پیکربندی امن

VMware ESXi 5.5

مرکز مدیریت راهبردی افتا

SCVI-VMWARE-ESXI -5.5

فروردین ۹۶

فهرست

پیش‌گفتار ۷
مقدمه ۸
تنظیمات ۱۱
SCVI-1: نصب ۱۱
SCVI-1-1: بروزرسانی سیستم ESXi را با آخرین patchها ۱۱
SCVI-1-2: اطمینان حاصل نمودن از سطح پذیرش Image Profile و VIB ۱۱
SCVI-1-3: اطمینان حاصل نمودن از load نشدن هیچ ماژول kernel غیر مجاز در Host ۱۱
SCVI-2: ارتباطات ۱۲
SCVI-2-1: پیکربندی NTP جهت هماهنگ‌سازی زمان ۱۲
SCVI-2-2: پیکربندی فایروال ESXi هر Host جهت محدودسازی دسترسی به سرویس‌های درحال اجرای Host ۱۳
SCVI-2-3: غیرفعال نمودن Managed Object Browser (MOB) ۱۳
SCVI-2-4: استفاده ننمودن از Self-signed Certificate پیشفرض برای ارتباطات ESXi ۱۴
SCVI-2-5: اطمینان از پیکربندی صحیح SNMP ۱۴
SCVI-2-6: جلوگیری از استفاده ناخواسته از API شبکه مربوط به dvfilter ۱۵
SCVI-2-7: SSLهای منقضی شده ویا لغو شده را از روی ESXi Host حذف گردد ۱۵
SCVI-3: ثبت وقایع Log ۱۶
SCVI-3-1: پیکربندی یک محل مجتمع جهت جمع‌آوری ESXi host core dump ۱۶
SCRO-3-2: پیکربندی logging ماندگار برای تمامیه Hostهای ESXi ۱۶
SCRO-3-3: پیکربندی log جهت ارسال به سرور خارجی ۱۷
SCVI-4: دسترسی ۱۸
SCVI-4-1: ایجاد یک حساب کاربری غیر root جهت دسترسی مدیریت محلی سرور ۱۸
SCVI-4-2: اتخاذ سیاست رمز عبور پیچیده برای رمزعبور کاربران ۱۹
SCVI-4-3: استفاده از اکتیودایرکتوری جهت اهراز هویت کاربران محلی ۱۹
SCVI-4-4: بررسی وضعیت عضویت در گروه ESX Admins اکتیودایرکتوری ۲۰
SCVI-5: کنسول ۲۱

SCVI-5-1: غیرفعال نمودن DCUI جهت جلوگیری از کنترل مدیریت محلی ۲۱
SCVI-5-2: غیرفعال سازی ESXi Shell بجز موارد عیب‌یابی و جمع‌آوری اطلاعات عیب‌یابی ۲۲
SCVI-5-3: غیرفعال سازی SSH ۲۲
SCVI-5-4: محدودسازی دسترسی CIM ۲۳
SCVI-5-5: فعال نمودن حالت Lockdown جهت محدودسازی دسترسی محلی و راه دور ۲۴
SCVI-5-6: حذف نمودن کلیدها SSH از روی فایل authorized_keys ۲۴
SCVI-5-7: تنظیم Timeout جهت بسته شدن خودکار Sessionهای Shell و SSH ۲۵
SCVI-5-8: تنظیم Timeout جهت سرویس Shell ۲۵
SCVI-5-9: تنظیم DCUI.Access و اعطای اجازه به کاربران مورد اطمینان جهت رد کردن یا لغو کردن حالت Lockdown ۲۶
SCVI-5-10: بررسی محتوای فایل پیکربندی در معرض دسترسی ۲۷
SCVI-6: Storage ۲۷
SCVI-6-1: فعال نمودن قابلیت احراز هویت CHAP دوسویه برای ترافیک iSCSI ۲۷
SCVI-6-2: اطمینان از یکتا بودن رمز احراز هویت CHAP ۲۹
SCVI-6-3: ایجاد مناسب منابع SAN با استفاده از Zone و Mask ۳۰
SCVI-6-4: صفر نمودن مقدار فایل‌های VMDK پیش از حذف ۳۰
SCVI-7: vNetwork ۳۱
SCVI-7-1: اطمینان از تنظیم سیاست Forged Transmit در vSwitch در حالت Reject ۳۱
SCVI-7-2: اطمینان از تنظیم سیاست MAC Address Change در vSwitch در حالت Reject ۳۱
SCVI-7-3: اطمینان از تنظیم سیاست Promiscuous Mode در vSwitch در حالت Reject ۳۲
SCVI-7-4: اطمینان از تنظیم نشدن Native VLAN در Port Group ۳۲
SCVI-7-5: اطمینان از تنظیم نشدن مقدار VLAN رزو شده برای سوییچ‌های فیزیکی که در Upstream قرار دارند. ۳۳
SCVI-7-6: اطمینان از تنظیم نشدن مقدار VLAN 4095 بجز برای Virtual Guest Tagging (VGT) ۳۴
SCVI-8: ماشین مجازی (VM) ۳۵
SCVI-8-1: ارتباطات ۳۵
SCVI-8-1-1: محدود کردن پیام‌های آگاه ساز VM در فایل VMX ۳۵
SCVI-8-1-2: محدود کردن اشتراک گذاری ارتباطات Console ۳۵

SCVI-8-2: سخت افزارها ۳۶
SCVI-8-2-1: حذف نمودن سخت افزارهای غیر مجاز – سخت افزار Floppy ۳۶
SCVI-8-2-2: حذف نمودن سخت افزارهای غیر معتبر – سخت افزار CD/DVD ۳۶
SCVI-8-2-3: حذف نمودن سخت افزارهای غیر معتبر – سخت افزار Parallel ۳۶
SCVI-8-2-4: حذف نمودن سخت افزارهای غیر مجاز – سخت افزار Serial ۳۷
SCVI-8-2-5: حذف نمودن سخت افزارهای غیر مجاز – سخت افزار USB ۳۷
SCVI-8-2-6: جلوگیری از جداسازی و تغییرات سخت افزار غیر مجاز ۳۸
SCVI-8-2-7: جلوگیری از اتصال سخت افزار غیر مجاز ۳۸
SCVI-8-3: Guest ۳۹
SCVI-8-3-1: غیر فعال نمودن اجزای سیستمی غیر ضروری و یا زاید داخل VM ۳۹
SCVI-8-3-2: حداقل رساندن موارد استفاده از کنسول VM ۳۹
SCVI-8-3-3: استفاده از پروتکل‌های امن برای دسترسی به پروت Virtual Serial ۴۰
SCVI-8-3-4: استفاده از Templeها جهت ایجاد VMها در هر جایی که امکان داشته باشد ۴۱
SCVI-8-4: Monitor ۴۱
SCVI-8-4-1: کنترل دسترسی به VMها از طریق APIهای dvfiler شبکه ۴۱
SCVI-8-4-2: کنترل آدرس VMsafe Agent ۴۲
SCVI-8-4-3: کنترل پورت VMsafe Agent ۴۲
SCVI-8-4-4: کنترل پیکربندی VMsafe Agent ۴۲
SCVI-8-4-5: غیرفعال نمودن Autologon ۴۳
SCVI-8-4-6: غیرفعال نمودن BIOS BBS ۴۳
SCVI-8-4-7: غیرفعال نمودن Host Interaction Protocol Handler در سیستم عامل مهمان ۴۳
SCVI-8-4-8: غیرفعال نمودن Unity Taskbar ۴۴
SCVI-8-4-9: غیرفعال نمودن Unity Active ۴۴
SCVI-8-4-10: غیرفعال نمودن محتوای Unity Window ۴۴
SCVI-8-4-11: غیرفعال نمودن بروزرسانی Unity Push ۴۵
SCVI-8-4-12: غیرفعال نمودن Drag and Drop Version Get ۴۵

SCVI-8-4-13: غیرفعال نمودن Drag and Drop Version Set ۴۵
SCVI-8-4-14: غیرفعال نمودن Shell Action ۴۶
SCVI-8-4-15: غیرفعال نمودن درخواست توپولوژی دیسک ۴۶
SCVI-8-4-16: غیرفعال نمودن وضعیت Trash Folder ۴۷
SCVI-8-4-17: غیرفعال نمودن Host Interaction Tray Icon در سیستم‌عامل مهمان ۴۷
SCVI-8-4-18: غیرفعال نمودن Unity ۴۷
SCVI-8-4-19: غیرفعال نمودن Unity Interlock ۴۸
SCVI-8-4-20: غیرفعال نمودن GetCreds ۴۸
SCVI-8-4-21: غیرفعال نمودن Host Guest File System Server ۴۸
SCVI-8-4-22: غیرفعال نمودن Guest Host Interaction Launch Menu ۴۹
SCVI-8-4-23: غیرفعال نمودن memSchedFakeSampleStats ۴۹
SCVI-8-4-24: غیرفعال نمودن عملیات کپی از طریق VM Console ۴۹
SCVI-8-4-25: غیرفعال نمودن عملیات Drag and Drop از طریق VM Console ۵۰
SCVI-8-4-26: غیرفعال نمودن Optionهای GUI در VM Console ۵۰
SCVI-8-4-27: غیرفعال نمودن عملیات‌های Paste در VM Console ۵۰
SCVI-8-4-28: کنترل دسترسی به کنسول VM از پروتکل VNC ۵۱
SCVI-8-4-29: غیرفعال نمودن تمام وضعیت‌ها بجز حالت VGA برای ماشین‌های مجازی ۵۱
SCVI-8-5: منابع ۵۲
SCVI-8-5-1: جلوگیری نمودن از مصرف بیش از حد منابع توسط ماشین مجازی ۵۲
SCVI-8-6: Storage ۵۲
SCVI-8-6-1: اجتناب از استفاده nonpersistent disks ۵۲
SCVI-8-6-2: غیرفعال نمودن shrinking دیسک مجازی ۵۳
SCVI-8-6-3: غیرفعال نمودن wiping دیسک مجازی ۵۳
SCVI-8-7: Tools ۵۴
SCVI-8-7-1: غیرفعال نمودن پیغام‌های VIX برای VM ۵۴
SCVI-8-7-2: محدود نمودن تعداد فایل‌های Log مربوط به VM ۵۴

SCVI-8-7-3: ممنانعت از ارسال اطلاعات Host به Guest.....۵۵
SCVI-8-7-4: محدود نمودن اندازه فایل‌های Log مربوط به VM ۵۵
پیوست.....۵۶
جدول ممیزی ۵۸

پیش‌گفتار

مرکز مدیریت راهبردی افتا[1] به منظور ساماندهی امنیت تجهیزات در حوزه فاوا[2]، پروژه «پیکربندی امن محصولات IT در کشور» را آغاز نموده است. یکی از گام‌های اساسی در این پروژه ارائه چک‌لیست و راهنمای پیکربندی امن برای محصولات IT می‌باشد. ارائه چک‌لیست برای محصولات داخلی بر عهده تولیدکننده محصول می‌باشد. تولید کننده ملزم است، چک‌لیست خود را در غالب ارائه شده از سمت مرکز افتا ارائه دهد. چک‌لیست‌های ارائه شده، توسط مرکز افتا مورد ارزیابی قرار گرفته و منتشر می‌گردد. سازمان‌های دولتی ملزم به استفاده از چک لیست‌های مذکور برای محصولات در حال استفاده خود هستند. همچنین سازمان‌های دولتی موظفند قبل از استفاده از محصولات IT، آن‌را مطابق چک‌لیست امنیتی مورد تایید مرکز افتا پیکربندی نمایند.

توجه به این نکته حائز اهمیت می‌باشد که چک‌لیست‌های ارائه شده، یک امنیت سطح پایه برای محصول ایجاد می‌نماید و سازمان‌ها ملزم هستند که برای رسیدن به سطح امنیت مورد نیاز خود، پس از اجرای مدیریت ریسک[3]، الزامات دیگری را نیز به این تنظیمات اضافه و مستند نمایند.

[1] امنیت فضای تولید و تبادل اطلاعات
[2] فناوری اطلاعات و ارتباطات
[3] Risk management

مقدمه

این سند راهنمایی برای پیکربندی امن VMware ESXi 5.5 است. در این سند مقادیر و تنظیمات امن برای سیاست‌های پیکربندی محصول مذکور ارائه شده است. مخاطب با استفاده از این سند توانایی پیاده‌سازی تنظیمات ارائه شده را خواهد داشت.

این سند توسط شرکت "فناوران توسعه امن ناجی" و به درخواست و تحت نظارت مرکز مدیریت راهبردی افتا تهیه گردیده است و از تلاش کارشناسان آن شرکت صمیمانه قدردانی می‌گردد. مرکز مدیریت راهبردی افتا ضمن استقبال از نظرات کارشناسان و متخصصان این حوزه برای غنای بیشتر این سند و دیگر اسناد مقاوم سازی، آمادگی دریافت پیشنهادات سازنده از طریق آدرس پست الکترونیکی Hardening@aftasec.ir را اعلام می‌دارد.

در ادامه، تنظیمات مورد نیاز برای پیکربندی امن VMware ESXi 5.5 آمده است. در این سند هر تنظیم با یک نام لاتین و شماره مختص آن آورده شده است. برای هر الزام دو بخش شرح اجمالی و نحوه پیاده‌سازی ارائه شده است. در بخش شرح اجمالی، توضیحی مختصر از ماهیت الزام بیان گردیده و در بخش نحوه پیاده‌سازی نیز، راهنمایی برای پیاده‌سازی الزام توسط مدیر سامانه ارائه شده است.

جدول ۱: گروه‌بندی و اختصارسازی نام برای محصولات IT

محصولات IT	
نام گروه	شماره گروه
نرم افزار آنتی ویروس	AV
سرویس‌دهنده نرم‌افزارهای کاربردی[1]	AS
احراز اصالت[2]	AU
اتوماسیون	AT
نرم‌افزار مدیریت پیکربندی[3]	CM
سیستم مدیریت پایگاه داده	DB
نرم‌افزار کاربردی رومیزی[4]	DA
سرویس گیرنده رومیزی[5]	DC
سرویس دایرکتوری[6]	DS
DNS سرور	DN
ایمیل سرور	ES
نرم‌افزار کاربردی سازمانی[7]	EA
دیوار آتش[8]	FI
تجهیزات قابل حمل[9]	HD
مدیریت هویت[10]	IM
سیستم تشخیص نفوذ[11]	ID

[1] Application Server
[2] Authentication
[3] Configuration Management System
[4] Desktop Application
[5] Desktop Client
[6] Directory Service
[7] Enterprise Application
[8] Firewall
[9] Handheld Device
[10] Identity Management
[11] Intrusion Detection System

محصولات IT	
نام گروه	شماره گروه
سرویس‌دهنده ایمیل[1]	MS
راهکارهای موبایلی[2]	MO
مسیریاب شبکه[3]	RO
سوئیچ شبکه	SW
سیستم عامل	OS
تجهیزات جانبی[4]	PD
سرویس دهنده[5]	SR
نرم‌افزار مجازی‌سازی[6]	VI
مرورگر وب	WB
سرویس‌دهنده وب	WS

[1] Mail Server
[2] Mobile Solution
[3] Network Router
[4] Peripheral Device
[5] Server
[6] Virtualization Software

تنظیمات

SCVI-1: نصب

SCVI-1-1: بروزرسانی سیستم ESXi را با آخرین patchها

شرح اجمالی:

نرم‌افزار VMware Update Manager ابزاری برای مدیریت بروزرسانی خودکار patchها برای Hostها و ماشین‌های مجازی vSphere است. ایجاد یک baseline راه مطمئنی جهت اطمینان پیدا کردن از patch بودن تمامی Hostها است بگونه‌ای که تمامی آن‌ها را در یک سطح patch شده باشند.

نحوه پیاده‌سازی:

از نرم‌افزار VMware Update Manager جهت تست و نصب نمودن patchها بر روی Hostها ESXi استفاده نمایید. VMware Update Manager یک Add-on برای VMware vCenter Server می‌باشد.

SCVI-1-2: اطمینان حاصل نمودن از سطح پذیرش Image Profile و VIB

شرح اجمالی:

ESXi Image Profile از چهار سطح پذیرش VIB پشتیبانی می‌نماید. یک VIB (vSphere Installation Bundle) مجموعه‌ای از فایل‌هایی است که به صورت یک بسته ارائه می‌شوند. VIB شامل فایل signature می‌باشد که جهت تایید سطح trust مورد استفاده قرار می‌گیرد.

نحوه پیاده‌سازی:

جهت پیاده سازی پیکربندی توصیه شده دستورات ذیل را در PowerCLI وارد نمایید.

```
# Set the Software AcceptanceLevel for each host
Foreach ($VMHost in Get-VMHost ) {
$ESXCli = Get-EsxCli -VMHost $VMHost
$ESXCli.software.acceptance.Set("PartnerSupported")
}
```

SCVI-1-3: اطمینان حاصل نمودن از load نشدن هیچ ماژول kernel غیر مجاز در Host

شرح اجمالی:

به صورت پیش‌فرض Hostهای ESXi اجازه load شدن ماژول‌های kernel که فاقد Signatureهای دیجیتالی معتبر را نمی‌دهد. این ویژگی ممکن است تغییر داده شده باشد که نتیجتا به load شدن ماژول‌های غیرمجاز می‌انجامد.

نحوه پیاده‌سازی:

جهت پیاده سازی پیکربندی توصیه شده دستورات ذیل را در PowerCLI وارد نمایید.

```
# To disable a module:
$ESXCli = Get-EsxCli -VMHost MyHost
$ESXCli.system.module.set($false, $false, "MyModuleName")
```

توجه داشته باشید پیش از غیرفعال نمودن ماژول‌های kernel، Hostها را در وضعیت maintenance قرار دهید.

SCVI-2: ارتباطات

SCVI-2-1: پیکربندی NTP جهت هماهنگ‌سازی زمان

شرح اجمالی:

پروتکل NTP (Network Time Protocol) باید جهت هماهنگ‌سازی زمان در Hostهای ESXi فعال و پیکربندی گردد. از صحت پیکربندی NTP Server روی Hostها و همچنین از درستی زمان در Event Log اطمینان حاصل نمایید.

نحوه پیاده‌سازی:

از طریق vSphere web client مراحل ذیل را اجرا نمایید.

۱. ابتدا Host را انتخاب نمایید.
۲. از منوی Manage -> Setting -> System -> Time Configuration بروید.
۳. بر روی دکمه Edit کلیک نمایید.
۴. بر روی Use Network Time Protocol کلیک نمایید.
۵. نام ویا IP مربوط به سرورهای NTP را به صورت مجزا (به کمک کاما) وارد نمایید.
۶. اگر وضعیت سرویس NTP بصورت Stopped است بر روی Start کلیک کنید.
۷. سیاست Startup را به صورت Start and stop with host قرار دهید.

۸. روی OK کلیک نموده و مراحل ذخیره می‌گردد.
۹. جهت پیاده سازی پیکربندی توصیه شده دستورات ذیل را در PowerCLI وارد نمایید.

```
# Set the NTP Settings for all hosts
# If an internal NTP server is used replace pool.ntp.org with
# the IP address of the internal NTP server
$NTPServers = "pool.ntp.org", "pool2.ntp.org" Get-VMHost | Add-VmHostNtpServer
$NTPServers
```

SCVI-2-2: پیکربندی فایروال ESXi هر Host جهت محدودسازی دسترسی به سرویس‌های درحال اجرای Host

شرح اجمالی:

به صورت پیش‌فرض فایروال ESXi فعال بوده و اجازه ارتباطات مربوط به Ping (ICMP) و کلاینت‌های DHCP و DNS / داده شده است. دسترسی باید تنها به سرویس‌ها از IP یا شبکه‌های محافظت شده وجود داشته باشد.

نحوه پیاده‌سازی:

از طریق vSphere web client مراحل ذیل را اجرا نمایید.

۱. ابتدا Host را انتخاب نمایید.
۲. از منوی Manage -> Setting -> System -> Security Profile بروید.
۳. در قسمت Firewall بر روی دکمه Edit کلیک نمایید.
۴. برای هر سرویس فعال (به طور مثال SSH)، یک حوزه IP جهت دسترسی داشتن وارد نمایید.

SCVI-2-3: غیرفعال نمودن Managed Object Browser (MOB)

شرح اجمالی:

Managed Object Browser (MOB) یک نرم‌افزار سروری تحت وب می‌باشد که به شما اجازه می‌دهد Objectهای وجود در سمت سرور را آزمایش نمایید. MOB به صورت پیش‌فرض بر روی vCenter نصب و اجرا می‌گردد.

نحوه پیاده‌سازی:

جهت پیاده سازی دستور ذیل را در ESXi Shell وارد نمایید

```
vim-cmd proxysvc/remove_service "/mob" "httpsWithRedirect"
```

نکته: شما نمی‌توانید MOB را هنگامی که یک Host در وضعیت lockdown می‌باشد غیرفعال نمایید.

SCVI-2-4: استفاده ننمودن از Self-signed Certificate پیشفرض برای ارتباطات ESXi

شرح اجمالی:

Certificateهای پیش‌فرض به وسیله CAهای Trusted امضا نشده‌اند و باید با Certificateهای معتبر که به وسیله CAهای Trusted امضا شده‌اند جایگزین گردند.

نحوه پیاده‌سازی:

می‌توان از ابزار VMware SSL Certificate Automation Tool جهت نصب یک Certificate امضا شده استفاده نمود.

جهت اطلاع از نحوه بکارگیری، به آدرس http://kb.vmware.com/kb/2057340 مراجعه نمایید.

SCVI-2-5: اطمینان از پیکربندی صحیح SNMP

شرح اجمالی:

بررسی کنید SNMP پیکربندی شده و تمام تنظیمات صحیح می‌باشد. اگر از SNMP استفاده نمی‌شود، باید غیرفعال شود.

ESXI از SNMPv3 پشتیبانی می‌کند که امنیت بالاتری نسبت به SNMPv1 و SNMPv2 دارد که شامل احراز هویت و رمزنگاری می‌شود.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Update the host SNMP Configuration (single host connection required)
Get-VmHostSNMP | Set-VMHostSNMP -Enabled:$true -ReadOnlyCommunity '<secret>'
```

در هر ESXi Host باید SNMP پیکربندی شود.

تنظیمات SNMP می‌تواند با استفاده از Host Profile پیکربندی و اعمال گردد.

SCVI-2-6: جلوگیری از استفاده ناخواسته از API شبکه مربوط به dvfilter

شرح اجمالی:

بررسی نمایید که dvfilter API در صورت عدم استفاده پیکربندی نشده باشد. اگر از virtual security appliance استفاده می‌شود پیکربندی این API ضروری می‌باشد.

نحوه پیاده‌سازی:

از طریق vSphere web client مراحل ذیل را اجرا نمایید.

۱. ابتدا Host را انتخاب نمایید.
۲. از منوی Manage -> Setting -> System -> Advanced System Setting بروید.
۳. مقدار Net.DVFilterBindIpAddress را در فیلتر وارد نمایید.
۴. بررسی کنید مقدار Net.DVFilterBindIpAddress خالی باشد.
۵. اگر یک Appliance مورد استفاده قرار می‌گیرد، مطمئن شوید که مقدار این پارامتر بر اساس IP صحیح تنظیم شده باشد.
۶. اطمینان حاصل نمایید که مقدار ورودی انتخاب شده باشد، روی icon ویرایش کلیک کنید.
۷. آدرس IP متناسب را وارد نمایید.
۸. روی OK کلیک نمایید.

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Set Net.DVFilterBindIpAddress to null on all hosts
Get-VMHost HOST1 | Foreach { Set-VMHostAdvancedConfiguration -VMHost $_ -Name
Net.DVFilterBindIpAddress -Value "" }
```

SCVI-2-7: SSLهای منقضی شده ویا لغو شده را از روی ESXi Host حذف گردد

شرح اجمالی:

SSLهای منقضی شده و یا لغو شده را از روی ESXi Host حذف گردد.

نحوه پیاده‌سازی:

Self-signed certificate با certificate از CA معتبر جایگزین گردد، یا به وسیله یک CA تجاری و یا به وسیله یک CA داخل سازمانی. این جایگزینی می‌تواند از روش‌های ذیل انجام پذیرد.

۱- جایگزینی Certificate و کلید پیشفرض ESXi از طریق ESXi Shell
۲- جایگزینی Certificate و کلید پیشفرض ESXi از طریق استفاده از دستور vifs
۳- جایگزینی Certificate و کلید پیشفرض ESXi از طریق استفاده از HTTPS PUT

درصورتی که به طور تصادفی self-signed certificate و کلید پیشفرض حذف شد یا شما اسم Host را تغییر دادید، یک self-signed certificate و کلید جدید از طریق ESXi Shell می‌توانید ایجاد نمایید.

SCVI-3: ثبت وقایع Log

SCVI-3-1: پیکربندی یک محل مجتمع جهت جمع‌آوری ESXi host core dump

شرح اجمالی:

جهت پیکربندی یک محل مجتمع جهت جمع‌آوری ESXi host core dump، از ESXi Dump Collector استفاده نمایید. سرویس VMware vSphere Network Dump Collector اجازه جهت جمع‌آوری اطلاعات تشخیص خطا از یک Host که دچار خطای بحرانی شده است را می‌دهد.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از ESXi Shell وارد نمایید.

```
# Configure remote Dump Collector Server
esxcli system coredump network set -v [VMK#] -i [DUMP_SERVER] -o [PORT]
# Enable remote Dump Collector
esxcli system coredump network set -e true
```

SCRO-3-2: پیکربندی logging ماندگار برای تمامیه Hostهای ESXi

شرح اجمالی:

Logهای سیستمی جهت ممیزی و تشخیص خطاها مورد نیاز می‌باشد. درصورتی که به صورت دائمی Logهای سیستمی ذخیره نشوند، بطور مثال بر روی یک datastore، پس از reboot شدن سیستم از بین خواهند رفت.

اطمینان حاصل نمایید که تنظیمات log سیستم به صورت ماندگار پیکربندی شده است تا در مواقع Reboot، از دست داده نشوند.

نحوه پیاده‌سازی:

از طریق vSphere web client مراحل ذیل را اجرا نمایید.

۱. ابتدا Host را انتخاب نمایید.
۲. از منوی Manage -> Setting -> System -> Advanced System Setting بروید.
۳. مقدار Syslog.global.LogDirرا در فیلتر وارد نمایید.
۴. مقدار Syslog.global.LogDir را در مسیر datastore دلخواه تنظیم نمایید.
۵. اطمینان حاصل نمایید که مقدار ورودی انتخاب شده باشد، روی icon ویرایش کلیک کنید.
۶. روی OK کلیک نمایید.

راه دیگر، دستور ذیل را در PowerCLI وارد نمایید.

```
# Set Syslog.global.logDir for each host
Get-VMHost | Foreach { Set-VMHostAdvancedConfiguration -VMHost $_ -Name
Syslog.global.logDir -Value "<NewLocation>" }
```

SCRO-3-3: پیکربندی log جهت ارسال به سرور خارجی

شرح اجمالی:

به صورت پیش‌فرض ESXi در فضای ذخیره داخلی یا ramdisk ذخیره می‌گردد. جهت محافظت logها از پیکربندی ارسال log به سرور خارجی در ESXi نیاز است.

نحوه پیاده‌سازی:

مراحل ذیل را انجام دهید.

۱. ابتدا یک سرور syslog نصب و پیکربندی نمایید. مانند vSphere Syslog Collector
۲. از طریق vSphere web client، Host را انتخاب نمایید.
۳. از منوی Manage -> Setting -> System -> Advanced System Setting بروید.

۴. مقدار Syslog.global.logHost را در فیلتر وارد نمایید.
۵. اطمینان حاصل نمایید که مقدار ورودی انتخاب شده باشد، روی icon ویرایش کلیک کنید.
۶. مقدار Syslog.global.logHost را متناسب با IP سرور Syslog وارد نمایید.
۷. روی OK کلیک نمایید.

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Set Syslog.global.logHost for each host
Get-VMHost | Foreach { Set-VMHostAdvancedConfiguration -VMHost $_ -Name
Syslog.global.logHost -Value "<NewLocation>" }
```

درهنگام پیکربندی ارسال log به سرور خارجی تنظیم مقدار Syslog.global.logDirUnique به true نیز توصیه می‌گردد.

تنظیمات Syslog باید برای تمامیه سرورهای ESXi تنظیم گردد.

SCVI-4: دسترسی

SCVI-4-1: ایجاد یک حساب کاربری غیر root جهت دسترسی مدیریت محلی سرور

شرح اجمالی:

حداقل یک حساب کاربری ایجاد نمایید و بجای کاربر root جهت امور مدیریتی استفاده نمایید.

نحوه پیاده‌سازی:

جهت ساختن حساب کاربری محلی باید از طریق vSphere Client نسبت به ایجاد آن اقدام نمود.

۱. ابتدا مستقیما به ESXi Host به وسیله vSphere client متصل شوید.
۲. با کاربر root وارد شوید.
۳. برگه مربوط به Local Users & Groups را انتخاب نمایید.
۴. یک کاربر ایجاد نمایید که دسترسی‌های ذیل را دارا باشد.
   - دسترسی Shell
   - به برگه Permissions رفته و بررسی نمایید که کاربر ایجاد شده در نقش Administrator قرار گرفته باشد.

۵. این مراحل را برای تمامی Hostهای ESXi تکرار نمایید.

SCVI-4-2: اتخاذ سیاست رمز عبور پیچیده برای رمزعبور کاربران

شرح اجمالی:

جهت جلوگیری از حملات مربوط به رمز عبور ضعیف، ایجاد سیاست رمز عبور پیچیده از بایدهای امنیتی می‌باشد.

نحوه پیاده‌سازی:

مراحل ذیل را انجام دهید.

۱. ابتدا در ESXi Shell با یک حساب کاربری با دسترسی administrator وارد شوید.
۲. فایل /etc./pam.d/passwd را باز نمایید.
۳. خط ذیل را پیدا نمایید.

```
/user set admin password=#123xX&123"%
```

۴. مقدار N را کمتر یا مساوی ۵ قرار دهید
۵. مقدار N0 را به disabled تغییر دهید
۶. مقدار N1 را به disabled تغییر دهید
۷. مقدار N2 را به disabled تغییر دهید
۸. مقدار N3 را به disabled تغییر دهید
۹. مقدار N4 را به ۱۴ یا بالاتر تغییر دهید

تنظیمات بالا وجود تعداد ۱۴ کاراکتر طول رمز عبور که حداقل یک کاراکتر از چهار نوع کاراکترهای خاص را داشته باشد الزام می‌نماید. به علاوه، حداقل ۵ تلاش برای ورود ناموفق اجازه داده می‌شود.

SCVI-4-3: استفاده از اکتیودایرکتوری جهت اهراز هویت کاربران محلی

شرح اجمالی:

سرور ESXi می‌تواند از اکتیودایرکتوری جهت مدیریت کاربران و گروه‌ها استفاده نماید. استفاده از یک سرویس احراز هویت توصیه شده است.

نحوه پیاده‌سازی:

از طریق vSphere web client:

۱. Host را انتخاب نمایید.
۲. از منوی Manage -> Setting -> System -> Authentication Services بروید.
۳. روی دکمه Join Domain کلیک نمایید.
۴. نام دامنه مورد نظر به همراه حساب کاربری که اجازه Join نمودن کامپیوتر را به domain دارد، را وارد نمایید.
۵. روی OK کلیک نمایید.

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Join the ESXI Host to the Domain
Get-VMHost HOST1 | Get-VMHostAuthentication | Set-VMHostAuthentication -Domain
domain.local -User Administrator -Password Passw0rd -JoinDomain
```

نکته: ۱. از Host Profile جهت انجام خودکار پیوستن به دامنه می‌توان استفاده کرد.

۲. جهت انتقال امن رمز عبور AD در بستر شبکه از vSphere Authentication proxy استفاده نمایید.

۳. اگر در اکتیودایرکتوری یک گروه به نام ESX Admins ساخته شود، تمام کاربرانی که عضو این گروه باشند به صورت پیش‌فرض دسترسی مدیریتی کامل روی تمام سرورهای ESXi آن دامنه را خواهند داشت.

SCVI-4-4: بررسی وضعیت عضویت در گروه ESX Admins اکتیودایرکتوری

شرح اجمالی:

گروهی که در AD به وسیله vSphere استفاده می‌شود توسط attribute، esxAdminsGroup تعیین می‌شود. به صورت پیش‌فرض، این attribute برای گروه ESX Admins تنظیم شده است. تمام اعضای گروه ESX Admins به صورت پیش‌فرض دسترسی مدیریتی کامل روی تمام سرورهای ESXi آن دامنه را خواهند داشت. مراحل ساخت این گروه را در AD تحت نظر دانسته و عضویت در آن را به کاربران خاص و بسیار مورد اعتماد محدود نمایید.

نحوه پیاده‌سازی:

۱. تنظیمات attribute، esxAdminsGroup مربوط به گروه ESX Admins را بررسی نمایید.
۲. لیست اعضای گروه در اکتیودایرکتوری را بررسی نمایید.
۳. هر عضو غیر مجاز را حذف نمایید.

SCVI-5: کنسول

SCVI-5-1: غیرفعال نمودن DCUI جهت جلوگیری از کنترل مدیریت محلی

شرح اجمالی:

DCUI اجازه پیکربندی تنظیمات سطح پایین سرور از قبیل IP، نام سرور و رمز root و نیز امکانات عیب یابی مانند فعال کردن Shell، مشاهده فایل‌های log، راه‌اندازی مجدد agentها و پیکربندی‌ها را می‌دهد. اعمالی که در DCUI انجام شود توسط vCenter قابل ردیابی نخواهد بود. حتی اگر حالت Lockdown فعال شود، کاربری که عضو گروه DCUI باشد امکان اعمال مدیریتی در DCUI را دارد و در این صورت از RBAC و کنترل ممیزی vCenter را دور خواهد زد. DCUI می‌تواند غیرفعال شود. با غیرفعال نمودن آن تمام اعمال مدیریتی محلی حذف شده، بنابراین این گونه اقدامات ضروری از طریق vCenter، به صورت متمرکز مدیریت و مشاهده خواهد شد.

نحوه پیاده‌سازی:

از طریق vSphere web client:

۱. Host را انتخاب نمایید.
۲. از منوی Manage -> Setting -> System -> Security Profile بروید.
۳. روی گزینه Services بروید.
۴. روی دکمه Edit کلیک نمایید.
۵. گزینه Direct Console UI را انتخاب نمایید.
۶. روی Stop کلیک کنید.
۷. نحوه شروع به کار را به Start and Stop Manually تغییر دهید.
۸. روی OK کلیک کنید.

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Set DCUI to start manually rather than automatic for all hosts
```

```
Get-VMHost | Get-VMHostService | Where { $_.key -eq "DCUI" } | Set-VMHostService -Policy Off
```

SCVI-5-2: غیرفعال سازی ESXi Shell بجز موارد عیب‌یابی و جمع‌آوری اطلاعات عیب‌یابی

شرح اجمالی:

تنها زمانی که نیاز به جمع‌آوری اطلاعات عیب‌یابی و یا عیب‌یابی سرور ESXi باشد باید Shell را فعال نمایید. به صورت پیش‌فرض Shell باید در تمام Hostها غیرفعال باشد.

نحوه پیاده‌سازی:

از طریق vSphere web client:

۱. Host را انتخاب نمایید.
۲. از منوی Manage -> Setting -> System -> Security Profile بروید.
۳. روی گزینه Services بروید.
۴. روی دکمه Edit کلیک نمایید.
۵. گزینه ESXi Shell را انتخاب نمایید.
۶. روی Stop کلیک کنید.
۷. نحوه شروع به کار را به Start and Stop Manually تغییر دهید.
۸. روی OK کلیک کنید.

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Set ESXi Shell to start manually rather than automatic for all hosts
Get-VMHost | Get-VMHostService | Where { $_.key -eq "TSM" } | Set-VMHostService -Policy Off
```

SCVI-5-3: غیرفعال سازی SSH

شرح اجمالی:

غیرفعال سازی SSH برای تمامی Hostهای ESXi جهت جلوگیری از دسترسی راه دور به ESXi Shell می‌باشد. تنها زمانی که نیاز به عیب یابی سیستمی بود SSH فعال شود.

نحوه پیاده‌سازی:

از طریق vSphere web client:

۱. Host را انتخاب نمایید.
۲. از منوی Manage -> Setting -> System -> Security Profile بروید.
۳. روی گزینه Services بروید.
۴. روی دکمه Edit کلیک نمایید.
۵. گزینه SSH را انتخاب نمایید.
۶. روی Stop کلیک کنید.
۷. نحوه شروع به کار را به Start and Stop Manually تغییر دهید.
۸. روی OK کلیک کنید.

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Set SSH to start manually rather than automatic for all hosts
Get-VMHost | Get-VMHostService | Where { $_.key -eq "TSM-SSH" } | Set-VMHostService
-
Policy Off
```

SCVI-5-4: محدودسازی دسترسی CIM

شرح اجمالی:

هرگز سطح دسترسی مدیریتی (مانند root) را برای ابزارهای مشاهده و مانیتورینگ سخت افزار بر مبنای CIM و یا نرم‌افزارهای مشابه طرف سوم[1] فراهم ننمایید.

برای هر نرم‌افزار CIM یک حساب کاربری برای آن سرویس با حداقل دسترسی مورد نیاز جهت آن نرم‌افزار ایجاد نمایید

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

[1] 3rd Party

```
# Create a new host user account -Host Local connection requiredNew-VMHostAccount -ID
ServiceUser -Password <password> -UserAccount
```

SCVI-5-5: فعال نمودن حالت Lockdown جهت محدودسازی دسترسی محلی و راه دور

شرح اجمالی:

حالت lockdown دسترسی محلی و راه دور را در Hostهای ESXi غیرفعال می‌کند. تمامیه مسائل مدیریتی باید از طریق vCenter انجام گیرد تا از سطح دسترسی و نقش‌های داده شده با حساب‌های کاربری اطمینان حاصل گردد.

نحوه پیاده‌سازی:

از طریق vSphere web client:

۱. Host را انتخاب نمایید.
۲. از منوی Manage -> Setting -> System -> Security Profile بروید.
۳. روی گزینه Lockdown Mode بروید.
۴. روی دکمه Edit کلیک نمایید.
۵. گزینه Enable Lockdown Mode را انتخاب نمایید.
۶. روی OK کلیک کنید.

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Enable lockdown mode for each host
Get-VMHost | Foreach { $_.EnterLockdownMode() }
```

SCVI-5-6: حذف نمودن کلیدها SSH از روی فایل authorized_keys

شرح اجمالی:

جهت کاربری روزانه تمامی Hostهای ESXi باید در حالت lockdown قرار بگیرند و سرویس SSH نیز غیرفعال گردد. حالت lockdown جلوی کاربران root جهت استفاده از کلیدهای مجاز را نمی‌گیرد. زمانی که شما از یک کلید دسترسی برای احراز هویت کاربر root استفاده می‌نمایید، از دسترسی کاربر root به Host از طریق SSH جلوگیری بعمل نمی‌آید حتی در زمانی که آن Host در حالت lockdown قرار گرفته شده باشد.

نحوه پیاده‌سازی:

جهت بررسی اضافه شدن کلیدهای SSH به فایل authorized_keys:

۱. از طریق Shell با کاربر root یا کاربری که دسترسی مدیریتی دارد در ESXi وارد شوید.
۲. محتوای فایل /etc/ssh/keys-root/authorized_keys را بررسی کنید
۳. در صورت خالی نبودن فایل، هر کلیدی که پیدا کردید حذف نمایید.

SCVI-5-7: تنظیم Timeout جهت بسته شدن خودکار Sessionهای Shell و SSH

شرح اجمالی:

مقدار Timeout جهت بسته شدن خودکار Sessionهای Shell و SSH را تنظیم نمایید.

نحوه پیاده‌سازی:

از طریق vSphere web client:

۱. Host را انتخاب نمایید.
۲. از منوی Manage -> Setting -> System -> Advanced System Settings بروید.
۳. مقدار ESXiShellInteractiveTimeOut را در فیلتر وارد نمایید.
۴. اطمینان حاصل نمایید که مقدار ورودی انتخاب شده باشد، روی icon ویرایش کلیک کنید.
۵. مقدار متناسب (300 یا کمتر) را وارد نمایید.
۶. روی OK کلیک نمایید.

نکته: مقدار 0 قابلیت Timeout را غیرفعال می‌نماید.

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Set Remove UserVars.ESXiShellInteractiveTimeOut to 300 on all hosts
Get-VMHost | Foreach { Set-VMHostAdvancedConfiguration -VMHost $_ -Name
UserVars.ESXiShellInteractiveTimeOut -Value 300 }
```

SCVI-5-8: تنظیم Timeout جهت سرویس Shell

شرح اجمالی:

جهت محدودسازی زمان اجرای سرویس‌ها می‌توان مقدار Timeout برای متوقف نمودن خودکار برای Shell و SSH تنظیم نمود.

نحوه پیاده‌سازی:

از طریق vSphere web client:

۱. Host را انتخاب نمایید.
۲. از منوی Manage -> Setting -> System -> Advanced System Settings بروید.
۳. مقدار ESXiShellTimeOut را در فیلتر وارد نمایید.
۴. اطمینان حاصل نمایید که مقدار ورودی انتخاب شده باشد، روی icon ویرایش کلیک کنید.
۵. مقدار متناسب (3600 یا کمتر) را وارد نمایید.
۶. روی OK کلیک نمایید.

نکته: مقدار 0 قابلیت Timeout را غیرفعال می‌نماید. همچنین توصیه می‌شود که مقدار ESXiShellInteractiveTimeOut همزمان با ESXiShellTimeOut تنظیم و استفاده گردد.

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Set UserVars.ESXiShellTimeOut to 3660 on all hosts
Get-VMHost | Foreach { Set-VMHostAdvancedConfiguration -VMHost $_ -Name
UserVars.ESXiShellTimeOut -Value 3600 }
```

SCVI-5-9: تنظیم DCUI.Access و اعطای اجازه به کاربران مورد اطمینان جهت رد کردن یا لغو کردن حالت Lockdown

شرح اجمالی:

یک لیستی از کاربران مورد اطمینان که توانایی رد شدن از حالت Lockdown را از طریق دسترسی به DCUI در مواقعی که Host از vCenter جدا شده باشد را تهیه کنید.

نحوه پیاده‌سازی:

از طریق vSphere web client:

۱. Host را انتخاب نمایید.
۲. از منوی Manage -> Setting -> System -> Advanced System Settings بروید.
۳. مقدار DCUI.Access را در فیلتر وارد نمایید.
۴. اطمینان حاصل نمایید که مقدار ورودی انتخاب شده باشد، روی icon ویرایش کلیک کنید.
۵. مقدار DCUI.Access را با استفاده از کاما، فهرستی از کاربران مورد اطمینان را وارد نمایید.
۶. روی OK کلیک نمایید.

SCVI-5-10: بررسی محتوای فایل پیکربندی در معرض دسترسی

شرح اجمالی:

فایل‌های پیکربندی که از طریق API وب ESXi در معرض دسترسی قرار می‌گیرد را مانیتور و بررسی نمایید که تغییرات بدون مجوز روی آن‌ها انجام نگرفته باشد.

نحوه پیاده‌سازی:

در حین تهیه نسخه پشتیبانی از پیکربندی، از شماره سریال به همراه پیکربندی نسخه پشتیبانی تهیه می‌شود. شماره سریال در هنگام بازیابی به همراه پیکربندی بازیابی می‌شود. این شماره در هنگام انجام عمل Recovery از روی CD (به صورت ترکیب شده با ESXi) و یا انجام عملیات تعمیر (از طریق مراحل نصب ESXi) حفظ نمی‌گردد. جهت تهیه نسخه پشتیبانی و بازیابی اطلاعات به روش ذیل عمل نمایید.

۱. از طریق دستور vicfg-cfgbackup از پیکربندی نسخه پشتیبانی تهیه کنید.
۲. عملیات Recovery از روی CD ویا تعمیر را اجرا نمایید.
۳. فایل پیکربندی را از طریق دستور vicfg-cfgbackup بازیابی نمایید.

در زمان بازیابی پیکربندی اطمینان حاصل نمایید که تمامی VMها در حالت خاموش قرار گرفته باشند.

Storage :SCVI-6

SCVI-6-1: فعال نمودن قابلیت احراز هویت CHAP دوسویه برای ترافیک iSCSI

شرح اجمالی:

با فعال نمودن CHAP دوسویه، که Mutual CHAP نیز گفته می‌شود، یک لایه امنیتی برای محافظت ایجاد می‌گردد تا initiator بتواند target را احراز هویت کند.

نحوه پیاده‌سازی:

از طریق vSphere web client:

۱. Host را انتخاب نمایید.
۲. از منوی Manage -> Storage -> Storage Adapters بروید.
۳. آداپتور iSCSI جهت پیکربندی یا روی نماد ایجاد یک آداپتور جدید کلیک نمایید.
۴. تحت مشخصات آداپتور، روی برگه Properites کلیک کرده و روی گزینه Edit در قسمت Authentication را کلیک کنید.
۵. روش احراز هویت را به Use bidirectional CHAP تغییر دهید.
۶. یک نام برای CHAP خروجی انتخاب نمایید.
   - اطمینان حاصل نمایید که نام وارد شده با نام پیکربندی شده در سمت رسانه ذخیره سازی شما یکسان باشد.
   - جهت تنظیم کردن نام CHAP در نام آداپتور iSCSI، نام initiator را استفاده نمایید.
   - جهت تنظیم کردن نام CHAP به چیزی غیر از نام آداپتور iSCSI، نام initiator را انتخاب ننمایید و نامی دلخواه را وارد نمایید.
۷. یک نام رمز برای CHAP خروجی جهت احراز هویت وارد نمایید. این رمز باید در سمت رسانه ذخیره سازی شنا نیز یکسان باشد.
۸. یک رمز برای CHAP ورودی وارد نمایید. اطمینان حاصل نمایید که رمز ورودی با خروجی یکسان نباشد.
۹. روی OK کلیک نمایید.
۱۰. بر روی دومین سمبل جهت اسکن آداپتور iSCSI کلیک نمایید.

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Set the Chap settings for the Iscsi Adapter
Get-VMHost | Get-VMHostHba | Where {$_.Type -eq "Iscsi"} | Set-VMHostHba # Use desired parameters here
```

SCVI-6-2: اطمینان از یکتا بودن رمز احراز هویت CHAP

شرح اجمالی:

در روش CHAP هر دو سمت کلاینت و سرور نیاز به داشتن رمز عبور برای ایجاد ارتباط دارند. هنگامی که CHAP را تنظیم می‌نمایید اطمینان حاصل کنید که برای هر ارتباط از یک رمز یکتا استفاده شده باشد.

نحوه پیاده‌سازی:

از طریق vSphere web client:

۱. Host را انتخاب نمایید.
۲. از منوی Manage -> Storage -> Storage Adapters بروید.
۳. آداپتور iSCSI جهت پیکربندی یا روی نماد ایجاد یک آداپتور جدید کلیک نمایید.
۴. تحت مشخصات آداپتور، روی برگه Properites کلیک کرده و روی گزینه Edit در قسمت Authentication را کلیک کنید.
۵. روش احراز هویت را به Use bidirectional CHAP تغییر دهید.
۶. یک نام برای CHAP خروجی انتخاب نمایید.
   - اطمینان حاصل نمایید که نام وارد شده با نام پیکربندی شده در سمت رسانه ذخیره سازی شما یکسان باشد.
   - جهت تنظیم کردن نام CHAP در نام آداپتور iSCSI، نام initiator را استفاده نمایید.
   - جهت تنظیم کردن نام CHAP به چیزی غیر از نام آداپتور iSCSI، نام initiator را انتخاب ننمایید و نامی دلخواه را وارد نمایید.
۷. یک نام رمز برای CHAP خروجی جهت احراز هویت وارد نمایید. این رمز باید در سمت رسانه ذخیره سازی شنا نیز یکسان باشد.
۸. یک رمز برای CHAP ورودی وارد نمایید. اطمینان حاصل نمایید که رمز ورودی با خروجی یکسان نباشد.
۹. روی OK کلیک نمایید.
۱۰. بر روی دومین سمبل جهت اسکن آداپتور iSCSI کلیک نمایید.

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Set the Chap settings for the Iscsi Adapter
Get-VMHost | Get-VMHostHba | Where {$_.Type -eq "Iscsi"} | Set-VMHostHba # Use
desired parameters here
```

SCVI-6-3: ایجاد مناسب منابع SAN با استفاده از Zone و Mask

شرح اجمالی:

از مکانیزم‌های zoneبندی و LUN mask جهت مجزا نمودن فعالیت‌های SAN استفاده نمایید. برای مثال، Zone که برای تست ایجاد شده باید به صورت مجزا درون SAN مدیریت شود تا مزاحم فعالیت zoneهای عملیاتی نباشد. به همین صورت، می‌توان Zoneهای مختلفی برای دپارتمان‌های مختلف ایجاد نمود. در ایجاد Zone باید هر گروه Host که نیاز به برقراری ارتباط با SAN را داشته باشند را در نظر گرفت. مکانیزم LUN Mask یک رویه است که یک LUN را در اختیار بعضی از Hostها قرار داده و برای بعضی دیگر از دسترس خارج می‌نماید.

نحوه پیاده‌سازی:

با استفاده از Hostهای ESXi، مدل zoneبندی single-initiator و یا مدل single-initiator-single-target را استفاده نمایید. مدل دومی مدلی توصیه شده می‌باشد. استفاده از یک مدل zoneبندی محدودتر از ایجاد اشکالات و اشتباهات پیکربندی که ممکن است روی SAN به وجود بیاید، جلوگیری می‌کند.

جهت یافتن جزئیات پیکربندی و توصیه‌های zoneبندی، با واحد پشتیبانی سازنده SAN یا SAN Switch تماس بگیرید. مشخصات zoneبندی و قابلیت‌های mask در هر SAN با توجه به سازنده آن متفاوت می‌باشد.

SCVI-6-4: صفر نمودن مقدار فایل‌های VMDK پیش از حذف

شرح اجمالی:

با صفر نمودن مقدار فایل‌های VMDK پیش از حذف نمودن از بازسازی مجدد آنها توسط کاربر به محتوای اصلی جلوگیری به عمل می‌آید.

نحوه پیاده‌سازی:

در زمان حذف یک فایل VMDK با محتوای حساس و ارزشمند:

۱. ماشین مجازی را ابتدا خاموش نمایید.
۲. دستور vmkfstools –writezeroes را پیش از حذف فایل از datastore در CLI وارد نمایید.

vNetwork :SCVI-7

SCVI-7-1: اطمینان از تنظیم سیاست Forged Transmit در vSwitch در حالت Reject

شرح اجمالی:

در هر vSwitch سیاست مربوط به Forged Transmit را در حالت reject تنظیم نمایید.

نحوه پیاده‌سازی:

از طریق vSphere web client:

۱. از منوی Hosts and Clusters -> vCenter -> Host بروید.
۲. در برگه مدیریت، روی Networking کلیک نموده و Virtual Switch را انتخاب نمایید.
۳. یک سوییچ استاندارد را از لیست انتخاب نموده و روی icon ویرایش کلیک کنید.
۴. برگه Security را انتخاب نمایید.
۵. مقدار Forged Transmits را به Reject تغییر دهید.
۶. روی OK کلیک کنید.

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# esxcli network vswitch standard policy security set -v vSwitch2 -f false
```

SCVI-7-2: اطمینان از تنظیم سیاست MAC Address Change در vSwitch در حالت Reject

شرح اجمالی:

در هر vSwitch سیاست مربوط به MAC Address Change را در حالت reject تنظیم نمایید.

نحوه پیاده‌سازی:

از طریق vSphere web client:

۱. از منوی Hosts and Clusters -> vCenter -> Host بروید.
۲. در برگه مدیریت، روی Networking کلیک نموده و Virtual Switch را انتخاب نمایید.
۳. یک سوییچ استاندارد را از لیست انتخاب نموده و روی icon ویرایش کلیک کنید.

۴. برگه Security را انتخاب نمایید.
۵. مقدار MAC Address Change را به Reject تغییر دهید.
۶. روی OK کلیک کنید.

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# esxcli network vswitch standard policy security set -v vSwitch2 -m false
```

SCVI-7-3: اطمینان از تنظیم سیاست Promiscuous Mode در vSwitch در حالت Reject

شرح اجمالی:

در هر vSwitch سیاست مربوط به Promiscuous Mode را در حالت reject تنظیم نمایید.

نحوه پیاده‌سازی:

از طریق vSphere web client:

۱. از منوی Hosts and Clusters -> vCenter -> Host بروید.
۲. در برگه مدیریت، روی Networking کلیک نموده و Virtual Switch را انتخاب نمایید.
۳. یک سوییچ استاندارد را از لیست انتخاب نموده و روی icon ویرایش کلیک کنید.
۴. برگه Security را انتخاب نمایید.
۵. مقدار Promiscuous Mode را به Reject تغییر دهید.
۶. روی OK کلیک کنید.

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# esxcli network vswitch standard policy security set -v vSwitch2 -p false
```

SCVI-7-4: اطمینان از تنظیم نشدن Native VLAN در Port Group

شرح اجمالی:

در ESXi از مفهوم Native VLAN وجود ندارد. هر Frame در VLAN اختصاص داده شده در Port Group دارای tag مخصوص به خود می‌باشد، اما Frameهایی که با VLAN اختصاص داده نشده باشند دارای tag نخواهند

بود بر همین اساس به صورت Native VLAN که در سوییچ فیزیکی tag خواهد خورد ارسال می‌گردد. برای مثال، Frameهای VLAN 1 در سوییچ‌های فیزیکی Cisco بدون tag خواهند بود، چون به عنوان Native VLAN فرض گرفته می‌شوند. حال آنکه در ESXi هر Frame که به عنوان VLAN 1 باشد tag 1 خواهد خورد؛ بنابراین ترافیکی که از سمت ESXi به مقصد Native VLAN ارسال می‌گردد به درستی Route نمی‌گردد (زیرا با tag اشتباه 1 ارسال می‌گردد درعوض ارسال بدون tag)، و به همین صورت ترافیک ورودی Native VLAN از سمت سوییچ فیزیکی برای ESXi قابل فهم نخواهد بود (زیرا به صورت بدون tag ارسال شده است). اگر در vSwitch از Native VLAN ID برای Port Group استفاده شود، ترافیک از VMها برای سوییچ که با Native VLAN پیکربندی شده باشد قابل فهم نخواهد بود، چون سوییچ انتظار ترافیک بدون tag را دارد.

نحوه پیاده‌سازی:

اگر مقدار پیش‌فرض 1 برای Native VLAN استفاده شده است، در vSwitch تعریف port group با هر مقداری بین 2 و 4094 باید انجام پذیرد. در غیر این صورت، باید port group را بدون هرگونه مقدار برای VLAN پیکربندی شود.

۱. از کلاینت vSphere web، Host مورد نظر را انتخاب نمایید.
۲. در برگه مدیریت، روی Networking، و سپس روی Virtual Switch کلیک نمایید.
۳. یک Standard Switch از لیست انتخاب کنید.
۴. دیاگرام Topology نشان داده شده انواع port groupهای موجود در vSwitch را نشان می‌دهد.
۵. برای هر port group در vSwitch، VLAN ID منصوب شده را بررسی نمایید.
۶. روی icon ویرایش کلیک کنید.
۷. در قسمت Properties، نام port group را قسمت معین شده ثبت کنید.
۸. VLAN ID جدید را در قسمت مربوطه وارد نموده یا از IDهای موجود یکی را انتخاب نمایید.

SCVI-7-5: اطمینان از تنظیم نشدن مقدار VLAN رزو شده برای سوییچ‌های فیزیکی که در Upstream قرار دارند.

شرح اجمالی:

از تنظیم نشدن مقدار VLAN رزو شده برای سوییچ‌های فیزیکی که در Upstream قرار دارند اطمینان حاصل کنید. برای مثال، این VLANها مقادیری است که توسط سوییچ فیزیکی Cisco Catalyst از VLANهای 1001 الی 1024 و 4094 رزو شده است. این مثدار در سوییچ‌های فیزیکی Nexus برابر 3968 الی 4047 و 4094 می‌باشد.

نحوه پیاده‌سازی:

مقدار تنظیم شده برای VLAN نباید با مقدار رزو شده در سوییچ‌های فیزیکی برابر باشد.

۱. از کلاینت vSphere web، Host مورد نظر را انتخاب نمایید.
۲. در برگه مدیریت، روی Networking، و سپس روی Virtual Switch کلیک نمایید.
۳. یک Standard Switch از لیست انتخاب کنید.
۴. دیاگرام Topology نشان داده شده انواع port groupهای موجود در vSwitch را نشان می‌دهد.
۵. برای هر port group در vSwitch، VLAN ID منصوب شده را بررسی نمایید.
۶. روی icon ویرایش کلیک کنید.
۷. در قسمت Properties، نام port group را قسمت معین شده ثبت کنید.
۸. VLAN ID جدید را در قسمت مربوطه وارد نموده یا از IDهای موجود یکی را انتخاب نمایید.

SCVI-7-6: اطمینان از تنظیم نشدن مقدار VLAN 4095 بجز برای Virtual Guest Tagging (VGT)

شرح اجمالی:

مقدار VLAN 4095 تنها در مواردی که Virtual Guest Tagging (VGT) نیاز است استفاده شود.

نحوه پیاده‌سازی:

مقدار تنظیم شده برای VLAN نباید با مقدار رزو شده در سوییچ‌های فیزیکی برابر باشد.

۱. از کلاینت vSphere web، Host مورد نظر را انتخاب نمایید.
۲. در برگه مدیریت، روی Networking، و سپس روی Virtual Switch کلیک نمایید.
۳. یک Standard Switch از لیست انتخاب کنید.
۴. دیاگرام Topology نشان داده شده انواع port groupهای موجود در vSwitch را نشان می‌دهد.
۵. برای هر port group در vSwitch، VLAN ID منصوب شده را بررسی نمایید.

۶. روی icon ویرایش کلیک کنید.
۷. در قسمت Properties، نام port group را قسمت معین شده ثبت کنید.
۸. VLAN ID جدید را در قسمت مربوطه وارد نموده یا از IDهای موجود یکی را انتخاب نمایید.

SCVI-8: ماشین مجازی (VM)

SCVI-8-1: ارتباطات

SCVI-8-1-1: محدود کردن پیام‌های آگاه ساز VM در فایل VMX

شرح اجمالی:

پیام‌های آگاه ساز را در فایل VMX مربوط به VM را محدود نمایید تا از پرشدن datastore و ایجاد زمینه حملات DoS جلوگیری شود.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "tools.setInfo.sizeLimit" -value 1048576
```

SCVI-8-1-2: محدود کردن اشتراک گذاری ارتباطات Console

شرح اجمالی:

با محدود کردن تعداد ارتباطات Console از مشاهده افراد غیرمجاز که اجازه مدیریتی ندارد جلوگیری می‌کند.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "RemoteDisplay.maxConnections" -value 1
```

SCVI-8-2: سخت افزارها

SCVI-8-2-1: حذف نمودن سخت افزارهای غیر مجاز – سخت افزار Floppy

شرح اجمالی:

هر سخت افزار فعال و متصل یک خطر بالقوه حملات می‌باشد. کاربران و proccessهای بدون مجوز در یک ماشین مجازی می‌توانند سخت افزارهای موجود را قبیل NIC و CD-ROM را به دستگاه متصل یا جدا نمایند. حمله کننده می‌تواند از این قابلیت جهت رخنه به امنیت ماشین مجازی کند. قطع و حذف نمودن سخت افزارهای غیر ضروری می‌تواند جلوی این خطرات را بگیرد.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Remove all Floppy drives attached to VMs
Get-VM | Get-FloppyDrive | Remove-FloppyDrive
```

SCVI-8-2-2: حذف نمودن سخت افزارهای غیر معتبر – سخت افزار CD/DVD

شرح اجمالی:

هر سخت افزار فعال و متصل یک خطر بالقوه حملات می‌باشد. کاربران و proccessهای بدون مجوز در یک ماشین مجازی می‌توانند سخت افزارهای موجود را قبیل NIC و CD-ROM را به دستگاه متصل یا جدا نمایند. حمله کننده می‌تواند از این قابلیت جهت رخنه به امنیت ماشین مجازی کند. قطع و حذف نمودن سخت افزارهای غیر ضروری می‌تواند جلوی این خطرات را بگیرد.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Remove all CD/DVD Drives attached to VMs
Get-VM | Get-CDDrive | Remove-CDDrive
```

SCVI-8-2-3: حذف نمودن سخت افزارهای غیر معتبر – سخت افزار Parallel

شرح اجمالی:

هر سخت افزار فعال و متصل یک خطر بالقوه حملات می‌باشد. کاربران و proccessهای بدون مجوز در یک ماشین مجازی می‌توانند سخت افزارهای موجود را قبیل NIC و CD-ROM را به دستگاه متصل یا جدا نمایند. حمله کننده می‌تواند از این قابلیت جهت رخنه به امنیت ماشین مجازی کند. قطع و حذف نمودن سخت افزارهای غیر ضروری می‌تواند جلوی این خطرات را بگیرد.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# In this Example you will need to add the functions from this post:
http://blogs.vmware.com/vipowershell/2012/05/working-with-vm-devices-in-powercli.html
# Remove all Parallel Ports attached to VMs
Get-VM | Get-ParallelPort | Remove-ParallelPort
```

SCVI-8-2-4: حذف نمودن سخت افزارهای غیر مجاز – سخت افزار Serial

شرح اجمالی:

هر سخت افزار فعال و متصل یک خطر بالقوه حملات می‌باشد. کاربران و proccessهای بدون مجوز در یک ماشین مجازی می‌توانند سخت افزارهای موجود را قبیل NIC و CD-ROM را به دستگاه متصل یا جدا نمایند. حمله کننده می‌تواند از این قابلیت جهت رخنه به امنیت ماشین مجازی کند. قطع و حذف نمودن سخت افزارهای غیر ضروری می‌تواند جلوی این خطرات را بگیرد.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# In this Example you will need to add the functions from this post:
http://blogs.vmware.com/vipowershell/2012/05/working-with-vm-devices-in-powercli.html
# Remove all Serial Ports attached to VMs
Get-VM | Get-SerialPort | Remove-SerialPort
```

SCVI-8-2-5: حذف نمودن سخت افزارهای غیر مجاز – سخت افزار USB

شرح اجمالی:

هر سخت افزار فعال و متصل یک خطر بالقوه حملات می‌باشد. کاربران و proccessهای بدون مجوز در یک ماشین مجازی می‌توانند سخت افزارهای موجود را قبیل NIC و CD-ROM را به دستگاه متصل یا جدا نمایند. حمله کننده می‌تواند از این قابلیت جهت رخنه به امنیت ماشین مجازی کند. قطع و حذف نمودن سخت افزارهای غیر ضروری می‌تواند جلوی این خطرات را بگیرد.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Remove all USB Devices attached to VMs
Get-VM | Get-USBDevice | Remove-USBDevice
```

SCVI-8-2-6: جلوگیری از جداسازی و تغییرات سخت افزار غیر مجاز

شرح اجمالی:

از جداسازی و تغییرات سخت افزار غیر مجاز جلوگیری بعمل آید.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.device.edit.disable" -value $true
```

SCVI-8-2-7: جلوگیری از اتصال سخت افزار غیر مجاز

شرح اجمالی:

از اتصال سخت افزار بدون مجوز جلوگیری بعمل آید.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.device.edit.disable" -value $true
```

Guest :SCVI-8-3

SCVI-8-3-1: غیر فعال نمودن اجزای سیستمی غیر ضروری و یا زاید داخل VM

شرح اجمالی:

با غیر فعال نمودن اجزای سیستمی غیر ضروری که تاثیری در پشتیبانی نرم‌افزار یا سرویس مورد استفاده در ماشین مجازی ندارند تعداد حملاتی که به ماشین مجازی می‌توان داشت، کاهش می‌یابد.

نحوه پیاده‌سازی:

این گام‌ها می‌تواند انجام پذیرد.

۱. غیر فعال سازی سرویس‌های غیر ضروری داخل سیستم عامل. برای مثال، اگر سیستم عامل برای اجرای سرویس فایل در نظر گرفته شده است، از خاموش بودن هر نوع سرویس وب در آن اطمینان حاصل نمایید.
۲. هر نوع سخت افزار فیزیکی را که نیاز ندارید جدا نمایید، مانند درایو CD/DVD یا Floppy و USB
۳. ویژگی Screen saver را خاموش کنید. اگر از لینوکس، BDS یا سولاریس به عنوان سیستم عامل مهمان در ماشین مجازی استفاده می‌کنید، از اجرا نمودن X Windows بجز موارد ضروری در سیستم بپرهیزید.

SCVI-8-3-2: حداقل رساندن موارد استفاده از کنسول VM

شرح اجمالی:

تنها زمانی که نیاز مبرم به استفاده از کنسول ماشین مجازی است اجازه استفاده از آن را بدهید. از Roleهای سفارشی شده جهت اعطای بهینه مجوزها استفاده نمایید.

نحوه پیاده‌سازی:

به صورت پیش‌فرض roleهای Virtual Machine Power User و Virtual Machine Administrator در vCenter دارای مجوز Virtual Machine.Interaction.Console Interaction می‌باشند. هرگز به افراد غیرمجاز برای داشتن این نقش‌ها بر روی ماشین‌های مجازی و یا فولدرهای ماشین مجازی مجوز صادر ننمایید.

۱. از طریق کلاینت vSphere، به Administrator\Roles در vCenter بروید.

۲. یک role سفارشی ساخته و با ویرایش آن تنها حداقل مجوزهای دسترسی را بدهید.
۳. در قدم بعد بر روی Object مورد نظر در قسمت Inventory بروید.
۴. بر روی برگه Permissions رفته و کاربران و roleهایی که به آن Object دسترسی دارند را مشاهده نمایید.
۵. هر نوع کاربر پیش‌فرض Admin و Power User را حذف و role سفارشی شده جدید را وارد نمایید.

SCVI-8-3-3: استفاده از پروتکل‌های امن برای دسترسی به پروت Virtual Serial

شرح اجمالی:

پورت‌های Virtual Serial اجازه ارتباط بین ماشین مجازی در بستر شبکه را می‌دهد. با این روش اجازه می‌دهد پورت Virtual Serial را به یک ارتباط TCP/IP بر روی یک ESXi Host متصل نمایید. درصورت نیاز به پورت Virtual Serial از اینکه از پروتکل امن استفاده می‌کند اطمینان حاصل نمایید.

نحوه پیاده‌سازی:

جهت پیکربندی ارتباط پورت Virtual Serial با پروتکل امن شبکه:

۱. استفاده از SSL – یا معادل TCP+SSL
۲. استفاده از SSL – TCP+SSL بر روی TCP بر روی IPv4 یا IPv6
۳. استفاده از SSL – TCP+SSL بر روی TCP بر روی IPv4
۴. استفاده از SSL – TCP+SSL بر روی TCP بر روی IPv6
۵. Telnet بر روی TCP همرا با SSL. ماشین مجازی و سیستم از راه دور[1] می‌توانند با یکدیگر مذاکره کرده و از SSL استفاده کنند درصورتی که سیستم از راه دور از گزینه اهراز هویت Telnet پشتیبانی کند. در غیر این صورت، در ارتباط از نوع غیر رمز[2] استفاده خواهد شد.
۶. Telnet – Telnet بر روی SSL بر روی TCP. در این صورت، مذاکرات SSL سریعا شروع شده و نمی‌توان از گزینه اهراز هویت در Telnet استفاده نمود.

[1] Remote
[2] Plain Text

SCVI-8-3-4: استفاده از Templeها جهت ایجاد VMها در هر جایی که امکان داشته باشد

شرح اجمالی:

استفاده از یک Template که در آن Image یک سیستم عامل Harden شده وجود دارد برای ایجاد Template مختص یک نرم‌افزار و استفاده از Template مختص یک نرم‌افزار برای ایجادماشین‌های مجازی دیگر.

نحوه پیاده‌سازی:

یک Template را برای ایجاد VMهای دیگر که شامل موارد Harden شده،Patch شده، و پیکربندی مناسب OS می‌باشد آماده نمایید. در صورت امکان، نرم‌افزارهای پیش نصب شده نیز در آن وجود داشته باشد، گرچه نیاز به توجه در این موارد به وجود می‌آید که نرم‌افزار وابستگی به مختصات ماشین مجازی خاصی پیدا نکند. در vSphere، شما می‌توانید یک Template را به یک ماشین مجازی و بالعکس به صورت فوری تبدیل نمایید، که این امر ایجاد تغییرات و بروزرسانی را تسریع می‌نماید.

Monitor :SCVI-8-4

SCVI-8-4-1: کنترل دسترسی به VMها از طریق APIهای dvfiler شبکه

شرح اجمالی:

جهت محافظت از ماشین‌های مجازی API مربوط به dvfilter شبکه را به درستی پیکربندی نمایید.

نحوه پیاده‌سازی:

در صورتی که ماشین مجازی نیاز به محافظت داشته باشد:

- فایل VMX را ویرایش نموده به صورتی که:
  - پیکربندی ethernet0.filter1.name = dvfilter1 جایی که ethernet0 یک کارت شبکه ماشین مجازی است که باید محافظت شود، filter1 تعداد فیلترهایی است که مورد استفاده قرار می‌گیرد، و dvfilter1 نام ماژول مسیر داده هسته[1] است که از ماشین مجازی محافظت می‌کند.
  - اطمینان حاصل نمایید که نام مسیر داده هسته به درستی وارد شده باشد.

[1] Data path kernel module

در صورتی که ماشین مجازی نیاز به محافظت نداشته باشد:

- فایل VMX را ویرایش نموده به صورتی که مقادیر ذیل حذف گردد:
  - پیکربندی ethernet0.filter1.name = dvfilter1 جایی که ethernet0 یک کارت شبکه ماشین مجازی است که باید محافظت شود، filter1 تعداد فیلترهایی است که مورد استفاده قرار می‌گیرد، و dvfilter1 نام ماژول مسیر داده هسته است که از ماشین مجازی محافظت می‌کند.

SCVI-8-4-2: کنترل آدرس VMsafe Agent

شرح اجمالی:

گزینه vmsafe.agentAddress را در فایل پیکربندی ماشین به درستی پیکربندی نمایید.

نحوه پیاده‌سازی:

در صورتی که ماشین مجازی توسط VMsafe در CPU و حافظه محافظت نگردد، در این صورت فایل پیکربندی ماشین مجازی را بررسی کنید که پیکربندی vmsafe.agentAddress وجود نداشته باشد. در صورتی که محافظت می‌شود اطمینان حاصل نمایید که مقدار صحیح وارد شده باشد.

SCVI-8-4-3: کنترل پورت VMsafe Agent

شرح اجمالی:

گزینه vmsafe.agentPort را در فایل پیکربندی ماشین به درستی پیکربندی نمایید.

نحوه پیاده‌سازی:

در صورتی که ماشین مجازی توسط VMsafe در CPU و حافظه محافظت نگردد، در این صورت فایل پیکربندی ماشین مجازی را بررسی کنید که پیکربندی vmsafe.agentPort وجود نداشته باشد. در صورتی که محافظت می‌شود اطمینان حاصل نمایید که مقدار صحیح وارد شده باشد.

SCVI-8-4-4: کنترل پیکربندی VMsafe Agent

شرح اجمالی:

گزینه vmsafe.enable را در فایل پیکربندی ماشین به درستی پیکربندی نمایید.

نحوه پیاده‌سازی:

در صورتی که ماشین مجازی توسط VMsafe در CPU و حافظه محافظت نگردد، در این صورت فایل پیکربندی ماشین مجازی را بررسی کنید که پیکربندی vmsafe.enable در وضعیت FALSE قرار گرفته باشد.

SCVI-8-4-5: غیرفعال نمودن Autologon

شرح اجمالی:

موارد غیرضروری autologon را غیرفعال نمایید تا سطح آسیب‌پذیر را کاهش دهید.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.ghi.autologon.disable" -value
$true
```

SCVI-8-4-6: غیرفعال نمودن BIOS BBS

شرح اجمالی:

با غیرفعال نمودن BIOS BBS سطح آسیب پذیر حملات را کاهش می‌دهید.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.bios.bbs.disable" -value $true
```

SCVI-8-4-7: غیرفعال نمودن Host Interaction Protocol Handler در سیستم عامل مهمان

شرح اجمالی:

با غیرفعال نمودن Host Interaction Protocol Handler در سیستم عامل مهمان سطح آسیب پذیر حملات را کاهش می‌دهید.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.ghi.protocolhandler.info.disable"
-value $true
```

SCVI-8-4-8: غیرفعال نمودن Unity Taskbar

شرح اجمالی:

با غیرفعال نمودن Unity Taskbar در سیستم عامل مهمان سطح آسیب پذیر حملات را کاهش می‌دهید.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.unity.taskbar.disable" -value
$true
```

SCVI-8-4-9: غیرفعال نمودن Unity Active

شرح اجمالی:

با غیرفعال نمودن Unity Active در سیستم عامل مهمان سطح آسیب پذیر حملات را کاهش می‌دهید.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.unityActive.disable" -value $True
```

SCVI-8-4-10: غیرفعال نمودن محتوای Unity Window

شرح اجمالی:

با غیرفعال نمودن محتوای Unity Window در سیستم عامل مهمان سطح آسیب پذیر حملات را کاهش می‌دهید.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.unity.windowContents.disable" -
value $True
```

SCVI-8-4-11: غیرفعال نمودن بروزرسانی Unity Push

شرح اجمالی:

با غیرفعال نمودن بروزرسانی Unity Push در سیستم عامل مهمان سطح آسیب پذیر حملات را کاهش می‌دهید.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.unity.push.update.disable" -value
$true
```

SCVI-8-4-12: غیرفعال نمودن Drag and Drop Version Get

شرح اجمالی:

با غیرفعال نمودن Drag and Drop Version Get در سیستم عامل مهمان سطح آسیب پذیر حملات را کاهش می‌دهید.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.vmxDnDVersionGet.disable" -value
$true
```

SCVI-8-4-13: غیرفعال نمودن Drag and Drop Version Set

شرح اجمالی:

با غیرفعال نمودن Drag and Drop Version Set در سیستم عامل مهمان سطح آسیب پذیر حملات را کاهش می‌دهید.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.guestDnDVersionSet.disable" -value
$true
```

SCVI-8-4-14: غیرفعال نمودن Shell Action

شرح اجمالی:

با غیرفعال نمودن Shell Action در سیستم عامل مهمان سطح آسیب پذیر حملات را کاهش می‌دهید.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.ghi.host.shellAction.disable" -value
$true
```

SCVI-8-4-15: غیرفعال نمودن درخواست توپولوژی دیسک

شرح اجمالی:

با غیرفعال نمودن درخواست توپولوژی دیسک در سیستم عامل مهمان سطح آسیب پذیر حملات را کاهش می‌دهید.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.dispTopoRequest.disable" -value
$true
```

SCVI-8-4-16: غیرفعال نمودن وضعیت Trash Folder

شرح اجمالی:

با غیرفعال نمودن وضعیت Trash Folder در سیستم عامل مهمان سطح آسیب پذیر حملات را کاهش می‌دهید.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.trashFolderState.disable" -value
$true
```

SCVI-8-4-17: غیرفعال نمودن Host Interaction Tray Icon در سیستم‌عامل مهمان

شرح اجمالی:

با غیرفعال نمودن Host Interaction Tray Icon در سیستم‌عامل مهمان سطح آسیب پذیر حملات را کاهش می‌دهید.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.ghi.trayicon.disable" -value $true
```

SCVI-8-4-18: غیرفعال نمودن Unity

شرح اجمالی:

با غیرفعال نمودن Unity در سیستم‌عامل مهمان سطح آسیب پذیر حملات را کاهش می‌دهید.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.unity.disable" -value $true
```

SCVI-8-4-19: غیرفعال نمودن Unity Interlock

شرح اجمالی:

با غیرفعال نمودن Unity Interlock در سیستم‌عامل مهمان سطح آسیب پذیر حملات را کاهش می‌دهید.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.unityInterlockOperation.disable" -
value $true
```

SCVI-8-4-20: غیرفعال نمودن GetCreds

شرح اجمالی:

با غیرفعال نمودن GetCreds در سیستم‌عامل مهمان سطح آسیب پذیر حملات را کاهش می‌دهید.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.getCreds.disable" -value $true
```

SCVI-8-4-21: غیرفعال نمودن Host Guest File System Server

شرح اجمالی:

با غیرفعال نمودن Host Guest File System Server سطح آسیب پذیر حملات را کاهش می‌دهید.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.hgfsServerSet.disable" -value
$true
```

SCVI-8-4-22: غیرفعال نمودن Guest Host Interaction Launch Menu

شرح اجمالی:

با غیرفعال نمودن Guest Host Interaction Launch Menu سطح آسیب پذیر حملات را کاهش می‌دهید.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.ghi.launchmenu.change" -value
$true
```

SCVI-8-4-23: غیرفعال نمودن memSchedFakeSampleStats

شرح اجمالی:

با غیرفعال نمودن memSchedFakeSampleStats سطح آسیب پذیر حملات را کاهش می‌دهید.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.memSchedFakeSampleStats.disable"
-
value $true
```

SCVI-8-4-24: غیرفعال نمودن عملیات کپی از طریق VM Console

شرح اجمالی:

با غیرفعال نمودن عملیات کپی از طریق VM Console سطح آسیب پذیر حملات را کاهش می‌دهید.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Add the setting to all VMs
```

```
Get-VM | New-AdvancedSetting -Name "isolation.tools.copy.disable" -value $true
```

SCVI-8-4-25: غیرفعال نمودن عملیات Drag and Drop از طریق VM Console

شرح اجمالی:

با غیرفعال نمودن عملیات Drag and Drop از طریق VM Console سطح آسیب پذیر حملات را کاهش می‌دهید.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.dnd.disable" -value $true
```

SCVI-8-4-26: غیرفعال نمودن Optionهای GUI در VM Console

شرح اجمالی:

با غیرفعال نمودن Optionهای GUI در VM Console سطح آسیب پذیر حملات را کاهش می‌دهید.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.setGUIOptions.enable" -value
$false
```

SCVI-8-4-27: غیرفعال نمودن عملیات‌های Paste در VM Console

شرح اجمالی:

با غیرفعال نمودن عملیات‌های Paste در VM Console سطح آسیب پذیر حملات را کاهش می‌دهید.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.paste.disable" -value $true
```

SCVI-8-4-28: کنترل دسترسی به کنسول VM از پروتکل VNC

شرح اجمالی:

دسترسی به ماشین مجازی از طریق پروتکل VNCرا به حداقل برسانید.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "RemoteDisplay.vnc.enabled" -value $false
```

SCVI-8-4-29: غیرفعال نمودن تمام وضعیت‌ها بجز حالت VGA برای ماشین‌های مجازی

شرح اجمالی:

تنها حالت VGA را برای کارت گرافیک ماشین مجازی فعال نگهدارید.

نحوه پیاده‌سازی:

بررسی کنید که تنظیمات پیشرفته ماشین مجازی svga.vgaonly در حالت TRUE می‌باشد.

جهت تغییر تنظیمات پیشرفته یک ماشین مجازی با استفاده از vSphere Client:

۱. اطمینان حاصل نمایید که ماشین مجازی در حالت خاموش می‌باشد.
۲. روی ماشین مجازی راست کلیک کنید.
۳. روی گزینه تنظیمات کلیک کنید تا پنجره تنظیمات ماشین مجازی باز شود.
۴. روی برگه Options کلیک کنید.
۵. از لیست سمت چپ، روی Advanced > General کلیک کنید.
۶. روی قسمت سمت راست پیکربندی، روی Configuration Parameters کلیک کنید.
۷. روی Add Row کلیک کنید.
۸. در ردیف جدید، تحت ستون نام، یک نام اختصاص دهید.

۹. در ردیف جدیدی، تحت ستون مقدار، یک مقدار جهت پیکربندی اختصاص دهید.
۱۰. ماشین مجازی را روشن نموده تا تغییرات اثر نمایند.

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "svga.vgaOnly" -value $true
```

SCVI-8-5: منابع

SCVI-8-5-1: جلوگیری نمودن از مصرف بیش از حد منابع توسط ماشین مجازی

شرح اجمالی:

با استفاده از محدودیت‌ها، منابع اشتراکی[1]، و منابع رزرو شده [2]می‌توان از مصرف بیش از حد منابع توسط ماشین مجازی جلوگیری کرد.

نحوه پیاده‌سازی:

- با استفاده از منابع اشتراکی یا رزرو شده منابع به صورت تضمین شده در اختیار VMهای مهم قرار می‌گیرد.
- با استفاده از محدودیت‌ها [3]می‌توان مصرف منابع را محدود به ماشین‌های مجازی نمود که از ریسک بالاتری برای حملات و خرابکاری‌ها، و یا جهت اجرای برنامه‌هایی با پتانسیل بالایی برای مصرف منابع دارند.

SCVI-8-6: Storage

SCVI-8-6-1: اجتناب از استفاده nonpersistent disks

شرح اجمالی:

دیسک‌های ایجاد شده برای ماشین‌های مجازی به صورت پیش‌فرض Dependent می‌باشند و تحت تاثیر snapshotها قرار می‌گیرند.

[1] Shares
[2] Reservations
[3] Limits

جهت اطمینان از این که دیسک ماشین مجازی تحت تاثیر snapshotها قرار نمی‌گیرد می‌توان آن را به حالت Independent قرار داد.

دیسک‌هایی که در حالت Independent قرار می‌گیرند می‌توانند در دو حالت Independent Persistent یا Independent Nonpersistent قرار گیرند.

دیسک‌هایی که در حالت Independent persistent قرار دارند اطلاعات خود را به صورت همیشگی روی دیسک ذخیره می‌کنند.

در حالت Independent Nonpersistent دیسک‌ها اطلاعات خود را پس از Reboot شدن سیستم از دست می‌دهند و هر نوع ردیابی حملات را غیرممکن می‌کند.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
#Alter the parameters for the following cmdlet to set the VM Disk Type:
Get-VM | Get-HardDisk | Set-HardDisk
```

SCVI-8-6-2: غیرفعال نمودن shrinking دیسک مجازی

شرح اجمالی:

درصورتی که shrinking دیسک مجازی به صورت مستمر استفاده شود می‌تواند به عدم دسترسی به دیسک و بروز عدم دسترسی به سرویس منجر شود. با غیرفعال نمودن این ویژگی می‌توان از بروز اینگونه حوادث جلوگیری نمود.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.diskShrink.disable" -value $true
```

SCVI-8-6-3: غیرفعال نمودن wiping دیسک مجازی

شرح اجمالی:

درصورتی که wiping دیسک مجازی به صورت مستمر استفاده شود می‌تواند به عدم دسترسی به دیسک و بروز عدم دسترسی به سرویس منجر شود. با غیرفعال نمودن این ویژگی می‌توان از بروز اینگونه حوادث جلوگیری نمود.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.diskWiper.disable" -value $true
```

SCVI-8-7: Tools

SCVI-8-7-1: غیرفعال نمودن پیغام‌های VIX برای VM

شرح اجمالی:

در صورتی که از زبان برنامه نویسی سفارشی VIX در محیط خود استفاده نمی‌کنید این ویژگی را باید غیرفعال کنید تا سطح آسیب پذیر کاهش یابد.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.vixMessage.disable" -value $true
```

SCVI-8-7-2: محدود نمودن تعداد فایل‌های Log مربوط به VM

شرح اجمالی:

جهت جلوگیری از رشد بدون کنترل Logها در تنظیمات VM پیکربندی مناسب را انجام دهید.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "log.keepOld" -value "10
```

SCVI-8-7-3: ممانعت از ارسال اطلاعات Host به Guest

شرح اجمالی:

تنظیمات VMware Tools را برای ارسال اطلاعات Host به Guest را در حالت غیرفعال قرار دهید.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "tools.guestlib.enableHostInfo" -value $false
```

SCVI-8-7-4: محدود نمودن اندازه فایل‌های Log مربوط به VM

شرح اجمالی:

با انجام پیکربندی ماشین مجازی از رشد بدون کنترل Logها جلوگیری نمایید. ماشین مجازی اطلاعات مربوط به عیب یابی را را در محل ذخیره Log درون VMFS Volume ذخیره می‌کند. کاربران یا پردازش‌های ماشین مجازی می‌توانند از روی قصد یا سهو از این اطلاعات سوء استفاده کنند. در طول زمان فایل Log می‌تواند فضای فایل‌های سیستمی را اشغال کند و مانع دسترسی به سرویس‌های شود.

نحوه پیاده‌سازی:

جهت پیاده‌سازی پیکربندی توصیه شده، دستور ذیل را با استفاده از PowerCLI وارد نمایید.

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "log.rotateSize" -value "1024000"
```

پیوست

در این بخش چک‌لیستی به منظور ممیزی محصول مورد نظر ارائه شده است. چک‌لیست شامل سه جدول است. جدول اول، جدول ممیز می‌باشد. در این جدول، اطلاعات مربوط به شخصی که پیکربندی امن را انجام می‌دهد یا آن را ممیزی می‌کند، وارد می‌شود. همچنین نتایج پیکربندی یا ممیزی به صورت اختصار در این جدول درج می‌گردد. جدول دوم، محل وارد کردن مشخصات سروری است که VMware ESXi 5.5 روی آن نصب شده است. جدول سوم، جدول تنظیماتی است که باید بررسی یا اعمال شوند. در صورت صحت اعمال تنظیم در هر ردیف، ستون وضعیت مربوط به آن با علامت √ نمایش داده خواهد شد.

ممیز	
ممیز: نام: ---------- ایمیل: ---------- تلفن: ----------	**تاریخ:**

تنظیمات	**تعداد**	**توضیحات**
تطابق		
عدم تطابق		
تنظیمات حذف شده		
تنظیمات اضافه شده		
مجموع تنظیمات اعمال شده		

مشخصات سرور	
آدرس MAC	
آدرس IP	
نام ماشین	
شماره اموال	
مدیر سیستم	نام: ---------- ایمیل: ---------- تلفن: ----------
تاریخ	

جدول ممیزی

جدول ممیزی خلاصه‌ای از تمامی الزامات بیان شده در متن سند می‌باشد. قابل ذکر است که ستون‌های "وضعیت" و "قابلیت پیاده‌سازی" باید توسط ممیز و برای هر سیستم حاوی این برنامه تکمیل گردد. در ستون وضعیت، ممیز باید از عبارت‌های "قبول" و "رد" متناسب با وضعیت الزام در محصول مورد ارزیابی استفاده نماید. در ستون قابلیت پیاده‌سازی، ممیز باید قابلیت پیاده‌سازی الزام برای محصول مورد ارزیابی را با عبارات "دارد" و "ندارد" بیان نماید. در صورتی که الزامی برای محصول مذکور قابلیت پیاده‌سازی نداشته باشد، علت عدم قابلیت پیاده‌سازی آن باید در ذیل جدول توضیح داده شود.

شناسه	وضعیت	تنظیمات	قابلیت پیاده‌سازی تنظیمات	مقدار پیش‌فرض	مقدار مطلوب
SCVI-1		نصب			
SCVI-1-1		بروزرسانی سیستم ESXi را با آخرین patchها	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-1-2		اطمینان حاصل نمودن از سطح پذیرش Image Profile و VIB	دارد	PartnerSupported	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-1-3		اطمینان حاصل نمودن از load نشدن هیچ ماژول kernel غیر مجاز در Host	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-2		ارتباطات			
SCVI-2-1		پیکربندی NTP جهت هماهنگ‌سازی زمان	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-2-2		پیکربندی فایروال ESXi هر Host جهت محدودسازی دسترسی به سرویس‌های درحال اجرای Host	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-2-3		غیرفعال نمودن Managed Object Browser (MOB)	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-2-4		استفاده ننمودن از Self-signed Certificate پیشفرض برای ارتباطات ESXi	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.

SCVI-2-5		اطمینان از پیکربندی صحیح SNMP	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-2-6		جلوگیری از استفاده ناخواسته از API شبکه مربوط به dvfilter	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-2-7		SSLهای منقضی شده ویا لغو شده را از روی ESXi Host حذف گردد	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-3		ثبت وقایع Log			
SCVI-3-1		پیکربندی یک محل مجتمع جهت جمع‌آوری ESXi host core dump	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-3-2		پیکربندی logging ماندگار برای تمامیه Hostهای ESXi	دارد	هنگام بوت از دیسک local= YES هنگام بوت از USB/SD= NO	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-3-3		پیکربندی log جهت ارسال به سرور خارجی	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-4		دسترسی			
SCVI-4-1		ایجاد یک حساب کاربری غیر root جهت دسترسی مدیریت محلی سرور	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-4-2		اتخاذ سیاست رمز عبور پیچیده برای رمزعبور کاربران	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-4-3		استفاده از اکتیودایرکتوری جهت اهراز هویت کاربران محلی	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-4-4		بررسی وضعیت عضویت در گروه ESX Admins اکتیودایرکتوری	دارد	ESX Admins	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-5		کنسول			
SCVI-5-1		غیرفعال نمودن DCUI جهت جلوگیری از کنترل مدیریت محلی	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-5-2		غیرفعال سازی ESXi Shell بجز موارد عیب‌یابی و جمع‌آوری اطلاعات عیب‌یابی	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-5-3		غیرفعال سازی SSH	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-5-4		محدودسازی دسترسی CIM	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.

SCVI-5-5		فعال نمودن حالت Lockdown جهت محدودسازی دسترسی محلی و راه دور	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-5-6		حذف نمودن کلیدها SSH از روی فایل authorized_keys	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-5-7		تنظیم Timeout جهت بسته شدن خودکار Sessionهای SSH و Shell		ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-5-8		تنظیم Timeout جهت سرویس Shell		ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-5-9		تنظیم DCUI.Access و اعطای اجازه به کاربران مورد اطمینان جهت رد کردن یا لغو کردن حالت Lockdown		ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-5-10		بررسی محتوای فایل پیکربندی در معرض دسترسی		ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-6		**Storage**			
SCVI-6-1		فعال نمودن قابلیت اهراز هویت CHAP دوسویه برای ترافیک iSCSI	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-6-2		اطمینان از یکتا بودن رمز اهراز هویت CHAP	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-6-3		ایجاد مناسب منابع SAN با استفاده از Zone و Mask	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-6-4		صفر نمودن مقدار فایل‌های VMDK پیش از حذف	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-7		**vNetwork**			
SCVI-7-1		اطمینان از تنظیم سیاست Forged Transmit در vSwitch در حالت Reject	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-7-2		اطمینان از تنظیم سیاست MAC Address Change در vSwitch در حالت Reject	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-7-3		اطمینان از تنظیم سیاست Promiscuous Mode در vSwitch در حالت Reject	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.

SCVI-7-4		اطمینان از تنظیم نشدن Native VLAN در Port Group	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-7-5		اطمینان از تنظیم نشدن مقدار VLAN رزو شده برای سوییچ‌های فیزیکی که در Upstream	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-7-6		اطمینان از تنظیم نشدن مقدار VLAN 4095 بجز برای Virtual Guest Tagging (VGT)	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-8		**ماشین مجازی (VM)**			
SCVI-8-1		**ارتباطات**			
SCVI-8-1-1		محدود کردن پیام‌های آگاه ساز VM در فایل VMX	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-8-1-2		محدود کردن اشتراک گذاری ارتباطات Console	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-8-2		**سخت افزارها**			
SCVI-8-2-1		حذف نمودن سخت افزارهای غیر مجاز – سخت افزار Floppy	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-8-2-2		حذف نمودن سخت افزارهای غیر معتبر – سخت افزار CD/DVD	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-8-2-3		حذف نمودن سخت افزارهای غیر معتبر – سخت افزار Parallel	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-8-2-4		حذف نمودن سخت افزارهای غیر مجاز – سخت افزار Serial	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-8-2-5		حذف نمودن سخت افزارهای غیر مجاز – سخت افزار USB	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-8-2-6		جلوگیری از جداسازی و تغییرات سخت افزار غیر مجاز	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-8-2-7		جلوگیری از اتصال سخت افزار غیر مجاز	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-8-3		**Guest**			
SCVI-8-3-1		غیر فعال نمودن اجزای سیستمی غیر ضروری ویا زاید داخل VM	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.

SCVI-8-3-2		حداقل رساندن موارد استفاده از کنسول VM	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-8-3-3		استفاده از پروتکل‌های امن برای دسترسی به پروت Virtual Serial	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-8-3-4		استفاده از Templeها جهت ایجاد VMها در هر جایی که امکان داشته باشد	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-8-4		**Monitor**			
SCVI-8-4-1		کنترل دسترسی به VMها از طریق APIهای dvfiler شبکه	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-8-4-2		کنترل آدرس VMsafe Agent	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-8-4-3		کنترل پورت VMsafe Agent	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-8-4-4		کنترل پیکربندی VMsafe Agent	دارد	ندارد	پیکربندی vmsafe.enable در وضعیت false
SCVI-8-4-5		غیرفعال نمودن Autologon	دارد	ندارد	غیرفعال نمودن Autologon
SCVI-8-4-6		غیرفعال نمودن BIOS BBS	دارد	ندارد	غیرفعال نمودن BIOS BBS
SCVI-8-4-7		غیرفعال نمودن Host Interaction Protocol Handler در سیستم عامل مهمان	دارد	ندارد	غیرفعال نمودن Host Interaction Protocol Handler در سیستم عامل مهمان
SCVI-8-4-8		غیرفعال نمودن Unity Taskbar	دارد	ندارد	غیرفعال نمودن Unity Taskbar
SCVI-8-4-9		غیرفعال نمودن Unity Active	دارد	ندارد	غیرفعال نمودن Unity Active
SCVI-8-4-10		غیرفعال نمودن محتوای Unity Window	دارد	ندارد	غیرفعال نمودن محتوای Unity Window
SCVI-8-4-11		غیرفعال نمودن بروزرسانی Unity Push	دارد	ندارد	غیرفعال نمودن بروزرسانی Unity Push
SCVI-8-4-12		غیرفعال نمودن Drag and Drop Version Get	دارد	ندارد	غیرفعال نمودن Drag and Drop Version Get
SCVI-8-4-13		غیرفعال نمودن Drag and Drop Version Set	دارد	ندارد	غیرفعال نمودن Drag and Drop Version Set
SCVI-8-4-14		غیرفعال نمودن Shell Action	دارد	ندارد	غیرفعال نمودن Shell Action
SCVI-8-4-15		غیرفعال نمودن درخواست توپولوژی دیسک	دارد	ندارد	غیرفعال نمودن درخواست توپولوژی دیسک
SCVI-8-4-16		غیرفعال نمودن وضعیت Trash Folder	دارد	ندارد	غیرفعال نمودن وضعیت Trash Folder

SCVI-8-4-17		غیرفعال نمودن Host Interaction Tray Icon در سیستم‌عامل مهمان	دارد	ندارد	غیرفعال نمودن Host Interaction Tray Icon در سیستم‌عامل مهمان
SCVI-8-4-18		غیرفعال نمودن Unity	دارد	ندارد	غیرفعال نمودن Unity
SCVI-8-4-19		غیرفعال نمودن Unity Interlock	دارد	ندارد	غیرفعال نمودن Unity Interlock
SCVI-8-4-20		غیرفعال نمودن GetCreds	دارد	ندارد	غیرفعال نمودن GetCreds
SCVI-8-4-21		غیرفعال نمودن Host Guest File System Server	دارد	ندارد	غیرفعال نمودن Host Guest File System Server
SCVI-8-4-22		غیرفعال نمودن Guest Host Interaction Launch Menu	دارد	ندارد	غیرفعال نمودن Guest Host Interaction Launch Menu
SCVI-8-4-23		غیرفعال نمودن memSchedFakeSampleStats	دارد	ندارد	غیرفعال نمودن memSchedFakeSampleStats
SCVI-8-4-24		غیرفعال نمودن عملیات کپی از طریق VM Console	دارد	ندارد	غیرفعال نمودن عملیات کپی از طریق VM Console
SCVI-8-4-25		غیرفعال نمودن عملیات Drag and Drop از طریق VM Console	دارد	ندارد	غیرفعال نمودن عملیات Drag and Drop از طریق VM Console
SCVI-8-4-26		غیرفعال نمودن Optionهای GUI در VM Console	دارد	ندارد	غیرفعال نمودن Optionهای GUI در VM Console
SCVI-8-4-27		غیرفعال نمودن عملیات‌های Paste در VM Console	دارد	ندارد	غیرفعال نمودن عملیات‌های Paste در VM Console
SCVI-8-4-28		کنترل دسترسی به کنسول VM از پروتکل VNC	دارد	ندارد	کنترل دسترسی به کنسول VM از پروتکل VNC
SCVI-8-4-29		غیرفعال نمودن تمام وضعیت‌ها بجز حالت VGA برای ماشین‌های مجازی	دارد	ندارد	غیرفعال نمودن تمام وضعیت‌ها بجز حالت VGA برای ماشین‌های مجازی
SCVI-8-5		**منابع**			
SCVI-8-5-1		جلوگیری نمودن از مصرف بیش از حد منابع توسط ماشین مجازی	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-8-6		**Storage**			
SCVI-8-6-1		اجتناب از استفاده nonpersistent disks	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-8-6-2		غیرفعال نمودن shrinking دیسک مجازی	دارد	ندارد	غیرفعال نمودن shrinking دیسک مجازی

SCVI-8-6-3		غیرفعال نمودن wiping دیسک مجازی	دارد	ندارد	غیرفعال نمودن wiping دیسک مجازی
SCVI-8-7		**Tools**			
SCVI-8-7-1		غیرفعال نمودن پیغام‌های VIX برای VM	دارد	ندارد	غیرفعال نمودن پیغام‌های VIX برای VM
SCVI-8-7-2		محدود نمودن تعداد فایل‌های Log مربوط به VM	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-8-7-3		ممانعت از ارسال اطلاعات Host به Guest	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.
SCVI-8-7-4		محدود نمودن اندازه فایل‌های Log مربوط به VM	دارد	ندارد	مطابق نحوه پیاده‌سازی اجرا گردد.