

بسمه تعالی

**امن سازی شبکه در بستر مجازی سازی**

**VMware vSphere**

**(بخش اول)**

## فهرست مطالب

۱	مقدمه	۱
۱	امن سازی سوئیچ های مجازی استاندارد	۲
۳	عملکرد حالت بی قاعده	۱-۲
۴	تغییرات آدرس MAC	۲-۲
۴	انتقال های جعلی	۳-۲
۵	جداسازی ترافیک شبکه با استفاده از VLAN ها	۳
۵	مزایای استفاده از VLAN در vSphere	۱-۳
۵	حالت های برچسب گذاری VLAN	۲-۳
۹	VLAN های خصوصی	۳-۳
۱۰	ایجاد یک VLAN خصوصی	۴-۳
۱۲	حذف یک VLAN خصوصی اصلی	۵-۳
۱۳	حذف یک VLAN خصوصی جانبی	۶-۳
۱۴	پیکربندی SNMP	۴
۱۴	امنیت پروتکل اینترنت	۵
۱۵	فهرست کردن انجمن های امنیتی موجود	۱-۵
۱۶	اضافه کردن یک انجمن امنیتی IPsec	۲-۵
۱۸	حذف یک انجمن امنیتی IPsec	۳-۵
۱۸	فهرست کردن سیاست های امنیتی IPsec موجود	۴-۵
۱۸	ایجاد یک سیاست امنیتی IPsec	۵-۵
۲۰	حذف یک سیاست امنیتی IPsec	۶-۵
۲۱	بهترین تجربه های امنیتی شبکه vSphere	۶
۲۱	توصیه های عمومی امنیت شبکه	۱-۶
۲۴	برچسب گذاری مؤلفه های شبکه	۲-۶
۲۴	مستند سازی و بررسی محیط vSphere VLAN	۳-۶
۲۵	اقدامات مربوط به جداسازی شبکه های با اهمیت بیشتر	۴-۶
۲۷	جداسازی شبکه مدیریتی	۱-۴-۶
۲۸	جداسازی ترافیک ذخیره سازی	۲-۴-۶
۲۸	جداسازی ترافیک VMotion	۳-۴-۶
۲۹	محدود کردن استفاده از سوئیچ های مجازی با vSphere Network Appliance API	۵-۶

## ۱ مقدمه

امن سازی شبکه vSphere یکی از بخش های ضروری در حفاظت از محیط مجازی شما است. امنیت شبکه در محیط vSphere ویژگی ها و موارد مشترک زیادی با امن سازی محیط در یک شبکه فیزیکی دارد، اما همچنین شامل ویژگی هایی است که تنها به ماشین های مجازی اعمال می شوند. در این گزارش به بیان برخی از مهم ترین توصیه ها و موارد مربوط به امن سازی شبکه در بستر مجازی سازی vSphere می پردازیم و بهترین تجربه های امنیتی را در این زمینه شرح می دهیم.

## ۲ امن سازی سوئیچ های مجازی استاندارد

ترافیک سوئیچ مجازی استاندارد<sup>۱</sup> را می توان در مقابل حملات لایه ۲ امن کرد. برای این کار می توان با استفاده از تنظیمات امنیتی سوئیچ ها، برخی از حالت های آدرس MAC را محدود کرد. هر آداپتور شبکه ماشین مجازی یک آدرس MAC اولیه<sup>۲</sup> و یک آدرس MAC مؤثر<sup>۳</sup> دارد.

- آدرس MAC اولیه: آدرس MAC اولیه زمانی که آداپتور ایجاد می شود به آن تخصیص داده می شود. اگر چه آدرس MAC اولیه را می توان از خارج سیستم عامل مهمان دوباره پیکربندی کرد، اما نمی تواند توسط سیستم عامل مهمان تغییر کند.
  - آدرس MAC مؤثر: هر آداپتور یک آدرس MAC مؤثر دارد که ترافیک ورودی شبکه که مقصد آن یک آدرس MAC متفاوت با آدرس MAC مؤثر است، را فیلتر می کند. سیستم عامل مهمان مسئول تنظیم آدرس MAC مؤثر است و معمولاً آدرس MAC مؤثر را به آدرس MAC اولیه منطبق می کند.
- در ابتدای ایجاد یک آداپتور شبکه ماشین مجازی، آدرس MAC مؤثر و آدرس MAC اولیه یکسان هستند. سیستم عامل مهمان می تواند در هر زمان دلخواه آدرس MAC مؤثر را به مقدار دلخواه تغییر دهد. اگر یک

<sup>۱</sup> Virtual standard switch

<sup>۲</sup> Initial MAC address

<sup>۳</sup> Effective MAC address

سیستم عامل آدرس MAC مؤثر را تغییر دهد، آداپتور شبکه آن سیستم ترافیکی که به مقصد آدرس MAC جدید است را دریافت می کند.

زمانی که بسته ها از طریق یک آداپتور شبکه ارسال می شوند، معمولاً سیستم عامل مهمان آدرس MAC مؤثر آداپتور خود را در فیلد آدرس MAC مبدأ فریم های اترنت قرار می دهد. همچنین آدرس MAC آداپتور شبکه گیرنده را در فیلد آدرس MAC مقصد قرار می دهد. آداپتور گیرنده بسته ها را تنها در صورتی پذیرش می کند که آدرس MAC مقصد بسته با آدرس MAC مؤثر آداپتور منطبق باشد.

یک سیستم عامل می تواند فریم ها را با یک آدرس MAC منبع جعلی ارسال کند. این بدان معنی است که یک سیستم عامل می تواند با جعل یک آداپتور شبکه که برای شبکه دریافت کننده مجاز است، حملات مخربی را روی دستگاه های شبکه انجام دهد.

با پیکربندی یک سیاست امنیتی روی پورت گروه ها<sup>۴</sup> یا پورت ها، ترافیک مجازی را در مقابل حملات جعل و رهگیری لایه ۲ امن نمایید. سیاست امنیتی روی پورت گروه های توزیع شده و پورت ها شامل گزینه های زیر است:

- حالت بی قاعده<sup>۵</sup>
- تغییرات آدرس MAC<sup>۶</sup>
- انتقال های جعلی<sup>۷</sup>

تنظیمات پیش فرض را می توان با انتخاب سوئیچ مجازی مربوط به میزبان در vSphere Web Client انجام داد.

## روش

۱. در vSphere Web Client میزبان مورد نظر را انتخاب کنید.

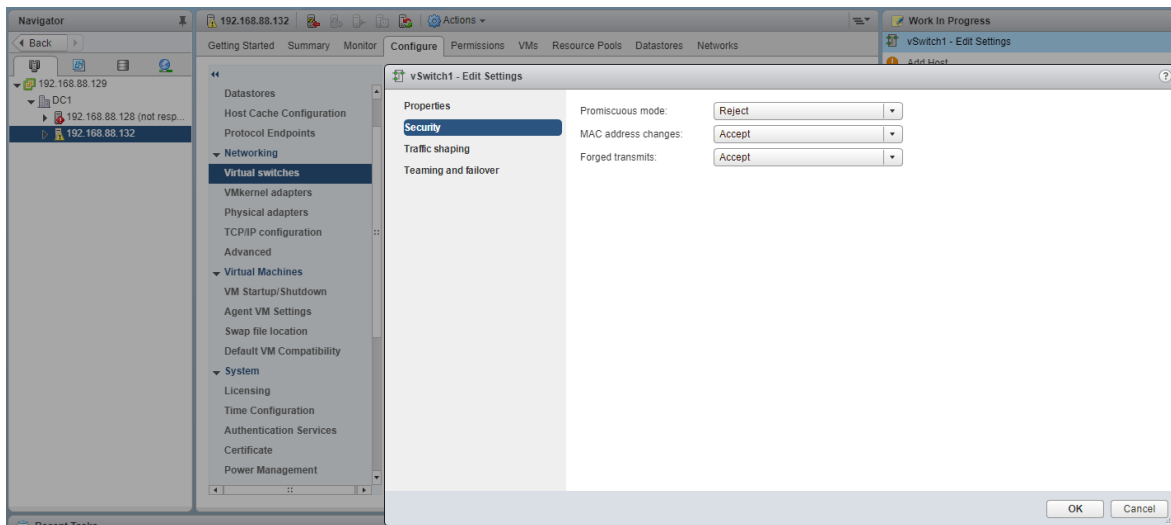
<sup>۴</sup> Port groups

<sup>۵</sup> Promiscuous mode

<sup>۶</sup> MAC address changes

<sup>۷</sup> Forged transmits

۲. برگه Configure را انتخاب کرده و سپس وارد قسمت Networking شوید.
۳. گزینه Virtual switches را انتخاب کرده تا لیست سوئیچ‌های مجازی موجود نمایش داده شود.
۴. سوئیچ مورد نظر را انتخاب و سپس دکمه Edit settings را کلیک کنید.
۵. در پنجره باز شده وارد بخش Security شوید.
۶. تنظیمات مربوط به حالت بی‌قاعده، تغییر آدرس MAC، و انتقال‌های جعلی در این پنجره قرار دارند که می‌توانید آن‌ها را به Accept یا Reject تنظیم کنید.



شکل ۱ تنظیمات امنیتی مربوط به آدرس MAC

## ۱-۲ عملکرد حالت بی‌قاعده

حالت بی‌قاعده هرگونه فیلترینگ پذیریشی که آداپتور ماشین مجازی انجام می‌دهد را از بین می‌برد، به گونه‌ای که سیستم‌عامل مهمان همه ترافیک‌های مشاهده شده روی سیم را دریافت می‌کند. به طور پیش‌فرض، آداپتور ماشین مجازی نمی‌تواند در حالت بی‌قاعده عمل کند.

اگرچه حالت بی‌قاعده می‌تواند برای ردیابی فعالیت شبکه مفید باشد، اما یک حالت ناامن است، زیرا هر آداپتور در حالت بی‌قاعده به تمام بسته‌ها دسترسی دارد، حتی اگر برخی از بسته‌ها تنها توسط یک آداپتور خاص دریافت شده باشند. این بدین معنی است که یک مدیر یا کاربر ریشه در یک ماشین مجازی، به صورت بالقوه می‌تواند ترافیکی را که به مقصد سایر سیستم‌عامل‌های مهمان یا میزبان است، را ببیند.

**نکته:** در بعضی موارد ممکن است یک دلیل قانونی وجود داشته باشد که یک سوئیچ مجازی استاندارد یا توزیع شده در حالت بی قاعده عمل کند. به عنوان مثال، اگر شما در حال اجرای نرم افزار تشخیص نفوذ شبکه یا شنود بسته هستید.

## ۲-۲ تغییرات آدرس MAC

سیاست امنیتی یک سوئیچ مجازی شامل گزینه MAC address changes است. این گزینه ترافیکی را تحت تأثیر قرار می دهد که یک ماشین مجازی دریافت می کند.

وقتی که گزینه MAC address changes به Accept تنظیم شده باشد، ESXi درخواست های مبنی بر تغییر آدرس MAC مؤثر به آدرسی متفاوت با آدرس MAC اولیه را می پذیرد.

وقتی که گزینه MAC address changes به Reject تنظیم شده باشد، ESXi به درخواست های مبنی بر تغییر آدرس MAC مؤثر به آدرسی متفاوت با آدرس MAC اولیه توجهی نمی کند. این تنظیمات از میزبان در مقابل جعل MAC محافظت می کند. پورتی که آداپتور ماشین مجازی از آن برای ارسال درخواست استفاده می کند غیرفعال شده و آداپتور ماشین مجازی هیچ فریم دیگری را دریافت نمی کند تا زمانی که آدرس MAC مؤثر با آدرس MAC اولیه مطابقت داشته باشد. سیستم عامل مهمان تشخیص نمی دهد که به درخواستش مبنی بر تغییر آدرس MAC، اهمیتی داده نشده است.

**نکته:** آغازکننده ی iSCSI متکی بر این است که بتواند درخواست تغییر آدرس MAC را از انواع خاصی از ذخیره سازی ها دریافت کند. در صورتی که از ESXi iSCSI با ذخیره سازی iSCSI استفاده می کنید، گزینه MAC address changes را به Accept تنظیم کنید.

## ۳-۲ انتقال های جعلی

گزینه Forged transmits ترافیکی را تحت تأثیر قرار می دهد که از یک ماشین مجازی انتقال داده شده است. زمانی که این گزینه به Accept تنظیم شده باشد، ESXi آدرس MAC منبع را با آدرس MAC مؤثر مقایسه نمی کند. برای محافظت در مقابل جعل MAC، می توانید گزینه Forged transmits را به Reject تنظیم کنید. اگر این کار را انجام دهید میزبان، آدرس MAC منبع که توسط سیستم عامل مهمان انتقال داده شده است را با

آدرس MAC مؤثر ماشین مجازی خود مقایسه می‌کند. در صورتی که این دو آدرس بر هم منطبق نباشند، میزبان ESXi بسته را نادیده می‌گیرد.

سیستم عامل مهمان تشخیص نمی‌دهد که آداپتور ماشین مجازی اش نمی‌تواند بسته‌ها را با استفاده از آدرس MAC جعلی ارسال کند. میزبان ESXi هر بسته‌ای با آدرس‌های جعلی را، قبل از تحویل، می‌پذیرد، و سیستم عامل مهمان ممکن است فرض را بر این بگذارد که بسته‌ها نادیده گرفته شده‌اند.

### ۳ جداسازی ترافیک شبکه با استفاده از VLANها

شبکه‌های محلی مجازی<sup>۸</sup> (VLANها) به ما اجازه می‌دهند که یک شبکه را به چندین دامنه همه‌پخشی منطقی در لایه ۲ از پشته پروتکلی شبکه، قطعه‌بندی کنیم.

#### ۱-۳ مزایای استفاده از VLAN در vSphere

بیکربندی VLAN در محیط vSphere مزایای خاصی را فراهم می‌کند.

- میزبان‌های ESXi را به یک توپولوژی VLAN که از قبل وجود دارد یکپارچه می‌کند.
- جداسازی و امن سازی ترافیک شبکه را انجام می‌دهد.
- ازدحام ترافیک شبکه را کاهش می‌دهد.

#### ۲-۳ حالت‌های برجسب گذاری VLAN

vSphere از سه حالت برجسب گذاری<sup>۹</sup> VLAN در ESXi پشتیبانی می‌کند: برجسب گذاری سوئیچ خارجی<sup>۱۰</sup> (EST)، برجسب گذاری سوئیچ مجازی<sup>۱۱</sup> (VST)، و برجسب گذاری مهمان مجازی<sup>۱۲</sup> (VGT). توضیحات مربوط به این سه حالت در جدول ۱ آمده است.

<sup>۸</sup> Virtual Local Area Networks

<sup>۹</sup> Tagging

<sup>۱۰</sup> External Switch Tagging

<sup>۱۱</sup> Virtual Switch Tagging

<sup>۱۲</sup> Virtual Guest Tagging

جدول ۱ حالت های مختلف برچسب گذاری VLAN

توصیف	شناسه VLAN روی پورت گروه های سوئیچ	حالت برچسب گذاری
سوئیچ فیزیکی برچسب گذاری VLAN را انجام می دهد. آداپتورهای شبکه میزبان به پورت های دسترسی سوئیچ فیزیکی متصل می شوند.	صفر	EST
سوئیچ مجازی قبل از این که بسته ها میزبان را ترک کنند، برچسب گذاری VLAN را انجام می دهد. آداپتورهای شبکه میزبان باید به پورت های trunk سوئیچ فیزیکی متصل شوند.	بین ۱ تا ۴۰۹۴	VST
ماشین مجازی برچسب گذاری VLAN را انجام می دهد. سوئیچ مجازی هنگامی که بسته ها را بین پشته شبکه ماشین مجازی و سوئیچ خارجی انتقال می دهد، برچسب های VLAN را حفظ می کند. آداپتورهای شبکه میزبان باید به پورت های trunk سوئیچ فیزیکی متصل شوند.  سوئیچ توزیع شده vSphere از یک نسخه اصلاح شده از VGT استفاده می کند. به دلایل امنیتی، شما می توانید یک سوئیچ توزیع شده را به گونه ای پیکربندی کنید تا تنها بسته هایی را که به VLAN های خاصی تعلق دارند را منتقل کند.	<ul style="list-style-type: none"> <li>• ۴۰۹۵ برای سوئیچ استاندارد</li> <li>• محدوده و VLAN های منحصر به فرد برای سوئیچ توزیع شده</li> </ul>	VGT

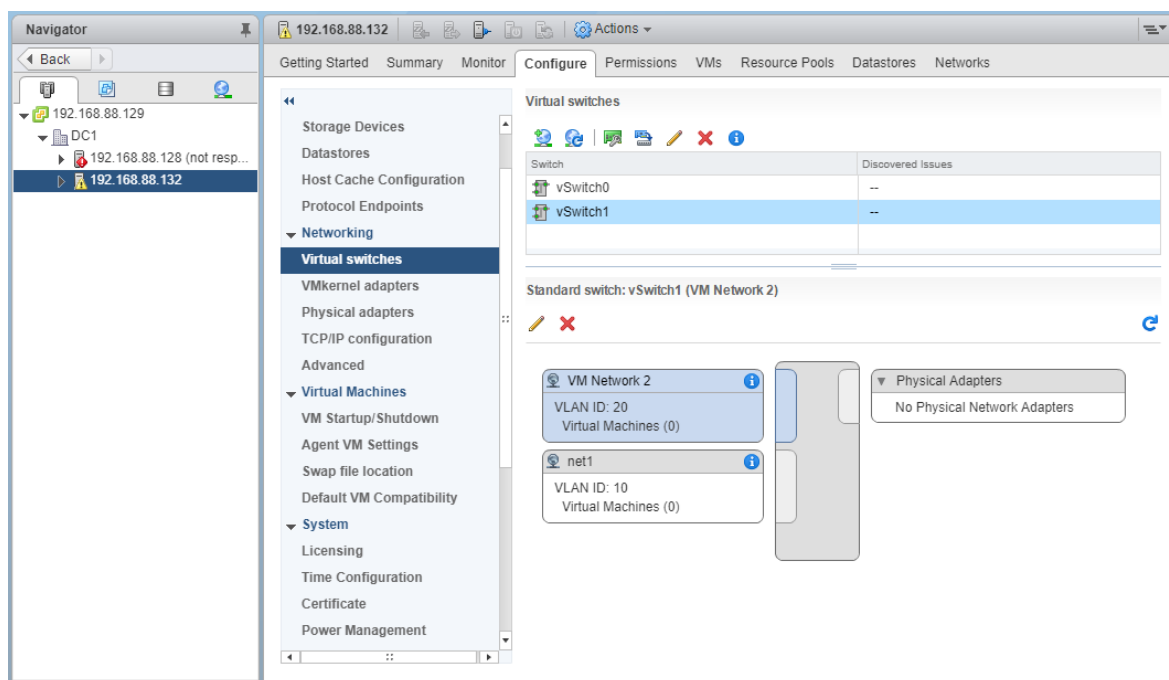
یادآودی: به منظور استفاده از VGT باید یک راه انداز VLAN trunking 802.1Q روی سیستم عامل مهمان ماشین مجازی نصب شده باشد.



به منظور ایجاد یک پورت گروه با یک VLAN ID مورد نظر بر روی یک سوئیچ مجازی استاندارد به صورت زیر عمل کنید.

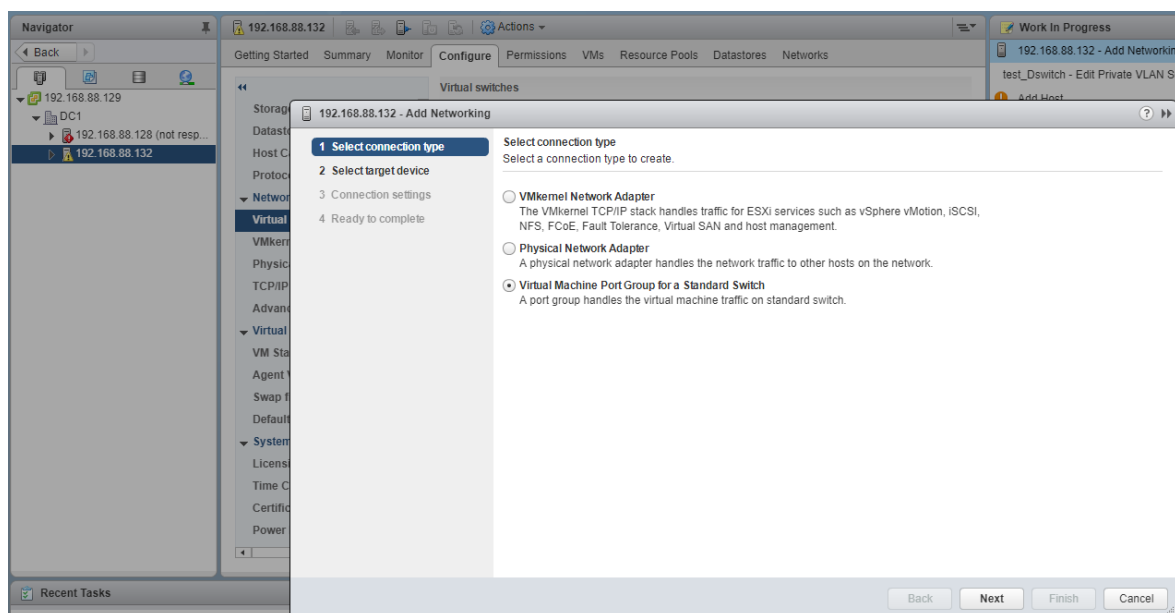
روش:

۱. در vSphere WebClient، میزبان مورد نظر را انتخاب کنید.
۲. به برگه Configure رفته، و در بخش Networking گزینه Virtual switches را انتخاب کنید. پنجره‌ای مشابه با پنجره زیر نمایش داده می‌شود که در آن لیست سوئیچ‌های مجازی استاندارد موجود بر روی این میزبان وجود دارد.



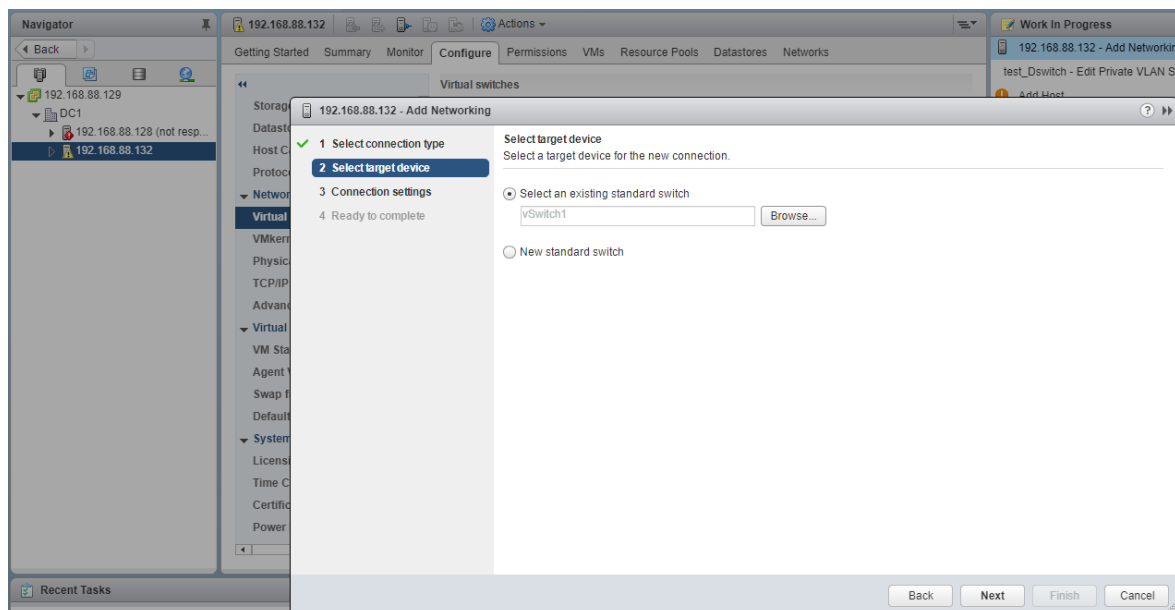
شکل ۲ ایجاد یک پورت گروه (۱)

۳. آیکون Add host networking را کلیک کرده و در صفحه نمایش داده شده Virtual Machine Port Group for a Standard Switch را انتخاب کنید.



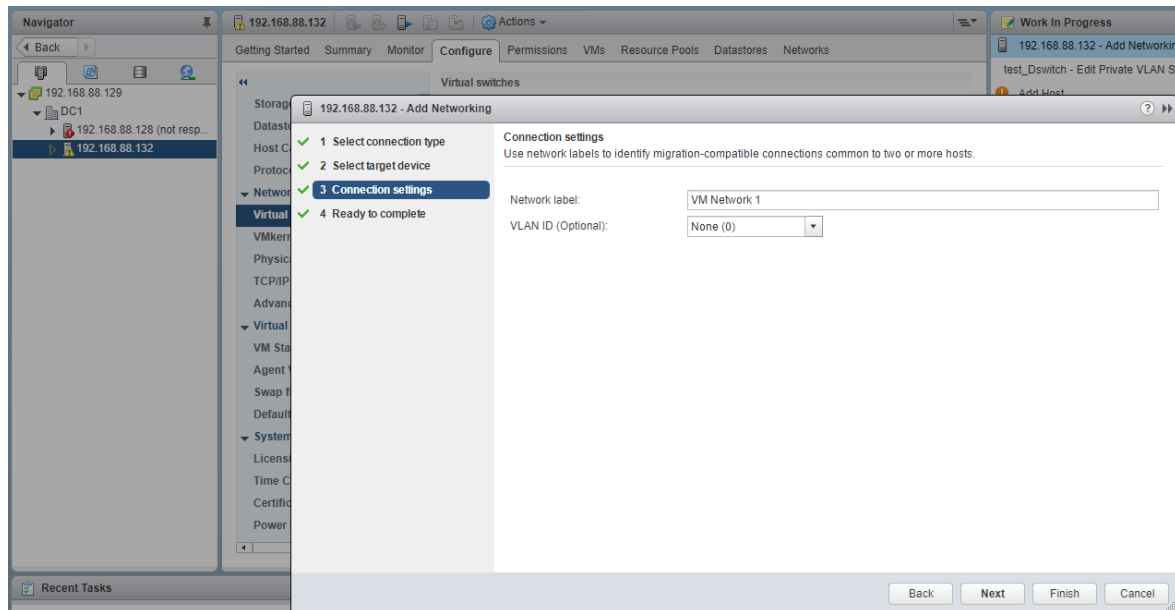
شکل ۳ ایجاد یک پورت گروه (۲)

۴. در قسمت Select an existing standard switch مورد نظر را انتخاب کنید.



شکل ۴ ایجاد یک پورت گروه (۳)

۵. در صفحه نمایش داده شده، Network label و VLAN ID مورد نظر را وارد کنید.



شکل ۵ ایجاد یک پورت گروه (۴)

۶ در نهایت با کلیک بر روی دکمه Finish پورت گروه مورد نظر با VLAN ID مشخص شده ساخته می شود.

### ۳-۳ VLAN های خصوصی

VLAN های خصوصی<sup>۱۳</sup> برای حل محدودیت های مربوط به شناسه VLAN مورد استفاده قرار می گیرند، و این کار را با اضافه کردن قطعه های بیشتر به یک دامنه همه پخش منطقی و تبدیل آن به چندین زیر دامنه ی همه پخش منطقی کوچکتر انجام می دهند.

یک VLAN خصوصی توسط شناسه VLAN اصلی<sup>۱۴</sup> خود شناخته می شود. یک شناسه VLAN اصلی می تواند چندین شناسه VLAN جانبی<sup>۱۵</sup> را همراه با خود داشته باشد. VLAN های اصلی بی قاعده هستند، و بنابراین پورت های روی یک VLAN خصوصی می توانند با پورت های پیکربندی شده به عنوان VLAN اصلی، ارتباط داشته باشند. پورت های روی یک VLAN جانبی می توانند Isolated باشند، یعنی تنها با پورت های بی

<sup>۱۳</sup> Private VLANs

<sup>۱۴</sup> Primary VLAN ID

<sup>۱۵</sup> Secondary VLAN ID

قاعده ارتباط داشته باشند، یا Community باشند، یعنی هم با پورت‌های بی‌قاعده و هم با سایر پورت‌های VLAN جانبی خود ارتباط داشته باشند.

برای این که بتوانیم از VLAN‌های خصوصی بین یک میزبان و بقیه شبکه فیزیکی استفاده کنیم، سوئیچ فیزیکی متصل به میزبان لازم است که سازگار با VLAN خصوصی بوده و با شناسه‌های VLAN که توسط ESXi استفاده می‌شوند، پیکربندی شده باشد. برای سوئیچ‌های فیزیکی که از یادگیری مبتنی بر MAC+VLAN ID پویا استفاده می‌کنند، همه شناسه‌های VLAN خصوصی متناظر باید ابتدا در پایگاه داده VLAN سوئیچ وارد شوند.

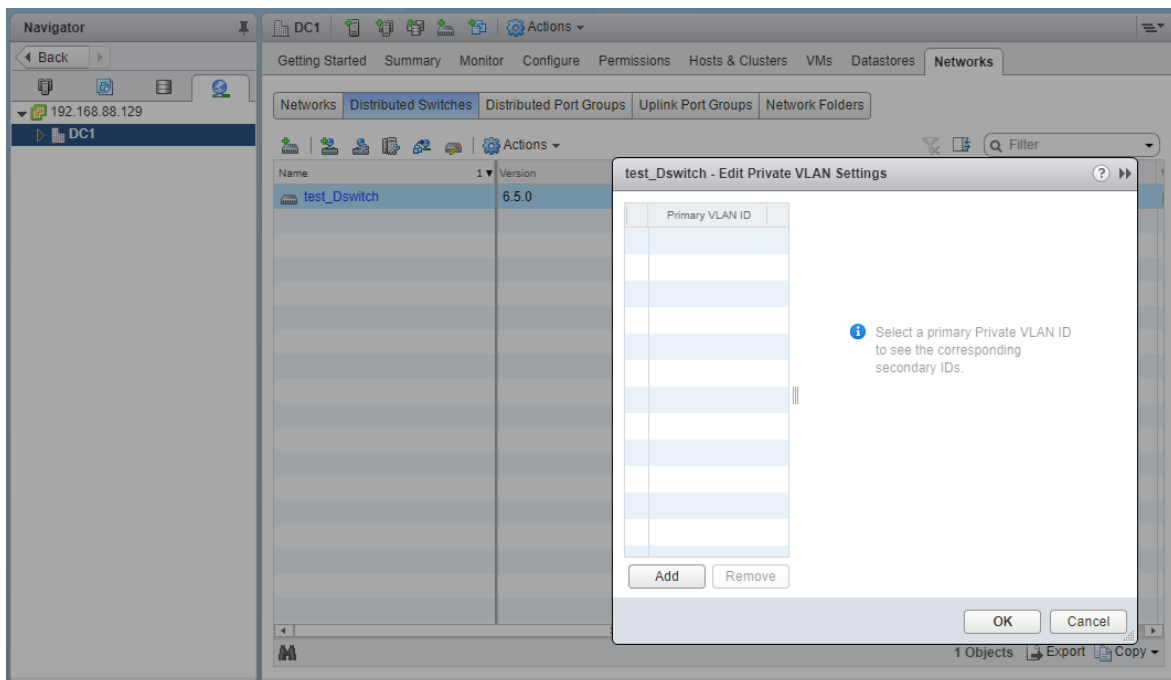
### ۴-۳ ایجاد یک VLAN خصوصی

VLAN‌های خصوصی مورد نیاز را روی سوئیچ توزیع شده vSphere ایجاد کنید تا توانایی تخصیص پورت‌های توزیع شده برای مشارکت در یک VLAN خصوصی را داشته باشید.

#### روش

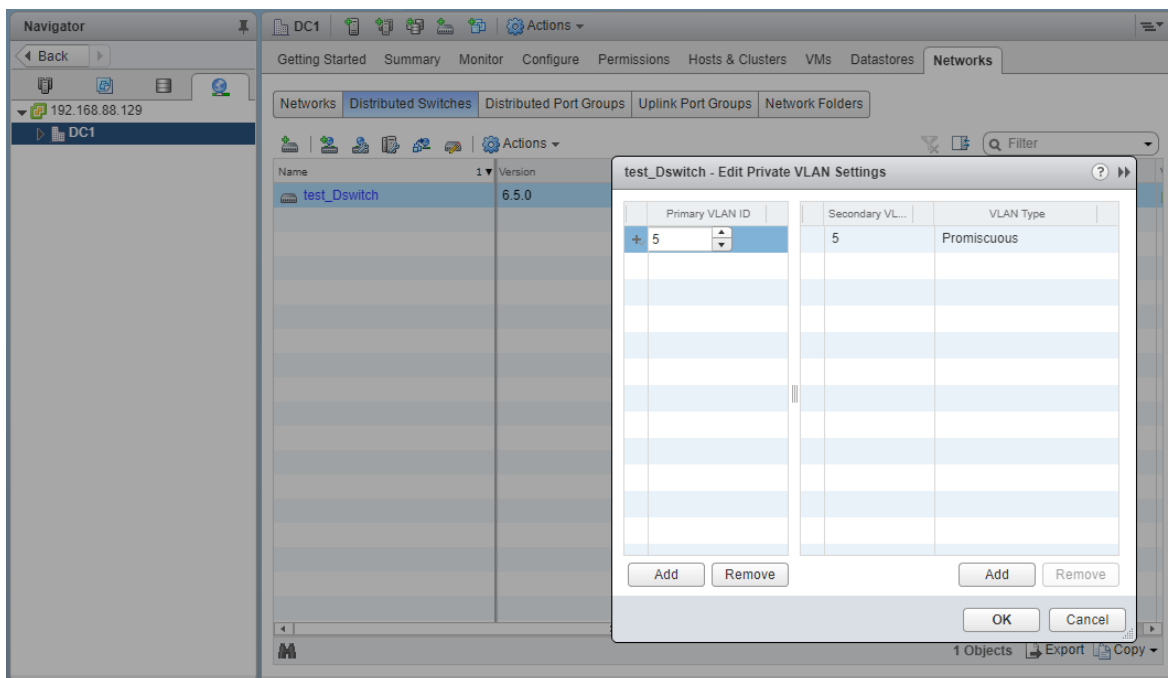
۷. در vSphere WebClient، سوئیچ توزیع شده را انتخاب کنید.

۸. به برگه Configure رفته، Settings را باز کرده و Private VLAN را انتخاب و Edit را کلیک کنید.



شکل ۶ ایجاد یک VLAN خصوصی (۱)

۹. برای اضافه کردن یک VLAN اصلی، زیر Primary VLAN ID بر روی Add کلیک کرده و ID یک VLAN اصلی را وارد کنید.



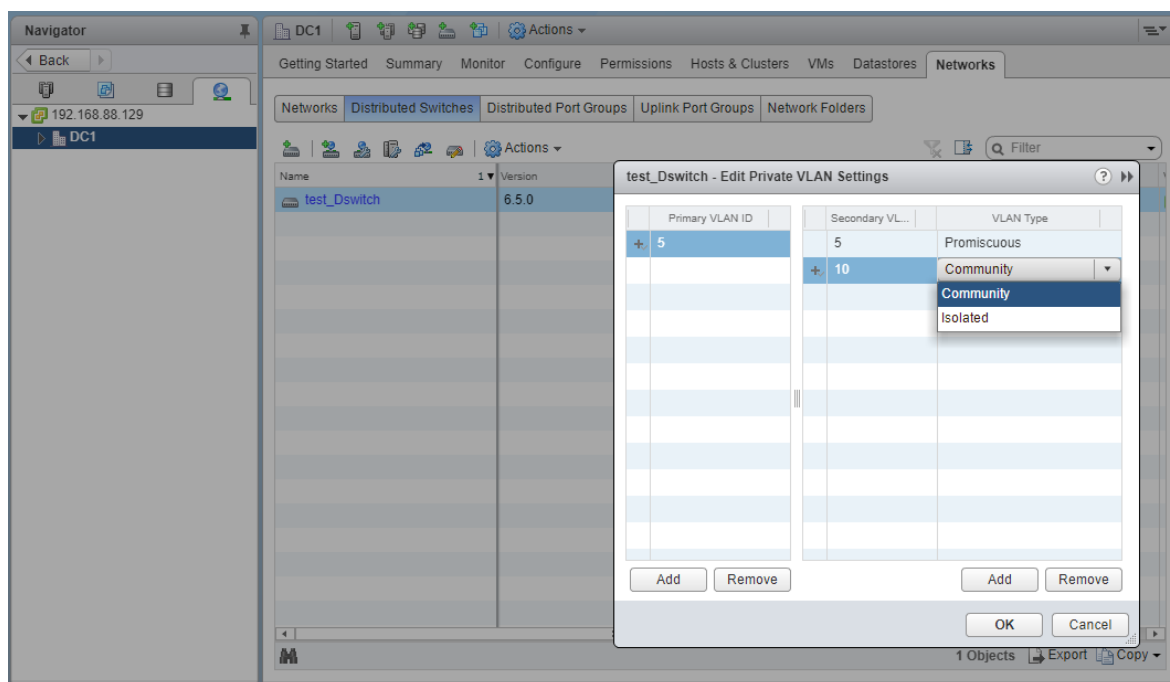
شکل ۷ ایجاد یک VLAN خصوصی (۲)

۱۰. روی علامت + که در جلوی شناسه VLAN اصلی قرار دارد کلیک کرده تا VLAN اصلی به لیست اضافه شود. VLAN خصوصی اصلی در جدول شناسه VLAN خصوصی جانبی نیز نمایش داده می شود.

۱۱. برای اضافه کردن یک VLAN جانبی، در پنجره سمت راست، بر روی Add کلیک کرده و شناسه VLAN را وارد کنید.

۱۲. روی علامت + که در جلوی شناسه VLAN جانبی قرار دارد کلیک کرده تا آن را به لیست اضافه کنید.

۱۳. از منوی کشویی ستون secondary VLAN type، Isolated یا Community را انتخاب کنید.



شکل ۸ ایجاد یک VLAN خصوصی (۲)

۱۴. OK را کلیک کنید.

### ۳-۵ حذف یک VLAN خصوصی اصلی

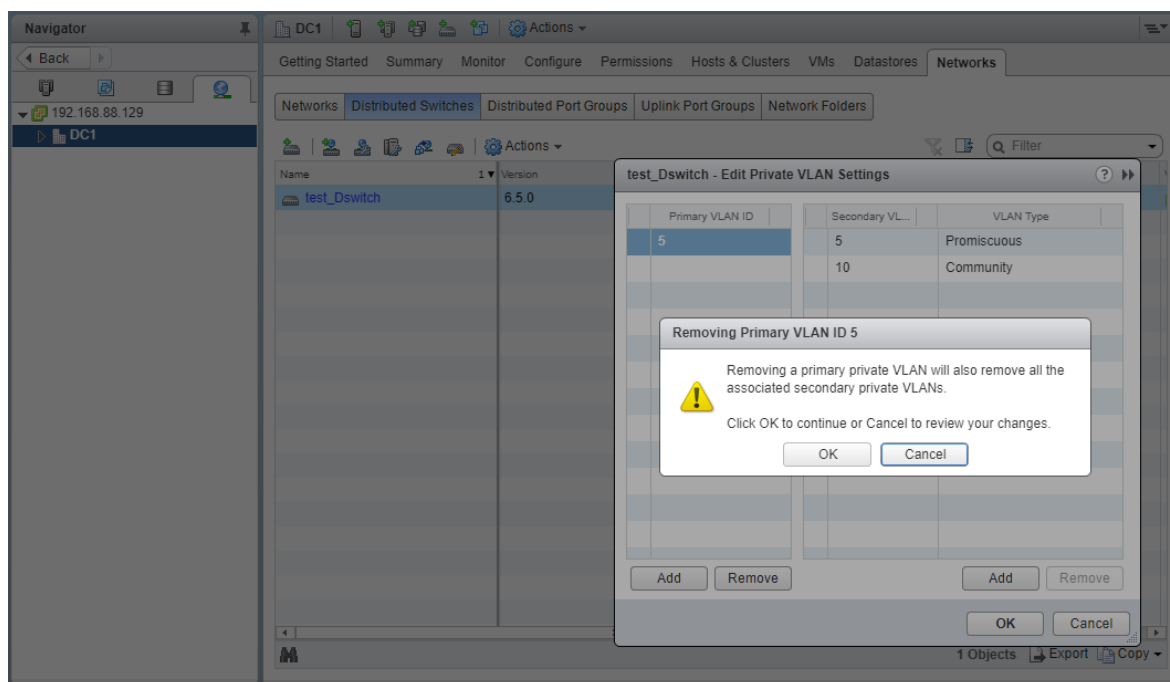
بهتر است که VLAN های خصوصی اصلی بدون استفاده را از پیکربندی سوئیچ توزیع شده vSphere خود حذف کنید. زمانی که یک VLAN خصوصی اصلی را حذف می کنید، تمام VLAN های خصوصی جانبی مرتبط با آن نیز حذف می شوند.

#### پیش نیازها

مطمئن شوید که هیچ پورت گروهی از VLAN اصلی و VLAN های جانبی مرتبط با آن استفاده نمی کند.

#### روش

۱. در vSphere WebClient، سوئیچ توزیع شده را انتخاب کنید.
۲. به برگه Configure رفته، Settings را باز کرده و Private VLAN را انتخاب کنید.
۳. Edit را کلیک کنید.
۴. VLAN خصوصی اصلی مورد نظر را انتخاب کرده و بر روی Remove و سپس OK کلیک کنید.



شکل ۹ حذف یک VLAN خصوصی اصلی

### ۶-۳ حذف یک VLAN خصوصی جانبی

بهتر است که VLAN های خصوصی جانبی بدون استفاده را از پیکربندی سوئیچ توزیع شده vSphere خود حذف کنید.

#### پیش نیازها

مطمئن شوید که هیچ پورت گروهی از VLAN جانبی استفاده نمی کند.

#### روش

۱. در vSphere WebClient، سوئیچ توزیع شده را انتخاب کنید.
۲. به برگه Configure رفته، Settings را باز کرده و Private VLAN را انتخاب کنید.
۳. Edit را کلیک کنید.
۴. یک VLAN خصوصی اصلی را انتخاب کنید، VLAN های خصوصی جانبی مرتبط با آن در سمت راست ظاهر می شوند.
۵. VLAN خصوصی جانبی مورد نظر را انتخاب کنید.
۶. بر روی Remove و سپس OK کلیک کنید.

## ۴ پیکربندی SNMP

از پیکربندی صحیح SNMP مطمئن شوید. اگر SNMP به صورت درست پیکربندی نشده باشد، اطلاعات تحت نظارت می‌توانند به یک میزبان مخرب فرستاده شوند. سپس میزبان مخرب می‌تواند از این اطلاعات استفاده کرده و طراحی یک حمله را انجام دهد. SNMP باید بر روی هر میزبان ESXi پیکربندی شود. شما می‌توانید از vCLI، PowerCLI یا vSphere Web Services SDK برای پیکربندی استفاده کنید.

### روش

۱. دستور `esxcli system snmp get` را اجرا کنید تا تعیین شود که آیا میزبان در حال استفاده از SNMP است.

```
The ESXi Shell can be disabled by an administrative user. See the
vSphere Security documentation for more information.
[root@localhost:~] esxcli system snmp get
Authentication:
Communities:
Enable: false
Engineid:
Hwsrc: indications
Largestorage: true
Loglevel: info
Notraps:
Port: 161
Privacy:
Remoteusers:
Syscontact:
Syslocation:
Targets:
Users:
V3targets:
[root@localhost:~]
```

شکل ۱۰ بررسی فعال بودن SNMP

۲. اگر سیستم شما به SNMP نیاز دارد، با اجرای دستور `esxcli system snmp set --enable true` مطمئن شوید که در حال اجرا است.

## ۵ امنیت پروتکل اینترنت

امنیت پروتکل اینترنت (IPsec) ارتباطات IP که از یک میزبان می‌آیند یا به یک میزبان می‌رسند را امن می‌کند. میزبان‌های ESXi از IPsec با استفاده از IPv6 پشتیبانی می‌کنند.



وقتی که IPsec را روی یک میزبان تنظیم می‌کنید، در حقیقت احراز اصالت و رمزنگاری را برای بسته‌های ورودی و خروجی فعال می‌کنید. زمان و چگونگی رمزنگاری ترافیک IP بستگی به نحوه‌ی تنظیم انجمن‌های امنیتی<sup>۱۶</sup> و سیاست‌های امنیتی<sup>۱۷</sup> دارد.

یک انجمن امنیتی مشخص می‌کند که سیستم چگونه ترافیک را رمزنگاری کند. زمانی که یک انجمن امنیتی را ایجاد می‌کنید، منبع و مقصد، پارامترهای رمزنگاری، و یک نام برای انجمن امنیتی را مشخص می‌کنید.

یک سیاست امنیتی مشخص می‌کند که سیستم چه زمانی باید رمزنگاری را انجام دهد. سیاست امنیتی شامل اطلاعات منبع و مقصد، پروتکل و جهتی است که ترافیک باید رمزنگاری شود، حالت (انتقال<sup>۱۸</sup> یا تونل<sup>۱۹</sup>)، و انجمن امنیتی مورد استفاده است.

## ۱-۵ فهرست کردن انجمن‌های امنیتی موجود

ESXi می‌تواند تمام انجمن‌های امنیتی موجود برای استفاده توسط سیاست‌های امنیتی را فهرست کند. این فهرست هم شامل انجمن‌های امنیتی ایجاد شده توسط کاربر است و هم شامل انجمن‌های امنیتی که VMkernel با استفاده از Internet Key Exchange نصب کرده است. می‌توان با استفاده از دستور `esxcli` vSphere CLI، فهرستی از انجمن‌های امنیتی موجود را مشاهده کرد.

### روش

- در خط فرمان، دستور `esxcli network ip ipsec sa list` را وارد کنید.

```
[root@localhost:~] esxcli network ip ipsec sa list
Name Source Address Destination Address State SPI Mode Encryption Algorithm Integrity Algorithm Lifetime
-----
sa1 fe80::ec5a:5699:9ac4:a2fe fe80::20c:29ff:fe63:b6a0 mature 0x1000 transport 3des-cbc hmac-shal infinite
[root@localhost:~]
```

شکل ۱۱ نمایش فهرست انجمن‌های امنیتی موجود

<sup>۱۶</sup> security associations

<sup>۱۷</sup> security policies

<sup>۱۸</sup> Transport

<sup>۱۹</sup> Tunnel

## ۲-۵ اضافه کردن یک انجمن امنیتی IPsec

می‌توان یک انجمن امنیتی را برای مشخص کردن پارامترهای رمزنگاری برای ترافیک IP مشخص، اضافه کرد. این کار را می‌توان با استفاده از دستور esxcli vSphere CLI انجام داد.

### روش

- در خط فرمان، دستور `esxcli network ip ipsec sa add` را با یک یا چند تا از گزینه‌هایی که در جدول ۲ آمده است، وارد کنید.

جدول ۲ گزینه‌های موجود برای دستور اضافه کردن انجمن امنیتی جدید

گزینه	توصیف
<code>--sa-source= source address</code>	ضروری. آدرس منبع را مشخص می‌کند.
<code>--sa-destination= destination address</code>	ضروری. آدرس مقصد را مشخص می‌کند.
<code>--sa-mode= mode</code>	ضروری. حالت انتقال یا تونل را مشخص می‌کند.
<code>--sa-spi= security parameter index</code>	ضروری. شاخص پارامتر امنیتی را مشخص می‌کند. شاخص پارامتر امنیتی، انجمن امنیتی را به میزبان معرفی می‌کند. این گزینه باید هگزادسیمال با پیشوند 0x باشد. هر انجمن امنیتی که ایجاد می‌کنید باید یک ترکیب منحصر به فرد از پروتکل و شاخص پارامتر امنیتی داشته باشد.
<code>--encryption-algorithm= encryption algorithm</code>	ضروری. با استفاده از یکی از پارامترهای زیر الگوریتم رمزنگاری را مشخص می‌کند. <ul style="list-style-type: none"> <li>• 3des-cbc</li> <li>• aes128-cbc</li> <li>• null (رمزنگاری انجام نمی‌دهد)</li> </ul>
<code>--encryption-key= encryption key</code>	این گزینه زمانی مورد نیاز است که یک الگوریتم رمزنگاری مشخص شده باشد. کلید رمزنگاری را تعیین می‌کند. کلیدها را

	می توان به صورت متن اسکی یا با یک هگزادسیمال با یک پیشوند 0x، وارد کرد.
--integrity-algorithm= authentication algorithm	ضروری. الگوریتم احرازاصالت را مشخص می کند، hmac-sha1 یا hmac-sha2-256.
--integrity-key= authentication key	ضروری. کلید احرازاصالت را تعیین می کند. کلیدها را می توان به صورت متن اسکی یا با یک هگزادسیمال با یک پیشوند 0x، وارد کرد.
--sa-name=name	ضروری. یک نام برای انجمن امنیتی ارائه می کند.

#### مثال: دستور ایجاد انجمن امنیتی جدید

مثال زیر به منظور خوانایی بیشتر حاوی خطوط اضافی است.

```
esxcli network ip ipsec sa add
--sa-source 3ffe:501:ffff:0::a
--sa-destination 3ffe:501:ffff:0001:0000:0000:0000:0001
--sa-mode transport
--sa-spi 0x1000
--encryption-algorithm 3des-cbc
--encryption-key 0x6970763672656164796c6f676f336465736362636f757432
--integrity-algorithm hmac-sha1
--integrity-key 0x6970763672656164796c6f67736861316f757432
--sa-name sa1
```

```
[root@localhost:~] esxcli network ip ipsec sa add --sa-source fe80::ec5a:5699:9ac4:a2fe --sa-destination fe80:
:20c:29ff:fe63:b6a0 --sa-mode transport --sa-spi 0x1000 --encryption-algorithm 3des-cbc --encryption-key 0x697
0763672656164796c6f676f336465736362636f757432 --integrity-algorithm hmac-sha1 --integrity-key 0x69707636726561
64796c6f67736861316f757432 --sa-name sa1
[root@localhost:~] █
```

شکل ۱۲ ایجاد انجمن امنیتی جدید

### ۳-۵ حذف یک انجمن امنیتی IPsec

می توان یک انجمن امنیتی را با استفاده از دستور ESXCLI vSphere CLI command حذف کرد. به این منظور باید اطمینان حاصل کنید که انجمن امنیتی که قصد حذف کردن آن را دارید، در حال حاضر در حال استفاده نباشد. در صورتی که سعی کنید که یک انجمن امنیتی که در حال استفاده است را حذف کنید، عملیات با شکست مواجه می شود.

روش

- در خط فرمان، دستور زیر را وارد کنید.

```
esxcli network ip ipsec sa remove --sa-name security_association_name
```

### ۴-۵ فهرست کردن سیاست های امنیتی IPsec موجود

فهرست سیاست های امنیتی موجود را می توان با استفاده از دستور ESXCLI vSphere CLI مشاهده کرد.

روش

- در خط فرمان دستور esxcli network ip ipsec sp list را وارد کنید.

```
[root@localhost:~]# esxcli network ip ipsec sp list
Name Source Address Source Port Destination Address Destination Port Protocol Flow Action Mode SA Name
-----
sp1 fe80::ec5a:5699:9ac4:a2fe/64 0 fe80::20c:29ff:fe63:b6a0/64 22 tcp out discard unknown none
[root@localhost:~]#
```

شکل ۱۳ نمایش فهرست سیاست های امنیتی موجود

### ۵-۵ ایجاد یک سیاست امنیتی IPsec

برای تعیین زمان استفاده از پارامترهای احرازصالت و رمزنگاری که در یک انجمن امنیتی تنظیم شده است، باید یک سیاست امنیتی تعریف شود. یک سیاست امنیتی را می توان با استفاده از دستور ESXCLI vSphere CLI command اضافه کرد. قبل از ایجاد یک سیاست امنیتی، بایستی یک انجمن امنیتی با پارامترهای احرازصالت و رمزنگاری مناسب، اضافه شود.

روش

- در خط فرمان دستور esxcli network ip ipsec sp add را با یکی یا بیشتر از گزینه های زیر وارد کنید.

جدول ۳ گزینه‌های موجود برای دستور اضافه کردن سیاست امنیتی جدید

گزینه	توصیف
--sp-source= source address	ضروری. آدرس منبع و طول پیشوند را مشخص می‌کند.
--sp-destination= destination address	ضروری. آدرس مقصد و طول پیشوند را مشخص می‌کند.
--source-port= port	ضروری. پورت مبدأ را مشخص می‌کند. پورت مبدأ باید یک عدد بین صفر تا ۶۵۵۳۵ باشد.
--destination-port= port	ضروری. پورت مقصد را مشخص می‌کند. پورت مقصد باید یک عدد بین صفر تا ۶۵۵۳۵ باشد.
--upper-layer-protocol= protocol	پروتکل لایه بالاتر را مشخص می‌کند که یکی از موارد زیر است. <ul style="list-style-type: none"> <li>• tcp</li> <li>• udp</li> <li>• icmp6</li> <li>• any</li> </ul>
--flow-direction= direction	جهتی را مشخص می‌کند که قصد نظارت بر ترافیک آن را داریم، که یکی از موارد in یا out است.
--action= action	به وسیله‌ی یکی از موارد زیر، مشخص می‌کند که در مواجه شدن با ترافیکی با پارامترهای مشخص شده چه عملی انجام شود. <ul style="list-style-type: none"> <li>• none: هیچ عملی انجام نمی‌دهد.</li> <li>• discard: اجازه نمی‌دهد که داده وارد یا خارج شود.</li> <li>• ipsec: از اطلاعات احراز اصالت و رمزنگاری عرضه شده در انجمن امنیتی استفاده می‌کند تا تعیین کند که آیا داده‌ها از یک منبع امن می‌آیند.</li> </ul>

--sp-mode= mode	حالت tunnel یا transport را مشخص می کند.
--sa-name=security association name	ضروری. نام انجمن امنیتی را مشخص می کند که این سیاست امنیتی باید از آن استفاده کند.
--sp-name=name	ضروری. یک نام برای سیاست امنیتی ارائه می کند.

### مثال: دستور ایجاد سیاست امنیتی جدید

مثال زیر به منظور خوانایی بیشتر حاوی خطوط اضافی است.

```
esxcli network ip ipsec add
--sp-source=2001:db8:1::/64
--sp-destination=2002:db8:1::/64
--source-port=23
--destination-port=25
--upper-layer-protocol=tcp
--flow-direction=out
--action=ipsec
--sp-mode=transport
--sa-name=sa1
--sp-name=sp1
```

### ۶-۵ حذف یک سیاست امنیتی IPsec

یک سیاست امنیتی از یک میزبان EXSi را می توان با استفاده از دستور ESXCLI vSphere CLI حذف کرد. به این منظور باید اطمینان حاصل کنید که سیاست امنیتی که قصد حذف کردن آن را دارید، در حال حاضر در حال استفاده نباشد. در صورتی که سعی کنید که یک سیاست امنیتی که در حال استفاده است را حذف کنید، عملیات با شکست مواجه می شود.

#### روش

- در خط فرمان، دستور زیر را وارد کنید.

```
esxcli network ip ipsec sp remove --sp-name security policy name
```

برای حذف همه سیاست‌های امنیتی می‌توان از دستور `esxcli network ip ipsec sp remove --remove-all` استفاده کرد.

## ۶ بهترین تجربه‌های امنیتی شبکه vSphere

با دنبال کردن بهترین تجربه‌ها برای امن کردن شبکه می‌توانید از صحت محیط vSphere خود اطمینان حاصل کنید.

### ۱-۶ توصیه‌های عمومی امنیت شبکه

دنبال کردن توصیه‌های عمومی امنیت شبکه، اولین قدم در امن سازی محیط شبکه است. پس از آن می‌توانید به موارد خاصی مانند امن کردن شبکه با استفاده از دیواره آتش یا استفاده از IPsec بپردازید.

- در صورتی که پروتکل درخت پوشا<sup>۲۰</sup> (STP) فعال است، مطمئن شوید که پورت‌های سوئیچ فیزیکی به Portfast پیکربندی شده‌اند. از آنجایی که سوئیچ‌های مجازی VMware از STP پشتیبانی نمی‌کنند، پورت‌های سوئیچ فیزیکی متصل به یک ESXi باید به منظور اجتناب از به وجود آمدن حلقه در شبکه سوئیچ فیزیکی، به Portfast پیکربندی شده باشند. در صورتی که Portfast تنظیم نشده باشد، ممکن است مسائل و مشکلات مربوط به کارایی و اتصال به وجود آید.
- مطمئن شوید که ترافیک Netflow برای یک سوئیچ مجازی توزیع شده<sup>۲۱</sup> تنها به آدرس‌های IP جمع کننده<sup>۲۲</sup>‌های مجاز فرستاده می‌شود. از آنجا که ارسال‌های Netflow رمزنگاری نمی‌شوند و ممکن است شامل اطلاعاتی در مورد شبکه مجازی باشند، این اطلاعات پتانسیل انجام حمله مردی در میانه موفق را افزایش می‌دهد. همچنین مطمئن شوید که همه آدرس‌های IP هدف Netflow صحیح هستند.

<sup>۲۰</sup> Spanning tree protocol

<sup>۲۱</sup> Distributed virtual switch

<sup>۲۲</sup> Collector

- مطمئن شوید که تنها مدیران مجاز با استفاده از کنترل دسترسی های مبتنی بر نقش، به مؤلفه های شبکه مجازی دسترسی دارند. به عنوان مثال، به مدیران ماشین مجازی تنها اجازه دسترسی به پورت گروه هایی<sup>۳۳</sup> را بدهید که ماشین های مجازی شان در آن ها قرار دارند. به مدیران شبکه اجازه دسترسی به همه مؤلفه های شبکه مجازی را بدهید، اما اجازه دسترسی به ماشین های مجازی را نه. محدود کردن دسترسی ها خطر پیکربندی های اشتباه، چه تصادفی باشد و چه مخرب، را کاهش داده و مفاهیم امنیتی کلیدی برای جدا کردن وظایف و دادن کمترین امتیازات را اجرا می کند.
- مطمئن شوید که پورت گروه ها به مقدار Native VLAN پیکربندی نشده اند. سوئیچ های فیزیکی از VLAN 1 به عنوان Native VLAN استفاده می کنند. فریم های روی یک Native VLAN با 1 برچسب گذاری نمی شوند. ESXi دارای Native VLAN نیست. فریم هایی که در یک پورت گروه با VLAN مشخص هستند برچسب دارند، و فریم هایی که در پورت گروهی هستند که برای آن VLAN تعریف نشده است برچسب ندارند. این مسأله می تواند یک مشکل را به وجود آورد. به عنوان مثال، فریم های روی VLAN 1 از یک سوئیچ فیزیکی سیسکو برچسب گذاری نشده اند، چون VLAN 1 روی آن سوئیچ فیزیکی Native VLAN است. اما، فریم هایی از میزبان ESXi که مربوط به VLAN 1 هستند با 1 برچسب گذاری شده اند. در نتیجه، ترافیکی که از یک میزبان ESXi به مقصد Native VLAN ارسال می شود به صورت درست مسیریابی نمی شود، چون به جای این که برچسب گذاری نشده باشد با 1 برچسب گذاری شده است. ترافیکی از سوئیچ فیزیکی که از Native VLAN می آید نیز قابل مشاهده نیست، چون برچسب گذاری نشده است. اگر پورت گروه سوئیچ مجازی ESXi از Native VLAN ID استفاده کند، ترافیک ماشین های مجازی روی آن پورت قابل مشاهده توسط Native VLAN روی سوئیچ نیست، چون سوئیچ انتظار ترافیک برچسب گذاری نشده را دارد.
- مطمئن شوید که پورت گروه ها برای VLAN های خود به مقادیری که توسط سوئیچ های فیزیکی رزرو شده است، پیکربندی نشده باشند. سوئیچ های فیزیکی VLAN ID های خاصی را برای اهداف داخلی خود رزرو می کنند و اغلب اجازه عبور به ترافیک هایی که به این مقادیر پیکربندی شده باشند را نمی

<sup>۳۳</sup> Port groups



- دهند. به عنوان مثال، سوئیچ های سیسکو کاتالیست معمولاً VLAN های ۱۰۲۴-۱۰۰۱ و ۴۰۹۴ را رزرو می کنند. استفاده از VLAN های رزرو شده ممکن است موجب وقفه در سرویس شبکه شود.
- مطمئن شوید که پورت گروه ها به VLAN با مقدار ۴۰۹۵ پیکربندی نشده باشند، مگر برای VGT. تنظیم یک پورت گروه به VLAN با مقدار ۴۰۹۵ حالت VGT را فعال می کند. در این حالت، سوئیچ مجازی همه فریم های شبکه را، بدون تغییر در برجسب VLAN به ماشین مجازی عبور می دهد، و برخورد با آن ها را به عهده ماشین مجازی می گذارد.
  - پیکربندی مربوط به نادیده گرفتن<sup>۲۴</sup> پیکربندی های سطح پورت روی یک سوئیچ مجازی توزیع شده، را محدود کنید. نادیده گرفتن پیکربندی سطح پورت، به صورت پیش فرض غیر فعال است. وقتی فعال می شود، شما می توانید برای یک ماشین مجازی، از تنظیمات امنیتی متفاوتی، نسبت به تنظیمات سطح پورت گروه استفاده کنید. برخی ماشین های مجازی خاص نیاز به پیکربندی های منحصر به فردی دارند، اما نظارت در این موارد ضروری است. اگر بر overrideها نظارت نشود، هر کسی که با یک سوئیچ مجازی توزیع شده با پیکربندی امنیت پایین تر، به یک ماشین مجازی دسترسی داشته باشد، ممکن است تلاش کند که از دسترسی خود بهره برداری کند.
  - مطمئن شوید که ترافیک mirror پورت سوئیچ مجازی توزیع شده، فقط به پورت های جمع کننده ی مجاز یا VLAN های مجاز ارسال می شود. یک سوئیچ توزیع شده vSphere می تواند ترافیک را از یک پورت به پورت دیگر mirror کند تا به وسیله های مربوط به ضبط بسته ها اجازه ی جمع آوری جریان های ترافیک خاص را بدهد. Port mirroring یک کپی از همه ترافیک مشخص شده را به صورت غیر رمز شده ارسال می کند. این ترافیک شامل کل داده های بسته های ضبط شده است و در صورت هدایت اشتباه می تواند منجر به افشای کل داده شود. در صورتی که port mirroring مورد نیاز است، مطمئن شوید که تمام VLAN ها، پورت ها و شناسه های uplink مقصد درست هستند.

<sup>۲۴</sup> Override

## ۲-۶ برچسب گذاری مؤلفه های شبکه

شناسایی مؤلفه های متفاوت معماری شبکه شما مهم است و به شما اطمینان می دهد که هیچ خطایی در هنگام رشد شبکه به وجود نمی آید.

بهترین تجربه های زیر را دنبال کنید:

- اطمینان حاصل کنید که پورت گروه ها با یک برچسب شبکه<sup>۲۰</sup> واضح پیکربندی شده اند. این برچسب ها به عنوان یک توصیف گر کاربردی برای پورت گروه شناخته می شوند و به شما کمک می کنند تا در هنگام پیچیده تر شدن شبکه، عملکرد هر پورت گروه را شناسایی کنید.
- اطمینان حاصل کنید که هر سوئیچ توزیع شده ی vSphere دارای برچسب شبکه واضح است که نشان دهنده ی عملکرد یا زیر شبکه IP سوئیچ است. این برچسب به عنوان یک توصیف گر کاربردی برای سوئیچ است، درست همان طور که سوئیچ های فیزیکی نیاز به نام میزبان دارند. به عنوان مثال، شما می توانید یک سوئیچ را با عنوان internal برچسب بزنید تا نشان دهید که آن برای شبکه داخلی است. برچسب یک سوئیچ مجازی استاندارد را نمی توان تغییر داد.

## ۳-۶ مستند سازی و بررسی محیط vSphere VLAN

به منظور اجتناب از مشکلات، به طور مرتب محیط VLAN خود را بررسی کنید. به طور کامل محیط VLAN را مستند کرده و مطمئن شوید که شناسه های VLAN تنها یک بار استفاده می شوند. مستندات شما می تواند به عیب یابی کمک کند و همچنین زمانی که می خواهید محیط را گسترش دهید، این مستندات ضروری است.

روش

۱. اطمینان حاصل کنید که تمام سوئیچ های مجازی و شناسه های VLAN ها به طور کامل مستند شده اند.
۲. اطمینان حاصل کنید که شناسه های VLAN برای همه پورت گروه های مجازی توزیع شده به طور کامل مستند شده اند.

<sup>۲۰</sup> Network label

۳. اطمینان حاصل کنید که شناسه‌های VLAN خصوصی برای همه سوئیچ‌های مجازی توزیع شده به طور کامل مستند شده‌اند.

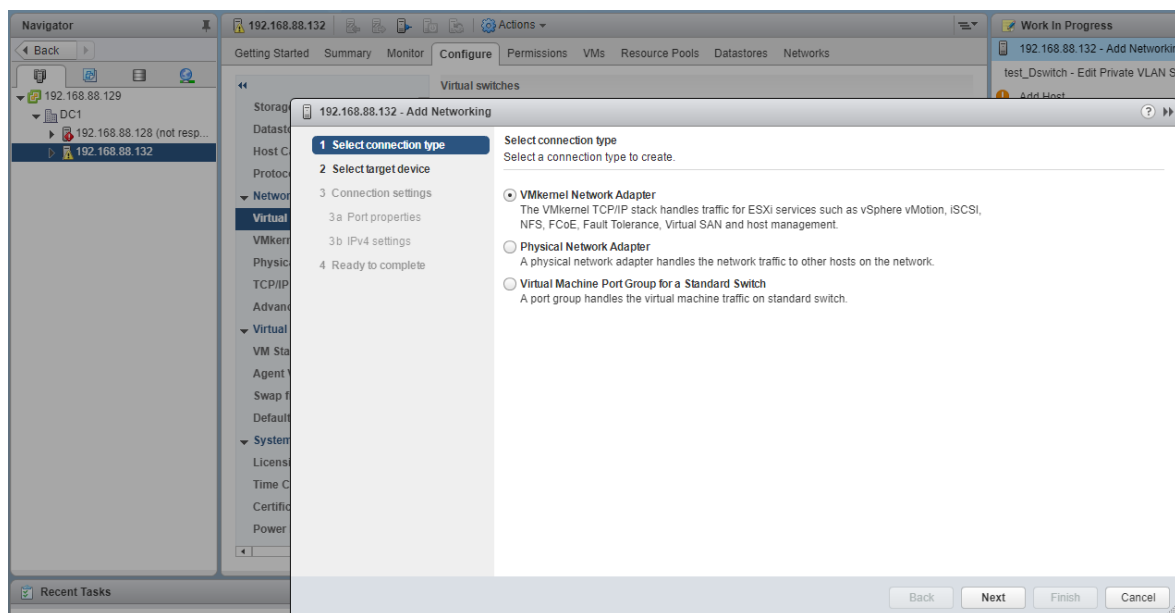
۴. اطمینان حاصل کنید که لینک‌های VLAN trunk تنها به پورت‌هایی از سوئیچ فیزیکی متصل می‌شوند که به عنوان لینک‌های trunk عمل می‌کنند.

## ۶-۴ اقدامات مربوط به جداسازی شبکه‌های با اهمیت بیشتر

پذیرفتن اقدامات مربوط به جداسازی<sup>۲۶</sup> شبکه‌های با اهمیت بیشتر به طور قابل توجهی امنیت شبکه در محیط vSphere شما را تقویت می‌کند. به منظور جداسازی نوع خاصی از ترافیک، به صورت زیر عمل کنید.

روش:

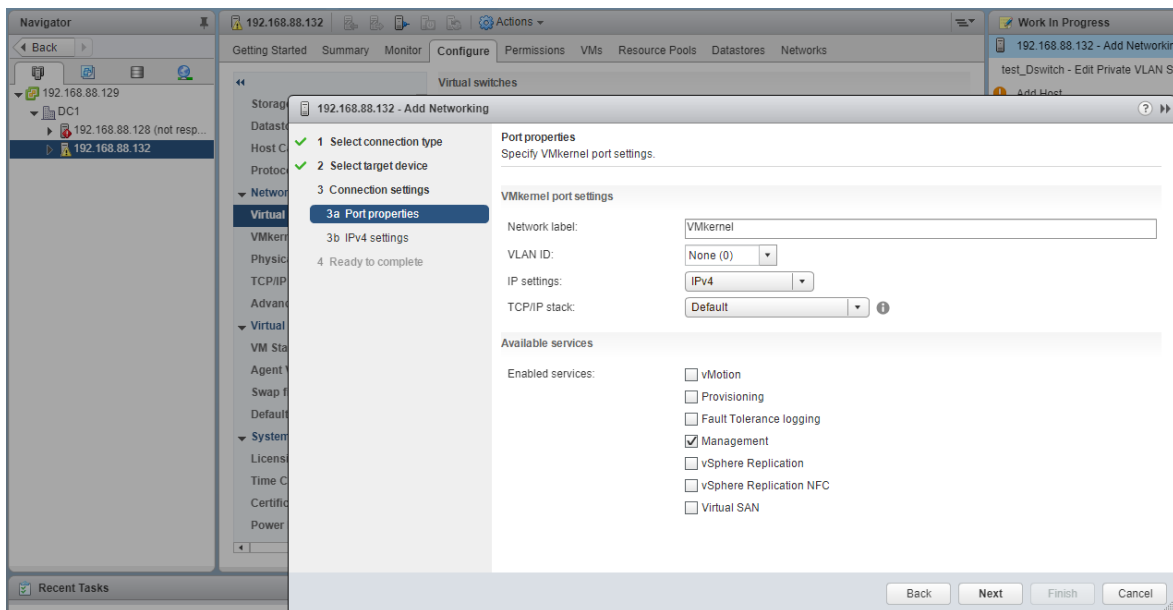
۱. در vSphere WebClient، میزبان مورد نظر را انتخاب کنید.
۲. به برگه Configure رفته، و در بخش Networking گزینه Virtual switches را انتخاب کنید.
۳. آیکون Add host networking را کلیک کرده و در صفحه نمایش داده شده VMkernel Network Adaptor را انتخاب کنید.



<sup>۲۶</sup> Isolation

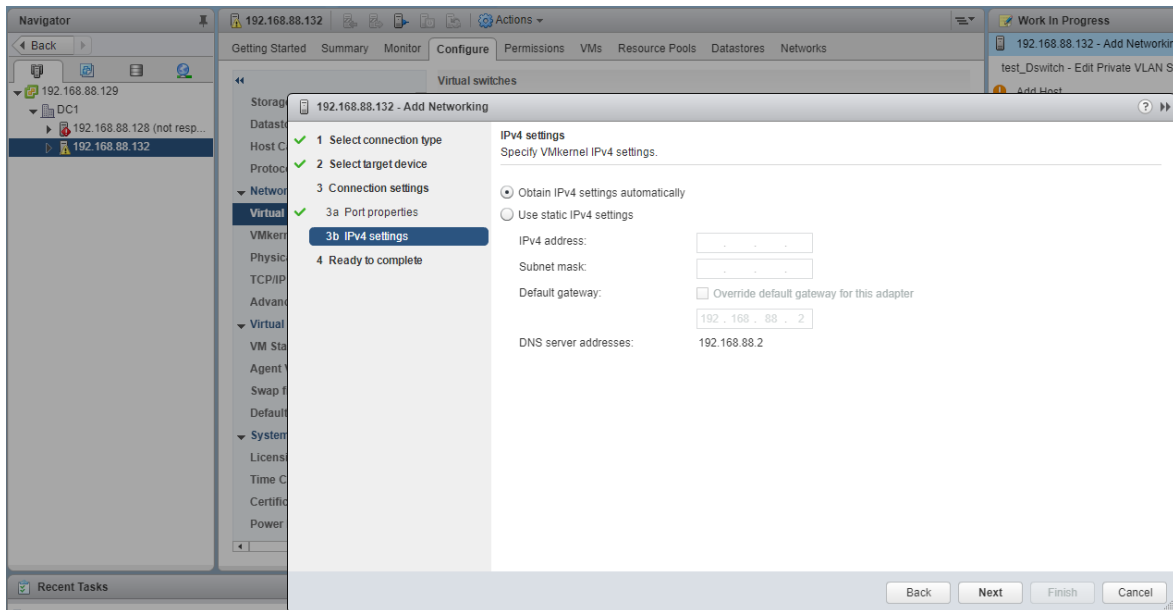
شکل ۱۴ جداسازی ترافیک (۱)

۴. در قسمت Select an existing standard switch سوئیچ مجازی مورد نظر را انتخاب کنید.
۵. در صفحه نمایش داده شده می توان Network label و VLAN ID را مشخص کرده و سایر تنظیمات مربوط به شبکه را انجام داد. در قسمت Available services با انتخاب هر کدام از گزینه ها می توان VLAN را به آن ترافیک اختصاص داد.



شکل ۱۵ جداسازی ترافیک (۲)

۶. در صفحه بعد تنظیمات مربوط به IP را انجام داده و در نهایت با کلیک بر روی دکمه Finish پورت گروه مورد نظر با VLAN ID مشخص شده به منظور عبور دادن نوع ترافیک مشخص شده، ساخته می شود.



شکل ۱۶ جداسازی ترافیک (۳)

## ۶-۴-۱ جداسازی شبکه مدیریتی

شبکه مدیریتی vSphere امکان دسترسی به واسط مدیریتی vSphere روی هر مؤلفه را به وجود می آورد. سرویس هایی که روی واسط مدیریتی اجرا می شوند، برای یک مهاجم فرصت دسترسی دارای امتیاز به سیستم ها را به وجود می آورند. به احتمال زیاد با دسترسی به این شبکه حملات از راه دور آغاز خواهد شد. اگر یک مهاجم به شبکه مدیریتی دسترسی پیدا کند، زمینه برای نفوذ بیشتر فراهم خواهد شد. دسترسی به شبکه مدیریتی را با محافظت از آن در سطح امنیتی امن ترین ماشین مجازی که روی میزبان ESXi یا روی کلاستر اجرا می شود، به شدت کنترل کنید. مهم نیست که چقدر شبکه مدیریتی محدود شده است، در هر صورت مدیران باید اجازه دسترسی به این شبکه را داشته باشند تا بتوانند پیکربندی میزبان های ESXi و سیستم سرویس دهنده vCenter را انجام دهند.

پورت گروه مدیریتی vSphere را در یک VLAN اختصاصی روی یک سوئیچ مجازی مشترک قرار دهید. تا زمانی که VLAN مربوط به پورت گروه مدیریتی به وسیله ترافیک تولیدی توسط ماشین های مجازی استفاده نشود، سوئیچ مجازی می تواند با ترافیک تولید (ترافیک ماشین مجازی) به اشتراک گذاشته شود. بررسی کنید که قطعه این شبکه (مدیریت) مسیریابی نشود، مگر به شبکه هایی که در آن ها دیگر موجودیت های مدیریتی وجود داشته باشند. به طور خاص، اطمینان حاصل کنید که ترافیک تولیدی ماشین مجازی به این شبکه (مدیریت) مسیریابی نشود.

با استفاده از یکی از رویکردهای زیر، دسترسی به عملکردهای مدیریت را با یک کنترل دقیق فعال کنید.

- برای محیط‌های بسیار حساس، یک دروازه کنترل‌شده یا سایر روش‌های کنترل‌شده را برای دسترسی به شبکه مدیریت، پیکربندی کنید. به عنوان مثال، لازم است که مدیران از طریق یک VPN به شبکه مدیریت متصل شوند و اجازه دسترسی را تنها به مدیران مورد اعتماد بدهند.
- جعبه‌های پرش که سرویس‌گیرنده‌های مدیریت را اجرا می‌کنند، را پیکربندی کنید.

## ۶-۴-۲ جداسازی ترافیک ذخیره‌سازی

اطمینان حاصل کنید که ترافیک ذخیره‌سازی مبتنی بر IP جداسازی شده است. ذخیره‌سازی مبتنی بر IP شامل iSCSI و NFS است. ماشین‌های مجازی ممکن است که سوئیچ‌های مجازی و VLANها را با پیکربندی‌های ذخیره‌سازی مبتنی بر IP به اشتراک بگذارند. این نوع پیکربندی ممکن است ترافیک ذخیره‌سازی مبتنی بر IP را در اختیار کاربران غیرمجاز ماشین مجازی قرار دهد.

ذخیره‌سازی مبتنی بر IP اغلب رمزنگاری نمی‌شود؛ هر کسی که به این شبکه دسترسی داشته باشد می‌تواند آن را ببیند. برای محدود کردن کاربران غیرمجاز از مشاهده ترافیک ذخیره‌سازی مبتنی بر IP، به صورت منطقی ترافیک شبکه‌ای ذخیره‌سازی مبتنی بر IP را از ترافیک تولیدی جدا کنید. همچنین آداپتورهای ذخیره‌سازی مبتنی بر IP را روی VLANها یا قطعات شبکه‌ای مجزا از شبکه مدیریت VMkernel، پیکربندی کنید تا کاربران غیرمجاز را در دیدن ترافیک محدود کنید.

## ۶-۴-۳ جداسازی ترافیک VMotion

ترافیک مهاجرت Vmotion به صورت متن آشکار انتقال داده می‌شود. هر کسی با دسترسی به شبکه‌ای که این ترافیک روی آن جریان دارد، می‌تواند آن را مشاهده کند. مهاجمان بالقوه می‌توانند با شنود ترافیک VMotion، محتویات حافظه یک ماشین مجازی را به دست آورند. همچنین آن‌ها می‌توانند با انجام حمله مردی در میانه، محتویات را در حین مهاجرت تغییر دهند.

ترافیک VMotion را روی یک شبکه مجزا، از ترافیک تولید جدا کنید. شبکه را به گونه‌ای تنظیم کنید که غیرقابل مسیریابی باشد، یعنی مطمئن شوید که هیچ مسیریابی لایه ۳ بین این شبکه و دیگر شبکه‌ها انجام نمی‌شود، تا بتوانید از دسترسی خارجی به شبکه جلوگیری کنید.

پورت گروه VMotion باید در یک VLAN اختصاصی روی سوئیچ مجازی مشترک قرار داده شود. تا زمانی که VLAN مربوط به پورت گروه VMotion توسط ترافیک تولیدی ماشین های مجازی استفاده نمی شود، می توان سوئیچ مجازی را با ترافیک تولیدی ماشین مجازی به اشتراک گذاشت.

## ۵-۶ محدود کردن استفاده از سوئیچ های مجازی با vSphere Network Appliance

### API

فقط در صورت نیاز از سوئیچ های مجازی با vSphere Network Appliance API استفاده کنید. اگر از محصولاتی استفاده نمی کنید که از vSphere Network Appliance API (DvFilter) استفاده می کنند، میزبان خود را به گونه ای پیکربندی نکنید که اطلاعات شبکه را به یک ماشین مجازی ارسال کند. اگر vSphere Network Appliance API فعال باشد، یک مهاجم ممکن است برای اتصال یک ماشین مجازی به فیلتر تلاش کند. این اتصال ممکن است دسترسی به شبکه دیگر ماشین های مجازی روی میزبان را فراهم آورد.

اگر از محصولی استفاده می کنید که از این API استفاده می کند، مطمئن شوید که میزبان به درستی پیکربندی شده است. بخش های مربوط به DvFilter در Developing and Deploying vSphere Solutions، vServices و ESX Agents را ببینید. اگر میزبان شما برای استفاده از API تنظیم شده باشد، مطمئن شوید که مقدار پارامتر Net.DVFilterBindIpAddress مطابق با محصولی است که از API استفاده می کند.

### روش

۱. به vSphere Web Client وارد شوید.
۲. میزبان را انتخاب کرده و بر روی Configure کلیک کنید.
۳. در قسمت System گزینه Advanced System Settings را انتخاب کنید.
۴. مطمئن شوید که مقدار پارامتر Net.DVFilterBindIpAddress خالی است.
۵. تنظیمات زیر را بررسی کنید.
  - اگر شما از تنظیمات DvFilter استفاده نمی کنید، مطمئن شوید که مقدار پارامتر خالی است.
  - اگر شما از تنظیمات DvFilter استفاده می کنید، اطمینان حاصل کنید که مقدار پارامتر مطابق با مقداری است که محصولی که از DvFilter استفاده می کند، از آن استفاده کرده است.

