بسمه تعالی

بهترین تجربه‌های امنیتی ابرناظر ESXi (بخش اول)

فهرست مطالب

۱ مقدمه

VMware یکی از مشهورترین شرکت‌هایی است که در زمینه مجازی‌سازی به‌صورت گسترده فعالیت دارد، VMware ESXi مشهورترین محصول این شرکت در این زمینه است. VMware ESXi یک ابرناظر نوع ۱ است که برای استقرار و خدمت‌رسانی رایانه‌های مجازی ارائه شده‌است و بارزترین مشخصه آن نصب به صورت مستقیم بر روی سخت‌افزار است که دیگر نیازی به یک سیستم‌عامل رابط نمی‌باشد، و در سرعت کارکرد سیستم بسیار مؤثر است. همانند تمامی محصولات نرم‌افزاری و سیستم‌عامل‌ها، زمانی‌که ESXi با تنظیمات پیش‌فرض نصب می‌شود بسیاری از موارد امنیتی در نظر گرفته نمی‌شوند. از سوی دیگر امنیت میزبان‌های ESXi یکی از مهم‌ترین موارد امن‌سازی محیط مجازی است. اگر میزبان‌های مجازی امن نباشند، امن‌کردن سیستم‌عامل مهمان که از این میزبان‌ها استفاده می‌کنند، غیرممکن است. بنابراین به‌منظور اطمینان از صحت استقرار محیط vSphere و افزایش امنیت ESXi باید از بهترین تجربیات امنیتی ESXi پیروی کنید. در بخش‌های مختلف این گزارش بهترین تجربه‌های امنیتی ابرناظر ESXi نسخه‌ی ٦,٥ شرح داده می‌شود.

۲ بهترین تجربه‌های امنیتی

ساختار ابرناظر ESXi دارای تعدادی ویژگی امنیتی درونی از قبیل جداسازی CPU، جداسازی حافظه و جداسازی دستگاه می‌باشد. می‌توان ویژگی‌های دیگری از قبیل حالت قفل، جایگزینی گواهی‌نامه و احرازاصالت کارت هوشمند را به منظور افزایش امنیت محیط تنظیم کرد.

میزبان‌های ESXi توسط دیواره آتش محافظت می‌شوند. می‌توان پورت‌ها را برای ترافیک ورودی و خروجی موردنیاز باز کرد، اما دسترسی به سرویس‌ها و پورت‌ها را محدود کرد. با استفاده از حالت قفل ESXi و دسترسی محدود به ESXi Shell می‌توان محیط امن‌تری را ساخت. در بخش‌های مختلف گزارش این موارد شرح داده می‌شوند.

۲-۱ مدیریت گواهی‌نامه برای میزبان‌های ESXi

در vSphere 6.0 به بعد، مرجع صدور گواهی‌نامه VMware (VMCA) برای هر میزبان ESXi جدید یک گواهی‌نامه امضا شده اختصاص می‌دهد که VMCA به صورت پیش‌فرض مرجعیت گواهی‌نامه ریشه را برعهده دارد.

شما می‌توانید این گواهی‌نامه‌ها را از vSphere Web Client و با استفاده از vim.CertificateManager API در vSphere Web Services SDK مشاهده و مدیریت کنید.

زمانی که سرویس‌دهنده vCenter و ESXi با یکدیگر ارتباط برقرار می‌کنند از SSL برای کنترل تمام ترافیک استفاده می‌شود. در vSphere نسخه ٦ به بعد، حالت‌های زیر برای گواهی‌نامه‌های میزبان‌های ESXi پشتیبانی می‌شود.

- **VMware Certifcate Authority (پیش‌فرض)**: به صورت پیش‌فرض، VMware Certificate Authority به عنوان CA برای میزبان های ESXi در نظر گرفته خواهد شد. اما می‌توان آن را به عنوان یک CA ریشه یا CA میانی تنظیم نمود. در این حالت کاربر می‌تواند گواهی‌نامه‌ها را از طریق کنسول تحت وب مشاهده و مدیریت کند.
- **Custom Certifcate Authority**: اگر می‌خواهید از گواهی‌نامه‌های سفارشی که توسط شخص سوم یا CA سازمانی، امضا شده‌است، استفاده کنید، باید این حالت را انتخاب کنید. در این حالت کاربر بایستی گواهی‌نامه‌ها را خودش مدیریت کند و از طریق کنسول تحت وب vSphere قادر به مشاهده و مدیریت آنها نخواهد بود.
- **Thumbprint Mode**: نسخه vSphere 5.5 از این حالت استفاده می‌کند و برای سازگاری در vSphere 6.x نیز پشتیبانی می‌شود. در این حالت، vCenter Server بررسی می‌کند که گواهی‌نامه به‌درستی قالب‌بندی شده‌باشد، اما اعتبار گواهی‌نامه را بررسی نمی‌کند که موجب می‌شود حتی گواهی‌نامه‌های منقضی‌شده، پذیرش شوند.

  از این روش تنها زمانی استفاده کنید که مجبور هستید، یا به تعبیر دیگری از دو روش دیگر نمی‌توانید استفاده کنید، یا با آن‌ها به مشکلی برخورده‌اید که قابل رفع نمی‌باشد. برخی از سرویس‌های vCenter نسخه ٦ به بعد ممکن است در این حالت، به‌درستی کار نکنند.

به‌منظور مدیریت گواهی‌نامه میزبان‌های ESXi باید امتیاز Certificates.Manage Certificates را دارا باشید که این امتیاز را می‌توان از vSphere Web Client تنظیم کرد. در ادامه بهترین تجربه‌ها برای مدیریت گواهی‌نامه‌های میزبان‌های ESXi بیان می‌شوند.

۲-۱-۱ ارتقای میزبان و گواهی‌نامه‌ها

اگر میزبان‌های ESXi را به نسخه ESXi 6.0 یا بالاتر ارتقا دهید، گواهی‌نامه‌های خودامضا[۱] (thumbprint) با گواهی‌نامه‌های VMCA-signed جایگزین می‌شود. اگر میزبان ESXi از گواهی‌نامه‌های سفارشی استفاده کند، در فرآیند ارتقا این حالت حفظ خواهد شد، حتی اگر گواهی‌نامه‌ها منقضی شده باشند یا نامعتبر باشند.

۲-۱-۲ تنظیمات پیش‌فرض گواهی‌نامه‌های ESXi

زمانی که یک میزبان به سامانه vCenter Server اضافه شود، vCenter Server یک درخواست امضای گواهی‌نامه (CSR) را برای میزبان به VMCA ارسال می‌کند. اکثر مقادیر پیش‌فرض برای موقعیت‌های زیادی مناسب هستند، اما قسمت اطلاعات مرتبط با شرکت را می‌توان تغییر داد. می‌توان هر کدام از تنظیمات پیش‌فرض را با استفاده از vSphere Web Client تغییر داد.

جدول ۱ تنظیمات ESXi CSR

پارامتر	مقدار پیش‌فرض	گزینه‌های پیشرفته
اندازه کلید	۲۰۴۸	N.A
الگوریتم کلید	RSA	N.A
الگوریتم امضای گواهی‌نامه	sha256WithRSAEncryption	N.A
نام متداول	نام میزبان، اگر میزبان توسط host name خود به vCenter Server اضافه شده‌باشد. آدرس IP میزبان، اگر میزبان توسط آدرس IP خود به vCenter Server اضافه شده‌باشد.	N.A
کشور	آمریکا	vpxd.certmgmt.certs.cn.country

[۱] self-signed

vpxd.certmgmt.certs.cn.email	vmca@vmware.com	آدرس پست‌الکترونیکی
vpxd.certmgmt.certs.cn.localityName	Palo Alto	موقعیت (شهر)
vpxd.certmgmt.certs.cn.organizationalUnitName	VMware Engineering	نام واحد سازمانی
vpxd.certmgmt.certs.cn.organizationName	VMware	نام سازمان
vpxd.certmgmt.certs.cn.state	California	ایالت یا استان
vpxd.certmgmt.certs.cn.daysValid	۱۸۲۵	تعداد روزهایی که گواهی‌نامه معتبر است
vpxd.certmgmt.certs.cn.hardThreshold	۳۰ روز	آستانه سخت[۱] برای انقضای گواهی‌نامه که در هنگام وقوع این آستانه، vCenter Server هشدار قرمز را نمایش می‌دهد.
vpxd.certmgmt.certs.cn.pollIntervalDays	۵ روز	فواصل نظرسنجی[۲] بررسی اعتبار گواهی‌نامه vCenter Server
vpxd.certmgmt.certs.cn.softThreshold	۲٤۰ روز	آستانه نرم[۳] برای انقضای گواهی‌نامه که در هنگام وقوع این آستانه، vCenter Server رویدادی[٤] را نمایش می‌دهد.
vpxd.certmgmt.mode	پیش‌فرض vmca است. هم‌چنین می‌توان حالت thumbprint یا custom را انتخاب کرد.	حالت گواهی‌نامه‌ها

[۱] Hard threshold

[۲] Poll interval

[۳] Soft Threshold

[٤] Event

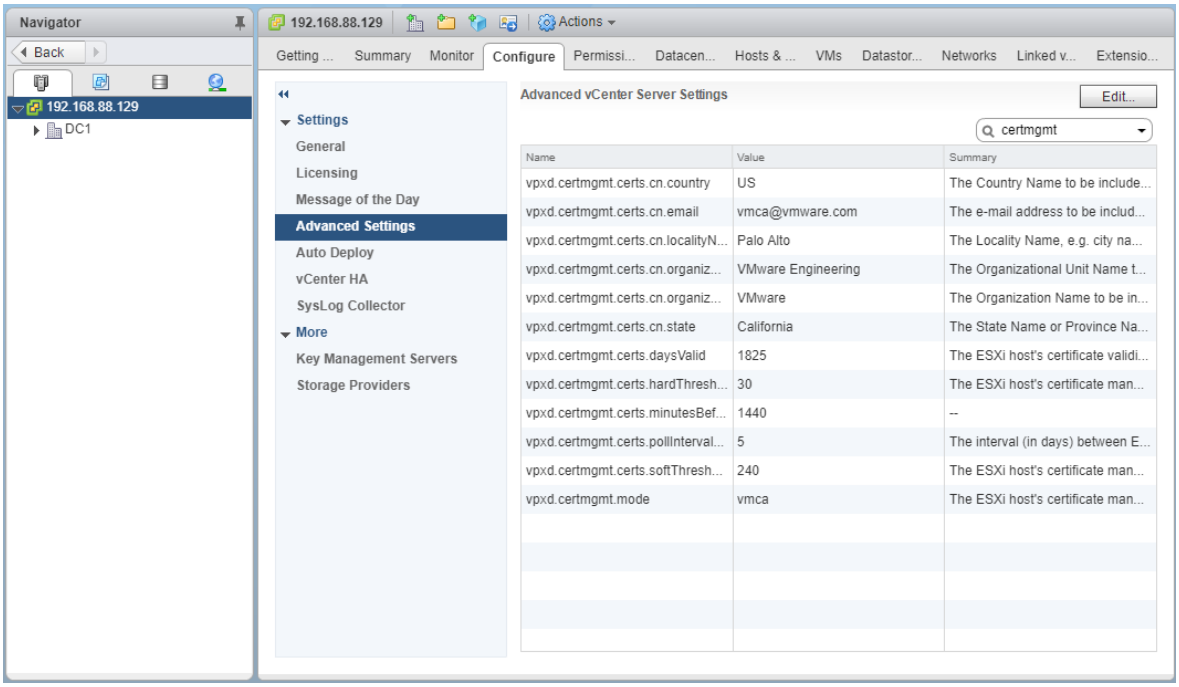
۲-۱-۲-۱ تغییر تنظیمات پیش‌فرض گواهی‌نامه‌ها

هنگامی که یک میزبان به سیستم سرویس‌دهنده vCenter اضافه می‌شود، سرویس‌دهنده vCenter یک درخواست امضای گواهی‌نامه (CSR) را برای میزبان به VMCA ارسال می‌کند. تنظیمات پیش‌فرض در CSR در جدول ۱ نشان داده شده‌است. می‌توان این تنظیمات را با استفاده از تنظیمات پیشرفته در سرویس‌دهنده vCenter در vSphere Web Client تغییر داد.

فرآیند:

۱. در vSphere Web Client، سرویس‌دهنده vCenterای که میزبان‌ها را مدیریت می‌کند، انتخاب کنید.
۲. گزینه Configure و پس از آن Advanced Settings را انتخاب کنید.
۳. در قسمت Filter box عبارت certmgmt را وارد کنید تا پارامترهای مدیریت گواهی‌نامه نشان داده شوند.
٤. مقادیر پارامترهای موردنظر خود را مطابق با سیاست‌های شرکت تغییر داده و در پایان OK را کلیک نمایید.

پس از انجام این فرآیند، زمانی که یک میزبان به vCenter Server اضافه شود، تنظیمات جدید برای CSRای که vCenter Server به VMCA ارسال می‌کند، استفاده می‌شود.



شکل ۱ تغییر تنظیمات پیش‌فرض گواهی‌نامه‌ها

توجه: تنظیمات انجام‌شده تنها بر روی گواهی‌نامه‌های جدید، اعمال می‌شود. اگر می‌خواهید گواهی‌نامه‌های میزبان‌هایی را که قبلا به vCenter Server اضافه شده‌اند را تغییر دهید، باید میزبان‌ها را قطع و مجدداً متصل کنید یا گواهی‌نامه‌ها را بازسازی کنید.

۲-۱-۳ مشاهده اطلاعات انقضای گواهی‌نامه برای چندین میزبان ESXi

اگر از ESXi نسخه ٦ به بعد استفاده می‌کنید، می‌توانید وضعیت گواهی‌نامه‌های تمام میزبان‌هایی را که توسط سیستم سرویس‌دهنده vCenter مدیریت می‌شوند را مشاهده کنید. اطلاعات نمایش داده شده به شما کمک می‌کند تا گواهی‌نامه‌هایی را که به زودی منقضی می‌شوند را شناسایی کنید.

شما می‌توانید اطلاعات وضعیت گواهی‌نامه‌ها برای میزبان‌هایی که از VMCA mode و هم‌چنین میزبان‌هایی که از custom mode استفاده می‌کنند، را در vSphere Web Client مشاهده کنید. توجه داشته باشید که نمی‌توانید وضعیت گواهی‌نامه‌های میزبان‌ها در thumbprint mode را مشاهده کنید.

فرآیند:

۱. در vSphere Web Client، میزبان را جست‌وجو کنید.
به صورت پیش‌فرض حالت گواهی‌نامه میزبان نشان داده نمی‌شود.
۲. بر روی گزینه Name field راست کلیک کرده و Show/Hide Columns را انتخاب کنید.
۳. گزینه Certificate Valid To را انتخاب و OK را کلیک کنید.
اگر یک میزبان به سرویس‌دهنده vCenter اضافه شده باشد یا پس از یک قطع اتصال مجدداً متصل شود، سرویس‌دهنده vCenter گواهی‌نامه‌هایی که در وضعیت Expiring،Expired ، Expiring shortlyیا Expiration imminent هستند را renew می‌کند. اگر گواهی‌نامه کمتر از ۸ ماه valid باشد در وضعیت Expiring، کمتر از ۲ ماه valid باشد در وضعیت ،Expiring shortly و کمتر از یک ماه در وضعیت Expiration imminent قرار می‌گیرد.
٤. (اختیاری) گزینه‌های دیگر، در صورتی که علاقه‌ای به مشاهده اطلاعات آن‌ها ندارید، را از حالت انتخاب خارج کنید.

۲-۱-٤ مشاهده جزئیات گواهی‌نامه برای یک میزبان ESXi

برای ESXi نسخه ٦ به بعد که در VMCA mode یا custom mode هستند، می‌توانید جزئیات گواهی‌نامه را از طریق vSphere Web Client مشاهده کنید. اطلاعات مرتبط با گواهی‌نامه می‌تواند برای debugging مفید باشد.

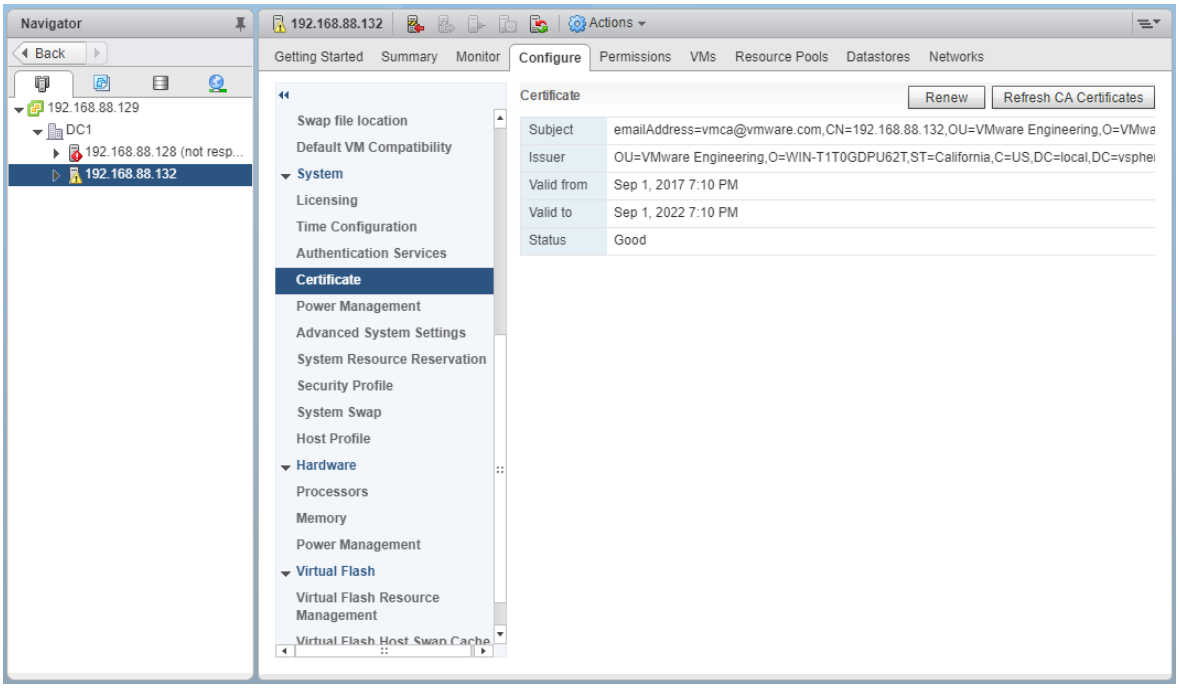
فرآیند:

۱. در vSphere Web Client، میزبان را جست‌وجو کنید.
۲. منوی Configure را انتخاب کنید.
۳. در بخش System گزینه Certificate را انتخاب کنید.

اطلاعات نمایش داده شده در جدول ۲ نشان داده شده است. این اطلاعات تنها در sigle-host قابل مشاهده است.

جدول ۲ اطلاعات مرتبط به گواهی‌نامه برای یک میزبان ESXi

فیلد	توصیف
Subject	Subject استفاده‌شده در مرحله تولید گواهی‌نامه.
Issuer	صادرکننده گواهی‌نامه.
Valid From	تاریخی که گواهی‌نامه تولید شده است.
Valid To	تاریخی که گواهی‌نامه منقضی می‌شود.
Status	وضعیت گواهی‌نامه در یکی از موارد زیر قرار دارد: Good: عملیات عادی Expiring: گواهی‌نامه به زودی منقضی می‌شود. Expiring shortly: ۸ ماه یا کمتر گواهی‌نامه منقضی می‌شود. (حالت پیش‌فرض). Expiration imminent: ۲ ماه یا کمتر گواهی‌نامه منقضی می‌شود. (حالت پیش‌فرض). Expired: گواهی‌نامه معتبر نیست، زیرا منقضی شده است.



شکل ۲ مشاهده جزئیات گواهی‌نامه برای یک میزبان ESXi

۲-۱-۵ بازسازی گواهی‌نامه‌های ESXi

اگر VMCA گواهی‌نامه‌ها را به میزبان‌های ESXi شما اختصاص داده است، شما می‌توانید این گواهی‌نامه‌ها را از vSphere Web Client بازسازی کنید. هم‌چنین می‌توانید تمامی گواهی‌نامه‌ها را از TRUSTED_ROOTS همراه با سرویس‌دهنده vCenter به‌روزرسانی کنید.

می‌توانید گواهی‌نامه‌ها را زمانی که منقضی شده‌اند، یا می‌خواهید گواهی‌نامه جدیدی را به یک میزبان اختصاص دهید یا دلایل دیگر، renew کنید. اگر گواهی‌نامه‌ها منقضی شده باشد، باید میزبان را ابتدا disconnect و مجدداً connect کنید.

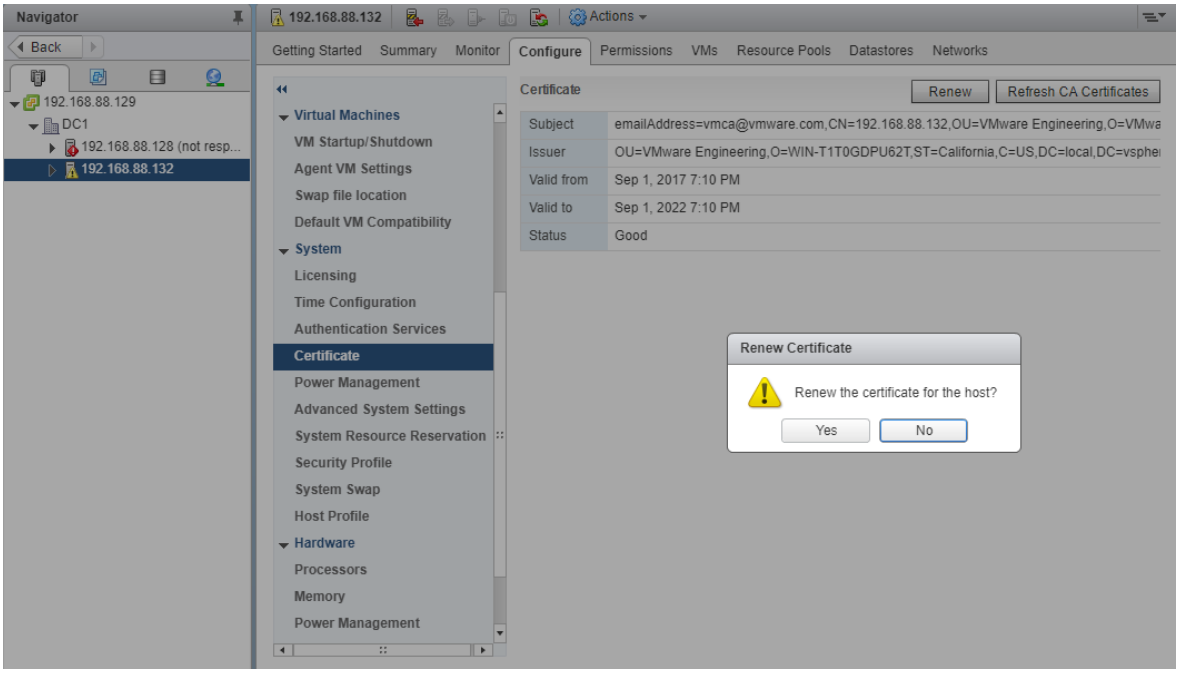
به صورت پیش‌فرض، سرویس‌دهنده vCenter گواهی‌نامه‌های یک میزبان با وضعیت Expired، Expiring immediately, یا Expiring را زمانی که میزبان به لیست اضافه شود یا مجدداً وصل شود، renew می‌کند.

فرآیند:

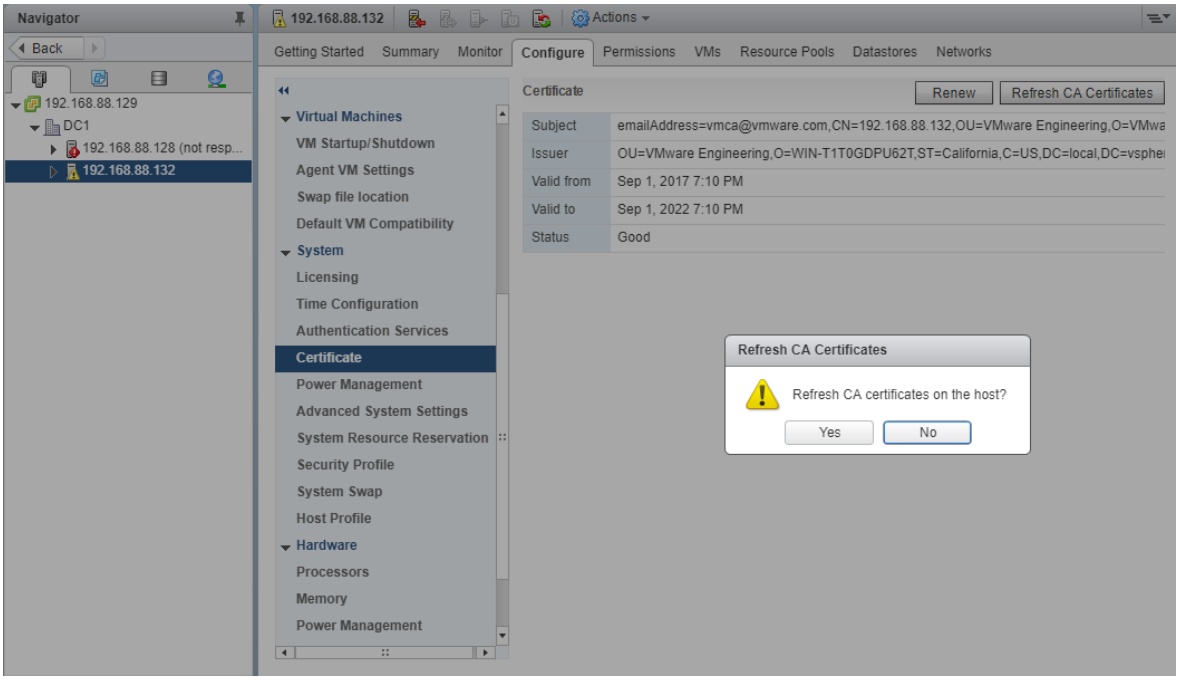
۱. در vSphere Web Client، میزبان را جست‌وجو کنید.
۲. منوی Configure را انتخاب کنید.
۳. در بخش System گزینه Certificate را انتخاب کنید.
٤. گزینه Renew یا Refresh CA Certificates را انتخاب کنید.

- Renew: یک گواهی‌نامه امضا شده تازه را برای میزبان از VMCA بازیابی می‌کند.
- Refresh CA Certificates: تمام گواهی نامه‌ها در محل TRUSTED_ROOTS در سرویس‌دهنده VECS را به میزبان push می‌کند.

۵. جهت تأیید گزینه OK را انتخاب کنید.



شکل ۳ بازسازی گواهی‌نامه‌های ESXi



شکل ٤ به‌روزرسانی گواهی‌نامه‌های ESXi

٦-١-٢ تغییر حالت گواهی‌نامه

در اکثر موارد استفاده از VMCA برای میزبان‌های ESXi در محیط‌تان، بهترین راه‌حل است. اگر در مواردی نیاز داشتید که از گواهی‌نامه‌های custom با root CA متفاوتی استفاده کنید، می‌توانید تنظیمات مربوطه در vCenter Server را به‌گونه‌ای انجام دهید که هنگامی که گواهی‌نامه‌ها را به‌روزرسانی می‌کنید، گواهی‌نامه‌های VMCA به‌صورت خودکار به میزبان‌ها اختصاص پیدا نکند. پس از انجام این تنظیمات، مدیریت گواهی‌نامه بر عهده کاربر خواهد بود.

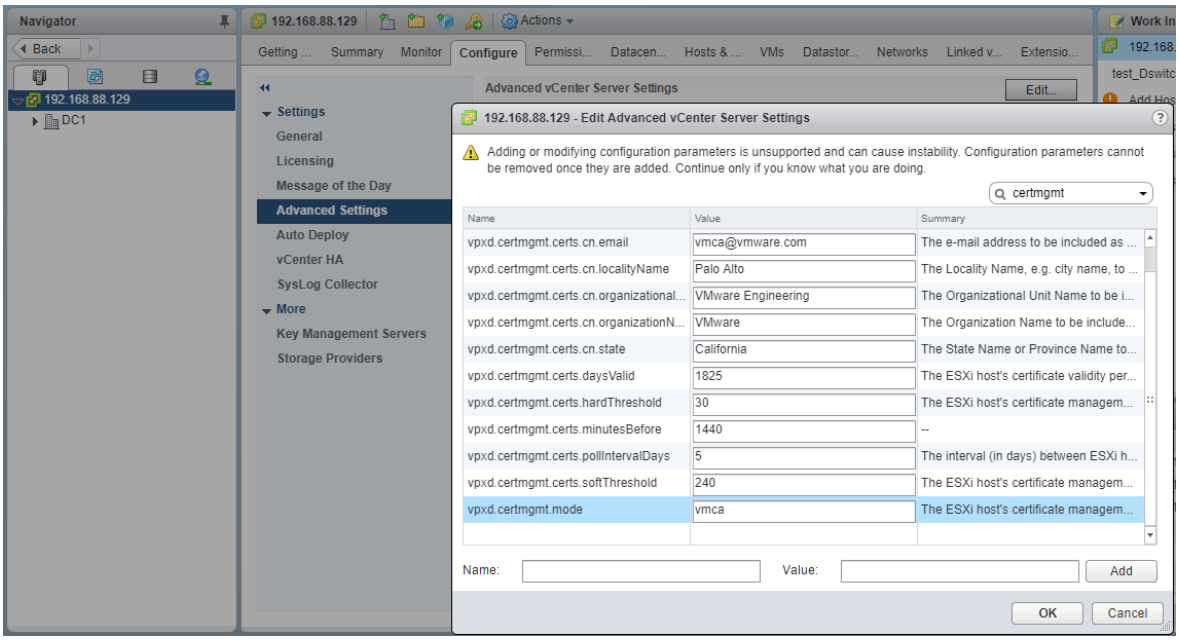
می‌توانید از بخش advanced settings در vCenter Server به‌منظور تغییر حالت گواهی‌نامه‌ها به حالت thumbprint یا حالت custom CA استفاده کنید.

فرآیند:

١. vCenter Server مربوطه که مدیریت میزبان‌ها را برعهده دارد را انتخاب کرده و گزینه Configure را کلیک کنید.
٢. گزینه Advanced را انتخاب کرده و پس از آن Edit را کلیک کنید.
٣. در قسمت Filter box، عبارت certmgmt را وارد کرده تا تنها کلیدهای مدیریت گواهی‌نامه نشان داده شوند.

٤. اگر می‌خواهید که خودتان مدیریت گواهی‌نامه‌های خود را انجام دهید، مقدار vpxd.certmgmt.mode را به custom تغییر دهید، و اما اگر می‌خواهید به‌صورت موقت از حالت thumbprint استفاده کنید، مقدار thumbprint را وارد کنید و در نهایت OK را کلیک کنید.

٥. سرویس vCenter Server را راه‌اندازی مجدد کنید.



شکل ٥ تغییر حالت گواهی‌نامه

۷-۱-۲ جایگزین‌کردن کلیدها و گواهی‌نامه‌های ESXi SSL

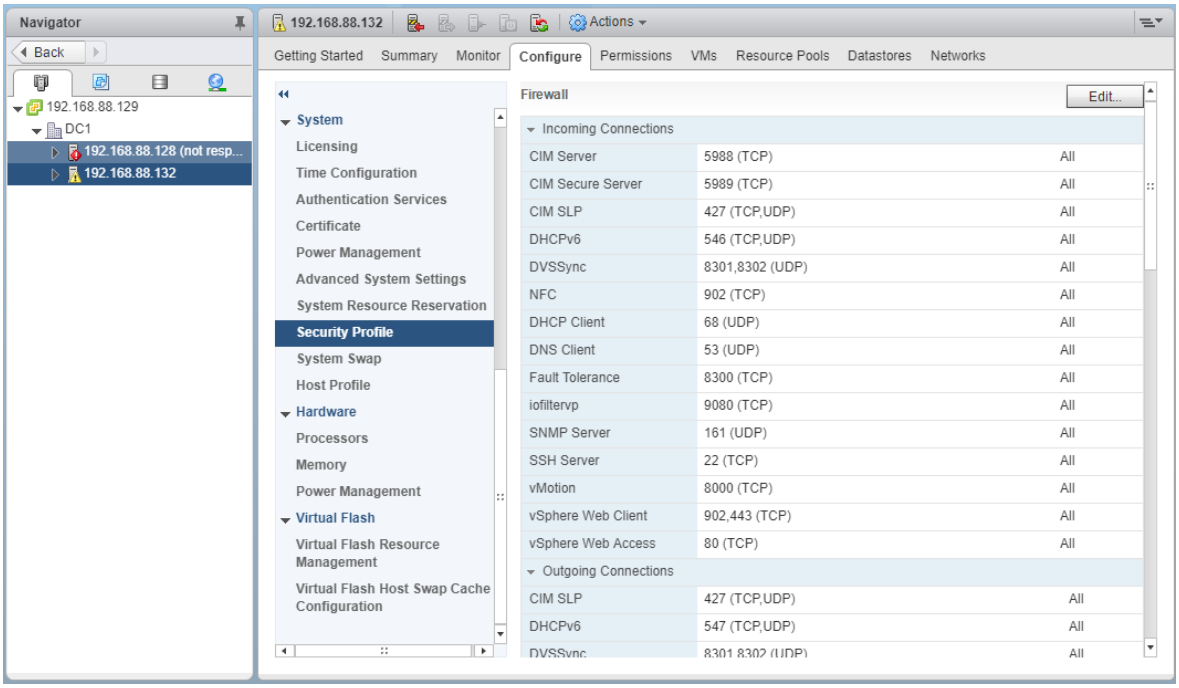
مطابق با سیاست امنیت شرکت شما، ممکن است نیاز داشته‌باشید تا گواهی‌نامه‌های ESXi SSL پیش‌فرض را با گواهی‌نامه‌های CA-signed شخص سوم برای هر میزبان، جایگزین کنید.

به‌صورت پیش‌فرض، اجزای vSphere از کلیدها و گواهی‌نامه‌های VMCA-signed که در طول فرآیند نصب تولید شده‌اند، استفاده می‌کنند. اگر به‌صورت تصادفی، گواهی‌نامه VMCA-signed حذف شود، میزبان از سیستم vCenter Server حذف می‌شود و باید دوباره اضافه گردد. هنگامی‌که میزبان اضافه می‌شود، vCenter Server گواهی‌نامه جدیدی را از VMCA درخواست می‌کند و به میزبان اختصاص می‌دهد.

بسته به سیاست شرکت، گواهی‌نامه‌های VMCA-signed را با گواهی‌نامه‌های commercial CA trusted CA یا organizational CA جایگزین کنید.

۲-۲ سفارشی‌سازی میزبان‌ها با Security Profile

شما می‌توانید تعداد زیادی از تنظیمات امنیتی مهم در میزبان‌تان را از طریق Security Profile که در vSphere Web Client در دسترس است، سفارشی سازی کنید. Security Profile به طور خاص برای مدیریت یک میزبان مفید است. اگر شما چندین میزبان را مدیریت می‌کنید، از CLIs یا SDKs و سفارشی‌سازی خودکار استفاده کنید.



شکل ٦ پروفایل امنیتی

۲-۳ تنظیمات دیواره آتش ESXi

دسترسی بی قید و شرط به سرویس‌هایی که روی یک میزبان ESXi اجرا می‌شوند می‌توانند یک میزبان را در معرض حملات بیرونی و دسترسی غیرمجاز قرار دهند. این خطر را به وسیله تنظیم دیواره آتش به گونه‌ای که تنها از شبکه‌های مجاز انجام گیرد، کاهش دهید.

ESXi دربرگیرنده‌ی یک دیواره آتش است که به صورت پیش‌فرض فعال است. در زمان نصب، دیواره آتش ESXi برای مسدود کردن ترافیک‌های ورودی و خروجی به جز ترافیک سرویس‌هایی که در Security Profile میزبان‌ها فعال شده‌اند، تنظیم شده است.

توجه: دیواره آتش اجازه ICMP ping و ارتباط با سرویس‌گیرنده‌های DHCP و DNS (فقط UDP) را می دهد.

شما می‌توانید پورت‌های دیواره آتش را به صورت زیر مدیریت کنید:

- از Security Profile برای هر میزبان در vSphere Web client استفاده کنید.
- از دستورات ESCLI از command line یا اسکریپت‌ها استفاده کنید.
- در صورتی که پورتی را که می‌خواهید باز کنید در Security Profile نباشد، از custom VIB استفاده کنید.

۲-۳-۱ مدیریت تنظیمات دیواره آتش ESXi

شما می‌توانید ورودی و خروجی ارتباطات دیواره آتش برای یک سرویس یا یک عامل مدیریتی را از vSphere Web Client یا command line تنظیم کنید.

توجه: اگر سرویس‌های مختلف قوانین پورت متداخل دارند، فعال‌کردن یک سرویس ممکن است دیگر سرویس‌ها را نیز فعال کند. شما باید به طور خاص تعیین کنید که چه آدرس‌های IP اجازه دسترسی به هر کدام از سرویس‌ها روی میزبان را دارند تا از این مسأله جلوگیری کنید.

فرآیند:

۱. میزبان موردنظر را در vSphere Web Client انتخاب کنید.
۲. بر روی گزینه Configure کلیک کنید.
۳. Security Profile را انتخاب کنید.

vSphere Web Client فهرستی از ارتباطات ورودی و خروجی فعال متناظر با پورت‌های دیواره آتش را نشان می‌دهد.

٤. در بخش Firewall گزینه Edit را انتخاب کنید.
۵. برای فعال‌سازی مجموعه قوانین آن را انتخاب کنید.

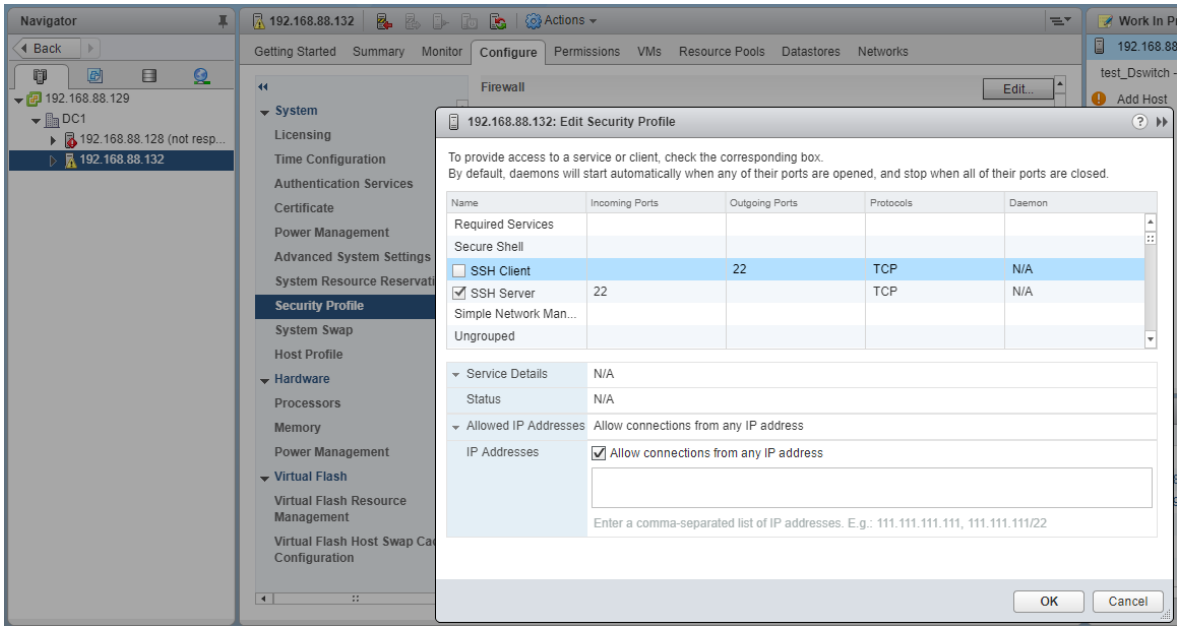
- Incoming Ports and Outgoing Ports: پورت‌هایی که vSphere Web Client برای سرویس باز می‌کند.
- Protocol: پروتکلی که سرویس استفاده می‌کند.
- Daemon: وضعیت Daemonهای همراه با سرویس.

۶. برای برخی از سرویس‌ها، شما می‌توانید جزئیات سرویس را نیز مدیریت کنید.

- از دکمه‌های Stop،Start یا Restart برای تغییر حالت موقت یک سرویس استفاده کنید.
- بخش Startup Policy را برای شروع به کار سرویس با میزبان یا با استفاده از پورت، تغییر دهید.

۷. برای بعضی از سرویس‌ها شما می‌توانید به طور صریح تعیین کنید که چه آدرس‌های IP از چه ارتباطاتی مجاز هستند.

۸. OK را انتخاب کنید.



شکل ۷ تنظیمات دیواره آتش ESXi

۲-۳-۲ اضافه‌کردن آدرس‌های IP مجاز برای یک میزبان ESXi

به صورت پیش‌فرض دیواره آتش برای تمام سرویس‌ها اجازه دسترسی به تمام آدرس‌های IP را می‌دهد. برای محدود کردن ترافیک، هر سرویس را تغییر دهید تا تنها ترافیک از مجموعه مدیریتی شما مجاز باشد. شما هم چنین می‌توانید سرویس‌هایی را که در محیط شما استفاده نمی‌شوند را ازحالت انتخاب خارج کنید.

شما می‌توانید از vSphere Web Client، vCLI یا PowerCLI برای بروزرسانی فهرست آدرس‌های IP مجاز برای یک سرویس استفاده کنید. به صورت پیش‌فرض تمام آدرس‌های IP برای یک سرویس مجاز هستند.

فرآیند:

۱. میزبان موردنظر را در Web Clientانتخاب کنید.
۲. بر روی گزینه Configure کلیک کنید.
۳. گزینه Security Profile را انتخاب کنید.
٤. در بخش Firewall گزینه Edit را کلیک کرده و از فهرست، سرویس مورد نظر را انتخاب کنید.
٥. در بخش Allowed IP Addresses گزینه Allow connections from any IP address را از حالت انتخاب خارج کنید و آدرس‌های IP شبکه‌هایی که مجاز به ارتباط با میزبان هستند را وارد کنید.

آدرس‌های IP را با ویرگول از یکدیگر جدا کنید. می‌توانید از قالب‌های زیر استفاده کنید:

- 192.168.0.0/24
- 192.168.1.2, 2001::1/64
- fd3e:29a6:0a81:e478::/64

٦. گزینه OK را انتخاب کنید.

۲-۳-۳ دستورات ESXi ESXCLI Firewall

اگر محیط شما شامل چندین میزبان ESXi باشد، توصیه می‌شود که از پیکربندی خودکار دیواره آتش توسط دستورات ESCLI یا vSphere Web Services SDK استفاده شود.

شما می‌توانید از ESXi Shell یا دستورات vSphere CLI برای تنظیم ESXi در خط فرمان جهت پیکربندی خودکار دیواره آتش استفاده کنید.

جدول ۳ دستورات دیواره آتش

دستور	توصیف
esxcli network firewall get	وضعیت فعال یا غیرفعال بودن دیواره آتش و لیستی از عملیات پیش‌فرض را برمی گرداند.
esxcli network firewall set --default-action	اگر به مقدار true تنظیم شود، عملیات pass پیش‌فرض انتخاب می‌شود ولی اگر به مقدار false تنظیم شود، عملیات drop انجام می‌شود.
esxcli network firewall set –enabled	فعال‌سازی یا غیرفعال‌سازی دیواره آتش ESXi انجام می‌شود.
esxcli network firewall load	ماژول دیواره آتش و فایل‌های پیکربندی مجموعه قوانین را بارگذاری می‌کند.

esxcli network firewall refresh	اگر ماژول دیواره آتش بارگذاری شده باشد، تنظیمات دیواره آتش را با خواندن فایل‌های مجموعه قوانین تازه‌سازی می‌کند.
esxcli network firewall unload	فیلترها و ماژول‌های دیواره آتش بارگذاری نشده را از بین می‌برد.
esxcli network firewall ruleset list	اطلاعات مجموعه‌ی قوانین را فهرست می‌کند.
esxcli network firewall ruleset set –allowedall	اگر به مقدار true تنظیم شود، به تمامی IPها اجازه دسترسی را می‌دهد و اگر به مقدار false تنظیم شود از لیست آدرس‌های IP مجاز استفاده می‌کند.
esxcli network firewall ruleset set –enabled ruleset-id=<string>--	به مقدار true یا false جهت فعال‌سازی یا غیرفعال‌سازی قوانین خاص استفاده می‌شود.
esxcli network firewall ruleset allowedip list	فهرستی از آدرس‌های IP مجاز برای مجموعه قوانین خاص را مشخص می‌کند.
esxcli network firewall ruleset allowedip add	اجازه دسترسی به مجموعه قوانین از آدرس‌های IP خاص یا محدوده ای از آدرس‌های IP را می‌دهد.
esxcli network firewall ruleset allowedip remove	دسترسی به مجموعه قوانین را از آدرس‌های IP خاص یا محدوده‌ای از آدرس‌های IP حذف می‌کند.
esxcli network firewall ruleset rule list	قوانین هر یک از مجموعه قوانین در دیواره آتش را فهرست می‌کند.

۲-۳-٤ سفارشی‌کردن سرویس‌های ESXi از Security Profile

یک میزبان ESXi شامل چندین سرویس است که به صورت پیش‌فرض اجرا می‌شوند. دیگر سرویس‌ها از قبیل SSH در قسمت Security Profile میزبان وجود دارند. شما می‌توانید این سرویس‌ها را در صورت نیاز و طبق سیاست‌های سازمان فعال یا غیرفعال کنید.

توجه داشته باشید که فعال‌سازی سرویس‌ها امنیت میزبان شما را تحت تاثیر قرار می‌دهد. سرویسی را جز در شرایط مورد نیاز فعال نکنید.

سرویس‌های در دسترس بستگی به VIBای دارند که روی میزبان شما نصب شده است. شما نمی‌توانید سرویس‌ها را بدون نصب یک VIB اضافه کنید. بعضی از محصولات VMware به طور مثال vSphere HA،

VIBها را روی میزبان‌ها نصب می‌کنند و سرویس‌ها و پورت‌های متناظر دیواره آتش را در دسترس قرار می دهند.

شما می‌توانید وضعیت سرویس‌های زیر را از vSphere Web Client تغییر دهید.

جدول ٤ سرویس‌های ESXi در Security Profile

سرویس	پیش‌فرض	توصیف
Direct Console UI	در حال اجرا	سرویس DCUI به شما اجازه می‌دهد با یک میزبان ESXi از کنسول محلی با استفاده از منوی مبتنی بر متن، تعامل برقرار کنید.
ESXi Shell	متوقف	ESXi Shell از طریق DCUI در دسترس است و شامل مجموعه‌ی کاملی از دستورات برای رفع مشکلات و بازسازی است. دسترسی به local ESXi Shell یا دسترسی به ESXi Shell با SSH را فعال کنید.
SSH	متوقف	SSh client که اجازه ارتباطات راه دور را از طریق Secure shell می‌دهد.
Load-Based Teaming Daemon	در حال اجرا	
Local Security Server Authentication (Active Directory Service)	متوقف	بخشی از سرویس اکتیو دایرکتوری. هنگامی که شما ESXi را برای اکتیو دایرکتوری تنظیم می‌کنید، این سرویس اجرا می‌شود.
I/O Redirector (Active Directory Service)	متوقف	بخشی از سرویس اکتیو دایرکتوری. هنگامی که شما ESXi را برای اکتیو دایرکتوری تنظیم می‌کنید، این سرویس اجرا می‌شود.
Network Login Server Directory (Active Service)	متوقف	بخشی از سرویس اکتیو دایرکتوری. هنگامی که شما ESXi را برای اکتیو دایرکتوری تنظیم می‌کنید، این سرویس اجرا می‌شود.
NTP Daemon	متوقف	دایمون پروتکل زمانی شبکه.
CIM Server	در حال اجرا	این سرویس توسط نرم‌افزارهای مدلی اطلاعات رایج (CIM) استفاده می‌شود.
SNMP Server	متوقف	.SNMP daemon

Syslog Server	متوقف	Syslog daemon. این سرویس از طریق تنظیمات پیشرفته در vSphere Web Client فعال می‌شود.
vSphere High Availability Agent	متوقف	عملکرد دسترس پذیری بالا vSphere را پشتیبانی می‌کند.
vProbe Daemon	متوقف	vProbe Daemon
VMware vCenter Agent	در حال اجرا	اجاره اتصال یک سرویس‌دهنده vCenter به یک میزبان ESXi را می‌دهد. به طور خاص، vpxa مجرای ارتباطی به دایمون میزبان است که با هسته ESXi ارتباط برقرار می‌کند.
X.Org Server	متوقف	این ویژگی اختیاری به صورت درونی برای طراحی‌های سه بعدی ماشین‌های مجازی استفاده می‌شود.

۲-۳-۵ فعال‌سازی یا غیرفعال‌سازی یک سرویس در Security Profile

شما می‌توانید سرویس‌های لیست شده در Security Profile را از vSphere Web Client فعال یا غیرفعال کنید.

پس از نصب، سرویس‌های مشخصی به صورت پیش‌فرض اجرا می‌شوند، در صورتی که دیگر سرویس‌ها متوقف هستند. در برخی از موارد نصب اضافه‌ای قبل از اینکه سرویس در vSphere Web Client در دسترس قرار گیرد، مورد نیاز است. به طور مثال سرویس NTP روشی برای بدست آوردن اطلاعات زمان دقیق است، اما این سرویس تنها هنگامی کار می‌کند که پورت‌های مورد نیاز در دیواره آتش باز شده باشند.

پیش‌نیاز:

به سرویس‌دهنده vCenter از طریق vSphere Web Client متصل شوید.

فرآیند:

۱. در vSphere Web Client، میزبان را جست‌وجو کنید.
۲. منوی Configure را انتخاب کنید.
۳. در بخش System گزینه Security Profile را انتخاب کنید و Edit را انتخاب کنید.
٤. به سرویسی که می‌خواهید تغییر دهید اسکرول کنید.

۵. در Service Details pane گزینه Start، Stop یا Restart برای یک بار تغییر وضعیت میزبان‌ها را انتخاب کنید و یا از منوی Startup Policy وضعیت میزبان در حین عملیات reboot را انتخاب کنید.

- Start automatically if any ports are open, and stop when all ports are closed: تنظیمات پیش‌فرض برای این سرویس‌ها است. اگر هر پورتی باز باشد، سرویس‌گیرنده تلاش می‌کند به منابع شبکه برای این سرویس متصل شود. اگر چند پورت باز باشد، اما پورت برای سرویس خاص بسته باشد، تلاش با شکست مواجه می‌شود. اگر پورت‌های خروجی مناسب باز باشد، سرویس متناظر آن راه‌اندازی می‌شود.
- Start and stop with host: سرویس پس از مدت کوتاهی از شروع به کار میزبان آغاز می شود و مدت کوتاهی قبل از خاموش شدن میزبان، متوقف می‌شود. همانند گزینه اول، این گزینه بدین معناست که سرویس به طور منظم تلاش می‌کند تا وظایفش را تکمیل کند، همانند تماس با سرویس‌دهنده NTP مشخص. اگر پورت بسته باشد اما پس از آن باز شود، سرویس‌گیرنده مدت کوتاهی پس از آن شروع به تکمیل کردن وظایفش می‌کند.
- Start and stop manually: میزبان تنظیمات سرویس توسط کاربر را، بدون توجه به اینکه پورت باز یا بسته است، حفظ می‌کند. وقتی که کاربر سرویس NTP را آغاز می‌کند، سرویس تا زمانی که میزبان روشن باشد، اجرا می‌شوند. اگر سرویس آغاز شود و میزبان خاموش شود، سرویس به عنوان بخشی از فرآیند خاموش شدن، متوقف می‌شود اما به محض اینکه میزبان روشن شود، سرویس مجدد آغاز می‌شود و حالت تعیین شده توسط کاربر را حفظ می‌کند.

توجه: این تنظیمات تنها روی تنظیمات سرویسی اعمال می‌شود که از طریق vSphere Web Client یا برنامه های کاربردی که با vSphere Web Services SDK تولید شده‌اند، اعمال می‌شود.

۴-۲ Lockdown Mode

جهت افزایش امنیت میزبان‌های ESXiتان می‌توانید آن‌ها را در حالت lockdown قرار دهید. در حالت lockdown عملیات به صورت پیش‌فرض توسط vCenter Server انجام می‌شود.

از نسخه ٦ به بعد vSphere شما می‌توانید حالت normal lockdown یا حالت strict lockdown که درجه های متفاوتی از lockdown را ارائه می‌دهند، را انتخاب کنید. هم‌چنین vSphere 6.x فهرست Exception

users را معرفی نمود. Exception users وقتی که میزبان به حالت Lockdown وارد می‌شود، امتیازات خود را از دست نمی‌دهند.

۲-٤-۱ فعال‌سازی یا غیرفعال‌سازی Lockdown Mode

کاربران مجاز می‌توانند حالت lockdown را با استفاده از چندین روش فعال کنند:

- هنگام استفاده از ویزارد Add Host به منظور اضافه کردن یک میزبان به یک سیستم سرویس‌دهنده vCenter.
- استفاده از vSphere Web Client . می‌توان در این دو حالت دو وضعیت normal lockdown یا strict lockdown را از vSphere Web Client فعال کرد.
- استفاده از DCUI.

کاربران مجاز می‌توانند حالت lockdown را از vSphere Web Client غیرفعال کنند. آن‌ها هم‌چنین می‌توانند حالت normal lockdown را از طریق DCUI غیرفعال کنند اما نمی‌توانند از طریق DCUI حالت strict lockdown را غیرفعال کنند.

توجه: اگر حالت lockdown را با استفاده از DCUI فعال یا غیرفعال کنید، مجوزها برای کاربران و گروه‌ها روی میزبان دور انداخته می‌شوند. به منظور جلوگیری از این امر، می‌توانید عملیات فعال‌سازی یا غیرفعال سازی را از طریق vSphere Web Client انجام دهید.

۲-٤-۲ فعال‌سازی Lockdown Mode با استفاده از vSphere Web Client

به منظور غیرفعال‌سازی دسترسی کامل به یک میزبان می‌توانید حالت strict lockdown را انتخاب کنید. در این حالت در صورتی که سرویس‌دهنده vCenter در دسترس نباشد، دسترسی به یک میزبان غیرممکن است و هم‌چنین امکانات SSH و ESXi Shell غیرفعال هستند.

فرآیند:

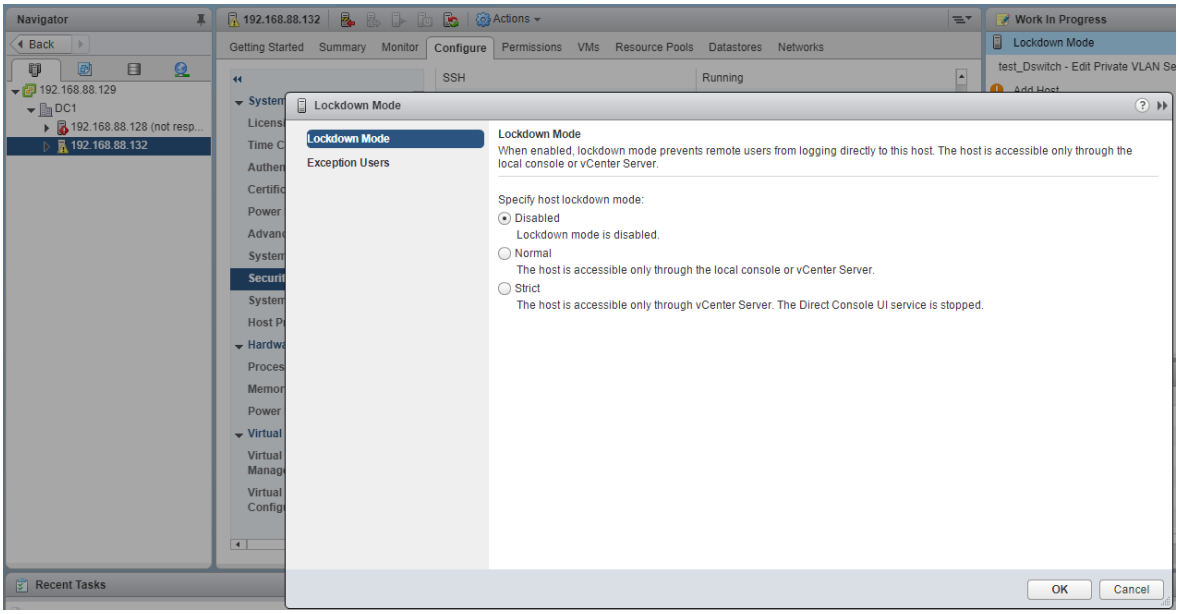
۱. میزبان را در vSphere Web Client انتخاب کنید.
۲. سربرگ Configure را انتخاب کنید.
۳. در بخش System گزینه Security Profile را انتخاب کنید.
٤. در پنل Lockdown mode گزینه Edit را کلیک کنید.

۵. Lockdown Mode را انتخاب کرده و یکی از حالت‌های زیر را با توجه به شرایط انتخاب کنید و ok را کلیک کنید:

a. Normal: در این حالت میزبان از طریق سرویس‌دهنده vCenter در دسترس قرار می‌گیرد. تنها کاربرانی که در لیست کاربران exception قرار گرفته‌اند و امتیازات مدیریتی دارند می توانند به DCUI وارد شوند. اگر SSH یا ESXi Shell فعال باشد، ممکن است دسترسی امکان‌پذیر باشد.

b. حالت Strict: در این حالت میزبان تنها از طریق سرویس‌دهنده vCenter در دسترس قرار می‌گیرد. اگر SSH یا ESXi Shell فعال باشد، نشست‌ها برای حساب‌های کاربری در DCUI اجرا می‌شود. کاربرانی که در لیست exception هستند و حقوق مدیریتی دارند، فعال باقی می‌مانند. سایر نشست‌ها خاتمه می‌یابد.

به منظور غیرفعال‌سازی حالت lockdown در گام ۵ پس از انتخاب Lockdown Mode گزینهNone را انتخاب کنید.



شکل ۸ فعال‌سازی Lockdown Mode

۲-۵ تخصیص مجوزها برای میزبان‌های ESXi

در بسیاری از موارد، شما به کاربران به واسطه تخصیص مجوز به ESXi host objects که به وسیله سیستم vCenter Server مدیریت می‌شوند، امتیاز دسترسی[۱] می‌دهید. اگر شما از standalone ESXi host استفاده می کنید، باید مجوزها را به صورت مستقیم اختصاص دهید.

۲-۵-۱ اختصاص مجوز به میزبان‌های ESXi تحت مدیریت سرویس‌دهنده vCenter

اگر میزبان ESXi شما توسط سرویس‌دهنده vCenter مدیریت می‌شود، وظایف مدیریتی را از طریق vSphere Web Client انجام دهید.

شما می‌توانید ESXi host object را در vCenter Server object hierarchy انتخاب کنید و نقش مدیریت را به تعداد محدودی از کاربران که مدیریت مستقیم روی ESXi host انجام می‌دهند، اختصاص دهید.

بهترین اقدام ایجاد حداقل یک حساب کاربری نام‌گذاری‌شده و تخصیص امتیاز مدیریتی کامل روی میزبان است و استفاده از این حساب کاربری به جای حساب ریشه است. گذواژه بسیار پیچیده را برای حساب ریشه تنظیم کنید و استفاده از این حساب کاربری ریشه را محدود کنید (حساب کاربری ریشه را حذف نکنید).

۲-۵-۲ تخصیص مجوز به Standalone ESXi Hosts

اگر محیط شما در برگیرنده‌ی سیستم vCenter Server نباشد، کاربران زیر از پیش تعریف شده هستند.

- کاربر ریشه
- vpxuser
- dcui user

شما می‌توانید کاربران محلی را اضافه کنید و custom roles را از منوی Management در vSphere Client تعریف کنید. Roleهای زیر از پیش تعریف شده هستند:

- Read Only: به کاربر اجازه می‌دهد که اشیا همراه با ESXi host را مشاهده کند اما هیچ تغییری به اشیا را وارد نسازند.

[۱] Privileges

- Administrator: نقش مدیریتی
- No Access: هیچ‌گونه دسترسی. این گزینه پیش‌فرض است.

شما می‌توانید مدیریت کاربران محلی و گروه‌ها و اضافه کردن local custom roles به یک ESXi host را با استفاده از یک vSphere Client که مستقیم به ESXi host متصل است، انجام دهید.

با استفاده از vSphere 6.0 شما می‌توانید از ESXCLI account Management commands برای مدیریت ESXi local user accounts استفاده کنید. شما می‌توانید ESXCLI permission Management commands را برای تنظیم یا حذف مجوزهای روی حساب‌های کاربری اکتیو دایرکتوری (کاربران و گروه‌ها) و روی حساب‌های کاربری ESXi local (تنها کاربران) استفاده کنید.

توجه: اگر شما کاربری را برای ESXi host توسط اتصال مستقیم به میزبان، تعریف کنید و هم‌چنین کاربری با همان نام در vCenter Server وجود داشته باشد، این کاربران با یکدیگر متفاوت هستند. اگر شما roleای را به یکی از این کاربران اختصاص دهید، کاربر دیگری نمی‌تواند به role یکسانی تخصیص یابد.

- **امتیازات کاربر ریشه**

به صورت پیش‌فرض هر میزبان ESXi تنها یک حساب کاربری ریشه یا role مدیریتی دارد. حساب کاربری ریشه می‌تواند برای مدیریت محلی و اتصال میزبان به vCenter Server استفاده شود. گذواژه بسیار پیچیده‌ای را برای حساب کاربری ریشه تنظیم کنید و استفاده ازآن را بسیار محدود کنید، به طور مثال برای در هنگام اضافه کردن یک میزبان به vCenter Server استفاده شود. حساب کاربری ریشه را حذف نکنید. در vSphere 5.1 و بعد، تنها کاربر ریشه با نقش مدیریتی اجازه اضافه کردن یک میزبان به vCenter Server را دارد. بهترین اقدام اطمینان حاصل کردن از این مورد است که هر حساب کاربری با نقش مدیریتی روی یک ESXi host به یک حساب کاربری خاص با حساب نام گذاری شده، اختصاص یافته است. از قابلیت‌های اکتیو دایرکتوری ESXi که به شما اجازه مدیریت اعتبارنامه‌های اکتیو دایرکتوری را می‌دهد، استفاده کنید.

نکته: اگر شما مجوز دسترسی برای کاربر ریشه را حذف کنید، باید ابتدا مجوز دیگری را در سطح ریشه تولید کنید که کاربر متفاوتی به نقش مدیریتی اختصاص یافته است.

- **امتیازات vpxuser**

سرویس‌دهنده vCenter از امتیازات vpxuser برای مدیریت فعالیت‌های میزبان استفاده می‌کند. سرویس‌دهنده vCenter روی میزبانی که آن را مدیریت می‌کند امتیازات مدیریتی دارد. به طور مثال، سرویس‌دهنده vCenter می‌تواند ماشین‌های مجازی را به/از میزبان‌ها منتقل کند و تغییرات پیکربندی را که برای پشتیبانی ماشین‌های مجازی مورد نیاز است، را انجام دهد. مدیران سرویس‌دهنده vCenter می‌توانند بیشتر عملیات همانند کاربر ریشه را روی میزبان انجام دهند و هم‌چنین وظایف زمان‌بندی، کار با نمونه‌ها و غیره را انجام دهند. به هر حال، مدیران سرویس‌دهنده vCenter نمی‌توانند به صورت مستقیم کاربران محلی و گروه‌ها را برای میزبان ایجاد، حذف یا ویرایش کنند. این وظایف می‌تواند تنها توسط کاربر با امتیازات مدیریتی به صورت مستقیم روی هر میزبان انجام شود.

توجه: شما نمی‌توانید vpuser را با استفاده از اکتیو دایرکتوری، مدیریت کنید.

اخطار: تحت هیچ شرایطی vpxuser را تغییر ندهید. گذرواژه را عوض نکنید. مجوزها را تغییر ندهید.اگر شما این کار را انجام دهید، شما ممکن است در هنگام کار با میزبان‌ها از طریق سرویس‌دهنده vCenter با مشکل مواجه شوید.

- **امتیازات کاربر DCUI**

کاربر DCUI روی میزبان‌ها اجرا می‌شود و به حقوق مدیریتی عمل می‌کند. هدف اصلی این کاربران، پیکربندی میزبان‌ها برای lockdown mode از Direct Console User Interface (DCUI) است. این کاربر همانند عاملی برای direct console عمل می‌کند و نمی‌تواند اصلاح شود یا توسط کاربران تعاملی استفاده شود.

٦-٢ کلیدهای ESXi SSH

از SSH keys می‌توان برای محدودکردن، کنترل و دسترسی امن به یک میزبان ESXi استفاده کرد. با استفاده از SSH keys می‌توان به کاربران مورد اعتماد و حتی به اسکریپت‌ها اجازه داد بدون نیاز به گذرواژه خاصی به میزبان مورد نظر وارد شوند. با استفاده از دستور vifs می‌توان SSH keys را در یک میزبان کپی کرد. هم چنین می‌توان از HTTPS PUT برای کپی‌کردن SSH keys به میزبان استفاده کرد. فعال‌کردن SSH و اضافه کردن SSH keys به میزبان موجب افزایش ریسک می‌شود و در حالت کلی برای محیط‌های با امنیت بالا توصیه نمی‌شود.

توجه: در ESXi 5.0 و نسخه‌های قبل از آن یک کاربر با SSH keys می‌توانست در lockdown mode هم به میزبان دسترسی داشته باشد. که این مشکل در ESXi 5.1 حل شد.

۲-۶-۱ امنیت SSH

با استفاده از SSH می‌توان از راه دور به ESXi Shell وارد شد و یک سری از عیب‌یابی‌ها را برای میزبان انجام داد. پیکربندی SSH در ESXi از امنیتی بالایی برخوردار است و دارای تنظیمات زیراست:

SSH protocol disabled :Version 1 VMware از نسخه ۱ پروتکل SSH پشتیبانی نمی‌کند و به جای آن از نسخه۲ این پروتکل استفاده می‌شود. در نسخه ۲ بسیاری از مسائل امنیتی موجود در نسخه ۱ برطرف شده است و روش امن‌تری را برای ارتباط با واسط مدیریتی فراهم آورده است.

Improved cipher strength: SSH برای اتصالات از الگوریتم رمزنگاری AES با طول بیت ۱۲۸ و ۲۵۶ پشتیبانی می‌کند.

توجه: این تنظیمات جهت محافظت از داده منتقل شده ارائه شده‌اند و قابل تغییر نیستند.

- **آپلود یک SSH key با استفاده از دستور vifs**

می‌توان از authorized keys برای ورود به یک میزبان با استفاده از SSH استفاده کرد. می‌توان authorized keys را با استفاده از دستور vifs بارگذاری کرد. authorized keys اجازه می‌دهند تا دسترسی از راه دور به یک میزبان احرازاصالت شود. وقتی که کاربران یا اسکریپت‌ها بخواهند به یک میزبان با استفاده از SSH دسترسی پیدا کنند، کلیدها احرازاصالت بدون گذرواژه را انجام می‌دهند. با استفاده از authorized keys شما به صورت خودکار (هنگامی که بخواهید اسکریپت‌هایی را برای انجام وظایف روزمره بنویسید، مفید هستند) احرازاصالت می‌شوید.

انواع SSH keys را که در ادامه گفته می‌شود را می‌توان در یک میزبان آپلود کرد:

- فایل authorized keys برای کاربر ریشه
- DSA key
- DSA public key
- RSA key
- RSA public key

توجه: به هیچ وجه فایل /etc/SSH/SSHd_config را تغییر ندهید.

فرآیند:

دستور vifs زیر را در خط فرمان برای آپلود کردن کلید SSH در مکان مناسب، تایپ کنید:

vifs --server hostname --username username --put filename /host/SSH_host_dsa_key_pub

نوع کلید	محل
user Authorized key files for the root	/host/SSH_root_authorized keys
DSA keys	/host/SSH_host_dsa_key
DSA public keys	/host/SSH_host_dsa_key_pub
RSA keys	/host/SSH_host_rsa_key
RSA public keys	/host/SSH_host_rsa_key_pub

- **آپلود کردن یک SSH keys با استفاده از HTTPS PUT**

همانطور که گفته شد با استفاده از authorized keys می‌توان به یک میزبان دسترسی پیدا کرد. این کلیدها را می‌توان با استفاده از HTTPS PUT آپلود کرد. با استفاده از کلیدهای اعتبارسنجی، شما این امکان را دارید که از راه دور به میزبان مورد نظر دسترسی پیدا کنید.هنگامی که کاربران و اسکریپت‌ها سعی دارند به یک میزبان دسترسی داشته باشند، کلیدها به آن‌ها این امکان را می‌دهند که بدون داشتن کلمه‌عبور وارد میزبان شوند.

کلیدهای SSH زیر قابل آپلود شدن با استفاده از HTTPS PUTها هستند:

- Authorized keys file for root user
- DSA key
- DSA public key
- RSA key
- RSA public key

توجه: فایل /etc/ssh/sshd_config را تغییر ندهید.

فرآیند:

۱- در برنامه آپلود خود key file را باز کنید.

۲- فایل خود را در مکان‌های زیر منتشر کنید.

مکان	نوع کلید
https://hostname_or_IP_address/host/ssh_root_authorized_keys	Authorized key files for the user root
https://hostname_or_IP_address/host/ssh_host_dsa_key	DSA keys
https://hostname_or_IP_address/host/ssh_host_dsa_key_pub	DSA public keys
https://hostname_or_IP_address/host/ssh_host_rsa_key	RSA keys
https://hostname_or_IP_address/host/ssh_host_rsa_key_pub	RSA public keys

۲-۷ استفاده از ESXi Shell

ESXi Shell به صورت پیش‌فرض بر روی ESXi غیرفعال است و می‌توان در صورت نیاز دسترسی محلی یا راه دور به shell را فعال کرد. توصیه می‌شود تنها در صورتی که نیازی به عیب‌یابی است ESXi Shell را فعال کنید.

ESXi Shell: با فعال‌کردن این سرویس می‌توان به ESXi Shell دسترسی پیدا کرد.

SSH: با فعال‌کردن این سرویس می‌توانید به صورت راه دور و با استفاده از SSH به میزبان مورد نظر دسترسی پیدا کرد.

Direct Console UI (DCUI): با فعال‌کردن این سرویس شما می‌توانید حتی وقتی که در lockdown mode هستید به صورت محلی و به عنوان کاربر ریشه به واسط کاربری کنسول (DCUI) متصل شده و lockdown mode را غیرفعال کنید. سپس می‌توانید به میزبان با استفاده از یک اتصال مستقیم به vSphere Client یا با فعال‌سازی ESXi Shell، دسترسی پیدا کنید.

کاربر ریشه و یا کاربران با نقش مدیریتی می‌توانند به ESXi Shell دسترسی داشته باشند. کاربرانی که در گروه های ESXi Admins اکتیو دایرکتوری هستند به صورت خودکار به نقش مدیریتی اختصاص داده می‌شوند. به صورت پیش‌فرض، تنها کابر ریشه می‌تواند دستورات سیستمی(مانند vmware –v)را در ESXi Shell اجرا کند.

توجه: تا هنگامی که نیاز نیست ESXi Shell را فعال نکنید.

۲-۷-۱ استفاده از vSphere Web Client جهت فعال‌کردن دسترسی به ESXi Shell

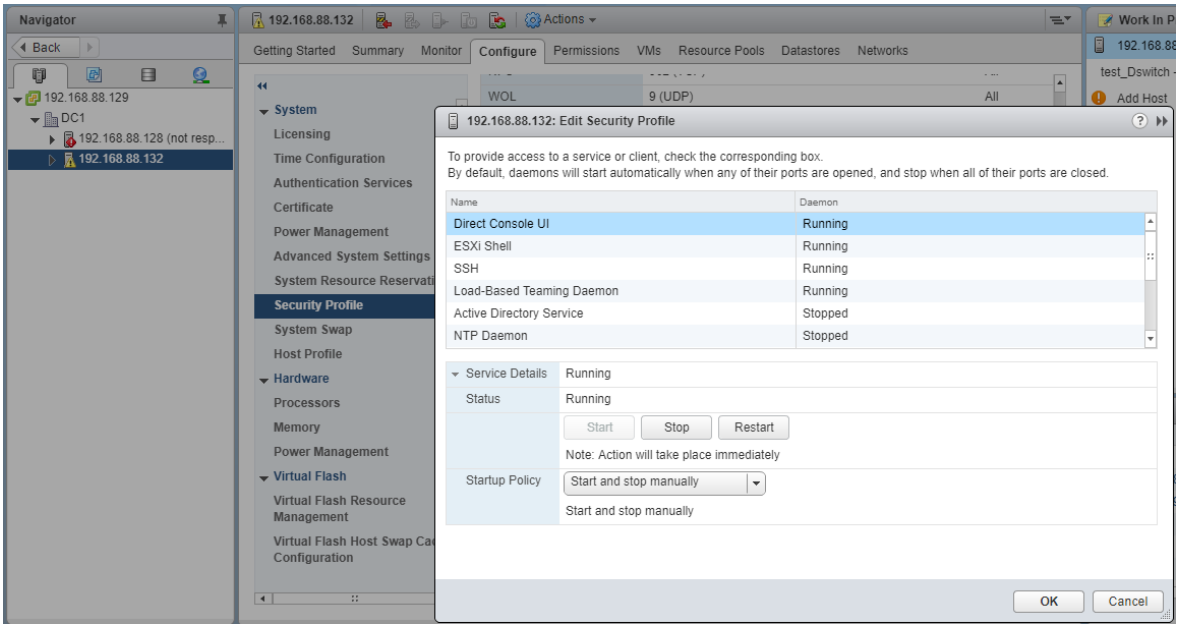
از vSphere Web Client به منظور فعال‌سازی دسترسی به ESXi Shell استفاده می‌شود: می‌توانید از vSphere Web Client برای دسترسی محلی و راه دور به ESXi Shell و تنظیم مدت زمان بیکار بودن و مدت زمان دسترس‌پذیری استفاده کنید.

پیش‌نیازها:

اگر می‌خواهید از کلیدهای SSH مجازاستفاده کنید باید آن‌ها را آپلود کنید.

فرآیند:

۱. میزبان را در vSphere Web Client، انتخاب کنید.
۲. سربرگ Configure را کلیک کنید.
۳. گزینه Security Profile را انتخاب کنید.
٤. در Services panel، گزینه Edit را کلیک کنید.
۵. یک سرویس را از لیست انتخاب کنید:
   a. ESXi Shell
   b. SSH
   c. Direct Console UI
٦. Service Details را کلیک کنید سپس Start and stop manually را انتخاب کنید.
۷. به منظور فعال‌کردن سرویس Start را انتخاب کرده و Ok را کلیک کنید.



شکل ۹ فعال‌کردن دسترسی به ESXI Shell

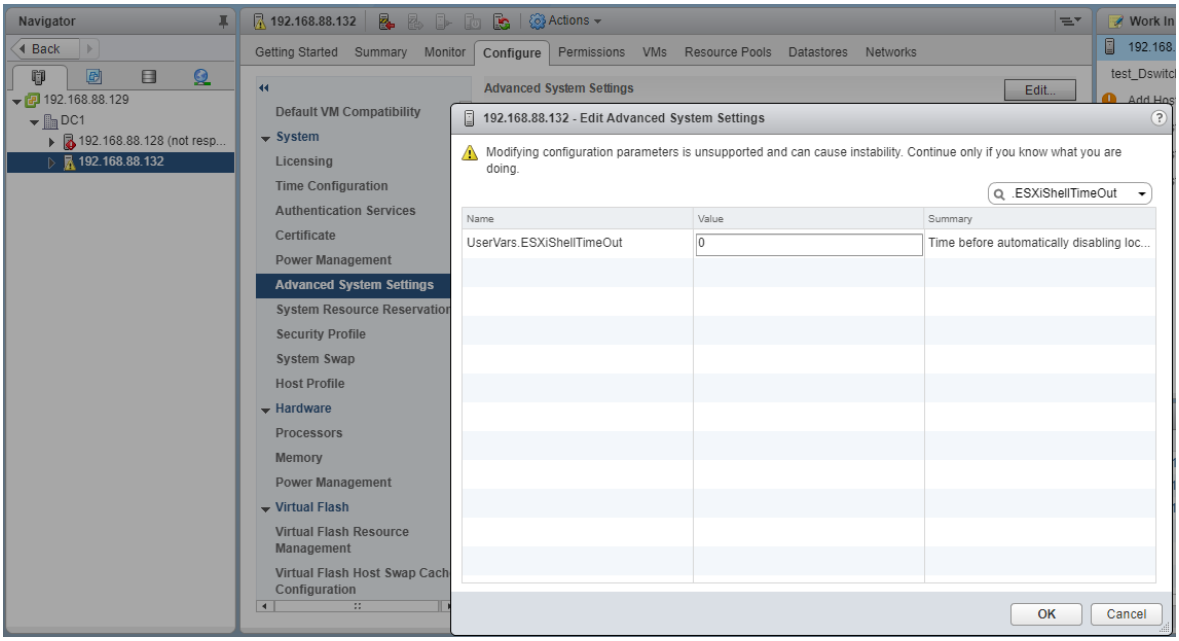
۲-۷-۲ تعیین یک مهلت زمانی برای دسترس‌پذیری ESXi Shell در vSphere Web Client

ESXi Shell به صورت پیش‌فرض غیرفعال است. شما می‌توانید یک زمان دسترس پذیری برای آن تعیین کنید. بدین‌ترتیب امنیت shell افزایش می‌یابد.

زمان دسترس‌پذیری مقدار زمان تعیین شده جهت ورود به میزبان بعد از فعال‌کردن ESXi Shell است. در صورت وارد نشدن در زمان تعیین شده این سرویس به صورت خودکار غیرفعال شده و کاربر نمی‌تواند وارد شود.

فرآیند:

۱. Host را در vSphere Web Client، انتخاب کنید.
۲. سربرگ Configure را کلیک کنید.
۳. گزینه Advanced System Settings را انتخاب کنید.
٤. گزینه UserVars.ESXiShellTimeOut را انتخاب کنید و آیکن Edit را کلیک کنید.
۵. تنظیمات مربوط به idle timeout را وارد کرده (توجه داشته باشید که شما باید SSH service را restart کنید) و OK را کلیک کنید.



شکل ۱۰ تعیین مهلت زمانی برای دسترس‌پذیری ESXi Shell

۲-۷-۳ تعیین یک مهلت زمانی برای Idle ESXi Shell Sessions در vSphere Web Client

اگر یک کاربر ESXi Shell را روی میزبان فعال کند و فراموش کند از نشست خود خارج شود، idle session به طور نامحدود برقرار است. با وجود چنین اتصالی احتمال اینکه یک نفر امتیاز دسترسی به میزبان را به‌دست آورد، افزایش می‌یابد. به منظور جلوگیری از این امر می‌توان یک مهلت زمانی برای نشست غیرفعال تعیین کرد.

idle timeou مدت زمانی است که کاربر قبل از آن می‌تواند از یک نشست غیرفعال خارج شود. می‌توان مهلت زمانی را برای هر دو نشست محلی و راه دور از طریق DCUI یا vSphere Web Client کنترل کرد.

فرآیند:

۱. میزبان را در vSphere Web Client، انتخاب کنید.
۲. سربرگ Configure را کلیک کنید.
۳. گزینه Advanced System Settings را انتخاب کنید.
٤. گزینه UserVars.ESXiShellTimeOut را انتخاب کنید و آیکن Edit را کلیک کنید و مقادیر timeout setting را وارد کنید.
۵. ESXi Shell service و SSH service را Restart کنید.

اگر نشست مورد نظر غیرفعال است کاربران به طور خودکار بعد از سپری شدن مهلت زمانی خارج می‌شوند.

۲-۷-٤ استفاده از DCUI جهت فعال‌کردن دسترسی به ESXi Shell

جهت فعال‌سازی دسترسی به ESXi Shell می‌توان از Use the Direct Console User Interface (DCUI) استفاده کرد: DCUI به شما اجازه تعامل با میزبان را به صورت محلی با استفاده از منوهای متنی را می‌دهد.

فرآیند:

۱. در داخل DCUI، دکمه F2 را فشار دهید تا به منوهای System Customization دسترسی پیدا کنید.
۲. گزینه Troubleshooting Options انتخاب کنید و دکمه Enter را بزنید.
۳. از منوی Troubleshooting Mode Options سرویس مورد نظر خود را فعال کنید.
٤. دکمه Enter را زده تا سرویس مورد نظر فعال شود.
۵. به منظور برگشت به منوی اصلی DCUI دکمه Esc را بزنید.

شکل ۱۱ فعال‌کردن دسترسی به ESXi Shell از طریق DCUI

۲-۷-۵ تعیین یک مهلت زمانی برای دسترس‌پذیری ESXi Shell در محیط DCUI

ESXi Shell به صورت پیش‌فرض غیرفعال است. می‌توانید به‌منظور افزایش امنیت در هنگامی که از shell استفاده می‌کنید، یک مهلت زمانی برای مدت دسترسی‌پذیری ESXi Shell تنظیم کنید.

فرآیند:

۱. از منوی Troubleshooting Mode Options، گزینه Modify ESXi Shell and SSH timeouts انتخاب کنید و کلید Enter را بزنید.
۲. مقدار availability timeout را وارد کنید (این کار مستلزم این است که SSH service و ESXi Shell به‌منظور تأثیر این مقداردهی restart شود).
۳. کلیدهای Enter و Esc را زده تا به منوی اصلی DCUI برگردید.
٤. کلید OK را بزنید.

۲-۷-٦ تعیین یک مهلت زمانی برای Idle ESXi Shell Sessions

اگر کاربر به ESXi Shell میزبان وارد شود و فراموش کند که از آن نشست خارج شود، نشست idle در مدت زمانی نامحدود، متصل باقی می‌ماند. اتصال باز می‌تواند پتانسیل دستیابی به دسترسی ممتاز به میزبان را افزایش دهد، که می‌توان از این مخاطره با تنظیم مهلت زمانی برای نشست idle جلوگیری کرد.

فرآیند:

۱. از منوی Troubleshooting Mode Options، گزینه Modify ESXi Shell and SSH timeouts انتخاب کرده و کلید Enter را بزنید.
۲. مقدار idle timeout را به ثانیه وارد کنید. (این کار مستلزم این است که SSH service، restart شود)
۳. کلیدهای Enter و Esc را زده تا به منوی اصلی DCUI برگردید.
٤. کلید OK را بزنید.

۲-۸ ورود به ESXi Shell جهت عیب‌یابی

تنظیمات مرتبط به ESXi را با استفاده از vSphere Web Client انجام دهید و به ESXi Shell تنها جهت اهداف عیب‌یابی وارد شوید.

فرآیند:

۱. با استفاده از یکی از روش‌های زیر به ESXi Shell، وارد شوید:
   - اگر دسترسی مستقیم به میزبان دارید، جهت باز شدن صفحه ورود کلیدهای Alt+F1 را فشار دهید.
   - اگر از راه دور به میزبان دسترسی دارید، از SSH استفاده کنید.
۲. نام کاربری و گذرواژه مشخص شده از قبل را وارد کنید.

۹-۲ تغییردادن تنظیمات ESXi Web Proxy

هنگامی که تنظیمات Web proxy را تغییر می‌دهید نکات زیر را مورد توجه قرار دهید.

- گواهی‌نامه‌هایی را که از گذرواژه استفاده می‌کنند را نصب نکنید. ESXi پراکسی‌های وبی که از گذرواژه استفاده می‌کنند را پشتیبانی نمی‌کند. اگر پراکسی وبی را نصب کنید که نیاز به گذرواژه داشته باشد، ESXi نمی‌تواند به طور صحیح شروع به کار کند.
- به منظور پشتیبانی از رمزنگاری برای نام‌های کاربری، گذرواژه و بسته‌ها، SSL به صورت پیش‌فرض برای ارتباطات vSphereWeb Services SDK فعال شده است.
- به منظور جلوگیری از سوءاستفاده از سرویس‌های ESXi، بیشتر سرویس‌های داخلی از طریق پورت ٤٤٣ در دسترس هستند.
- حتی با وجود upgrade کردن، certificate قبلی در جای خودش باقی می‌ماند.

۱۰-۲ مدیریت فایل‌های رخداد ESXi

فایل‌های رخداد نقش مهمی را در هنگام وقوع حملات و رخنه‌های امنیتی ایفا می‌کنند. اقدامات زیر را در جهت افزایش امنیت میزبان‌ها انجام دهید:

- رخدادنگاری دائمی[۱] را فعال کنید. به صورت پیش‌فرض رخدادهای میزبان‌های ESXi در حافظه فایل‌های سیستمی ذخیره می‌شوند. بنابراین هنگامی که میزبان راه‌اندازی مجدد می‌شود، همه‌ی آن‌ها از بین می‌روند و فقط به مدت ٢٤ساعت داده‌های مربوط به رخداد ذخیره می‌شوند. هنگامی که

[۱] Persistent Logging

رخدادنگاری دائمی فعال می‌شود، یک رکورد از فعالیت‌های سرویس‌دهنده برای میزبان اختصاص می‌یابد.

- رخدادنگاری از راه دور[1] به یک میزبان مرکزی موجب جمع‌آوری فایل‌های رخداد درون یک میزبان مرکزی می‌شود، که اجازه نظارت تمام میزبان‌ها را با یک ابزار می‌دهد. هم‌چنین می‌توان جستجو و تجزیه و تحلیل فایل‌های رخداد را انجام داد که می‌تواند باعث آشکار شدن مواردی مانند حملات هماهنگ شده بر روی چندین میزبان باشد.
- جهت پیکربندی sysylogهای امن روی میزبان‌های ESXi می‌توان از دستوراتی همچون vCLI یا PowerCLI و یا حتی از یک API Client استفاده کرد.
- از پیکربندی و صحت تنظیمات سرویس‌دهنده syslog از قبیل تنظیم صحیح پورت‌ها، اطمینان حاصل کنید.

۲-۱۰-۱ پیکربندی syslogها بر روی ESXiها

همه ESXiها دارای یک سرویس sysylog (به نام vmsyslog) هستند که این سرویس تمام پیام‌های VmKernel و سایر تجهیزات را در یک فایل رخداد ثبت می‌کند. تا ۳۰ میزبان پیشتیبانی می‌شود.

به منظور پیکربندی سرویس syslog می‌توان از دستور esxcli system syslog vCLI و یا vSphere Web Client استفاده کرد.

فرآیند:

۱- در vSphere Web Client میزبان را انتخاب کنید.

۲- سربرگ Configure را انتخاب کنید.

۳- در قسمت System گزینه Advanced System Settings را انتخاب کنید.

٤- Syslog را انتخاب کنید.

٥- برای تغییر تنظیمات گزینه Edit icon را انتخاب کنید.

[1] Remote Logging

جدول ۵ پیکربندی syslogها

گزینه	توضیحات
Syslog.global.defaultRotate	تعیین حداکثر مقدار بایگانی‌ها. می‌توان این مقدار را به صورت کلی ویا مختص به یک sublogger تعیین کرد.
Syslog.global.defaultSize	تعیین اندازه پیش‌فرض رخدادها. می‌توان این مقدار را به صورت کلی ویا مختص به یک sublogger تعیین کرد.
Syslog.global.LogDir	تعیین مسیری که فایل رخداد ذخیره می‌شود. مسیر می‌تواند بر روی یک فایل NFS ویا VMFS ذخیره شود. تنها مسیری که بعد از reboot شدن از بین نمی‌رود /scratch/ است. مسیر باید به صورت [datastorename] path_to_file مشخص شده باشد. برای مثال مسیر /systemlogs [storage1] اشاره به /vmfs/volumes/storage1/systemlogs/ دارد.
Syslog.global.logDirUnique	با انتخاب این گزینه یک زیر مسیر با نام میزبان ESXi تحت Syslog.global.LogDir ایجاد می‌شود.
Syslog.global.LogHost	با این گزینه میزبان و پورتی انتخاب می‌شوند که قرار است پیام‌های syslog به آن‌ها ارسال شوند. این گزینه می‌تواند شامل پروتکل و پورت مربوطه باشد. برای مثال آدرس ssl://hostName1:1514، tcp، udp وssl پشتیبانی می‌شوند. میزبان مورد نظر باید قبلاً syslog را نصب کرده باشد و به درستی پیکربندی شده باشد تا بتواند پیام‌های syslog را ارسال کند.

٦- این گزینه اختیاری است و جهت تعیین مجدد اندازه و چرخش[1] فایل رخداد استفاده می‌شود.

a- نام فایل رخدادی را که می‌خواهید تغییر دهید.

b- آیکن Edit را انتخاب کرده و مقدار مورد نظر را برای اندازه فایل رخداد و چرخش را وارد کنید.

[1] Rotation

۷- Ok را کلیک کنید.

۲-۱۰-۲ مکان‌های فایل رخداد ESXi

ESXi با استفاده از امکانات syslog فعالیت میزبان را در فایل‌های رخداد ذخیره می‌کند.

جدول ٦ فایل‌های رخداد ESXi

جزء	محل قرارگیری	هدف
VMkernel	/var/log/vmkernel.log	ثبت فعالیت‌های مربوط به ماشین‌های مجازی و ESXi.
VMkernel warnings	/var/log/vmkwarning.log	ثبت فعالیت‌های مربوط به ماشین‌های مجازی
VMkernel summary	/var/log/vmksummary.log	تعیین اطلاعات مربوط به زمان فعال و در دسترس پذی برای ESXi.
ESXi host agent log	/var/log/hostd.log	حاوی اطلاعات مربوط به عامل‌هایی که میزبان ESXi و ماشین‌های مجازی آن را مدیریت می کنند.
vCenter agent log	var/log/vpxa.log/	حاوی اطلاعات مربوط به عامل‌هایی که با vcentre ارتباط برقرار می‌کنند.
Shell log	/var/log/vpxa.log	حاوی یک رکورد از تمام انواع دستوراتی که در ESXi shell وجود دارد.
Authentication	/var/log/auth.log	حاوی همه رخدادهایی که مربوط به احرازاصالت سیستم محلی است
System messages	/var/log/syslog.log	حاوی تمام پیام‌های رخداد می‌باشد که می‌توان از آن برای عیب‌یابی استفاده کرد
Virtual machines	/vmfs/volumes/datastore/virtual machine/vwmare.log	حاوی رخدادهای مربوط به میزان برق مصرفی و همچنین اطلاعات مربوط به خرابی سیستم ویا تغییرات سخت‌افزاری مجازی و همچنین هماهنگی زمانی و غیره است.

۲-۱۰-۳ امن‌سازی Fault Tolerance Logging Traffic

هنگامی که شما گزینه Fault Tolerance (FT) را فعال می‌کنید در حقیقت VMware vLockstep ورودی‌ها و رخدادهای مربوط به ماشین مجازی اصلی را جمع‌آوری کرده و به ماشین مجازی ثانویه ارسال می‌کند. (ماشین مجازی ثانویه بر روی یک میزبان دیگر در حال اجرا است).

این logging traffic بین ماشین مجازی اصلی وثانویه شامل اطلاعاتی همچون مشخصه‌های شبکه میزبان و داده‌های محل ذخیره‌سازی است. ولی این موضوع را باید در نظر گرفت که این اطلاعات رمز نشده هستند. این ترافیک می‌تواند شامل شامل داده‌های حساس مانند گذرواژه باشد. از این رو برای جلوگیری از افشای چنین اطلاعاتی باید مطمئن شد که شبکه ما امن است. به عنوان مثال می‌توان از یک private network برای FT logging استفاده کرد.