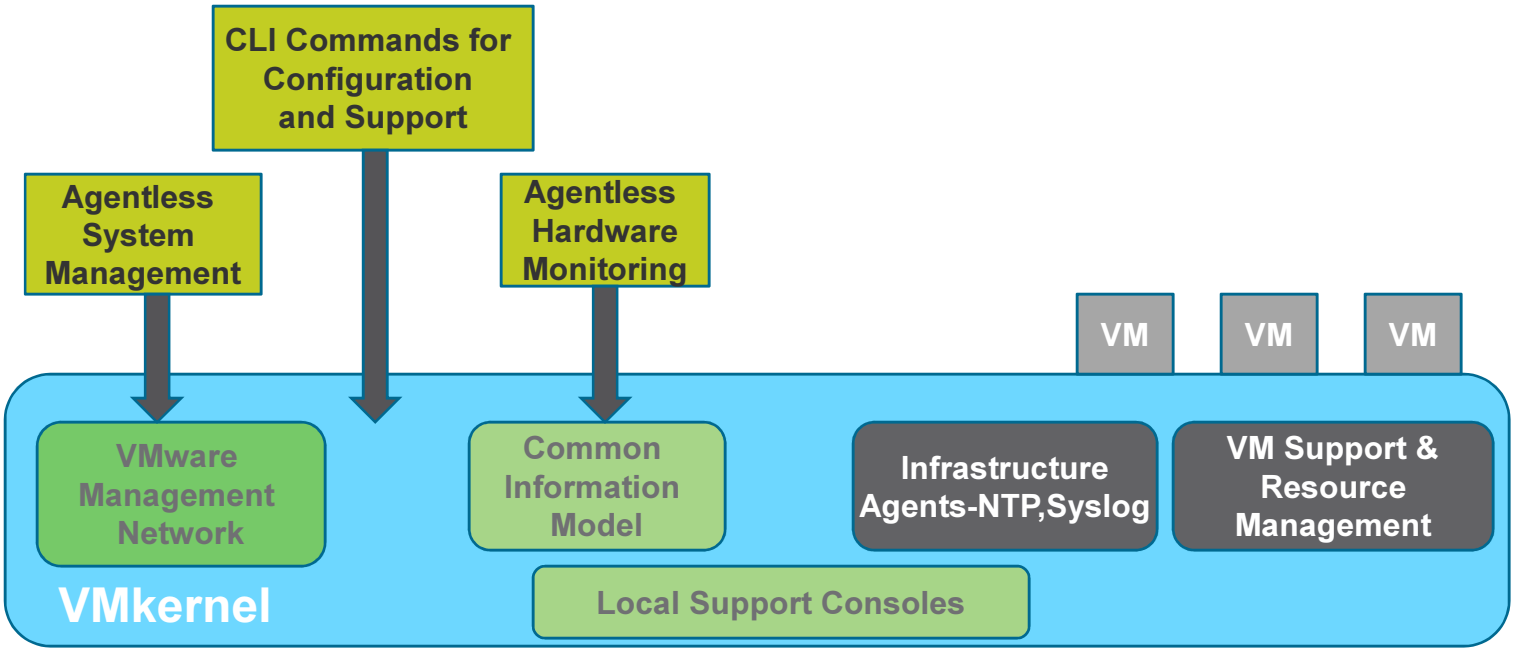
- **Simplified hypervisor patching and updating**
  - Small code base produces fewer patches
  - Easy recovery with dual-image architecture
  - VMware and 3rd party components updated independently

- **Memory Hardening**
  - Kernel, User mode applications & executable components are located at random, non-predictable memory addresses

- **Trusted Platform Module(TPM)**
  - Leverages Intel TPM to provide attestation of hypervisor image based on hardware root of trust.

ESXi Architectural Overview

- Digital signatures ensure integrity of kernel modules
- Rich API allows "**agentless**" management



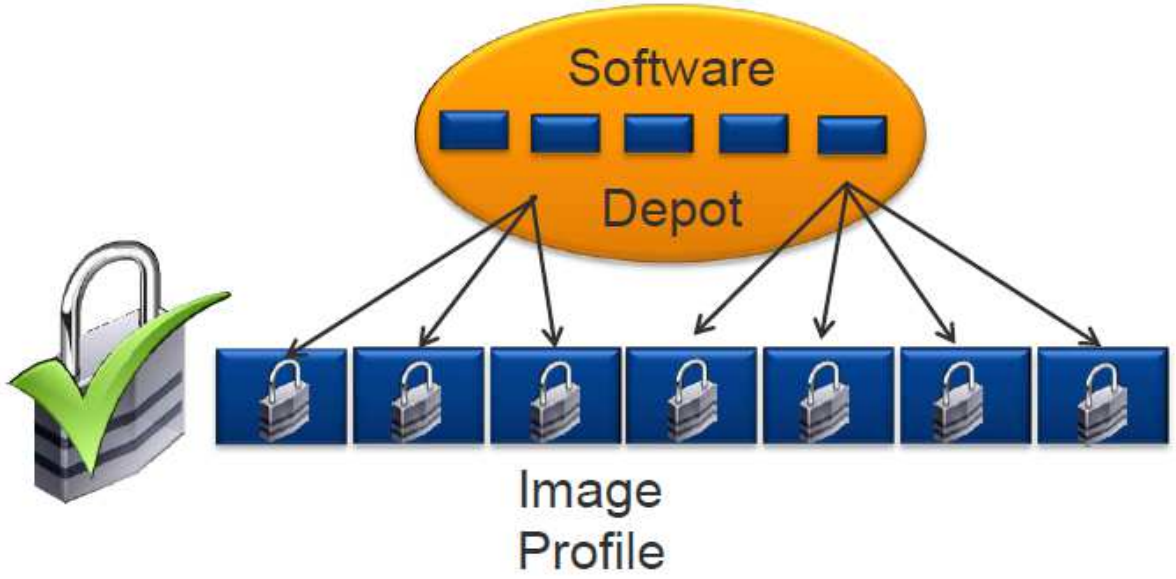
ESXi Software Packaging

Security Starts Before You Install…

vmware

vSphere Installation Bundles (VIBs)

- **ESXi distributed as collection of vSphere Installation Bundles(VIBs)**
  - ~60 VIBs in VMware distribution
  - ~300MB (~150MB with out VMware Tools)
- **Additional 3rd Party/Partner VIBs also available**
- **VMware and Partner VIBs digitally signed**



ESXi Image Profile

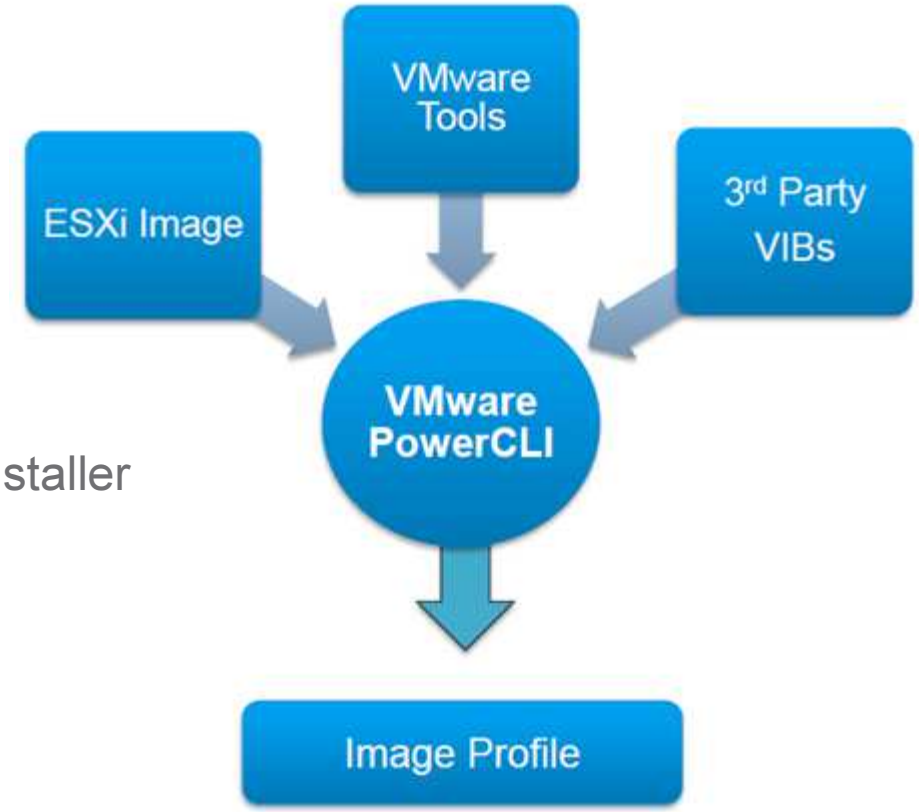
- **Image Profile assigns an "Acceptance Level"**
  - VMware Certified
  - VMware Supported
  - Partner Supported
  - Community Supported

- **Only VIBs signed at or above the assigned Acceptance Level can be added to the Image**
  - Acceptance Level can be changed using ESXCLI

```
~ # esxcli software acceptance get
PartnerSupported
~ # esxcli software vib list
Name                           Version                            Vendor  Acceptance Level  Install Date
-----------------------------  ---------------------------------  ------  ----------------  ------------
ata-pata-amd                   0.3.10-3vmw.510.0.0.726909         VMware  VMwareCertified   2012-07-14
ata-pata-atiixp                0.4.6-4vmw.510.0.0.726909          VMware  VMwareCertified   2012-07-14
ata-pata-cmd64x                0.2.5-3vmw.510.0.0.726909          VMware  VMwareCertified   2012-07-14
ata-pata-hpt3x2n               0.3.4-3vmw.510.0.0.726909          VMware  VMwareCertified   2012-07-14
ata-pata-pdc2027x              1.0-3vmw.510.0.0.726909            VMware  VMwareCertified   2012-07-14
ata-pata-serverworks           0.4.3-3vmw.510.0.0.726909          VMware  VMwareCertified   2012-07-14
ata-pata-sil680                0.4.8-3vmw.510.0.0.726909          VMware  VMwareCertified   2012-07-14
ata-pata-via                   0.3.3-2vmw.510.0.0.726909          VMware  VMwareCertified   2012-07-14
```

Modifying/Customizing Image Profiles

- **Image Builder CLI**
  - Included with PowerCLI
  - Create Image Profiles
  - Add/Remove 3rd Party drivers
- **Export Images**
  - ISO
    - Image-boots host into ESXi Installer
    - Import to Update Manager
  - ZIP
    - Used with Auto Deploy
    - Offline repository



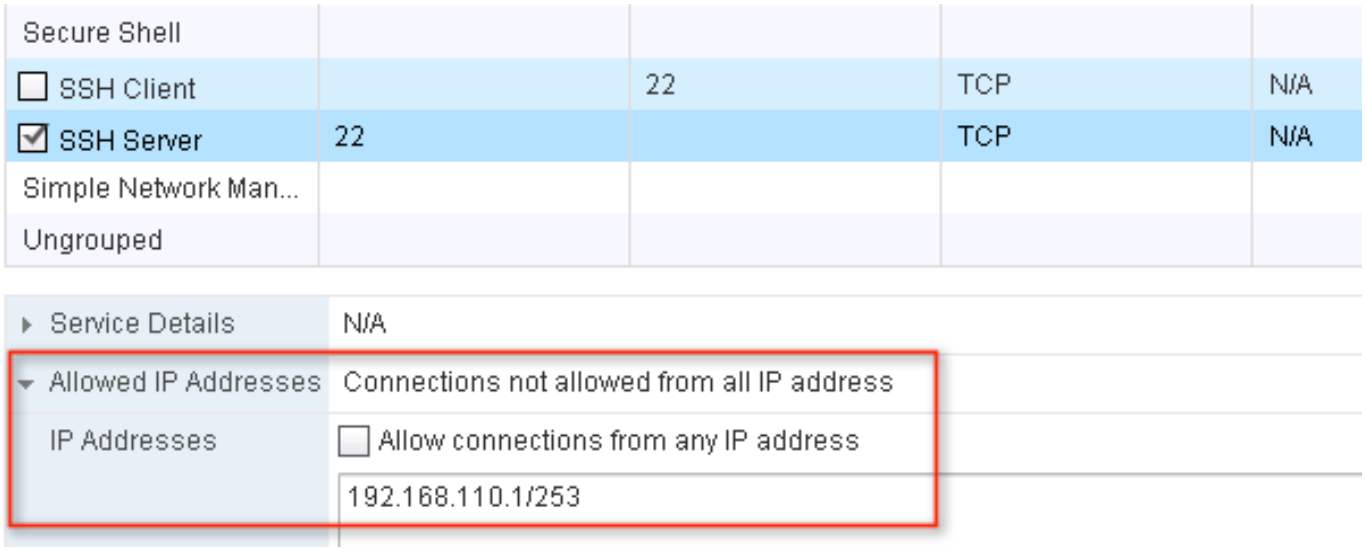
The ESXi Firewall

Controlling Access to the Host…

vmware®

The ESXi Firewall

- **ESXi management network protected by local firewall**
  - Non-essential incoming/outgoing traffic blocked by default
  - Control service start-up on boot
  - Ability to restrict access to range of IP addresses



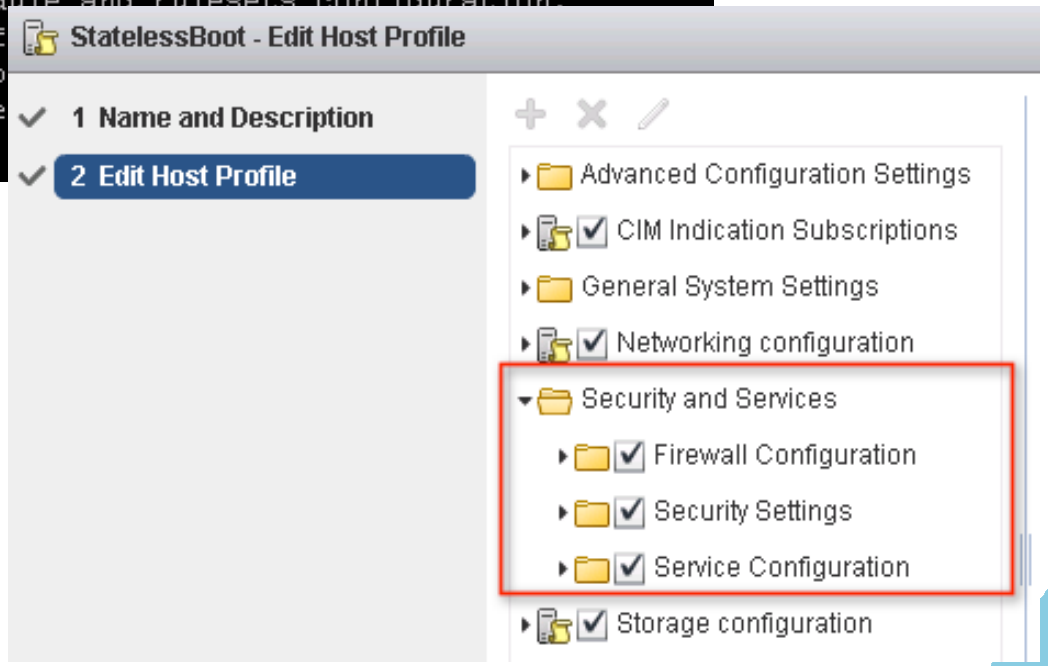
The ESXi Firewall

- Firewall configurable from GUI, CLI and Host Profile

```
~ # esxcli network firewall
Usage: esxcli network firewall {cmd} [cmd options]

Available Namespaces:
  ruleset               Commands to list and update firewall ruleset
                        configuration

Available Commands:
  get                   Get the firewall status.
  load                  Load firewall module and rulesets configuration.
  refresh               Load ruleset conf
  set                   Set firewall enab
  unload                Allow unload fire
~ #
```



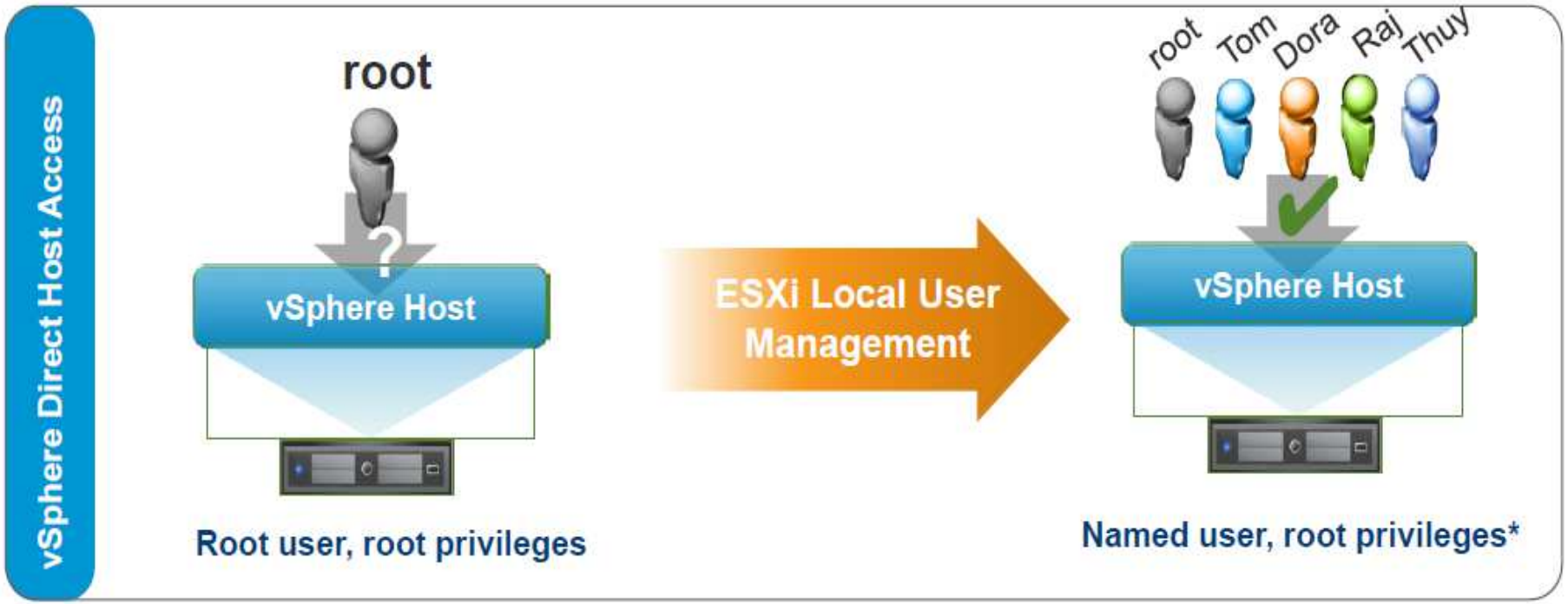
vmware

ESXi Shell & Local User Security

vmware

ESXi - User Model Security Enhancements

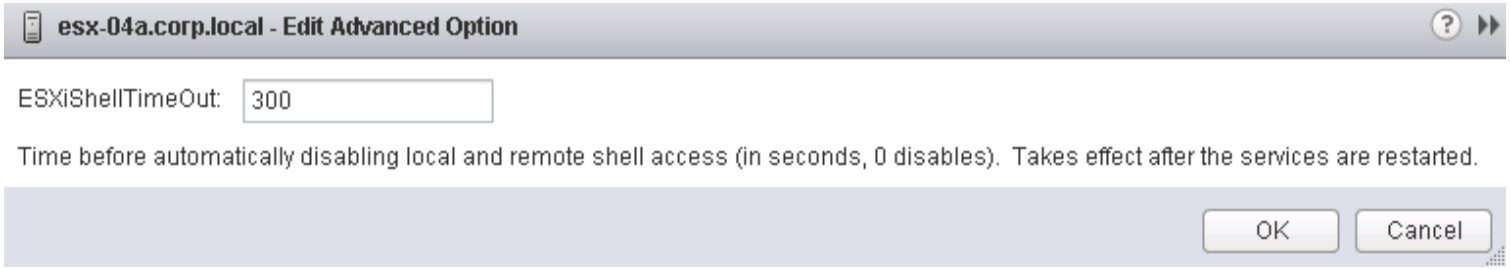
- Named users provides for more auditability
  - Local users with admin privileges equivalent to root
  - Users operate using their own account, full admin privileges
  - Limit use of the root account



vmware

ESXi - Shell Timeout

- **ESXiShellTimeOut**
  - Advanced setting used to set timeout for Shell/SSH availability



- **ESXiShellInteractiveTimeOut (*new in 5.1*)**
  - Advanced Setting used to automatically timeout inactive Shell Sessions

vmware

ESXi - Lockdown Mode

- **What is Lockdown mode**
  - Restrict users from logging in directly to the hypervisor
  - Only vCenter (vpxuser) allowed to manage the host in lockdown mode ESXi Shell access denied for all users

- **Why lock down your infrastructure?**
  - Single point of management for your infrastructure - through vCenter

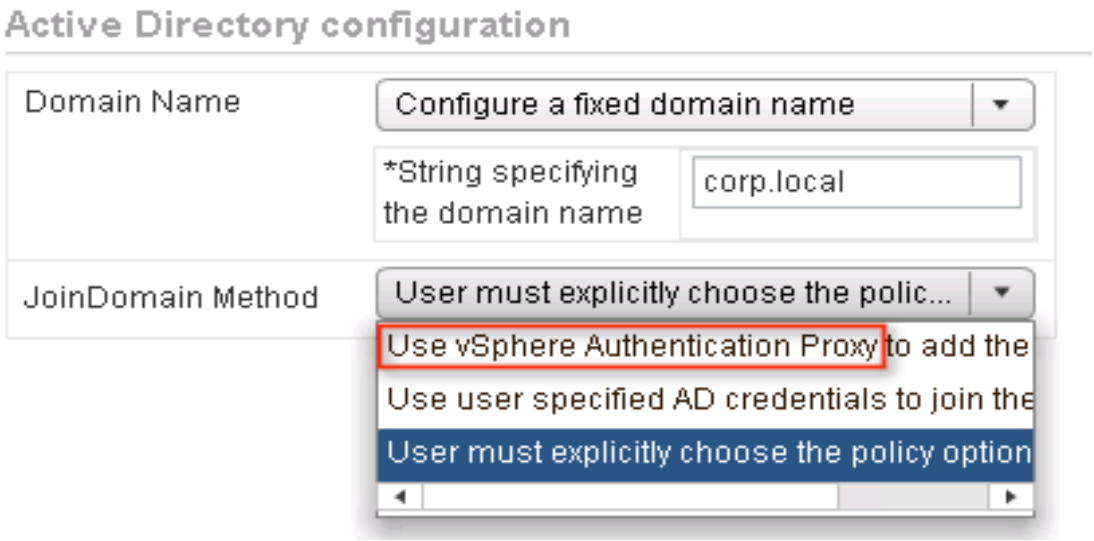
Service	Default Configuration	Recommended Configuration	Total Lockdown Configuration
Lockdown	Off	On	On
ESXi Shell	Off	Off	Off
SSH	Off	Off	Off
Direct Console UI (DCUI)	On	On	Off

vmware

ESXi Authentication through Active Directory

- To protect Active Directory domain user credentials use the VMware Authentication Proxy
  - Included with the vCenter Server install media
  - Uses certificate vs. storing/passing domain credentials

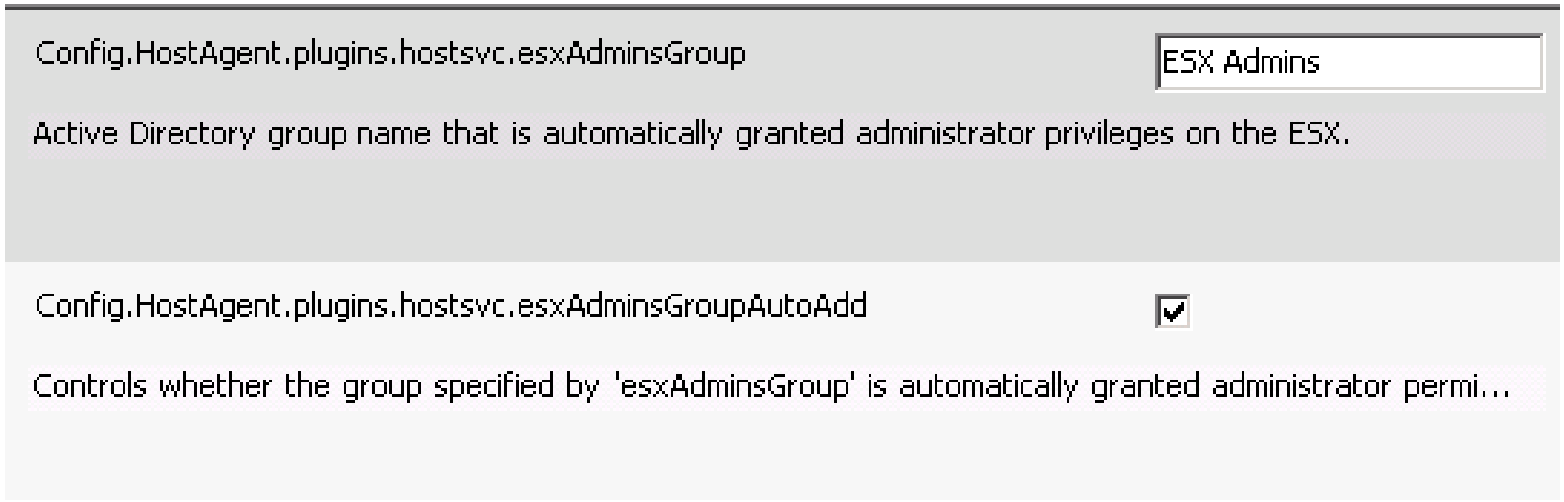
- Configure in Host Profile to prevent storing AD user credentials



vmware

ESXi and Active Directory cont.

- By default users in the Active Directory “ESX Admins” group are granted administrator access
  - To disable this behaviour disable “**esxAdminsGroupAutoAdd**”
  - To change the group name set “**esxAdminsGroup**”

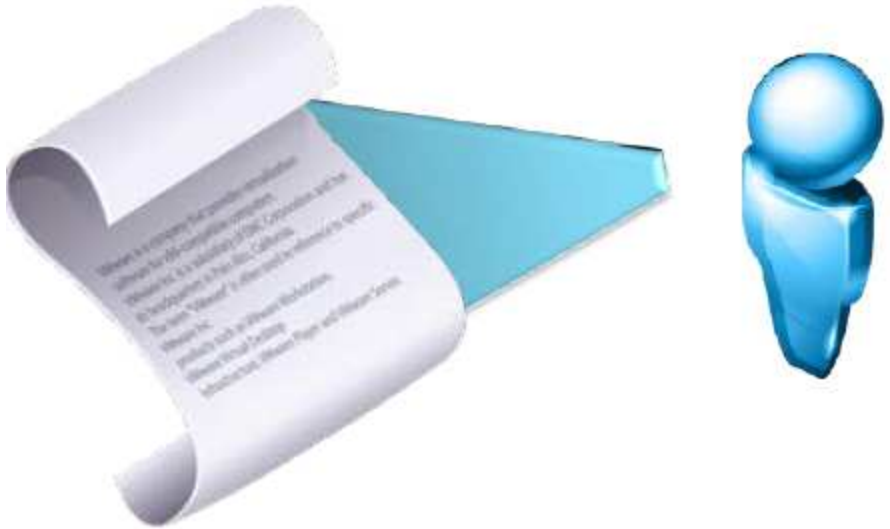


Host Logs and Activity Monitoring

vmware®

ESXi Improved Logging

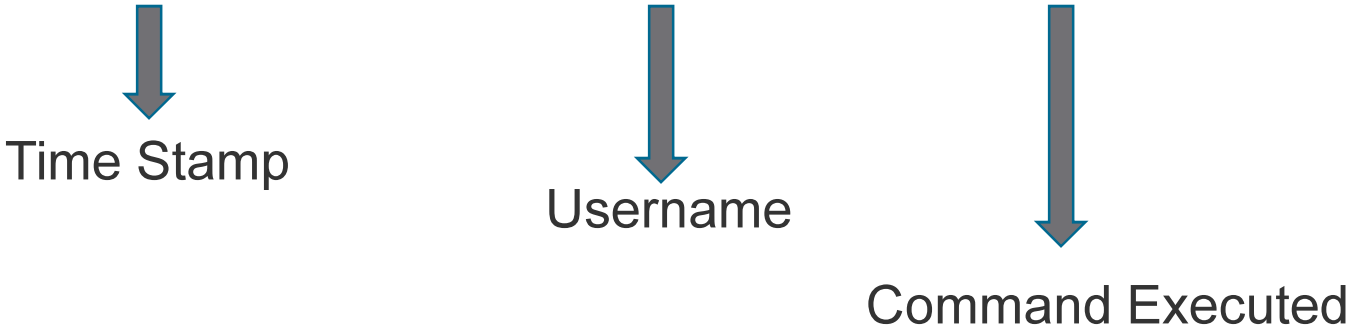
- All administrator actions logged (commands executed)
- All authentication events logged – successful & unsuccessful
- Direct Console activity is logged using the username instead if “dcui” user



vmware

ESXi Logs: Admin Activity on Hypervisor Shell

```
2012-07-10T13:03:43Z ESXShell: ESXi shell login enabled
2012-07-10T13:03:43Z SSH: SSH login enabled
2012-07-10T13:03:55Z ESXShell: ESXi Shell available
2012-07-10T13:03:57Z shell[1000047077]: Interactive shell session started
2012-07-10T13:03:59Z shell[1000047077]: [root]: vmware -vl
2012-07-10T15:49:02Z shell[1000064535]: Interactive shell session started
2012-07-10T15:49:06Z shell[1000064535]: [testuser]: ls -la
2012-07-10T15:49:15Z shell[1000064535]: [testuser]: cat /etc/passwd
2012-07-10T15:49:22Z shell[1000064535]: [testuser]: vi etc/passwd
2012-07-10T15:49:28Z shell[1000064535]: [testuser]: cat /etc/group
2012-07-10T15:49:38Z shell[1000064535]: [testuser]: cat /var/log/shell.log
```



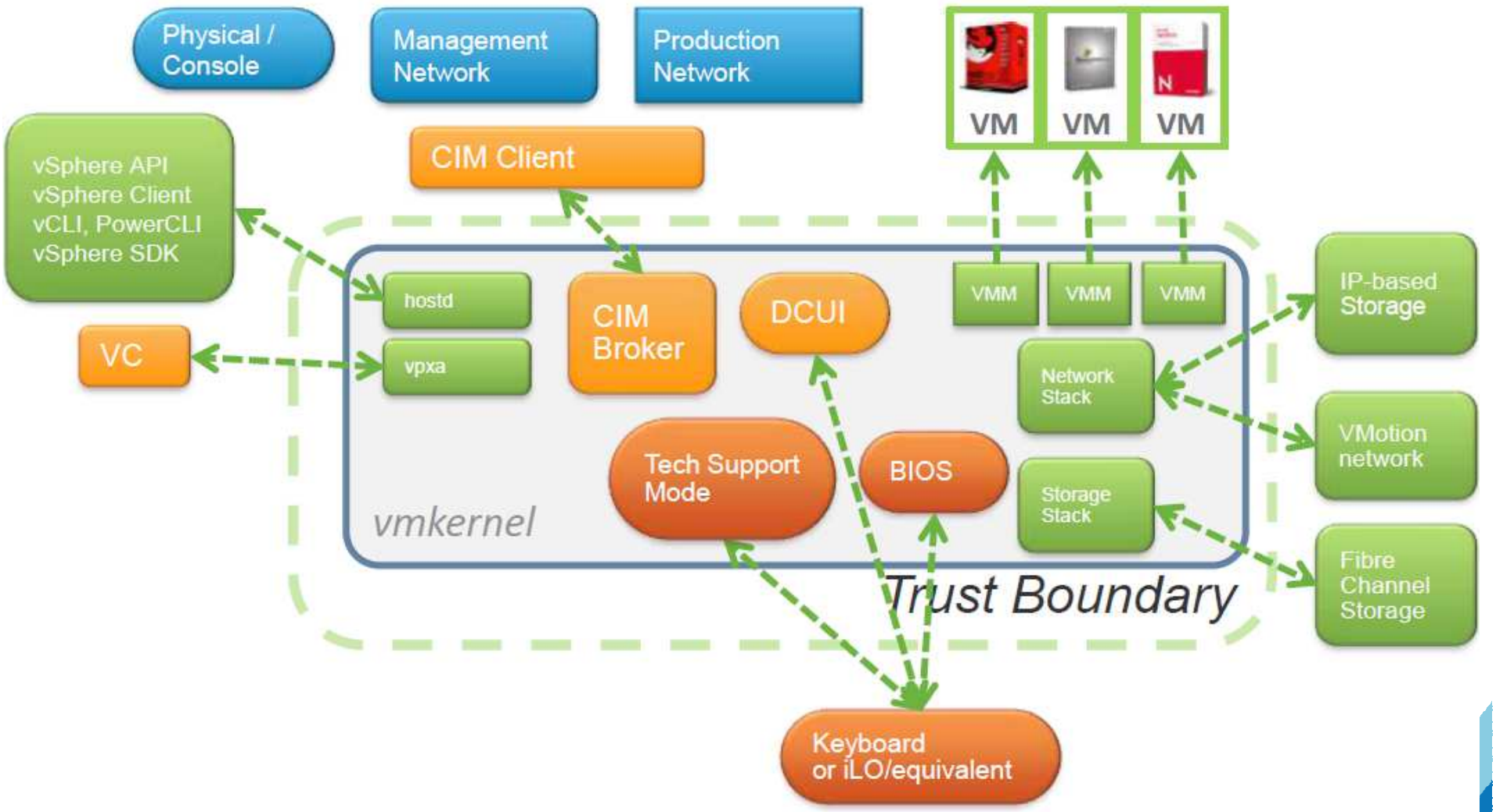
vmware

Hardening Guidelines

Classification & Customization
based on the environment needs…

vmware

Define the Threat Model-ESXi



vmware

Risk Assessment & Control – Leveraging the Hardening Guide

- Environment Profiling - Classification of environment based on security needs
- Types of Guidelines & Recommendation Levels
- Implementation

vmware

Environment Profiling

Profile	Environment	Guidelines
Profile 3	Enterprise	Should be implemented in all environments
Profile 2	DMZ	Should be implemented for more sensitive environments, e.g. those handling more sensitive data, those subject to stricter compliance rules, etc.
Profile 1	SSLF-Specialized Security Limited Functionality	Should be implemented in the highest security environments, e.g. top-secret government or military, extremely sensitive data, etc.

Control Type

Control Type	Definition
Operational	Recommendations on how to operate or interact with the administrative components of the system.
Configuration	Recommends a certain configuration of components, either to reduce risk or to provide a compensating control
Parameter	Specifies a configuration parameter to enable or disable in specific products

Implementation - An abstract from the hardening guide

Control Type	Component	Title	Vulnerability Discussion	Profile
Parameter	ESXI	Disable HGFS	Prevents file transfer to Guest OS	1
Operational	ESXI-Storage	Zero out vmdk prior to deletion.	Shreds sensitive data to prevent data reconstruction from physical disk	1,2
Configuration	ESXI	Configure the ESXi host firewall to restrict access to services running on the host	Restrict Access	1,2,3

ESXi Security Summary

- ESXi is a Full Featured Hypervisor
  - Small, light-weight and secure
  - Designed for one purpose - to host VMs
- ESXi Image Comprised of VIBs
  - Ensures integrity, prevents tampering, instils confidence
- Enhanced auditing capabilities
  - All activity logged under named user accounts
- Locked down
  - Firewall, ESXiShellTimout, ESXiShellInteractiveTimeOut, Lockdown Mode
- Customization based on environment needs
  - Align with hardening guide

Questions?

Write to me @
Cedric.rajendran@gmail.com
www.virtualknightz.com

vmware