

۲۰/۹/۸۷

امنیت vSphere

برای متخصصان امنیت، مدیران و کارشناسان زیرساخت مجازی سازی

ترجمه و تألیف:

مهندس روزبه نوروزی

CISSP, PMP

مهندس سرزانه واشقانی فراهانی

کارشناسی ارشد مهندسی شبکه‌های کامپیوتری

کاری از: گروه آموزشی پرده‌های روزبه

مشاوره و آموزش تخصصی فناوری و امنیت اطلاعات



**NAGHOOS
PUBLICATION**

۱۳۹۷

سرشناسه : نوروزی، روزبه، ۱۳۵۷-
 عنوان و نام پدیدآور : امنیت Sphere برای متخصصان امنیت، مدیران و کارشناسان زیر ساخت مجازی سازی / ترجمه و
 تالیف روزبه نوروزی، فرزانه واشقی، قراهنی (کاری از گروه آموزشی پژوهی روزبه)
 مشخصات نشر : انتشارات ناقوس-۱۳۹۷
 مشخصات ظاهری : ۳۷۰ص: مصور جدول، نمودار.
 شابک : 978-600-473-118-8
 وضعیت فهرست نویسی : فیپا
 موضوع : وی، ام، وی، وی اسفر
 موضوع : VMware vSphere :
 موضوع : کامپیوترها-سیستم های مجازی
 موضوع : Virtual computersystems :
 شناسه افزوده : واشقی قراهنی، فرزانه، ۱۳۷۰-
 رده بندی کنگره : ۱۳۹۷: ۷۶/۹/۹۰ QA
 رده بندی دیوید : ۰۰۵/۴۳۶:
 شماره کتابخانه ملی : ۵۱۵۱۹۳۸



برای خرید Online به آدرس زیر مراجعه کنید:

www.naqhoospress.ir

انتشارات ناقوس

نام کتاب :	امنیت Sphere برای متخصصان امنیت، مدیران و کارشناسان زیر ساخت مجازی سازی
ناشر :	انتشارات ناقوس
ترجمه و تالیف :	روزبه نوروزی، فرزانه واشقی، قراهنی
چاپ اول :	۱۳۹۷ :
تیراژ :	۱۰۰ :
قیمت با یک عدد DVD :	۶۵۰۰۰۰ ریال
چاپ و صحافی :	نارنجستان
شابک :	۹۷۸-۶۰۰-۴۷۳-۱۱۸-۸ :
ISBN :	978-600-473-118-8 :

طبقه حقوق برای ناشر محفوظ است. این اثر به صورت حروفچینی یا چاپ مجدد چاپ است. پلی کپی، فتوکپی، راج دیگر چاپ ممنوع است و پیگرد قانونی دارد.

مرکز پخش: انتشارات ناقوس

۱- بلوار کشاورز-خیابان آذر-کوچه پارسی پلاک ۱۰

تلفن و فاکس : ۶۶۴۷۸۹۵۱-۶۶۴۷۸۹۵۲

مقدمه مولف:

کتابی مورد نیاز کتابخانه هر سازمان IT محور:

زیرساخت های فناوری اطلاعات بار بزرگی از خدمات IT را به دوش میکشند و به نوعی نقش تعیین کننده ای در پیشرفت و توسعه سازمان دارند. تمامی سرویس ها فضای سایبری در صورتی موفق خواهند بود که بر روی زیرساختی قابل اعتماد و پایدار بنا شده باشند. زیرساخت های فناوری اطلاعات چون برق برای کشور هستند که نبود یا خلل در آن، بسیاری از فعالیت های شرکتی و روزگار امروز را بی معنا میکند. انتخاب هادر حوزه زیرساخت های فناوری اطلاعات بایستی با دید باز و پس از بررسی اثرات مترتب و ابعاد آن انجام شوند. از سویی هر گاه فناوری زیرساخت ها استفاده شد بایستی با کلیه جنبه های آن بکار گرفته شوند. برای مثال استفاده از زیرساخت مجازی بدون در نظر گرفتن امنیت مورد نیاز، باعث شده است علی رغم مزایای فراوان این زیرساخت، برخی از سروس دهندگان تلاش کنند که به سرر های فیزیکی مهاجرت کند!! که تعجب بر انگیز است ولی در نظر نگرفتن پیاده سازی زیرساخت مجازی با تمامی خصوصیات و ملزومات آن، مالک سرویس را نسبت به آن بی اعتماد کرده است.

مثالی دیگر از این دست را میتوان اتخاذ فناوری های SDN (برای نمونه NSX) نام برد. تا زمانی که سازمان ارزیابی درستی از نقاط قوت و ضعف این فناوری ندارد و آنرا با رقبا مقایسه نکرده است نمیتواند قدمی برای اجرای آن بردارد. بله درست است NSX در مقوله امنیت بسیار خوب عمل میکند اما اثرات نامطلوب آن در صورت استفاده نابجا و نابهنگام بسیار خطرناک است و میتواند برخی نفوذ های امنیتی را موجب شود که هیچ گاه قابل کشف نباشند. در خصوص امنیت vSphere نبایستی دیدگاهمان جهت گیری شده به پیاده سازی NSX باشد چرا که محل اعرایی از NSX برای امن سازی در این خصوص وجود ندارد. همانطور که شرکت معظم VMware مستند قابل توجهی برای امن سازی این زیرساخت بدون توجه به NSX داده است دیده میشود امن سازی vSphere جدای مقوله NSX است. تا زمانی که زیرساخت امن نداشته باشید و طراحی آن بصورت امن انجام نشده باشد امکان مقابله با بدخواهان و هکر ها و اصولا کشف نفوذ و تلاشهای کارشناسان SOC هم بی معنا است. طراحی

زیرساخت امن نیازمند دید همه جانبه و عمیق در طراحی زیرساخت، فراهم آوری طرح شبکه قابل دفاع، با دید بالا است.

نکته آخر که باید یادآور شد آن است که امن سازی زیرساخت مجازی یا هر زیرساختی برخلاف تصور متخصصان معمول امنیت، با برآورده کردن خواست های یکسری چک لیست های مقاوم سازی حاصل نمیشود. چک لیست ها برای کنترل تنظیمات، بصورت امن هستن ولی اگر ما کلا از پایه امنیت را در vSphere در نظر نگرفته ایم نایبستی برای امنیت به Hardening اکتفا کنیم. بنا بر این اصل و مشاهده این خلاء امنیتی بزرگ در کشور و برای کمک به امنیت زیرساخت های مهم کشور و ارتقای دانش این مرز و بوم و سازمانها تصمیم گرفته شد کتابی در حوزه امنیت vSphere توسط گروه آموزشی پژوهشی روزبه (در راستای رسالت تاسیس آن به رهبری تحریردرآید.

در ترجمه کتاب معماری امن شده است از واژگان فارسی استفاده شود و همانگونه که میدانیم این موضوع ممکن است در بعضی موارد درک معنا را مشکل کند. لذا سعی شده است در مواقعی که جملات غامض شده اند یا از نویس موضوع برطرف شده است یا به ناچار از واژه یا واژه های انگلیسی عینا استفاده شده است.

نکته مهم در این بین آن است که با توجه به سطح بالای مفاهیم این مستند لازم است پیاده کننده آن چند نکته را مد نظر داشته باشد

۱. خود او از دانش امنیتی پایه در حد SSCP برخوردار باشد. با امور را با کمک به همراه با تخصص امنیت پیش ببرد
 ۲. تسلط نسبی به کلیه مقولات مجازی سازی مهم به نظر میرسد چرا که در اطلاعات دانشی فیما بین امنیت و خود موضوع نیازمند سطح دانش و تجربه در حد مناسبی است تا نتیجه مناسبی حاصل گردد.
- شایان ذکر است گروه آموزشی پژوهشی روزبه و شرکت امن گستران روزبه با در اختیار داشتن کارشناسان مسلط در حوزه مجازی سازی و امنیت، آماده ارائه خدمات کامل در این حوزه است. ضمناً در صورت نیاز به آموزش امن سازی vSphere و سایر محصولات VMware و دوره های تخصصی امنیت اطلاعات میتوانید با آکادمی آموزش روزبه در آدرس های ذیل تماس حاصل نمایید.

با توجه به وسعت استفاده از vSphere وجود این کتاب در کتابخانه هر سازمان و رجوع مکرر به آن اجباری مینماید. در این میان سعی داریم با همت دلسوزان این مرز و بوم در کاری مشترک، تلاشهایی برای ارتقای امنیت زیرساخت مجازی کشور برداشته شود در همین

رابطه سایت www.VMwaresecurity.ir برای ای نشر و اشتراک دانش در حوزه امنیت محصولات VMware به همراه فروم های لازم ایجاد میگردد.

لازم است از دقت و پیگیری در خور توجه سرکار خانم فرزانه واشقانی فراهانی برای ارایه بهینه این کتاب ، حمایت های جناب آقای ترک تبریزی مدیر امور فناوری اطلاعات بانک ملت در راستای پیاده سازی سیاستها و طرح های امنیتی در آن بانک، راهنمایی های جناب آقایان مهرداد توکلی و نوید برادران اساتید مجازی سازی، و پیگیری های جناب آقای محمد حمایتی عدل در خصوص چاپ بهینه کتاب قدردانی گردد. ضمناً تشکر فراوان خدمت جناب آقای اکبری شمیرانی مدیرکل امنیت بانک ملت تقدیم میگردد چراکه اراده راسخ ایشان در پیاده سازی امنیت بصورت علمی و پیگیر، راهکارهای اجرایی و اصولاً تعهد ایشان به امنیت (Management Commitment)، مثال زدنی است. ضمناً در صورت وجود نظر در خصوص کتاب یا وجود اشکال در آن، صمیمانه خواهشمند است با مدیر کانال تلگرامی گروه منعکس شود.

روزبه نوروزی

CISSP, PMP

مدیر و مؤسس گروه آموزشی پژوهشی روزبه

مشاوره و آموزش فناوری و امنیت اطلاعات

www.roozbehgroup.com

راههای ارتباطی

https://t.me/roozbeh_learning آدرس کانال تلگرامی آموزش

www.Roozbeh.Academy

آدرس وبسایت آکادمی آموزش روزبه، مجری تخصصی دوره های امنیت اطلاعات

www.CISSP-Iran.com نقطه ارتباطی شما با مدرک عالی امنیت اطلاعات

www.vmwaresecurity.ir آموزش و پژوهش در خصوص مجازی سازی

فهرست مطالب

فصل اول: امنیت اطلاعات و فضای سایبری امروزه

- ۳..... امنیت اطلاعات و فضای سایبری امروزه
- ۴..... مدل جامعیت، محرمانگی، در دسترس بودن
- ۴..... آشنایی با برخی موضوعات مهم در امنیت اطلاعات
- ۷..... نقش زیرساخت مجازی در فناوری اطلاعات
- ۸..... مجازی سازی چگونه به کسب و کار کمک می نماید ؟
- ۸..... مروری بر اصطلاحات مجازی سازی
- ۹..... در مجازی سازی باید چه چیزی را بسنجیم؟
- ۹..... ۱- آشنایی با vSphere
- ۹..... آشنایی با سرویس های زیرساختی
- ۱۰..... vCenter چیست؟
- ۱۰..... ۲- درباره امنیت vsphere
- ۱۲..... مستندات مرتبطی که پیشنهاد می گردد مطالعه شوند

فصل دوم: امنیت در محیط vsphere

- ۱۵..... امنیت در محیط vsphere
- ۱۵..... امن سازی Hypervisor ESXi
- ۱۷..... خودکار سازی مدیریت میزبان ESXi
- ۱۸..... امن سازی همه ماشین های میزبان vcenter

۱۹.....	پیگر بندی vcenter با تعیین هویت یکباره.....
۲۰.....	امن سازی ماشین های مجازی.....
۲۱.....	حفاظت از لایه شبکه مجازی.....
۲۳.....	خط مشی های امنیت شبکه در سازمان تان را در نظر بگیرید.....
۲۴.....	اتصالات امر به ذخیره سازی مجازی.....
۲۵.....	رمز های عبور در محیط vsphere شما.....

فصل سوم: مجوزها در vsphere و وظایف مدیریت کاربر

۳۱.....	مجوزها در vShere و وظایف مدیر کاربر.....
۳۱.....	به روش امنیت و منابع در این زمینه.....
۳۲.....	درک تخصیص مجوز در vsphere.....
۳۳.....	مفهوم مدل مجوز در سرور vcenter.....
۳۵.....	وراثت سلسله مراتبی مجوزها.....
۳۷.....	تنظیمات مجوز چندگانه.....
۴۱.....	کاربران و گروه ها.....
۴۲.....	اضافه کردن یک مجوز به فهرست اشیا.....
۴۴.....	تغییر تنظیمات اعتبارسنجی کاربر.....
۴۵.....	مجوزهای جهانی.....
۴۸.....	مجوزهای جهانی مکمل مجوزهای برجسب شی.....
۴۹.....	استفاده از نقش ها برای اختصاص امتیازات.....
۵۰.....	نقش های سفارشی در سرور vcenter و ESXi.....

۵۱.....	نقش‌های سیستم سرور vcenter.....
۵۲.....	نقش مدیر.....
۵۲.....	نقش مدیر بدون رمزنگاری.....
۵۳.....	ایجاد یک نقش سفارشی.....
۱۲۰.....	ویرایش یک نقش.....
۵۵.....	به روش‌ها برای نقش‌ها و مجوزها.....
۵۶.....	امتیازات مورد نیاز برای وظایف متداول.....

فصل چهارم: امن‌سازی میزبان‌های ESXi

۶۳.....	امن‌سازی میزبان‌های ESXi.....
۸۹.....	مشاهده جزئیات بیشتر برای یک میزبان ESXi.....
۹۰.....	تجدید یا تازه کردن گواهینامه‌های ESXi.....
۹۰.....	تغییر حالت گواهینامه.....
۹۱.....	جایگزینی گواهینامه‌های ESXi SSL و کلیدها.....
۹۷.....	استفاده از گواهینامه‌های سفارشی با گسترش خودکار.....
۹۸.....	بازیابی گواهینامه ESXi و پوشه‌های کلید.....
۱۰۰.....	سفارشی‌سازی میزبان‌ها با پروفایل‌های امن.....
۱۰۰.....	پیکربندی دیوار آتش ESXi.....
۱۱۰.....	سفارشی‌سازی سرویس‌های ESXi با پروفایل‌های امنیتی.....
۱۱۲.....	فعال و غیرفعال کردن یک سرویس در پروفایل امنیتی.....
۱۱۳.....	حالت Lockdown.....

- ۱۲۰..... مدیریت سطوح پذیرش میزبان‌ها و VIB‌ها
- ۱۲۲..... تخصیص حقوق به میزبان‌های ESXi
- ۱۲۲..... تخصیص مجوز به میزبان‌های ESXi که توسط سرور vCenter مدیریت می‌شوند
- ۱۲۲..... تخصیص مجوز به میزبان‌های Standalone ESXi
- ۱۲۳..... حقوق کاربر ریشه
- ۱۲۴..... حقوق vpxuser
- ۱۲۴..... امتیازات کاربر dcui
- ۱۲۵..... استفاده از اکتیو دایرکتوری برای مدیریت کاربران ESXi
- ۱۲۵..... پیکربندی یک میزبان برای استفاده از اکتیو دایرکتوری
- ۱۲۶..... اضافه کردن یک میزبان به دامنه سرور دایرکتوری
- ۱۲۷..... مشاهده تنظیمات سرویس دایرکتوری
- ۱۲۷..... استفاده از پروکسی احراز هویت vSphere
- ۱۲۹..... اضافه کردن یک دامنه به پروکسی احراز هویت vSphere با vSphere Web Client
- ۱۳۰..... اضافه کردن یک دامنه به پروکسی احراز هویت vSphere با دستورات camconfig
- ۱۳۱..... اضافه کردن یک میزبان به یک دامنه با استفاده از پروکسی احراز هویت vSphere
- ۱۳۲..... فعال کردن احراز هویت کاربر برای پروکسی احراز هویت vSphere
- ۱۳۴..... تولید یک گواهینامه جدید برای پروکسی احراز هویت vSphere
- ۱۳۵..... پروکسی احراز هویت vSphere را برای استفاده از گواهینامه‌های سفارشی تنظیم کنید
- ۱۳۷..... پیکربندی کارت هوشمند احراز هویت برای ESXi
- ۱۳۸..... فعال کردن احراز هویت با کارت هوشمند

۱۳۹.....	غیرفعال کردن احراز هویت کارت هوشمند
۱۳۹.....	احراز هویت با نام کاربری و رمز عبور در مواقعی که مشکلات ارتباطی رخ می‌دهد
۱۴۰.....	استفاده از کارت هوشمند برای احراز هویت در حالت Lockdown
۱۴۰.....	استفاده از ESXi Shell
۱۴۱.....	استفاده از vSphere Web Client برای فعال کردن دسترسی به ESXi Shell
۱۴۲.....	ایجاد یک زمانبندی برای در دسترس‌پذیری ESXi Shell در vSphere Web Client
۱۴۳.....	ایجاد یک زمانبندی برای جلسات ESXi Shell ایده‌آل در vSphere Web Client
۱۴۳.....	استفاده از کنسول مستقیم رابط کاربری (DCUI) برای فعال کردن دسترسی به ESXi Shell
۱۴۴.....	ایجاد یک زمانبندی برای در دسترس‌پذیری ESXi Shell در کنسول مستقیم رابط کاربری
۱۴۵.....	ایجاد یک زمانبندی برای جلسات ESXi Shell ایده‌آل
۱۴۵.....	ورود به ESXi Shell برای عیب‌یابی
۱۴۶.....	UEFI Secure Boot برای میزبان‌های ESXi
۱۴۶.....	مرور بر UEFI Secure Boot
۱۴۷.....	عیب‌یابی UEFI Secure Boot
۱۴۷.....	اجرای اسکریپت اعتبارسنجی بوت امن روی یک میزبان ESXi با قابلیت‌ها اضافه شده
۱۴۹.....	ESXi Log Files
۱۴۹.....	پیگیری syslog روی میزبان‌های ESXi
۱۵۰.....	مکان‌های ESXi Log File
۱۵۱.....	امن‌سازی ترافیک Log تحمل خطا

فصل پنجم: امن سازی سیستم های سرور vCenter

۱۵۵.....	امن سازی سیستم های سرور vCenter
۱۵۵.....	به روش های امنیت سرور vCenter
۱۵۵.....	به روش های کنترل دسترسی سرور vCenter
۱۵۸.....	از میزبان با سیستم عامل ویندوز سرور vcenter محافظت کنید.
۱۵۹.....	ارتباط شبکه سرور v center را محدود کنید.
۱۶۲.....	به روش های امنیت vcenter server Applia
۱۶۳.....	نیازمندی های رمز سرور Vcenter و رفتار lock out
۱۶۴.....	بررسی کردن اثر انگشت ها برای احراز هویت میزبان های قدیمی ESXI
۱۶۵.....	اعتبار گواهینامه SSL را از طریق چه پوشه شبکه که فعال است بررسی کنید
۱۶۵.....	پورت های مورد نیاز برای سرور Vcenter و کنترل کننده های سرویس های پلتفرم
۱۷۱.....	پورت های TCP و UDP اضافی سرور Vcenter

فصل ششم: امن سازی ماشین های مجازی

۱۷۷.....	امن سازی ماشین های مجازی
۱۷۷.....	فعال و غیرفعال کردن بوت امن برای یک ماشین مجازی
۱۷۹.....	۲- محدود کردن پیام های اطلاعاتی از ماشین های مجازی به فایل های VMAX
۱۷۹.....	۳- جلوگیری از shrinking دیسک مجازی
۱۸۲.....	استفاده از کنسول ماشین مجازی را کاهش دهید
۱۸۳.....	جلوگیری از ماشین های مجازی در تصاحب منابع

- ۱۸۴..... غیرفعال کردن کارکردهای غیرضروری درون ماشین‌های مجازی
- ۱۸۴..... حذف تجهیزات سخت‌افزاری غیرضروری
- ۱۸۵..... غیرفعال کردن ویژگی‌های نمایشی بدون استفاده
- ۱۸۶..... ویژگی‌های نهان را غیرفعال کنید
- ۱۸۷..... غیرفعال کردن انتقال‌های پوشه HGFS
- ۱۸۷..... غیرفعال کردن عملیات‌های COPY و PASTE بین سیستم عامل مهمان و کنسول از راه دور
- ۱۸۸..... محدود کردن اسنای داده‌ی حساسی که در clipboard کپی شده است

فصل هفتم: رمزگذاری ماشین مجازی

- ۱۹۵..... رمزگذاری ماشین مجازی
- ۱۹۵..... چگونه رمزگذاری ماشین مجازی vSphere از محیط شما محافظت می‌کند
- ۱۹۶..... چه کلیدهایی استفاده می‌شوند
- ۱۹۷..... چه چیزهایی رمزگذاری می‌شود؟
- ۱۹۷..... چه چیزی رمز شده نمی‌باشد
- ۱۹۸..... چه کسی می‌تواند عملیات رمزگذاری را انجام دهد
- ۱۹۸..... من چگونه می‌توانم عملیات‌های رمزنگاری را انجام دهم
- ۱۹۸..... اجزای رمزگذاری ماشین مجازی vSphere
- ۱۹۸..... سرور مدیریت کلید
- ۱۹۹..... سرور vCenter
- ۱۹۹..... میزبان‌های ESXi
- ۲۰۰..... جریان فرآیند رمزگذاری

۲۰۱.....	رمزگذاری دیسک مجازی
۲۰۳.....	پیش‌نیازها و امتیازات مورد نیاز برای وظایف رمزگذاری
۲۰۳.....	نقش‌ها و امتیازات رمزگذاری
۲۰۳.....	حالت رمزگذاری میزبان
۲۰۵.....	نیازمندی‌های فضای دیسک
۲۰۵.....	انجام vMotion بصورت رمزنگاری شده
۲۰۵.....	چه چیزی رمزنگاری می‌شود
۲۰۵.....	حالت‌های vSphere Motion رمز شده
۲۰۶.....	بهره‌ش‌های رمزنگاری، مشکلات و راهکارها
۲۰۶.....	به روش‌های رمزگذاری ماشین مجازی
۲۰۹.....	مشکلات رمزنگاری ماشین‌های مجازی

فصل هشتم: استفاده از رمزگذاری در محیط vSphere

۲۱۶.....	استفاده از رمزگذاری در محیط vSphere
۲۱۶.....	راه‌اندازی مدیریت کلید Server Cluster از رمزگذاری در محیط vSphere
۲۱۶.....	افزودن یک KMS به سرور vCenter
۲۱۷.....	استفاده از گزینه Root CA Certificate برای ایجاد یک ارتباط مطمئن
۲۱۸.....	استفاده از گزینه گواهی‌نامه برای ایجاد یک ارتباط مطمئن
۲۱۸.....	استفاده از گزینه درخواست امضای گواهی‌نامه جدید برای ایجاد یک ارتباط مطمئن
۲۱۹.....	از گزینه بارگذاری کلید خصوصی و گواهی‌نامه برای ایجاد یک ارتباط مطمئن استفاده کنید:
۲۲۴.....	ایجاد ماشین مجازی رمز شده:

۲۲۷.....	رمزگشایی ماشین مجازی یا دیسک مجازی رمزگذاری شده:
۲۲۹.....	سیاست رمزگذاری را برای دیسک‌های مجازی تغییر دهید:
۲۲۹.....	حل مشکل کلیدهای گم شده یا غیرقابل دسترس:
۲۳۱.....	رمزگذاری ماشین مجازی vSphere و Core Dumps:
۲۳۱.....	Core Dump ها در میزبان‌های ESXi:
۲۳۲.....	core dump و بسته‌های VM-Support:
۲۳۲.....	core dump در سیستم‌های سرور vCenter:
۲۳۲.....	جمع‌آوری بسته VM-Support برای میزبان ESXi که از رمزگذاری استفاده می‌کند:
۲۳۴.....	باز کردن یا رمزگذاری مجدد Core Dump رمزگذاری شده:

فصل نهم: امن سازی شبکه vSphere

۲۳۹.....	امن سازی شبکه vSphere:
۲۳۹.....	معرفی امنیت شبکه vSphere
۲۳۹.....	دیوارهای آتش:
۲۴۰.....	قطعه قطعه سازی (ناحیه بندی):
۲۴۱.....	از دسترسی‌های غیرمجاز جلوگیری کنید:
۲۴۱.....	امن سازی شبکه با دیوارهای آتش:
۲۴۲.....	دیوارهای آتش برای پیکربندی با سرور vCenter:
۲۴۳.....	ارتباط با سرور vCenter از طریق یک دیواره آتش:
۲۴۴.....	ارتباط با میزبان‌های ESXi از طریق دیوارهای آتش:
۲۴۴.....	دیوارهای آتش برای پیکربندی‌های محیط‌های بدون سرور vCenter:

۲۴۵	وصل شدن به کنسول ماشین مجازی از طریق یک دیواره آتش:
۲۴۶	امن سازی سویچ فیزیکی
۲۴۷	امن سازی پورت های سویچ استاندارد با سیاست های امنیتی
۲۴۷	امن سازی سویچ های استاندارد vSphere
۲۵۰	محافظت از سویچ استاندارد و VLAN ها
۲۵۲	امن سازی سویچ های توزیع شده vSphere و گروه های توزیع شده پورت
۲۵۴	امن سازی ماشین های مجازی با استفاده از VLAN ها
۲۵۵	ملاحظات امنیتی برای VLAN ها
۲۵۵	امن سازی VLAN ها
۲۵۶	ایجاد شبکه های چندگانه با یک میزبان ESX/ESXi
۲۵۹	پروتکل IPsec
۲۶۰	فهرست انجمن های امنیتی موجود:
۲۶۰	اضافه کردن یک انجمن امنیتی IPsec
۲۶۱	حذف کردن یک انجمن امنیتی IPsec
۲۶۲	فهرست سیاست های امنیتی IPsec های موجود:
۲۶۲	یک سیاست امنیتی IPsec ایجاد کنید
۲۶۳	حذف یک سیاست امنیتی IPsec
۲۶۴	اطمینان از پیکربندی مناسب NMP
۲۶۵	به روش امنیت شبکه vSphere
۲۶۵	توصیه های عمومی امنیت شبکه

فصل دهم: روش‌های اشتراکی بین چند عنصر از vSphere

۲۶۹.....	همگام‌سازی ساعت‌ها در شبکه vSphere
۲۶۹.....	همگام‌سازی ساعت ESXi با سرور زمان شبکه:
۲۷۰.....	پیکربندی تنظیمات همگام‌سازی زمان در تجهیزات سرور vCenter
۲۷۳.....	به روش‌های امنیت ذخیره‌سازی:
۲۷۴.....	امنکردن ذخیره‌سازهای iSCSI:
۲۷۴.....	امن‌سازی پت iSCSI SAN
۲۷۷.....	بررسی کنید که ارسال اطلاعات عملکرد میزبان به مهمان غیرفعال است:
۲۷۸.....	تنظیمات وقفه‌ها برای ESX Shell و vSphere Web Client:
۲۷۸.....	وقفه ESXi Shell:
۲۷۸.....	وقفه vSphere Web Client:

فصل یازدهم: مدیریت پروتکل TLS

۲۸۱.....	مدیریت پروتکل TLS:
۲۸۱.....	انجام تنظیمات با Configuration utility
۲۸۱.....	پورت‌هایی که در غیرفعال‌سازی نسخه‌های TLS نقش دارند
۲۸۲.....	Disabling TLS Versions in vSphere
۲۸۳.....	نصب ابزار تنظیم TLS
۲۸۴.....	انجام پشتیبان‌گیری بصورت دستی
۲۸۷.....	Disable TLS Versions on vCenter Server Systems

۲۸۷.....	Disable TLS Versions on ESXi Hosts
۲۸۹.....	Disable TLS Versions on Platform Services Controller systems
۲۹۰.....	Revert TLS Configuration Changes
۲۹۲.....	غیرفعال سازی نسخه TLS روی مدیر بروزرسانی vSphere

فصل دوازدهم: حقوق تعیین شده

۲۹۹.....	حقوق تعیین شده
۲۹۹.....	حقوق دسترسی ها
۳۰۰.....	توانمندی دیپلوی اتوماتیک پروفایل ایمیج
۳۰۱.....	امتیازات گواهینامه ها
۳۰۱.....	حقوق دسترسی کتابخانه محتوا
۳۰۴.....	حقوق انجام عملیات رمزگذاری
۳۰۶.....	امتیازات مرکز داده
۳۰۷.....	امتیازات Data Store
۳۰۸.....	امتیازات Datastore Cluster
۳۰۸.....	Distributed Switch Privileges
۳۰۹.....	ESXi Agent Manager Privileges
۳۰۹.....	Extension Privileges
۳۱۰.....	Folder Privileges
۳۱۱.....	Global Privileges
۳۱۲.....	Host CIM Privileges

٢١٢.....	:Host Configuration Privileges
٢١٤.....	:Host Inventory
٢١٥.....	:Host Local Operation Privileges
٢١٦.....	:Host vSphere Replication Privileges
٢١٦.....	:Host Profile Privileges
٢١٧.....	:Network Privileges
٢١٨.....	:Performance Privileges
٢٢١.....	:Permission Privileges
٢٢٢.....	:Profile-Driven Storage Privileges
٢٢٢.....	:Resource Privileges
٢٢٢.....	:Scheduled Task Privileges
٢٢٥.....	:Session Privileges
٢٢٦.....	:Storage Views Privileges
٢٢٨.....	:Task Privileges
٢٢٩.....	:Transfer Service Privileges
٢٣٠.....	:Virtual Machine Configuration Privileges
٢٣١.....	:Virtual Machine Guest Operations Privileges
٢٣٢.....	:vPpvt Group Privileges
٢٣٣.....	:vApp Privileges
٢٣٤.....	:vServices Privileges

۳۳۵.....	vSphere Tagging Privileges
----------	----------------------------

فصل سیزدهم: تغییرات نسخه ۶.۷ در حوزه امنیت

۳۳۹.....	تغییرات نسخه ۶.۷ در حوزه امنیت
۳۳۹.....	TPM2.0 برای ماشین‌های مجازی
۳۴۰.....	پشتیبانی از Microsoftvirtualization Based Security
۳۴۱.....	رابط کاربری دسته بندی شده
۳۴۲.....	ارسال لاگها به چندین مخزن مختلف
۳۴۲.....	در این نسخه تمام امور مربوط به تطابق با FIPS ۱۴۰-۲ است

منابع

۳۴۴.....	منابع
----------	-------