vSphere 6 Webcast – Security Update

Mike Foley – vSphere Technical Marketing – Security

June 17th 2015

vSphere 6 Security Update

Mike Foley – vSphere Technical Marketing – Security

Agenda

- vSphere 6 Hardening Guide Update
- vSphere 6 Security Update
  - Access control enhancements
  - Auditing improvements
  - Certificate Management

vSphere Hardening Guide Update

vmware

vSphere Hardening Guide: Production-ready Security

What it does

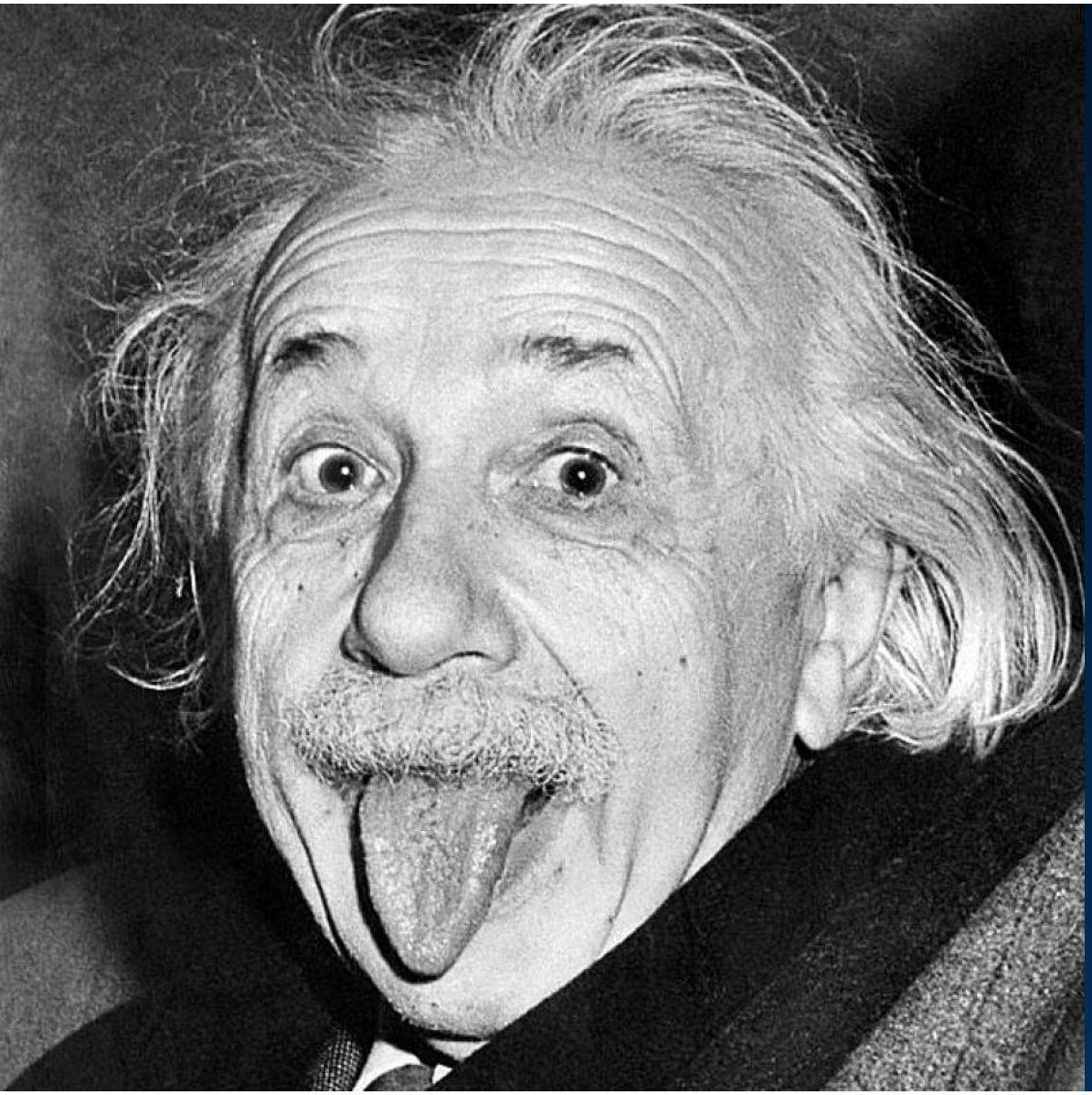
- Prepares system for operational readiness
  - Auditing
  - Control
  - Active Directory
  - NTP
  - Syslog
- May disable some ease-of-use features
  - Features meant for POC and test environments
- Reduces attack surface
  - Disables un-used functionality

Why it exists

- Provides audit guidelines for compliance standards
  - Core element of PCI, HIPAA, SOX, DISA, etc.
- Makes the product less susceptible to threats and vulnerabilities
- Acts as a tool to generate discussion on risk management
  - vSphere Security Guide (part of vSphere 6 doc set) is an important companion document

vSphere 6 Hardening Guide: major improvements

- The old guide was
  - Difficult to implement
  - Contained a mix of Operational Guidance and Programmatic Guidance
    - Which is which?
  - Difficult to understand
  - Operational Guidance is hard to measure
  - Cumbersome to produce
    - Excel is NOT a good tool to “edit” text with
- New guide is
  - Easy to implement
  - New Focus is on Programmatic Guidance
  - Goal to be mostly accessible via API’s and/or CLI’s
  - Automation, Automation, Automation
  - Leverage vSphere API’s
  - Easier to produce
    - Benefit: More time spent on content!

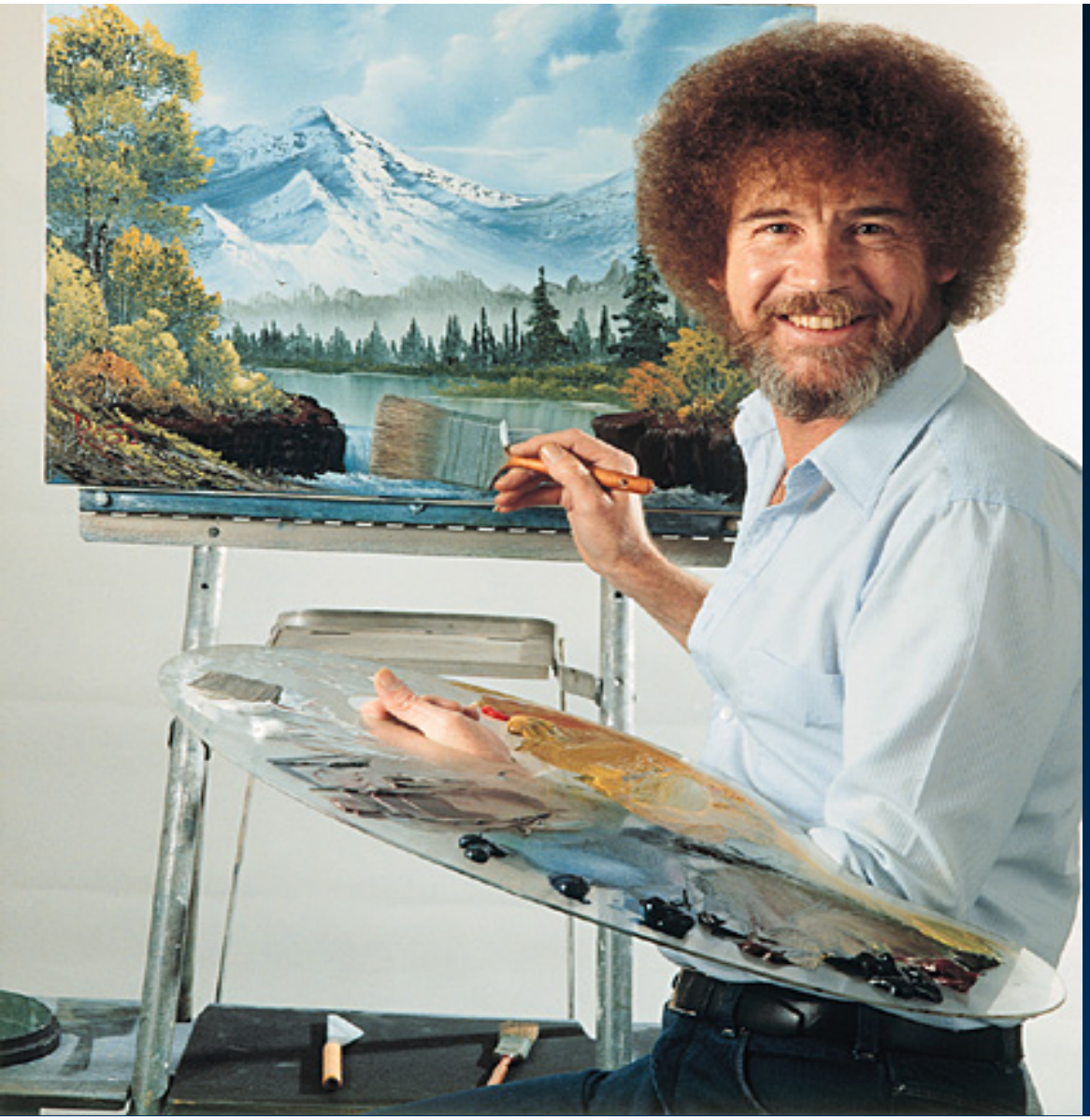


Programmatic Guidance

This is what becomes the Hardening Guide

- Focused on setting up the product in a secure manner
- Easy to assess
  - E.g., set this value to “True”
- Eventual goal: Hardening Guide is entirely automatable
  - Almost there!

Science

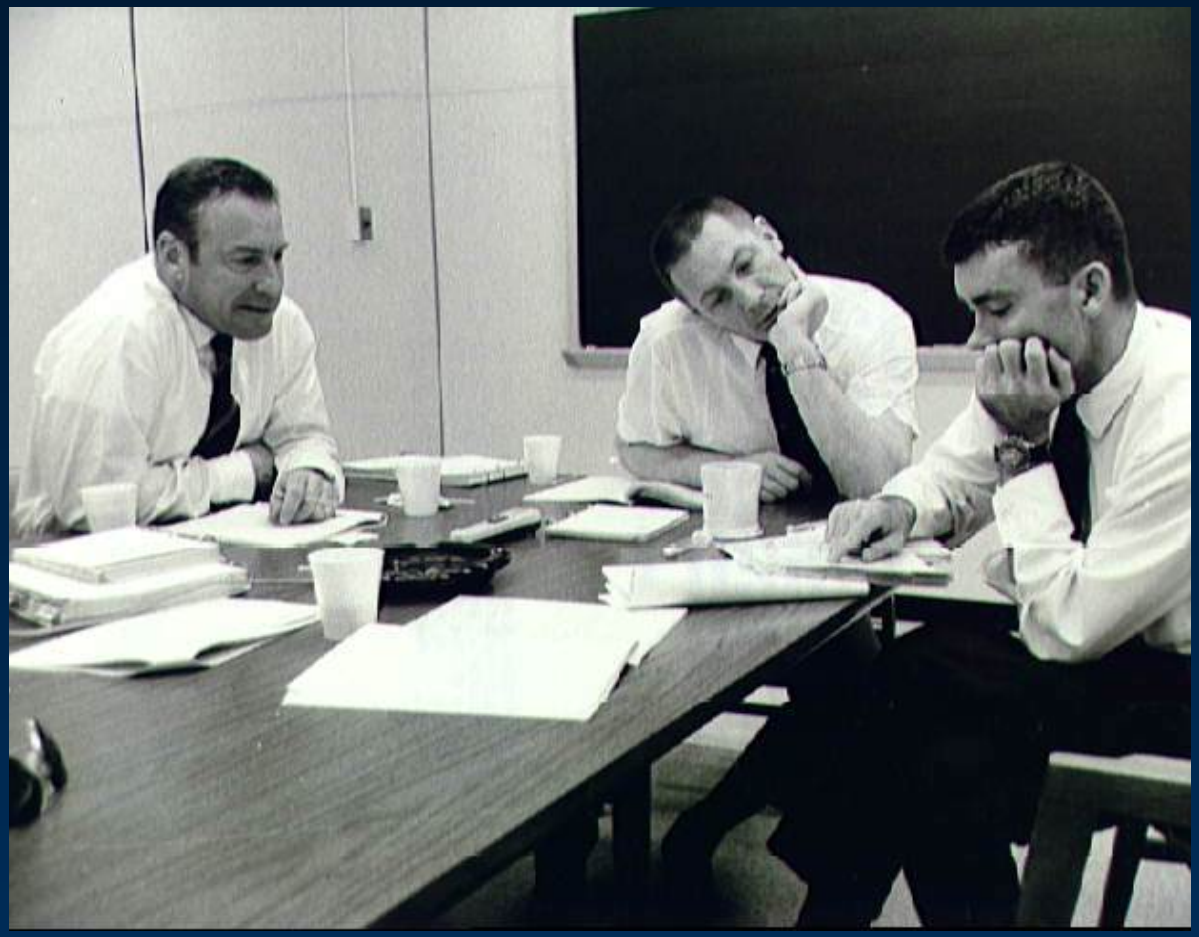


Operational Guidance

This becomes "Best Practices"

- Focuses on how to run a secure production environment
- Guidelines can be addressed or mitigated in multiple ways
  - Implementation is site-specific: architecture, policy, use case, risk, etc.
- May require cross-functional support across an enterprise
- Moved to the vSphere Security guide

Art

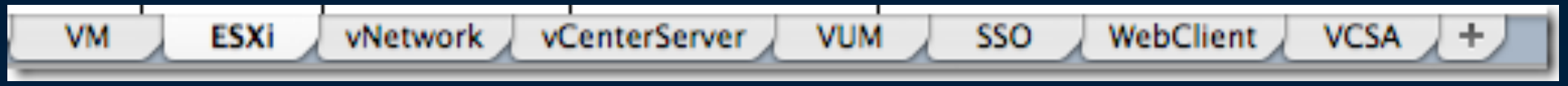


Top to Bottom Review

- First major release in many years
- Based on the incorporation of newer technologies and removal of older technologies guidelines were
  - Updated
    - e.g References, PowerCLI,
  - Added
    - e.g TPS settings
  - Removed
    - e. g “VMsafe” settings
- Delivered as:
  - XLS
  - PDF

New Taxonomy

- Old guide grouped by tabs



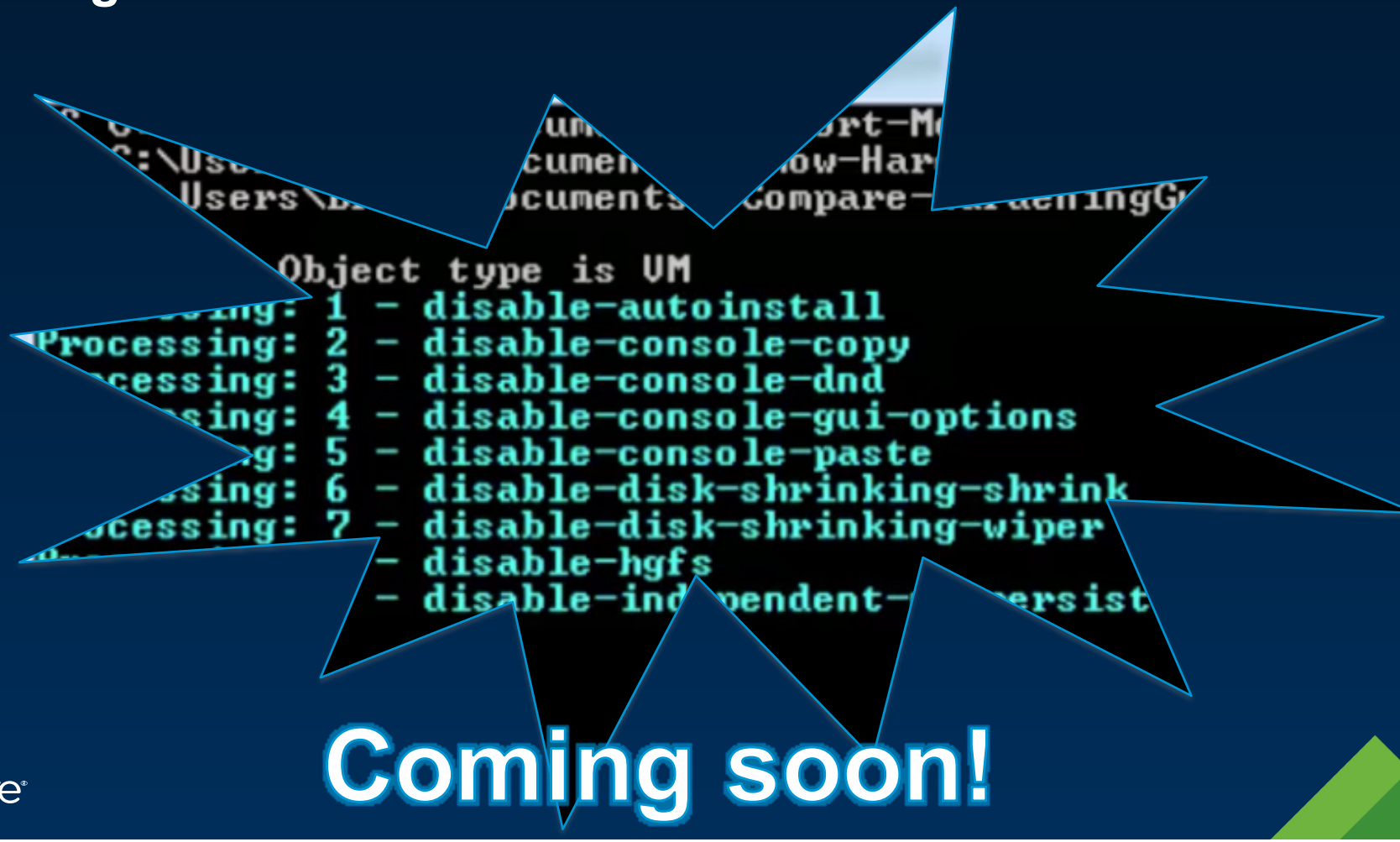
- New guide now a flat namespace
  - `Enable-remote-syslog` on the ESXi tab

    Becomes
  - `ESXi.enable-remote-syslog`
- Each guideline is now unique
- Enables automation
  - Creates the ability to iterate through the Hardening Guide more easily
  - Sets the stage for more cool things coming in the future!

vSphere 6 Hardening Guide Availability

Now Available!

Hardening Guide Automation?



Coming soon!

vSphere 6 Security Update

vmware

Five Major Security Enhancements in vSphere 6.0

1	Increased flexibility of Lockdown Mode
2	Added CAC smart card authentication to DCUI
3	Improved ESXi password and account management
4	Enhanced auditability of ESXi admin actions
5	Added full certificate lifecycle management

Flexible Lockdown Mode

Two Modes

- **Normal**
  - DCUI not stopped
  - Users on the DCUI.Access list can access DCUI
- **Strict**
  - DCUI stopped

Exception Users

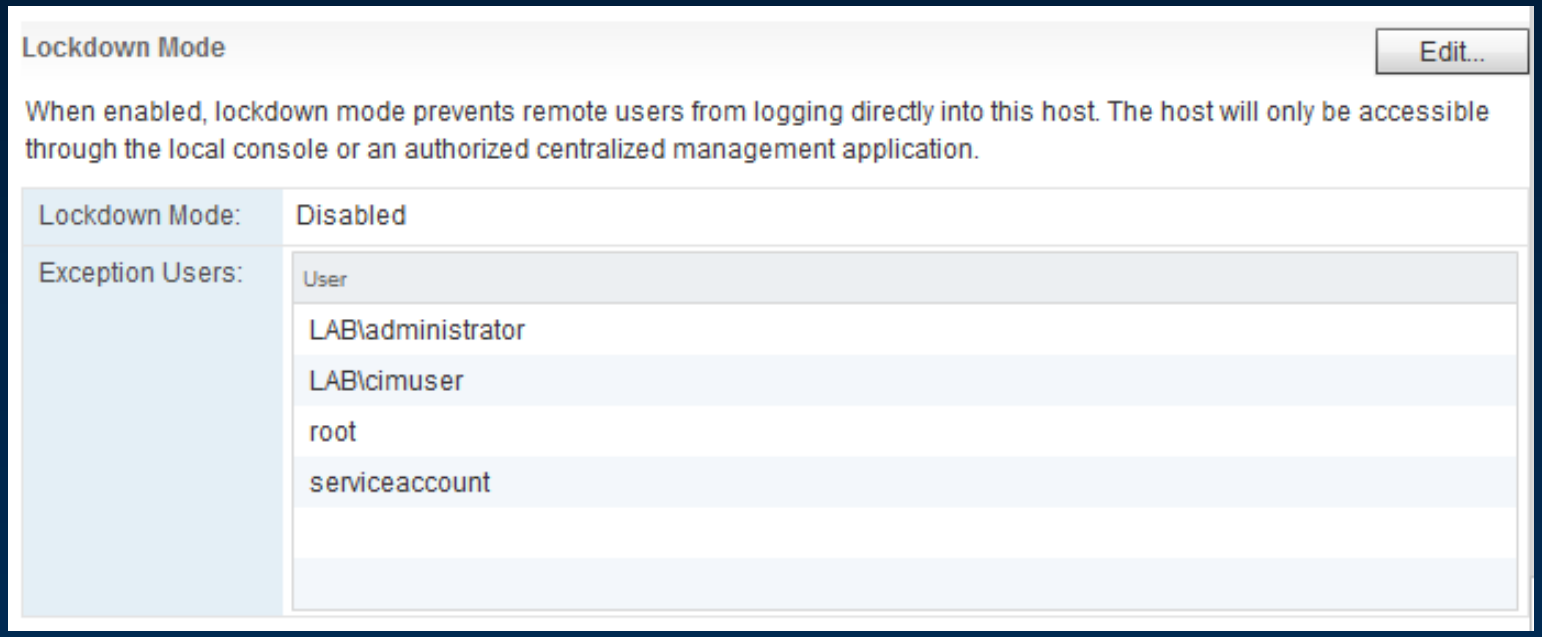
- Host or AD users with permissions defined locally on the host
- Used primarily for 3rd party applications (service accounts) that need host access when normal or strict lockdown mode is enabled
- Can be added from vSphere Web Client
- Not recommended for user accounts

ESXi Shell and SSH Independency

- Users registered in Exception Users list can access the host via ESXi Shell and SSH* during any lockdown mode

*You must have the Administrator role to SSH into any ESXi system

Web Client – Lockdown Mode



Lockdown Mode and PowerCLI

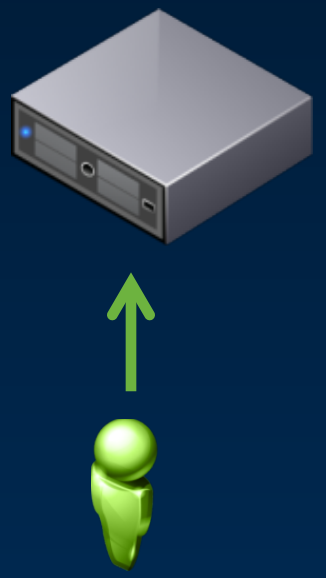
```
$level = New-Object VMware.Vim.HostLockdownMode
#Populate with level of lockdown:(lockdownDisabled,lockdownNormal,lockdownStrict)
$level = "lockdownStrict"
$esxihosts = get-vmhost
foreach ($esxihost in $esxihosts)
{
$myhost = Get-VMHost $esxihost | Get-View
$lockdown = Get-View $myhost.ConfigManager.HostAccessManager
Write-Host "----------"
Write-Host "Setting Lockdown mode to " $level
$lockdown.ChangeLockdownMode($level)
$lockdown.UpdateViewData()
$lockdownstatus = $lockdown.LockdownMode
Write-Host "Lockdown mode on $esxihost is set to $lockdownstatus"
Write-Host "----------"
}
```

Lockdown Mode and the Hardening Guide

- The setting being removed or reclassified are:
  - disable-dcui – Use Strict Lockdown Mode or don't put the user on the DCUI.Access list
  - disable-esxi-shell – Disabled by default, may stay purely as an auditable setting
  - disable-ssh – Disabled by Default, may stay purely as an auditable setting
- Also, instead of "enable-lockdown-mode"
  - ESXi.enable-strict-lockdown-mode
  - ESXi.enable-normal-lockdown-mode
- But which Lockdown Mode should I choose?
  - It's up to you and your security folks to decide which mode is appropriate for your environment
  - As always, the guide is a set of **guidelines** and **not** mandates.

CAC Smart Card Authentication to DCUI – Fed Customers Only

- **Currently works only for US Federal customers**
- Enables DCUI access using Common Access Cards (CAC) and Personal Identity Verification (PIV) cards
- ESXi server must be part of an Active Directory domain
- vSphere Web Client UI for enabling smart card authentication on an host and adding root certificates
- When Active Directory is unreachable
  - Fallback to Username/Password
- When vCenter is unreachable
  - Still works if AD is available
- When lockdown mode is enabled
  - Normal – Smart Card user must be on the Exception Users list
  - Strict – DCUI is disabled/stopped. No DCUI logins of any type



Local ESXi Account and Password Management Enhancements

New ESXCLI Commands

- **Account**
  - Create a new local user
  - List local user accounts
  - Remove local user account
  - Modify local user account
- **Permissions**
  - List permissions defined on the host
  - Set / Remove permission for a user or group

Account Lockout

- Two configurable parameters:
  - Maximum allowed failed login attempts (default = 10)
  - Lockout duration (default = 2min)
- Configurable via vCenter Host Advanced System Settings
- Available for SSH and vSphere Web Services SDK
- DCUI and console Shell are not locked

Complexity Rules via Advanced Settings

- No editing of PAM config files on the host required anymore
- Configurable via vCenter Host Advanced System Settings

Password Complexity in PowerCLI

```
#Set the Password Policy
$passwordpolicy = “retry=3 min=disabled,disabled,disabled,7,7”

#Get the list of connected ESXi hosts
$VMHosts = Get-VMHost | Where {$_.ConnectionState -eq "Connected"}

#Loop through the lists of hosts and set the Advanced Setting
foreach ($VMHost in $VMHosts) {
Set-VMHostAdvancedConfiguration -VMHost $VMHost -Name
“Security.PasswordQualityControl" -Value $passwordpolicy
}
```

Improved Auditability of ESXi Admin Actions

- Prior to 6.0, actions taken at the vCenter level by a named user would show up in ESXi logs with the “vpxuser” username.
  - [user=vpxuser]
  - This made for difficult forensic tracking of user actions.

```
2014-10-22 11:19:20.368  2014-10-22T15:19:56.159Z esxi-vsan-1.lab.local Hostd: [FFB74B70 info 'Hostsvc.AppConfigOptionsProvider(Config.HostAgent.)' opID=685f3dda-39 user=vpxuser] Set called with key 'Config.HostAgent.log.level' value '"info"'
source  event_type  hostname  appname  vmw_opid  vmw_user
```

- In 6.0, all actions taken at vCenter against an ESXi server now show up in the ESXi logs with the vCenter username
  - [user=vpxuser:CORP\Administrator]

```
2014-10-22 21:39:33.578  NoneZ esx-02a.corp.local Hostd: 2014-10-22T21:38:21.896Z info hostd[400C1B70] [Originator@6876 sub=Hostsvc.AppConfigOptionsProvider(Config.HostAgent.) opID=269dca9d-4f-7e93 user=vpxuser:CORP\Administrator] Set called with key 'Config.HostAgent.log.level' value '"verbose"'
source  event_type  hostname  vmw_opid  vmw_user
```

Certificate Lifecycle Management for vCenter and ESXi

- Introduced new vCenter solutions for a complete certificate lifecycle management:

VMware Certificate Authority
VMCA

- **Provisions** each ESXi host and each vCenter Server and vCenter Server service with certificates that are signed by VMCA.

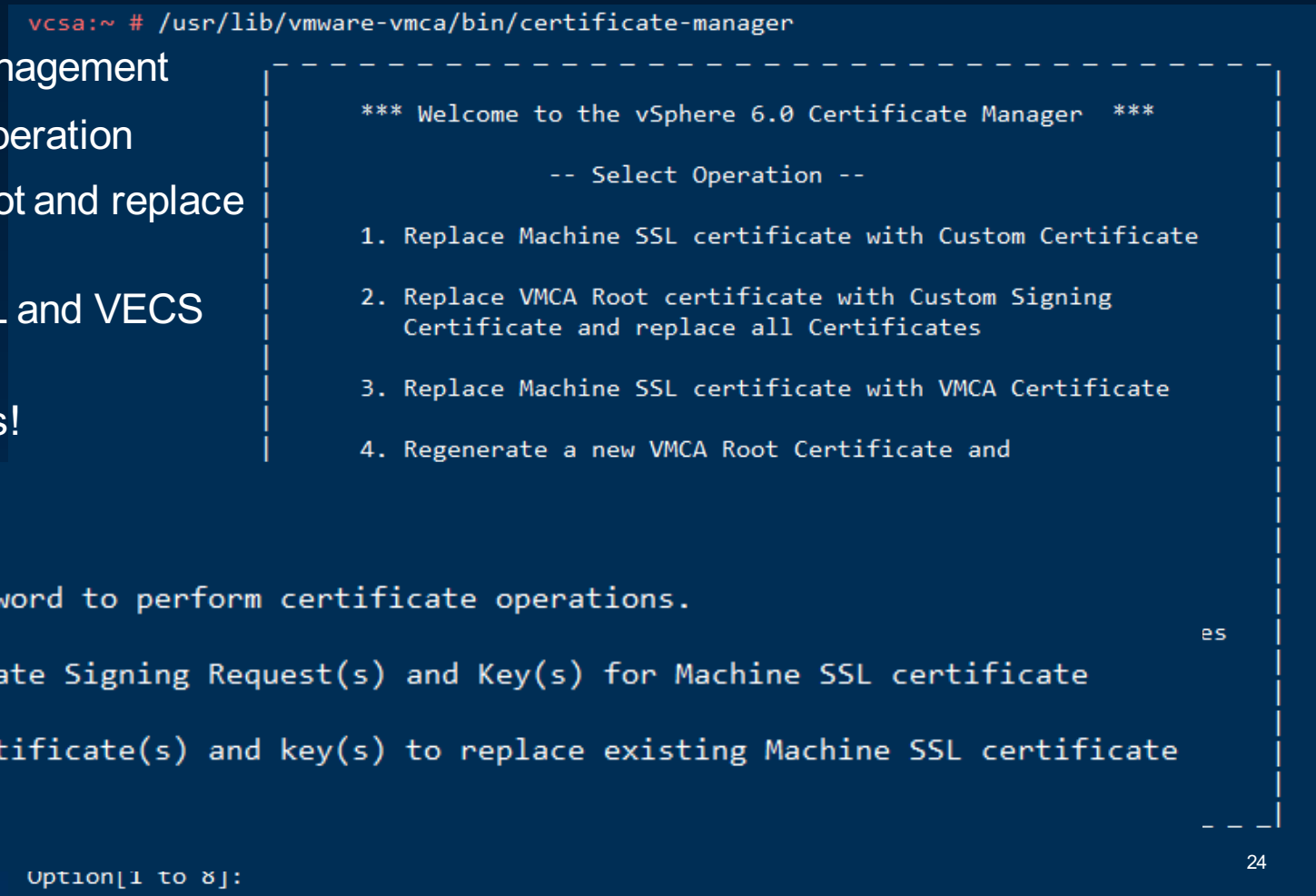
VMware Endpoint Certificate Service
VECS

- **Stores** all certificates and private keys for vCenter Server and vCenter Server services.
- Managing VECS is done via vecs-cli

- While you can decide not to use VMCA in your certificate chain, you must use VECS to store all certificates, and keys for vCenter Server and services.
- All ESXi certificates are stored locally on the host.

Certificate Manager

- Simplifies 3rd Part Cert Management
- Revert to last performed operation
- Regenerate new VMCA root and replace all certificates
- No fumbling with OpenSSL and VECS CLI's
- It will even generate CSR's!



Certificate Replacement Options for vCenter

VMCA Default

- VMCA provides the **Root** certificate
- All vSphere certificates chain to VMCA
- Regenerate certificates on demand **easily**

VMCA Enterprise

- **Replace** VMCA CA cert with a **subordinate** CA certificate from the Enterprise PKI
- Upon **removal** of the old VMCA CA certificate, all old certificates will be **regenerated**

Custom

- **Disable VMCA** as CA
- Provision your own **custom** certificates for each solution user and endpoint
- More **complicated** *For highly security conscious customers only*

ESXi Certificate Provisioning and VMCA

- ESXi booted from installation media will always have an auto-generated certificate
- When added to vCenter, VMCA will provision a certificate signed by VMCA as the root CA
- Auto Deploy
  - Signed certificate stored by the Auto Deploy server in its local certificate store and re-used on boot
  - If VMCA is not available then the host will cycle through shutdown and reboot until VMCA is available
- Host Upgrades
  - Custom certificates will be retained.
- New Certificate Manager Utility
  - Menu-based
  - Located in:
    - Windows - C:\Program Files\VMware\vCenter Server\vmcad certificate-manager
    - VCSA - /usr/lib/vmware-vmca/bin/certificate-manager

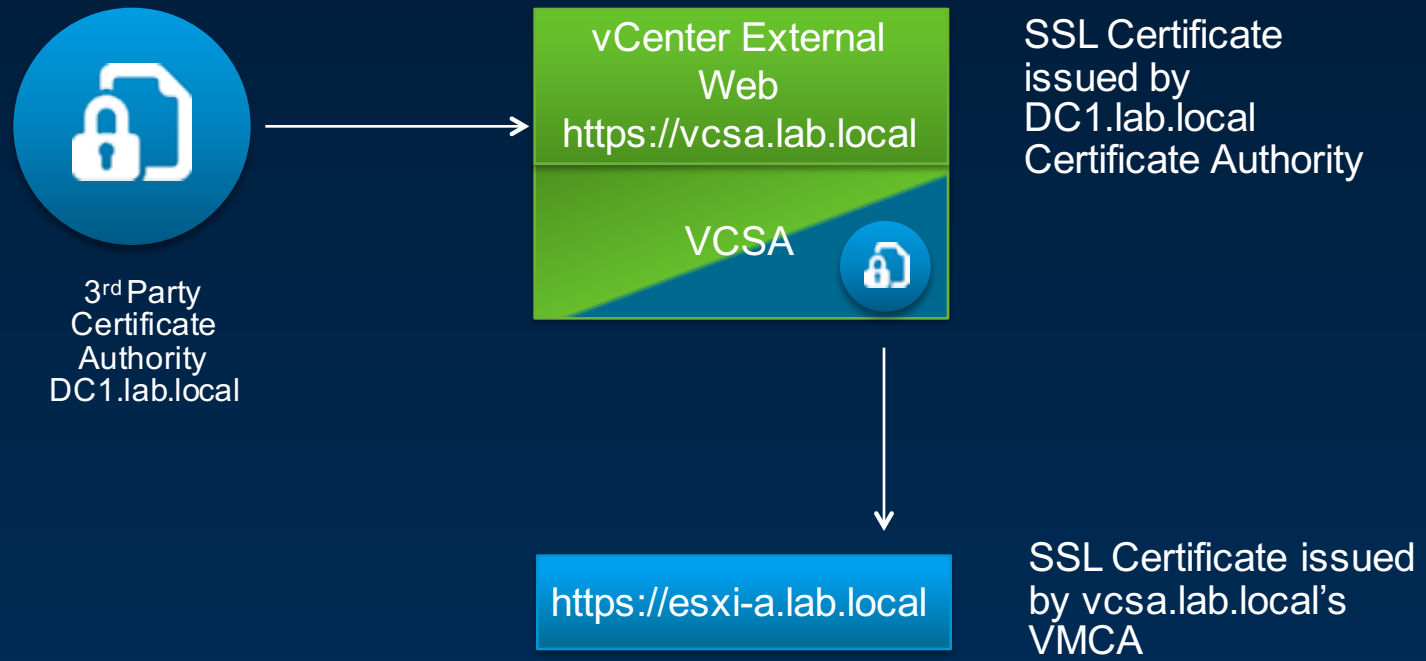
Certificate Replacement Options for ESXi

VMCA Authority	Custom CA Mode	Thumbprint mode
• VMCA provisions the host certificates. • Host certificates include the full chain.	• Allows you to use your own custom certificates. • Requires an Enterprise CA	• Legacy mode • Can be used to retain 5.5 certificates during upgrade.

ESXi 3rd party certificates replacement (No VMCA)

- Replacement is the same as 5.5
  - ESXi Shell
  - vifs command
  - HTTPS PUT
- Major change when using Custom/3rd Party certificates
  - Must update TRUSTED_ROOTS store in VECS on vCenter with the custom root certificates to ensure trust relationship
    - Done using a vecs-cli command
  - If custom root certificates have not been added to VECS then VMCA will overwrite custom certificates on the host
- If you are using VMCA then VMCA will manage all ESXi certificate replacement

Demo: How to use 3rd Party Certificate for External access



Demo Time

Review

- New Lockdown Modes
  - Easier to adopt plus increased flexibility of implementation!
- CAC Card support for ESXi DCUI Login
  - Keeping our U.S. Federal customers happy
- Improved ESXi password and account management
  - New Automation capabilities and ESXCLI enhancements
- Enhanced auditability of ESXi admin actions
  - Linking vCenter usernames to ESXi tasks providing better auditability and forensic usability
- Added full certificate lifecycle management
  - Certificate management made easy when using VMCA

Call to Action

- Review the Hardening Guide with your security team
  - Explain that it is a set of guidelines and not mandates.
  - Explain that vSphere already is “secure out of the box” by passing Common Criteria and that the Hardening Guide is for ensuring secure operations of “production” systems
- Explore the blogs and videos for vSphere 6 security updates
  - Especially review the updated vSphere 6 Security manual. LOTS of work went into this!!
- Consider moving to vSphere 6 sooner rather than later to take advantage of these updates
- Discuss with your security team the options VMCA bring to the table
  - VMCA only
  - External custom SSL certificate + VMCA for ESXi & vSphere solutions
  - VMCA as a subordinate certificate authority (Full root chaining to your PKI)
  - Not using VMCA
    - Least desirable choice! Still need to use VECS!

Questions?

http://blogs.vmware.com/vsphere/author/mike_foley

vmware

Helpful Resources

- Lockdown Mode Blog Article
  - http://blogs.vmware.com/vsphere/2015/03/vsphere-6-0-lockdown-modes.html
- VMCA Overview and Root Certificate Download Blog Article
  - http://blogs.vmware.com/vsphere/2015/03/vmware-certificate-authority-overview-using-vmca-root-certificates-browser.html
- Lockdown Mode Exception Users
  - http://blogs.vmware.com/vsphere/2015/03/vsphere-6-0-lockdown-mode-exception-users.html
- Videos!
  - vSphere 6 Certificate Infrastructure: http://youtu.be/KaBF11Vd6aM
  - ESXi Certificates in vSphere 6: http://youtu.be/txTx9rwqKp0
  - Lockdown Mode in vSphere 6: http://youtu.be/vC5VyUGB2Zk