بسمه تعالی

امن‌سازی شبکه در بستر مجازی‌سازی VMware vSphere

(بخش دوم)

فهرست مطالب

۱ مقدمه

شبکه‌ی مجازی یکی از مؤلفه‌های اصلی برای برقراری ارتباط بین ماشین‌های مجازی در محیط vSphere است. بنابراین رعایت نکات امنیتی در پیکربندی شبکه در محیط vSphere یکی از موارد ضروری در حفاظت از یک محیط مجازی است. سوئیچ‌های مجازی از مهم‌ترین اجزای یک شبکه‌ی مجازی در محیط vSphere هستند، که ارتباط بین میزبان‌ها و ماشین‌های مجازی آن‌ها با یکدیگر و همچنین با شبکه‌ی فیزیکی را برقرار می‌کنند. سوئیچ‌های مجازی در محیط vSphere به دو نوع سوئیچ استاندارد vSphere[۱] و سوئیچ توزیع‌شده‌ی vSphere[۲] تقسیم می‌شوند. سوئیچ استاندارد vSphere ترافیک شبکه را در سطح میزبان مدیریت می‌کند، در حالی‌که سوئیچ توزیع‌شده‌ی vSphere می‌تواند مدیریت ترافیک شبکه را در سطح مرکز داده[۳] (بین میزبان‌های مختلف) انجام دهد. در این گزارش به معرفی سوئیچ توزیع‌شده‌ی vSphere می‌پردازیم و پیکربندی‌های مختلف این نوع سوئیچ، از جمله پیکربندی‌ها و قابلیت‌های امنیتی را شرح می‌دهیم.

۲ معماری سوئیچ توزیع‌شده‌ی vSphere

یک سوئیچ توزیع‌شده‌ی vSphere امکان مدیریت متمرکز و نظارت بر پیکربندی شبکه همه میزبان‌هایی که با آن مرتبط هستند را به‌وجود می‌آورد. سوئیچ توزیع‌شده‌ی vSphere برروی سیستم سرویس‌دهنده‌ی vCenter تنظیم می‌شود و تنظیمات آن به تمام میزبان‌هایی که با آن مرتبط هستند انتشار پیدا می‌کند.

در حالت کلی یک سوئیچ شبکه در محیط vSphere شامل دو بخش منطقی به نام‌های سطح داده[۴] و سطح مدیریتی[۵] است. سطح داده عملیات سوئیچ‌کردن بسته، فیلترکردن، برچسب‌گذاری، و غیره را انجام می‌دهد. سطح مدیریتی یک ساختار کنترلی است که به‌منظور پیکربندی قابلیت‌های سطح داده استفاده می‌شود. یک

---

[۱] vSphere Standard Switch (VSS)

[۲] vSphere Distributed Switch (VDS)

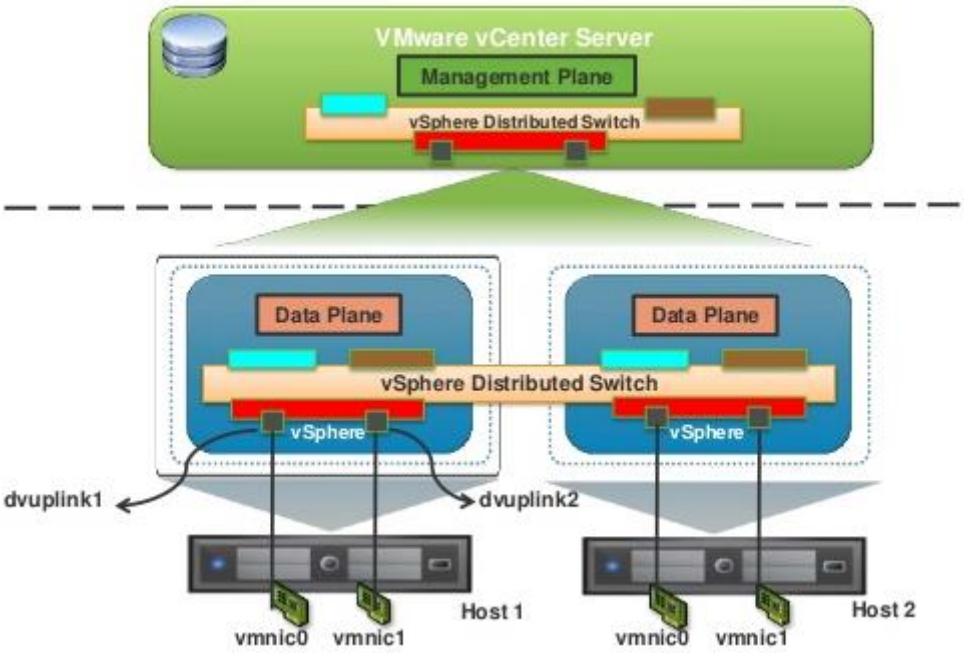
[۳] Data center

[۴] Data plane

[۵] Management plane

سوئیچ استاندارد vSphere شامل هر دو سطح داده و مدیریتی است و بنابراین می‌توان پیکربندی و نگهداری هر سوئیچ استاندارد را به‌صورت منحصربه‌فرد و جداگانه انجام داد.

سوئیچ توزیع‌شده‌ی vSphere سطوح داده و مدیریتی را از یکدیگر جدا می‌کند. قابلیت‌های مدیریتی سوئیچ توزیع‌شده برروی سیستم سرویس‌دهنده‌ی vCenter قرار می‌گیرد که برای ما امکان مدیریت پیکربندی شبکه در سطح یک مرکز داده را به‌وجود می‌آورد. سطح داده به‌صورت محلی برروی هر میزبانی که با سوئیچ توزیع‌شده ارتباط دارد، باقی می‌ماند. بخش سطح داده سوئیچ توزیع‌شده، سوئیچ پروکسی میزبان[۶] نیز نامیده می‌شود. پیکربندی‌های شبکه برروی سرویس‌دهنده‌ی vCenter ایجاد می‌شوند (سطح مدیریتی)، به‌صورت خودکار به همه‌ی سوئیچ‌های پروکسی میزبان‌ها (سطح داده) منتقل می‌شوند. معماری یک سوئیچ توزیع‌شده‌ی vSphere در شکل ۱ نشان داده شده است.



شکل ۱: معماری یک سوئیچ توزیع‌شده‌ی vSphere

سوئیچ توزیع‌شده‌ی vSphere دو انتزاع را معرفی می‌کند که برای ایجاد پیکربندی‌های شبکه به‌صورت سازگار با NIC های فیزیکی، ماشین‌های مجازی، و سرویس‌های VMKernel استفاده می‌شوند.

[۶] Host proxy switch

- پورت‌گروه uplink: یک پورت‌گروه uplink یا پورت‌گروه dvuplink در هنگام ایجاد سوئیچ توزیع‌شده تعریف می‌شود و سوئیچ توزیع‌شده می‌تواند یک یا چند uplink داشته باشد. یک uplink یک قالب است که برای پیکربندی اتصالات فیزیکی میزبان و همچنین سیاست‌های شکست[۷] و تعادل بار[۸] استفاده می‌شود. NICهای فیزیکی از میزبان به uplinkها در سوئیچ توزیع‌شده نگاشت می‌شوند. در سطح میزبان، هر NIC فیزیکی به یک پورت uplink با یک شناسه خاص متصل می‌شود. تنظیمات مربوط به شکست و تعادل بار بر روی uplinkها انجام می‌شوند و به صورت خودکار به سوئیچ‌های پروکسی میزبان (سطح داده) منتقل می‌شوند. به این ترتیب می‌توان پیکربندی‌های مربوط به شکست و تعادل بار را به صورت سازگار برای NICهای فیزیکی تمام میزبان‌هایی که با سوئیچ توزیع‌شده مرتبط هستند، اعمال کرد.
- پورت‌گروه توزیع‌شده[۹]: پورت‌گروه‌های توزیع‌شده اتصال شبکه به ماشین‌های مجازی را تأمین کرده و ترافیک VMKernel را تنظیم می‌کنند. هر پورت‌گروه توزیع‌شده را می‌توان بااستفاده از یک برچسب شبکه، که باید در مرکز داده فعلی منحصربه‌فرد باشد، شناسایی کرد. مواردی از قبیل دسته‌بندی NIC[۱۰]، شکست، تعادل بار، VLAN، امنیت، شکل‌دهی ترافیک[۱۱] و دیگر سیاست‌ها را می‌توان روی پورت گروه‌های توزیع‌شده پیکربندی کرد. پورت‌های مجازی که به یک پورت‌گروه توزیع‌شده متصل هستند، ویژگی‌های مشابهی که برای پورت‌گروه توزیع‌شده پیکربندی شده‌اند، را به اشتراک می‌گذارند. همانند پورت‌گروه‌های uplink، پیکربندی‌هایی که در پورت‌گروه‌های توزیع‌شده در سرویس‌دهنده vCenter (سطح مدیریتی) تنظیم می‌شوند به‌صورت خودکار به تمام میزبان‌های سوئیچ توزیع‌شده، ازطریق سوئیچ‌های پروکسی میزبان (سطح داده) منتشر می‌شوند. به این ترتیب می‌توان یک گروه از ماشین‌های مجازی را به‌صورتی پیکربندی کرد، با تخصیص‌دادن ماشین‌های مجازی به پورت‌گروه توزیع‌شده مشابه، که پیکربندی‌های شبکه‌ی مشابهی را به‌اشتراک بگذارند.

---

[۷] Failover

[۸] Load balancing

[۹] Distributed port group

[۱۰] NIC teaming

[۱۱] Traffic shaping

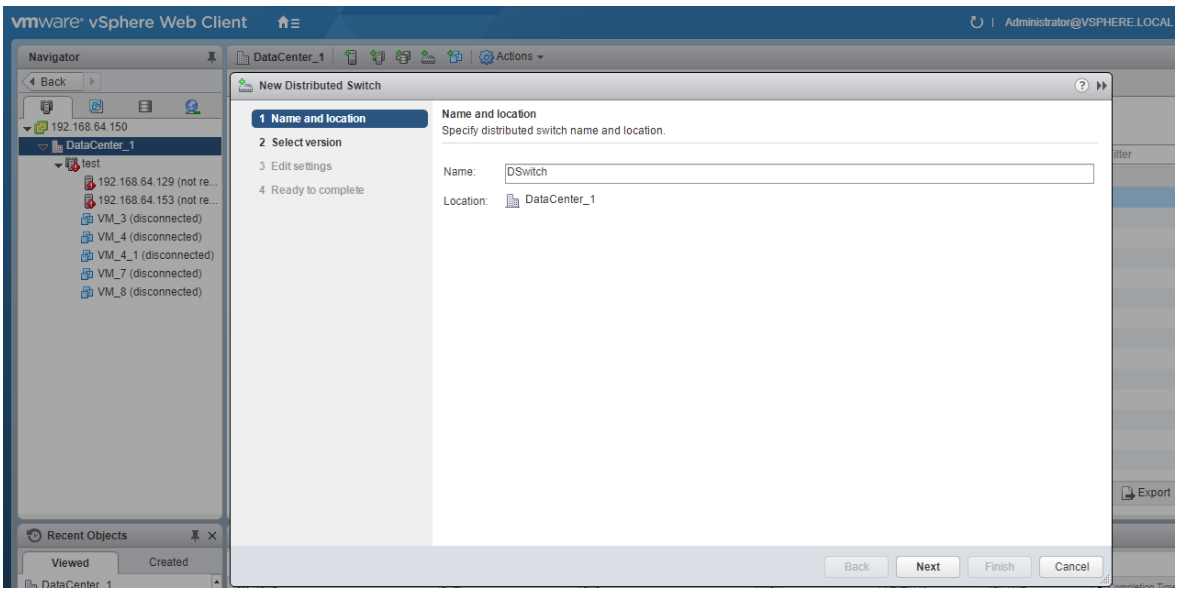
۳ ایجاد یک سوئیچ توزیع‌شده‌ی vSphere

یک سوئیچ توزیع‌شده‌ی vSphere را برروی یک مرکز داده ایجاد کنید تا بتوانید پیکربندی شبکه چندین میزبان را به‌صورت همزمان و از یک مکان مرکزی، مدیریت کنید.

روش

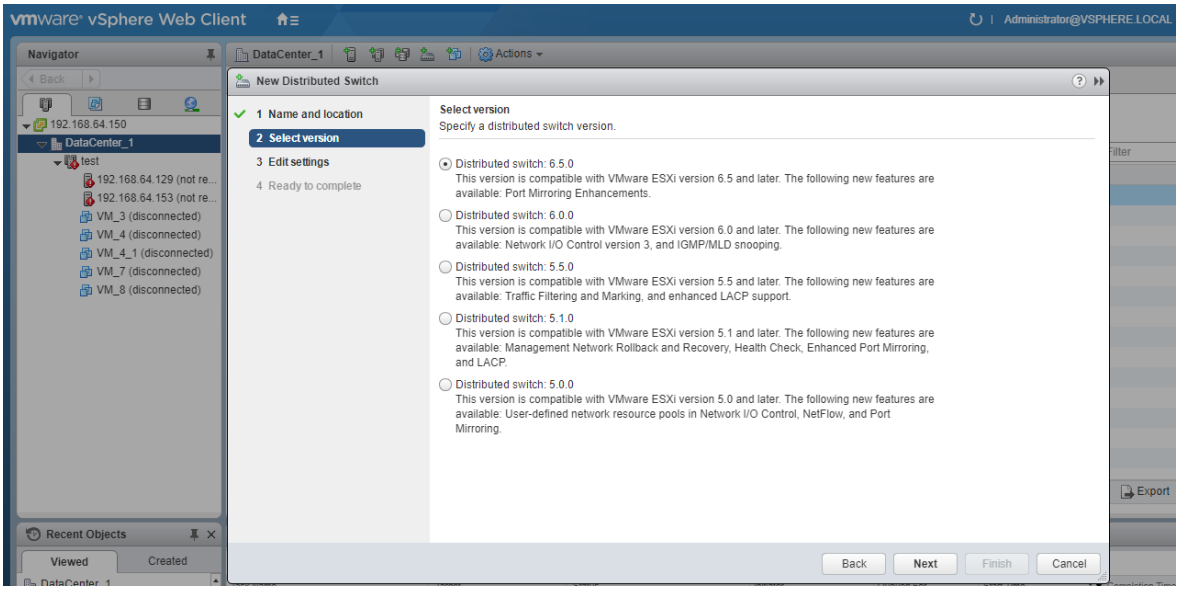
۱. در vSphere Web Client برروی مرکز داده راست‌کلیک کرده و Distributed Switch > New Distributed Switch را انتخاب کنید.

۲. با واردکردن نام برای سوئیچ توزیع‌شده، یا پذیرش نام تولیدشده، و کلیک‌کردن Next به صفحه بعد بروید (شکل ۲).



شکل ۲: ایجاد سوئیچ توزیع‌شده‌ی vSphere – انتخاب نام

۳. در این صفحه نسخه‌ی سوئیچ توزیع‌شده را انتخاب کنید (شکل ۳). لازم به ذکر است که نسخه‌ی سوئیچ توزیع‌شده با ESXi همان نسخه و نسخه‌های بعد از آن سازگار است، ولی ویژگی‌های منتشرشده در نسخه‌های بعدی از سوئیچ توزیع‌شده‌ی vSphere را پشتیبانی نمی‌کند.



شکل ۳: ایجاد سوئیچ توزیع‌شده‌ی vSphere – انتخاب نسخه

٤. در صفحه‌ی ویرایش تنظیمات، تنظیمات سوئیچ توزیع‌شده را پیکربندی کنید (شکل ٤).

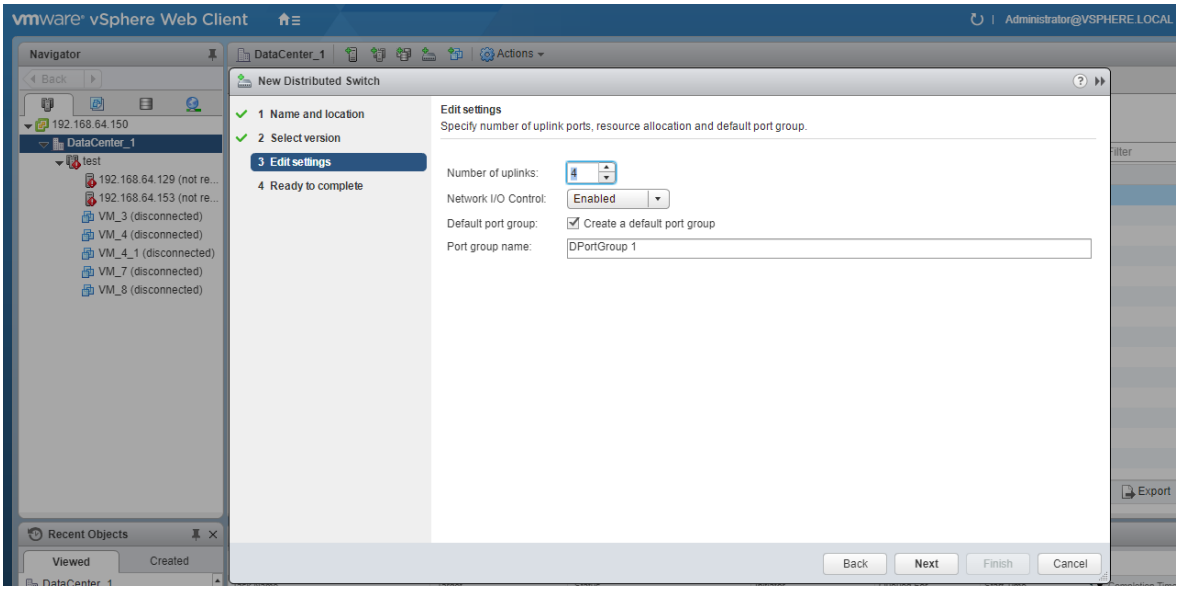
أ. تعداد uplinkها را تعیین کنید. پورت‌های uplink سوئیچ توزیع‌شده را به NICهای فیزیکی میزبان‌های مرتبط با آن متصل می‌کنند.

ب. Network I/O Control را فعال یا غیرفعال کنید. با استفاده از Network I/O Control می‌توانید دسترسی به منابع شبکه را برای انواع خاصی از زیرساخت‌ها و ترافیک بار کاری، با توجه به نیازمندی‌های استقرار خود، اولویت‌بندی کنید. Network I/O Control به طور مداوم بر بار I/O برروی شبکه نظارت می‌کند و به‌صورت پویا منابع موجود را تخصیص می‌دهد.

ج. با انتخاب Create a default port group می‌توانید یک پورت‌گروه توزیع‌شده‌ی جدید، با تنظیمات پیش‌فرض، را برای این سوئیچ ایجاد کنید.

د. برروی Next کلیک کنید.

٥. با کلیک برروی Finish فرآیند ایجاد سوئیچ توزیع‌شده‌ی جدید خاتمه می‌یابد.



شکل ٤: ایجاد سوئیچ توزیع‌شده‌ی vSphere – ویرایش تنظیمات

نکته: به‌منظور ارتقای نسخه‌ی سوئیچ توزیع‌شده پس از ایجاد آن، برروی سوئیچ توزیع‌شده کلیک‌راست کرده و Upgrade > Upgrade Distributed Switch را انتخاب کنید.

نکته: با انتخاب آیکون مربوط به ویرایش تنظیمات یک سوئیچ توزیع‌شده‌ی vSphere می‌توان تنظیمات عمومی و پیشرفته را برای آن سوئیچ ویرایش کرد. تنظیمات عمومی برای یک سوئیچ توزیع‌شده‌ی vSphere عبارتند از نام سوئیچ، تعداد uplinkها، و غیره. تعداد پورت‌های سوئیچ توزیع‌شده قابل ویرایش نیست. تنظیمات پیشرفته برای یک سوئیچ توزیع‌شده‌ی vSphere شامل پروتکل کشف سیسکو[۱۲]، حداکثر MTU برای سوئیچ، و غیره است. به‌منظور فعال‌سازی فریم‌های جامبو[۱۳]، می‌توان مقداری بزرگتر از ۱۵۰۰ بایت را در فیلد Maximum MTU قرار داد.

[۱۲] Cisco Discovery Protocol

[۱۳] Jumbo frames

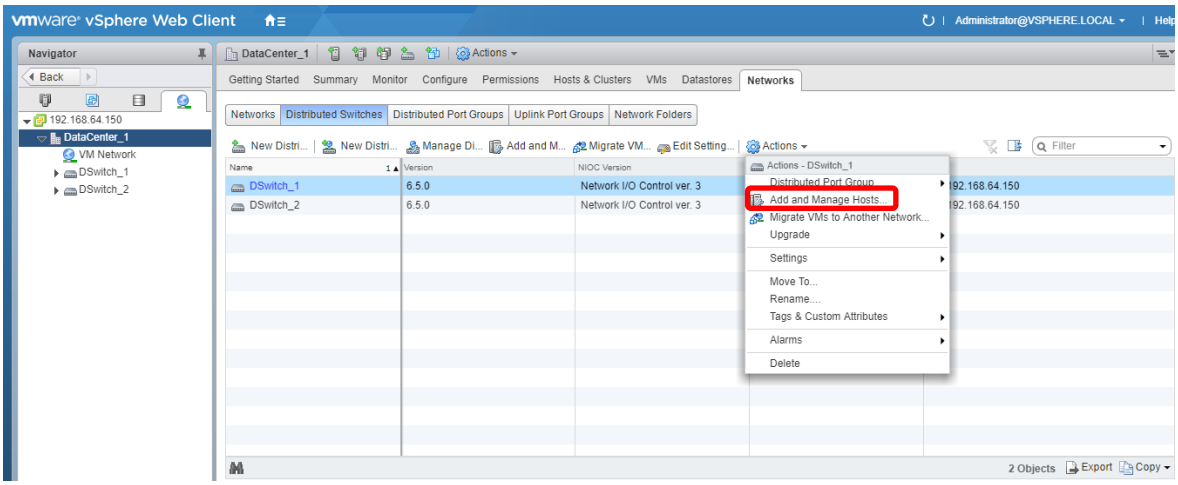
٤ اضافه‌کردن میزبان به سوئیچ توزیع‌شده‌ی vSphere

شبکه‌های مجازی در یک سوئیچ توزیع‌شده‌ی vSphere را می‌توان با اضافه‌کردن میزبان‌ها به سوئیچ و اتصال آداپتورهای شبکه‌ی آن‌ها به سوئیچ، ایجاد و مدیریت کرد. برای ایجاد پیکربندی شبکه‌ای یکنواخت در چندین میزبان روی سوئیچ توزیع‌شده، می‌توان از یک میزبان به‌عنوان الگو استفاده‌کرده و پیکربندی آن را به سایر میزبان‌ها اعمال کرد. به‌منظور مدیریت شبکه‌ی محیط vSphere بااستفاده از یک سوئیچ توزیع‌شده‌ی vSphere باید میزبان‌ها را به سوئیچ مرتبط کنید. با این کار می‌توان NICهای فیزیکی، آداپتورهای VMkernel و آداپتورهای شبکه‌ی ماشین‌های مجازی میزبان‌ها را به سوئیچ توزیع‌شده وصل کرد.

روش

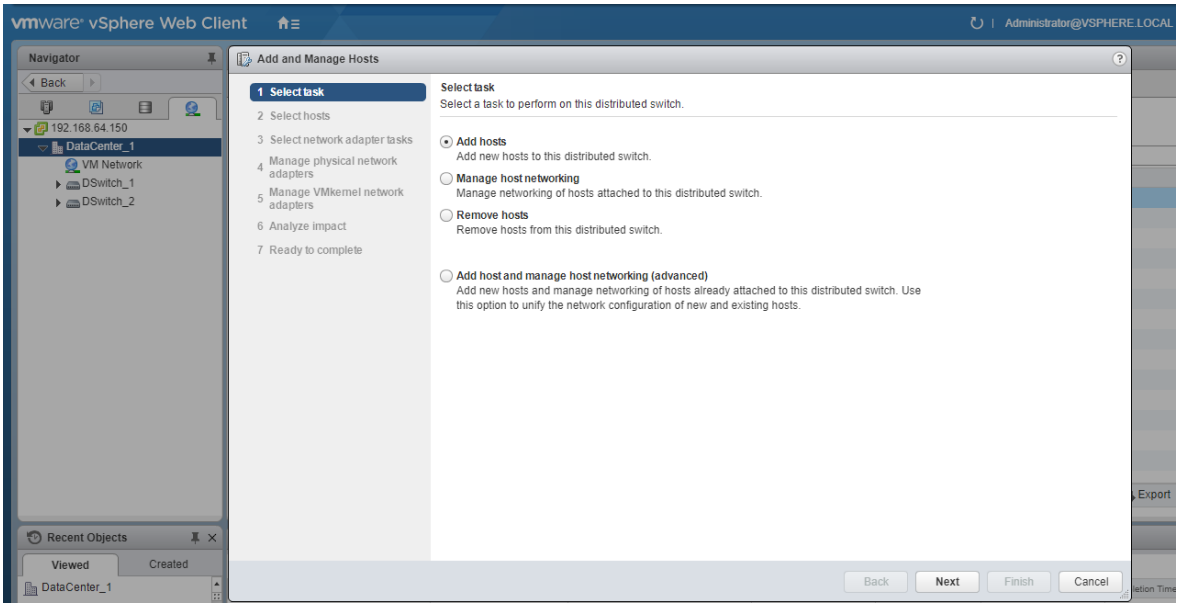
١. در vSphere Web Client سوئیچ توزیع‌شده را انتخاب کنید.

٢. از منوی Actions گزینه‌ی Add and Manage Hosts را انتخاب کنید (شکل ٥).



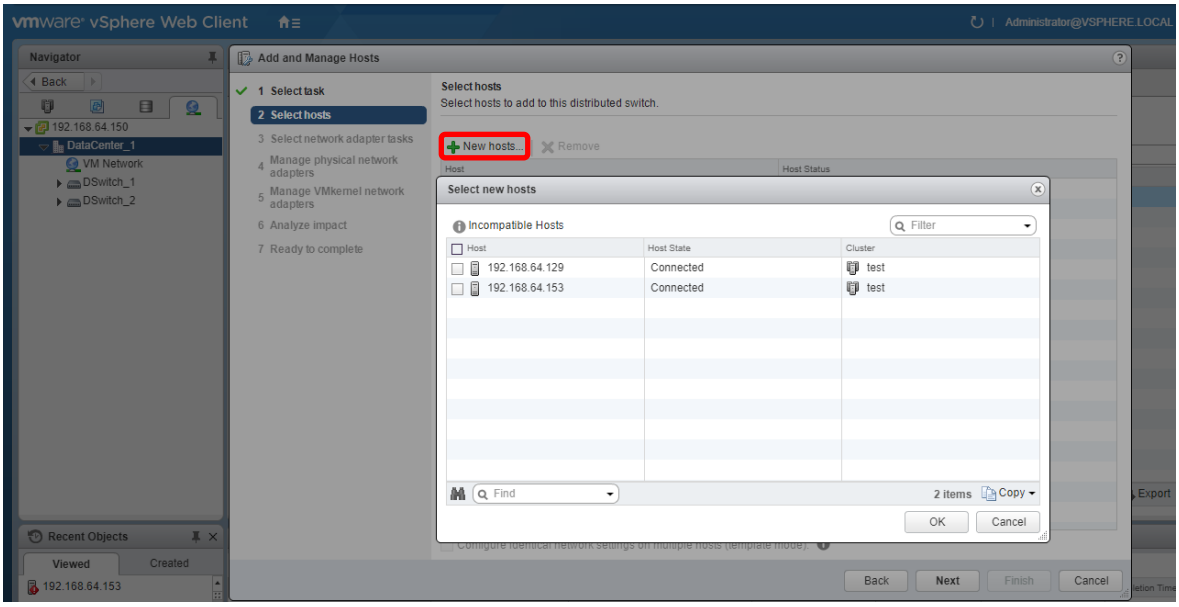
شکل ٥: اضافه‌کردن میزبان به سوئیچ توزیع‌شده‌ی vSphere

٣. در صفحه‌ی انتخاب کار، Add hosts را انتخاب کرده و برروی Next کلیک کنید (شکل ٦).



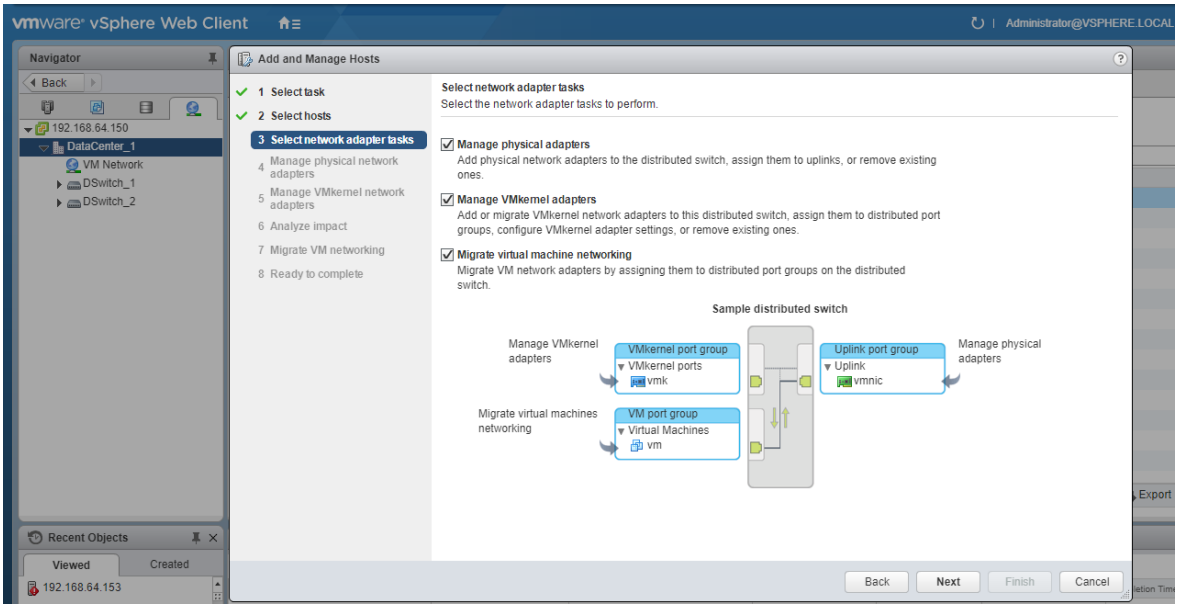
شکل ٦: اضافه‌کردن میزبان به سوئیچ توزیع‌شده‌ی vSphere – انتخاب کار

٤. در صفحه‌ی انتخاب میزبان، New hosts را کلیک کرده، و میزبان‌های موردنظر را انتخاب کنید (شکل ٧).



شکل ٧: اضافه‌کردن میزبان به سوئیچ توزیع‌شده‌ی vSphere – انتخاب میزبان

٥. در صفحه‌ی Select network adapter tasks کارهای موردنظر برای پیکربندی آداپتورهای شبکه‌ی سوئیچ توزیع‌شده را انتخاب کنید (شکل ٨).



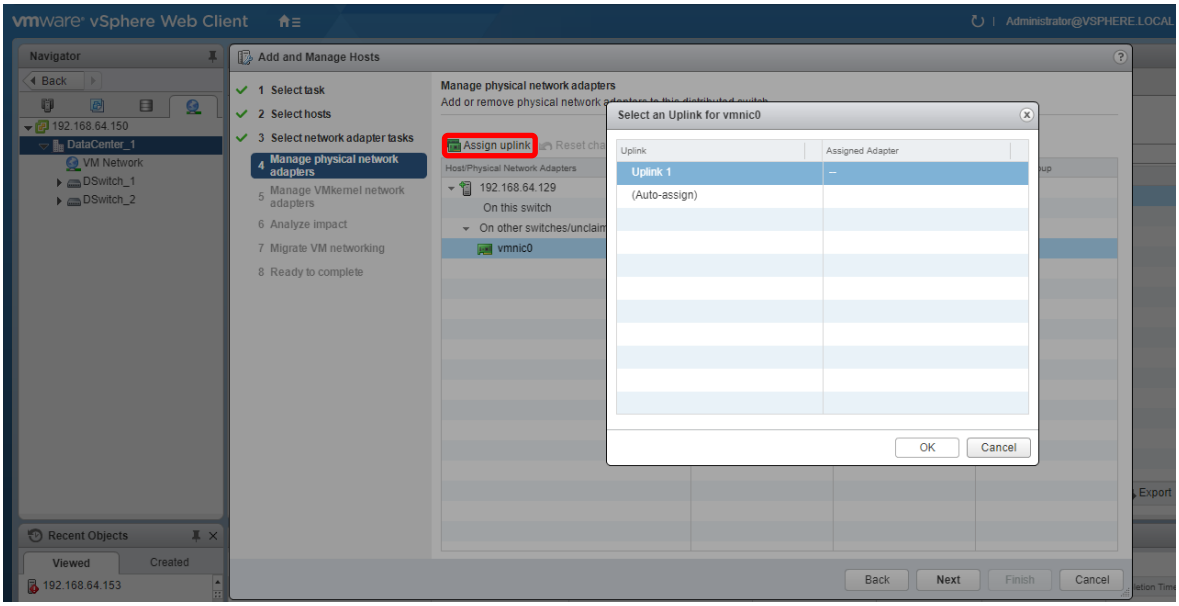
شکل ۸: اضافه‌کردن میزبان به سوئیچ توزیع‌شده‌ی vSphere – انتخاب کارهای آداپتورهای شبکه

٦. در صفحه‌ی Manage physical network adapters پیکربندی NICهای فیزیکی سوئیچ توزیع‌شده را انجام دهید (شکل ۹).

أ. از لیست On other switches/unclaimed، یک NIC فیزیکی را انتخاب کنید. درصورتی‌که NICهای فیزیکی را انتخاب کنید که در حال حاضر به دیگر سوئیچ‌ها متصل هستند، این NICها به سوئیچ توزیع‌شده‌ی فعلی مهاجرت پیدا می‌کنند.

ب. Assign uplink را کلیک کرده و یک uplink را انتخاب کنید.

به‌منظور داشتن یک پیکربندی شبکه‌ی سازگار، می‌توانید یک NIC فیزیکی یکسان از هر میزبان را به uplink یکسانی از سوئیچ توزیع‌شده متصل کنید. به‌عنوان مثال، درصورتی‌که دو میزبان را به سوئیچ توزیع‌شده متصل کرده‌اید، vmnic1 هرکدام را به Uplink1 از سوئیچ توزیع‌شده متصل کنید.

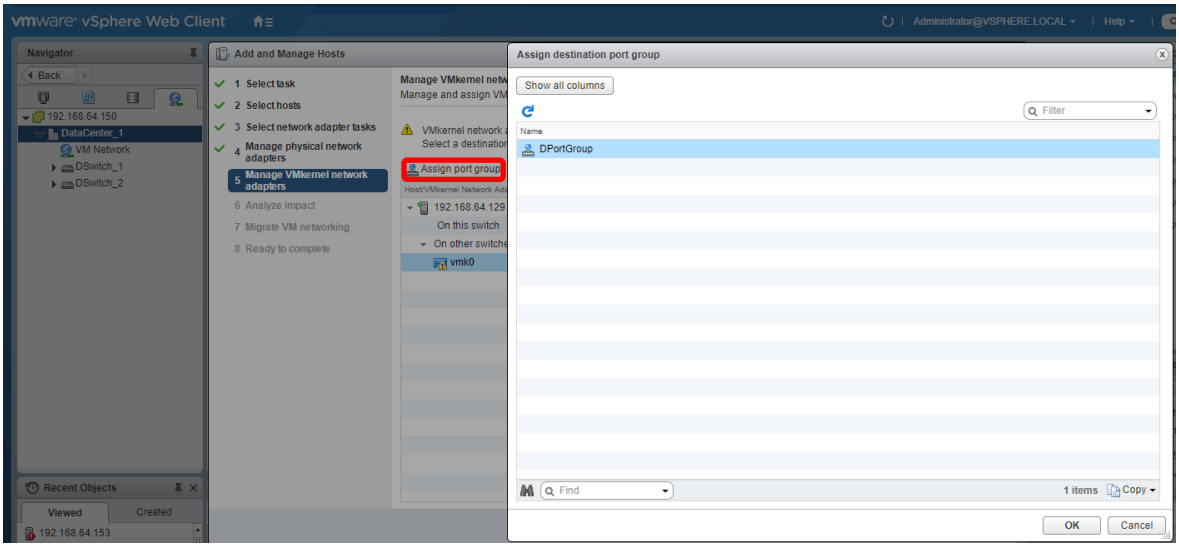


شکل ۹: اضافه‌کردن میزبان به سوئیچ توزیع‌شده‌ی vSphere – مدیریت آداپتورهای شبکه‌ی فیزیکی

۷. در صفحه‌ی Manage VMkernel network adapters، آداپتورهای VMkernel را پیکربندی کنید (شکل ۱۰).

أ. یک آداپتور Vmkernel را انتخاب کنید و Assign port group را کلیک کنید.

ب. یک پورت‌گروه توزیع‌شده را انتخاب کنید.

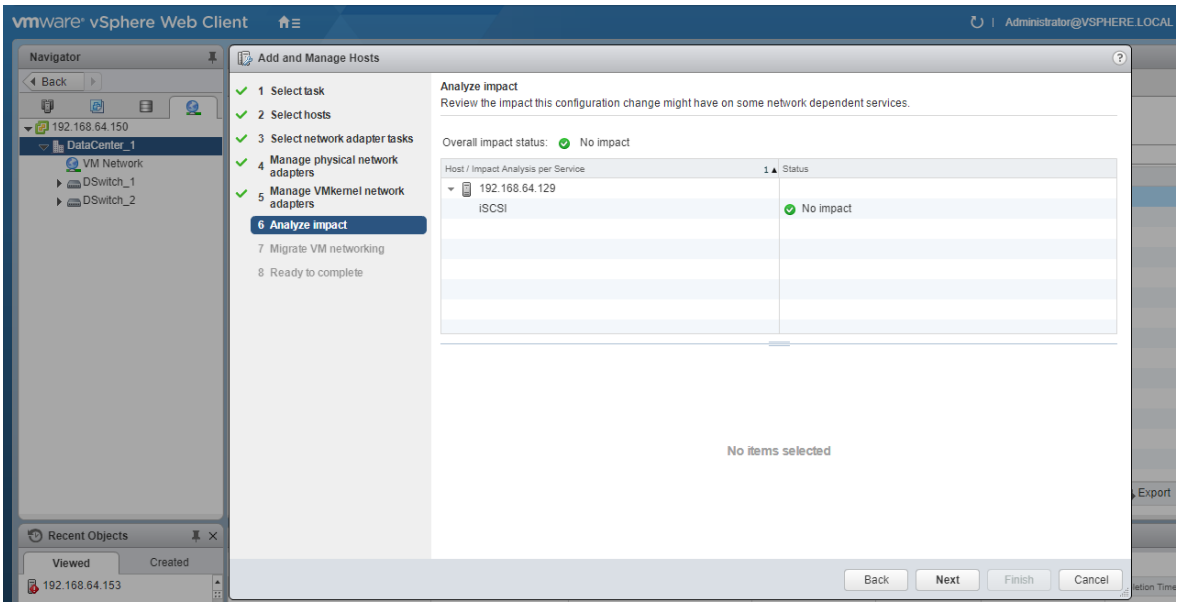


شکل ۱۰: اضافه‌کردن میزبان به سوئیچ توزیع‌شده‌ی vSphere – مدیریت آداپتورهای شبکه‌ی VMkernel

۸. در صفحه‌ی Analyze impact سرویس‌های تحت‌تأثیر قرارگرفته و همچنین سطح تأثیر آن‌ها را بررسی کنید (شکل ۱۱).

- No impact: پس از اعمال پیکربندی جدید شبکه، iSCSI به عملکرد عادی خود ادامه خواهد داد.
- Important impact: در صورتی‌که پیکربندی جدید شبکه اعمال شود، عملکرد عادی iSCSI ممکن است با اختلال مواجه شود.
- Critical impact: در صورتی‌که پیکربندی جدید شبکه اعمال شود، عملکرد عادی iSCSI دچار وقفه خواهد شد.

درصورتی‌که تأثیر روی iSCSI مهم[۱۴] یا حیاتی[۱۵] باشد، می‌توان برروی ورودی iSCSI کلیک کرد و دلایلی که در پنجره‌ی جزئیات تحلیل نشان داده می‌شود را مرور کرد. می‌توانید پس از انجام عیب‌یابی[۱۶] با پیکربندی‌های خود ادامه کار را انجام دهید.



شکل ۱۱: اضافه‌کردن میزبان به سوئیچ توزیع‌شده‌ی vSphere – تحلیل تأثیر پیکربندی بر سرویس‌های شبکه

۹. در صفحه‌ی Migrate VM networking، شبکه‌ی ماشین‌های مجازی را پیکربندی کنید (شکل ۱۲).

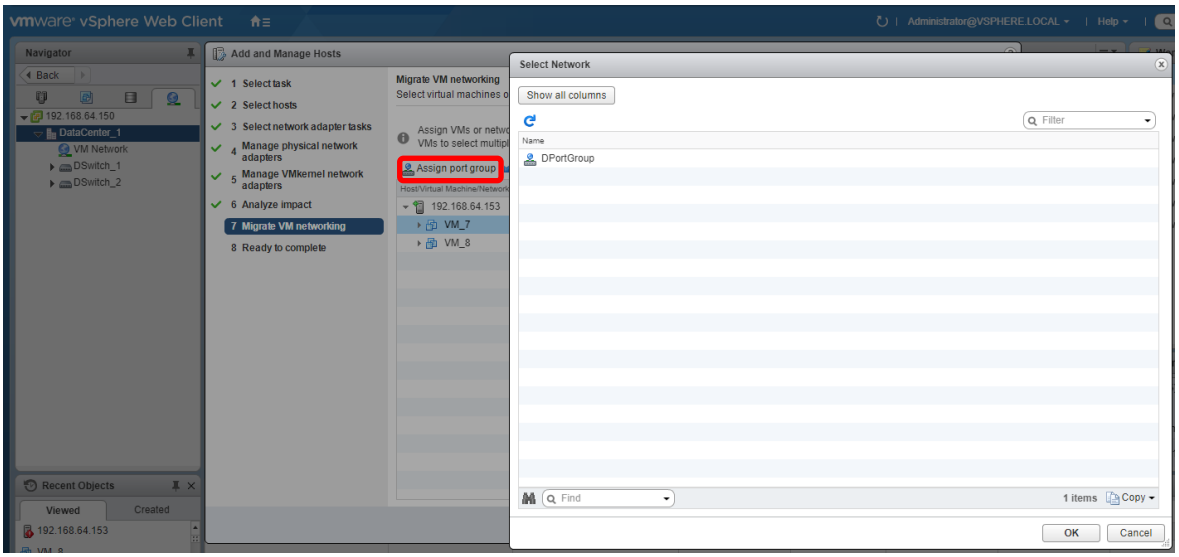
[۱۴] Important

[۱۵] Critical

[۱۶] Troubleshoot

أ. برای اتصال تمام آداپتورهای شبکه‌ی یک ماشین مجازی به یک پورت‌گروه توزیع‌شده، آن ماشین مجازی را انتخاب کنید. در صورتی که قصد انتخاب تنها یک آداپتور شبکه‌ی خاص را دارید، همان آداپتور از ماشین مجازی را انتخاب کنید.

ب. Assign port group را انتخاب کرده و یک پورت‌گروه توزیع‌شده را از لیست انتخاب کنید.



شکل ۱۲: اضافه‌کردن میزبان به سوئیچ توزیع‌شده‌ی vSphere – مهاجرت ماشین‌های مجازی

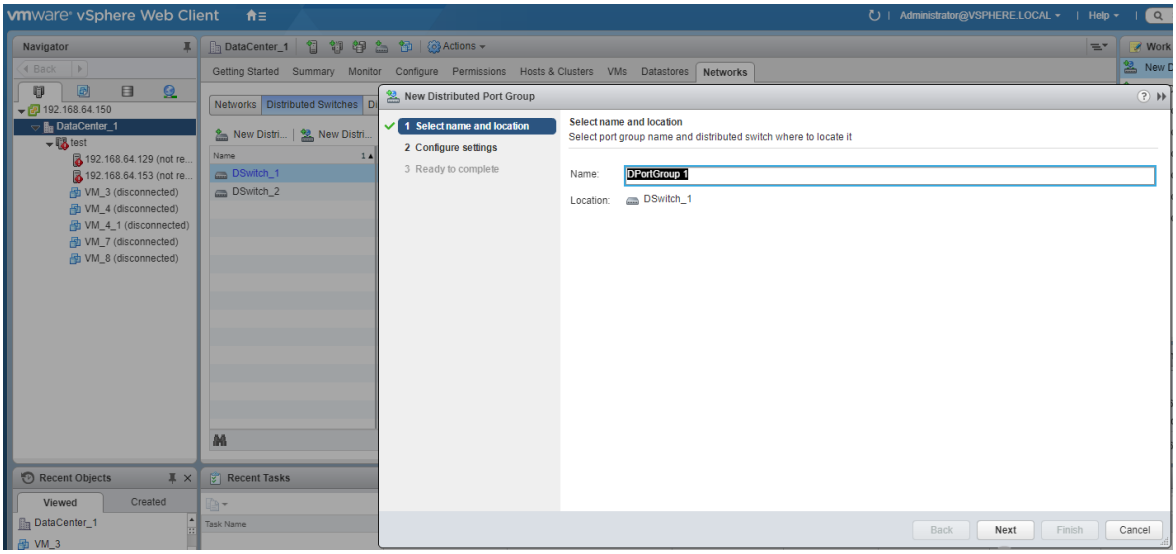
۵ پورت‌گروه‌های توزیع‌شده

یک پورت‌گروه توزیع‌شده می‌تواند پیکربندی‌های اختصاصی را برای پورت‌های مختلف در یک سوئیچ توزیع‌شده‌ی vSphere انجام دهد.

۵-۱ اضافه‌کردن یک پورت‌گروه توزیع‌شده

روش

۱. در vSphere Web Client سوئیچ توزیع‌شده و سپس New distributed port group را انتخاب کنید (شکل ۱۳).

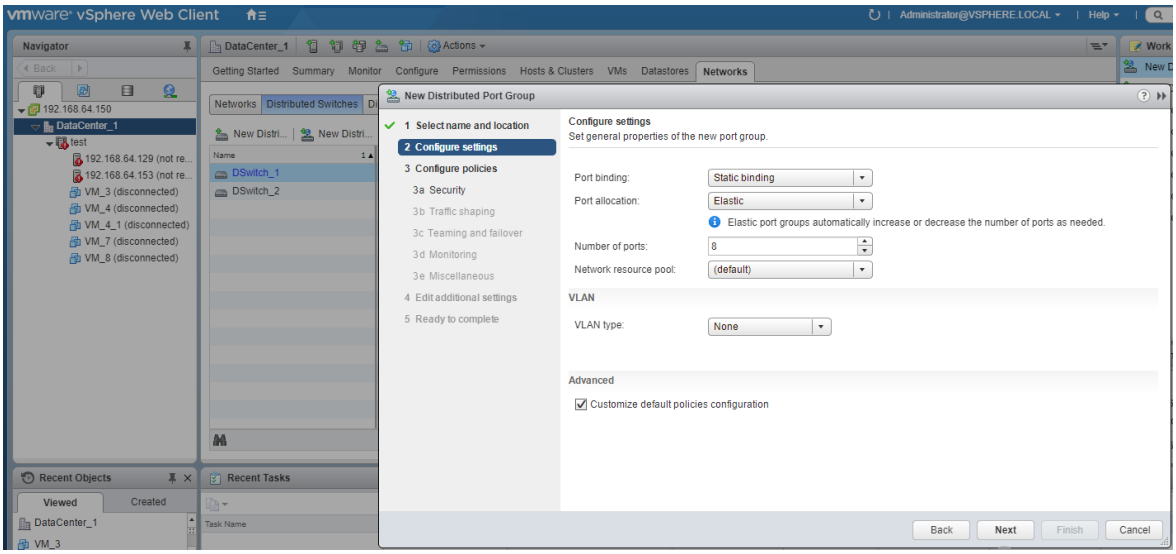


شکل ۱۳: ایجاد یک پورت‌گروه توزیع‌شده – انتخاب نام

۲. در صفحه‌ی تنظیمات پیکربندی، ویژگی‌های عمومی را برای پورت‌گروه توزیع‌شده‌ی جدید تنظیم کنید (شکل ١٤). این تنظیمات شامل موارد زیر است:

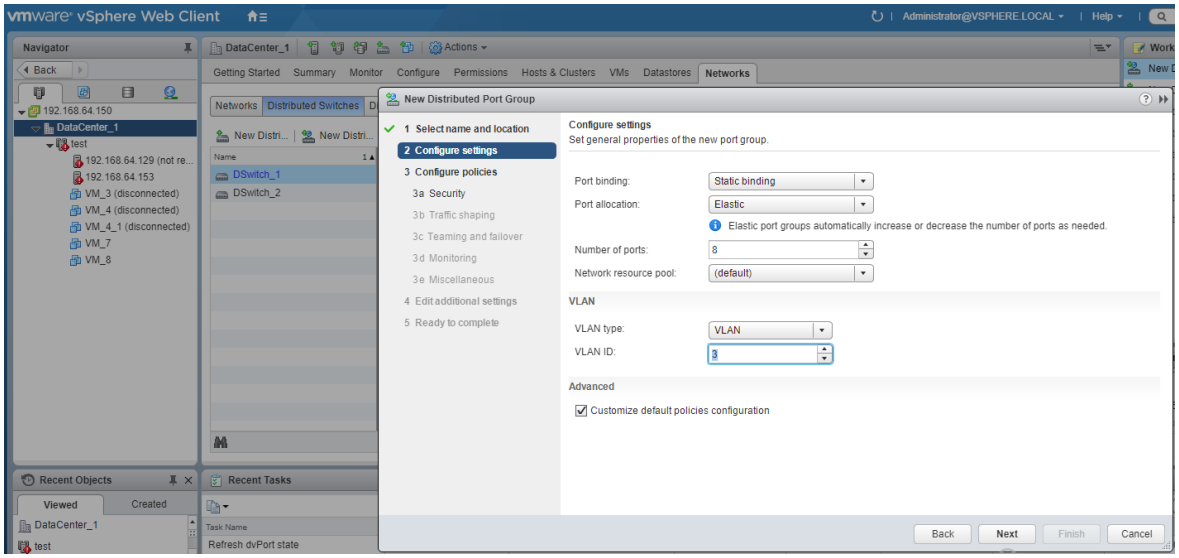
- Port binding: این گزینه مشخص می‌کند که چه زمانی پورت‌ها به ماشین‌های مجازی متصل به پورت‌گروه توزیع‌شده تخصیص داده شوند.
  - ✓ Static binding: همان زمانی که ماشین مجازی به پورت‌گروه توزیع‌شده متصل می‌شود، پورت به ماشین مجازی تخصیص می‌یابد.
  - ✓ Dynamic binding: در اولین زمانی که ماشین مجازی، پس از اتصال به پورت‌گروه توزیع‌شده، روشن شود، پورت به ماشین مجازی تخصیص پیدا می‌کند.
  - ✓ Ephemeral - no binding: انقیاد پورت انجام نمی‌شود. شما می‌توانید همزمان به این‌که به میزبان متصل هستید، یک ماشین مجازی را به پورت‌گروه توزیع‌شده با انقیاد پورت موقت، اختصاص دهید.
- Port allocation
  - ✓ Elastic: تعداد پیش‌فرض پورت‌ها ۸ است. زمانی‌که تمام پورت‌ها تخصیص داده شوند، یک مجموعه‌ی جدید ۸تایی از پورت‌ها ایجاد می‌شود. این حالت، حالت پیش‌فرض است.
  - ✓ Fixed: تعداد پیش‌فرض پورت‌ها ۸ است. زمانی‌که تمام پورت‌ها تخصیص داده شوند، هیچ پورت دیگری ایجاد نمی‌شود.

- Number of ports: تعداد پورت‌های پورت‌گروه توزیع‌شده را نشان می‌دهد.
- Network resource pool: درصورتی‌که از قبل استخر[۱۷] منابع شبکه تعریف شده باشد، در این قسمت می‌توان آن را به پورت‌گروه توزیع‌شده تخصیص داد.
- VLAN: می‌توان یکی از گزینه‌های زیر را برای VLAN انتخاب کرد:
  - ✓ None: از VLAN استفاده نمی‌کند.
  - ✓ VLAN: یک عدد بین ۱ تا ٤٠٩٤ برای VLAN ID انتخاب می‌شود (شکل ۱۵).
  - ✓ VLAN truncking: یک محدوده از VLAN IDها برای ترانک انتخاب می‌شود (شکل ١٦).
  - ✓ Private VLAN: درصورتی‌که روی سوئیچ توزیع‌شده VLAN خصوصی تعریف شده باشد می‌توان یک VLAN خصوصی را در این قسمت انتخاب کرد. در ادامه توضیحات بیشتری در مورد Private VLANها ارائه خواهد شد.
- Advanced: به‌منظور سفارشی‌سازی پیکربندی‌ها برای پورت‌گروه توزیع‌شده‌ی جدید، این کادر را تیک بزنید.

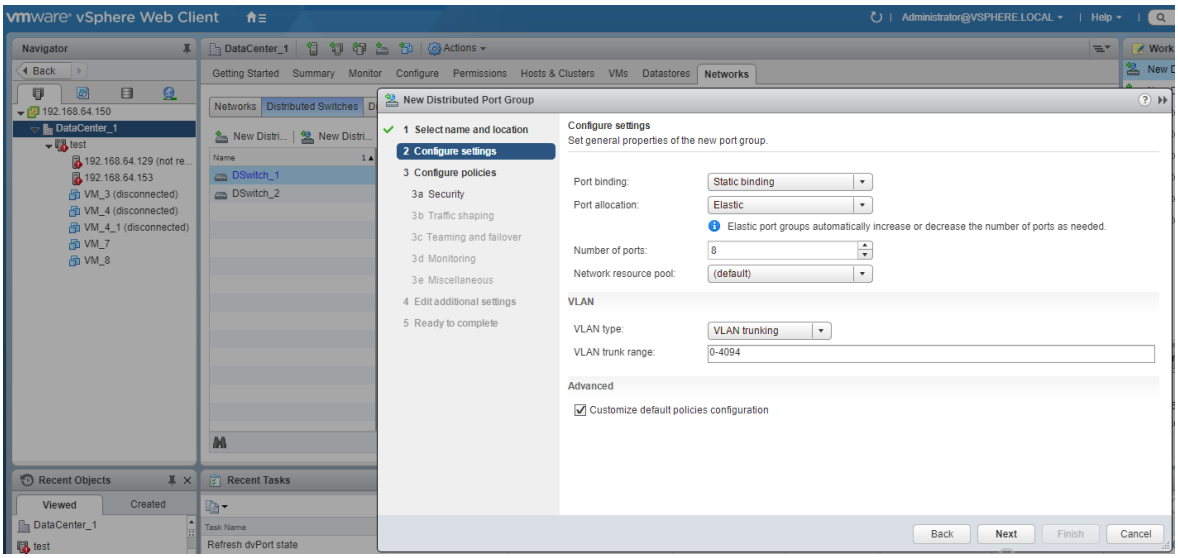


شکل ١٤: ایجاد یک پورت‌گروه توزیع‌شده – تنظیمات پیکربندی

[۱۷] Pool



شکل ۱۵: ایجاد یک پورت‌گروه توزیع‌شده – تخصیص شناسه VLAN به پورت‌گروه

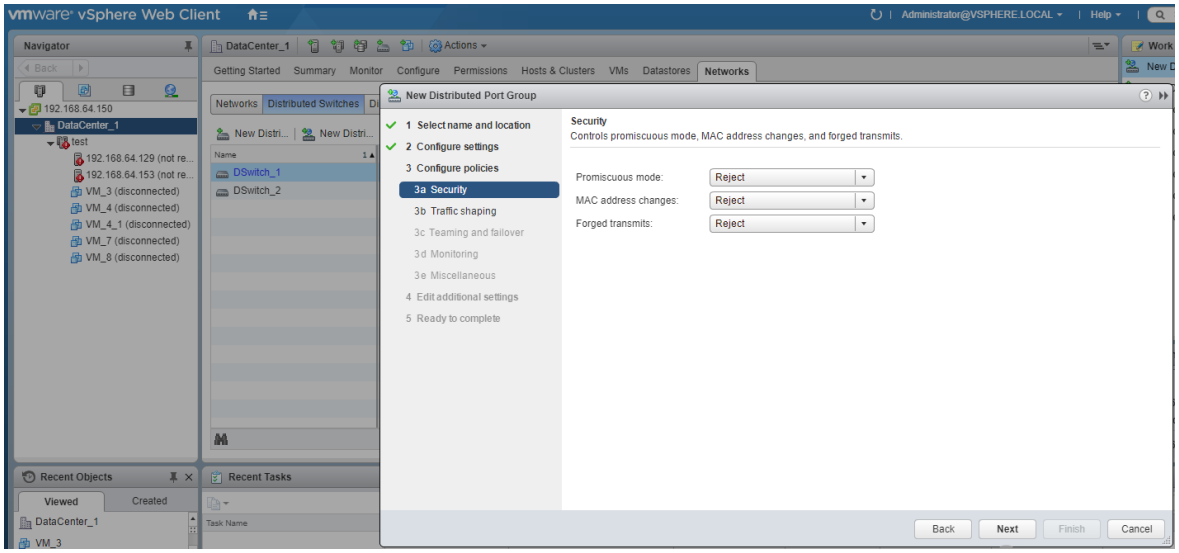


شکل ۱۶: ایجاد یک پورت‌گروه توزیع‌شده – تخصیص یک محدوده از شناسه‌های VLAN به پورت‌گروه

۳. در صفحه‌ی Security می‌توان موارد امنیتی زیر را ویرایش کرد (شکل ۱۷):

- Promiscuous mode
  - Reject: حالت بی‌قاعده فعال نیست و هر ماشین مجازی تنها فریم‌های مربوط به خود را دریافت می‌کند و قادر به مشاهده‌ی فریم‌های سایر ماشین‌های مجازی نیست.
  - Accept: حالت بی‌قاعده فعال است و سوئیچ به ماشین مجازی اجازه می‌دهد تا تمام فریم‌هایی که از سوئیچ عبور می‌کنند و با VLAN آن ماشین مجازی مطابقت دارند، را دریافت کند.

- MAC address changes
  - Reject: درصورتی‌که این گزینه به Reject تنظیم شده باشد و سیستم‌عامل مهمان آدرس MAC آداپتور را به مقداری متفاوت با آن آدرسی که در فایل پیکربندی vmx. است تغییر دهد، سوئیچ همه‌ی فریم‌های ورودی به آداپتور ماشین مجازی را نادیده می‌گیرد[۱۸]. زمانی‌که سیستم‌عامل مهمان آدرس MAC را به مقدار اولیه خود برگرداند، ماشین مجازی دریافت فریم‌ها را از سر می‌گیرد.
  - Accept: درصورتی‌که سیستم‌عامل مهمان آدرس MAC یک آداپتور شبکه را تغییر دهد، آداپتور فریم‌ها را در آدرس جدید دریافت می‌کند.
- Forged transmits
  - Reject: سوئیچ هر فریم خروجی که آدرس MAC منبع آن با آدرسی که در فایل پیکربندی vmx. است، متفاوت باشد را نادیده می‌گیرد.
  - Accept: سوئیچ هیچ فیلترینگی انجام نمی‌دهد و به همه‌ی بسته‌های خروجی اجازه‌ی ارسال می‌دهد.



شکل ۱۷: ایجاد یک پورت‌گروه توزیع‌شده – تنظیمات امنیتی

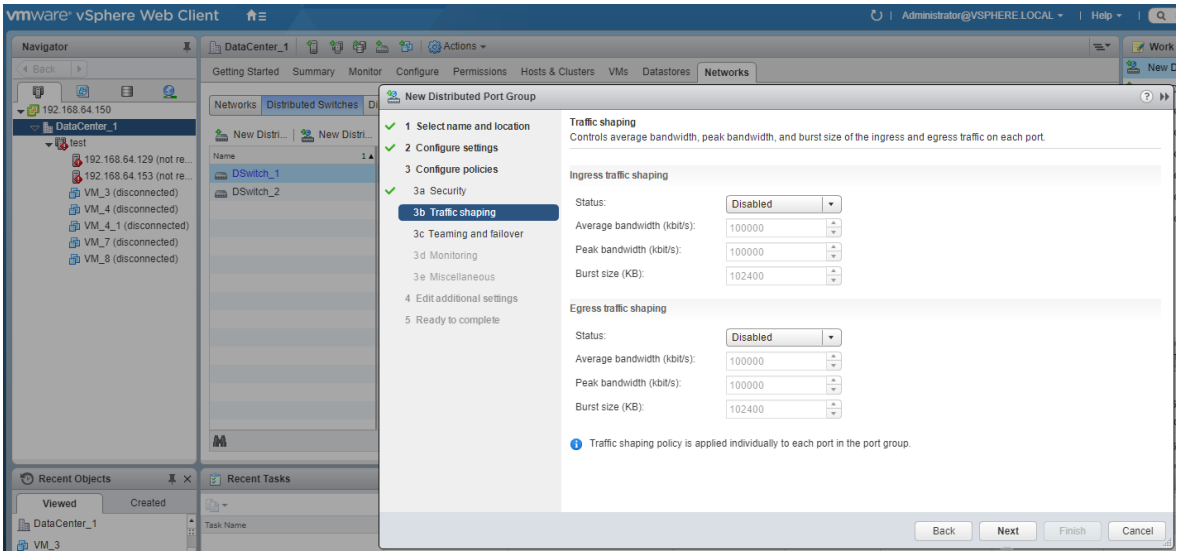
[۱۸] Drop

٤. در صفحه‌ی Traffic shaping، می‌توان شکل‌دهی ترافیک ورودی یا خروجی را فعال یا غیرفعال کرد (شکل ۱۸).

- Status: درصورتی‌که شکل‌دهی ترافیک ورودی یا خروجی را فعال کنید، بر روی مقدار پهنای باند شبکه‌ی تخصیص‌داده‌شده به هر آداپتور مجازی مرتبط با این پورت‌گروه خاص، محدودیت قرار می‌دهید. اگر این سیاست را غیرفعال کنید، سرویس‌ها به‌صورت پیش‌فرض یک اتصال آزاد به شبکه‌ی فیزیکی خواهندداشت.
- Average bandwidth: تعداد بیت در ثانیه را تعیین می‌کند که به‌طور میانگین در طول زمان، اجازه عبور از یک پورت را دارند. این مقدار همان بار متوسط مجاز[۱۹] است.
- Peak bandwidth: تعداد بیت در ثانیه را تعیین می‌کند که در زمان ارسال و دریافت یک ترافیک انفجاری[۲۰]، اجازه عبور از یک پورت را دارند. درواقع این گزینه پهنای باند استفاده‌شده توسط پورت را در زمان انفجار ترافیک افزایش می‌دهد.
- Burst size: حداکثر تعداد بایت‌هایی را نشان می‌دهد که می‌توان در یک انفجار مشاهده کرد. اگر این پارامتر تنظیم شود، پورت ممکن است، تا زمانی‌که از تمام پهنای باند اختصاص داده شده خود استفاده نکند، به‌صورت انفجاری ترافیک دریافت کند. هرگاه پورت، درهنگام وجود ترافیک انفجاری، نیاز به پهنای باند بیشتری نسبت به پهنای باند میانگین تعیین‌شده داشته‌باشد، ممکن است به‌طور موقت داده ها را با سرعت بالاتر انتقال دهد. این پارامتر تعداد بایت‌هایی که ممکن است در ترافیک انفجاری انباشته شوند را افزایش داده و در نتیجه انتقال با سرعت بیشتری انجام می‌شود.

[۱۹] Allowed average load

[۲۰] Burst



شکل ۱۸: ایجاد یک پورت‌گروه توزیع‌شده – شکل‌دهی به ترافیک

۵. در صفحه‌ی Teaming and failover، می‌توان تنظیمات زیر را ویرایش کرد (شکل ۱۹):

- Load balancing: مشخص می‌کند که یک uplink چگونه انتخاب شود.
  - Route based on originating virtual port: یک uplink را براساس پورت مجازی که ترافیک از طریق آن به سوئیچ توزیع‌شده وارد می‌شود انتخاب می‌کند.
  - Route based on IP hash: یک uplink براساس یک درهم‌سازی[۲۱] از آدرس‌های IP منبع و مقصد هر بسته، انتخاب می‌شود. برای بسته‌های غیر IP، هر آن‌چه در آفست‌های مربوط به این آدرس‌ها است، برای محاسبه درهم‌سازی استفاده می‌شود.
  - Route based on source MAC hash: یک uplink براساس درهم‌سازی آدرس اترنت انتخاب می‌شود.
  - Route based on physical NIC load: یک uplink براساس بارهای فعلی NICهای فیزیکی انتخاب می‌شود.
  - Use explicit failover order: همیشه از اولین گزینه در لیست آداپتورهای فعال مشخص‌شده برای failover، استفاده می‌کند.

[۲۱] Hash

نکته: دسته‌بندی مبتنی بر IP نیاز دارد که سوئیچ فیزیکی با EtherChannel پیکربندی شود. برای سایر گزینه‌ها EtherChannel را غیرفعال کنید.

- Network failure detection: روشی که برای تشخیص شکست استفاده می‌شود را تعیین می‌کند.
  - Link status only: تنها به وضعیت لینک که آداپتور شبکه ارائه می‌دهد، وابسته است. این گزینه خطاهای ناشی از کشیدن کابل و خطاهای برق سوئیچ فیزیکی را تشخیص می‌دهد، اما خطاهای پیکربندی مانند پورت سوئیچ فیزیکی که توسط پروتکل درخت پوشا[۲۲] مسدود شده است، یا پیکربندی اشتباه به VLAN غلط یا کشیدن کابل در طرف دیگر سوئیچ فیزیکی، را شناسایی نمی‌کند.
  - Beacon probing: یک نشانه[۲۳] را ارسال می‌کند و به بررسی‌های انجام شده توسط آن برروی همه‌ی NICهای قرارگرفته در تیم (دسته) گوش می‌دهد. بااستفاده از این اطلاعات، علاوه بر اطلاعات وضعیت لینک، شکست لینک را تعیین می‌کند. این حالت تعداد زیادی از شکست‌هایی که با بررسی وضعیت لینک به‌تنهایی قابل شناسایی نیستند را شناسایی می‌کند.

نکته: Beacon probing را به‌همراه تعادل بار مبتنی بر درهم‌سازی IP استفاده نکنید.

- Notify switches: Yes یا No را برای اخطاردادن به سوئیچ‌ها در هنگام شکست، انتخاب کنید. اگر Yes را انتخاب کنید، هرگاه یک NIC مجازی که به سوئیچ توزیع‌شده متصل است، یا هرگاه ترافیک یک NIC مجازی، به دلیل وقوع یک رویداد شکست، بر روی یک NIC فیزیکی متفاوت در تیم مسیریابی شود، به‌منظور به‌روزرسانی جداول جستجوی سوئیچ‌های فیزیکی، یک اخطار بر روی شبکه ارسال می‌شود. در تقریباً همه موارد، این فرآیند مطلوب است تا پایین‌ترین تأخیر ممکن برای رویدادهای شکست و مهاجرت با vMotion وجود داشته باشد.

[۲۲] Spanning Tree Protocol

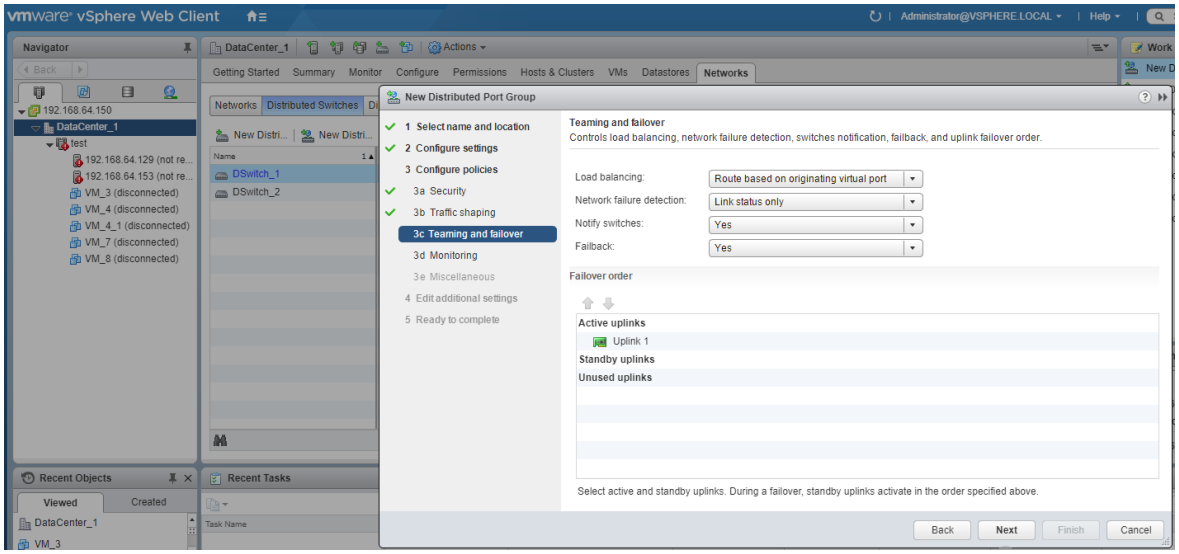
[۲۳] Beacon

- Failback: Yes یا No را برای فعال یا غیرفعال کردن failback انتخاب کنید. این گزینه تعیین می‌کند که چگونه یک آداپتور فیزیکی پس از ترمیم[۲۴] از یک شکست، به وظیفه فعال خود بازگردانده شود. اگر این گزینه به Yes تنظیم شده باشد، آداپتور بلافاصله پس از ترمیم به وظیفه فعال خود بازگردانده می‌شود، و جایگزین آداپتور جانشینی[۲۵] می‌شود که جای آن را گرفته بود. اگر این گزینه به No تنظیم شده باشد، یک آداپتور شکست‌خورده، حتی پس از ترمیم، غیرفعال باقی می‌ماند تا زمانی‌که یک آداپتور فعال فعلی دچار شکست شود و نیاز به جایگزین پیدا کند.
- Failover order: چگونگی توزیع بار کاری بین uplinkها را مشخص می‌کند. برای استفاده از برخی uplinkها، و ذخیره‌ی بقیه‌ی uplinkها برای موارد اضطراری که uplinkهای مورد استفاده با شکست مواجه می‌شوند، استفاده می‌شود. این شرایط را با قراردادن uplinkها در گروه‌های مختلف تنظیم کنید:
  - Active uplinks: تا زمانی که اتصال آداپتور شبکه برقرار و فعال است، به استفاده از این uplinkها ادامه می‌دهد.
  - Standby uplinks: درصورتی‌که اتصال آداپتور یکی از uplinkهای فعال از بین برود، از این uplinkها استفاده می‌شود.
  - Unused uplinkes: از این uplinkها استفاده نمی‌شود.

نکته: زمانی‌که از تعادل بار با استفاده از درهم‌سازی IP استفاده می‌کنید، standby uplinkها را پیکربندی نکنید.

[۲۴] Recovering

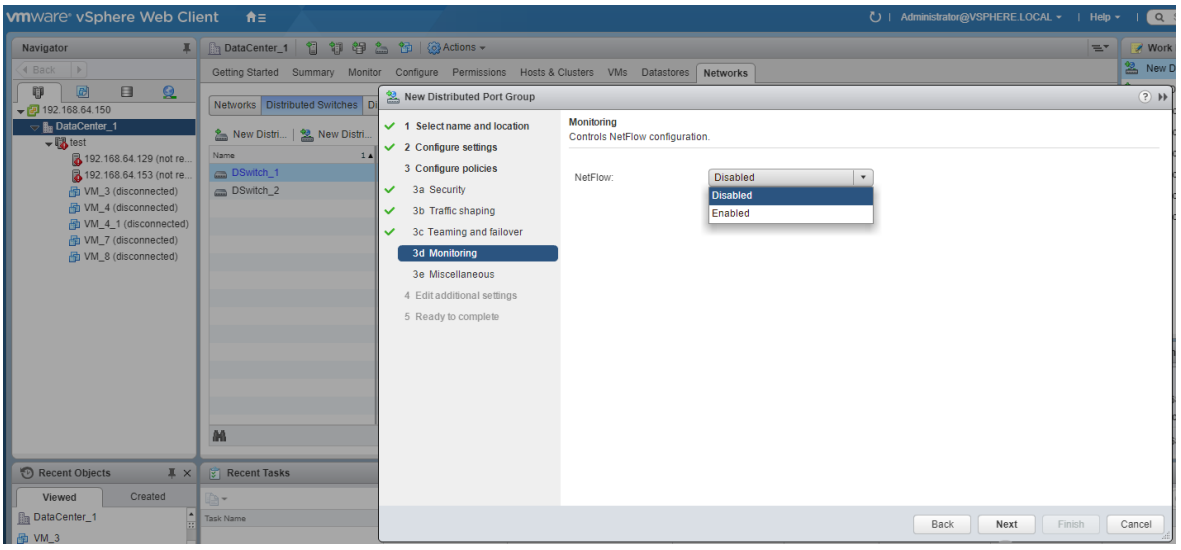
[۲۵] Standby



شکل ۱۹: ایجاد یک پورت‌گروه توزیع‌شده – دسته‌بندی و شکست

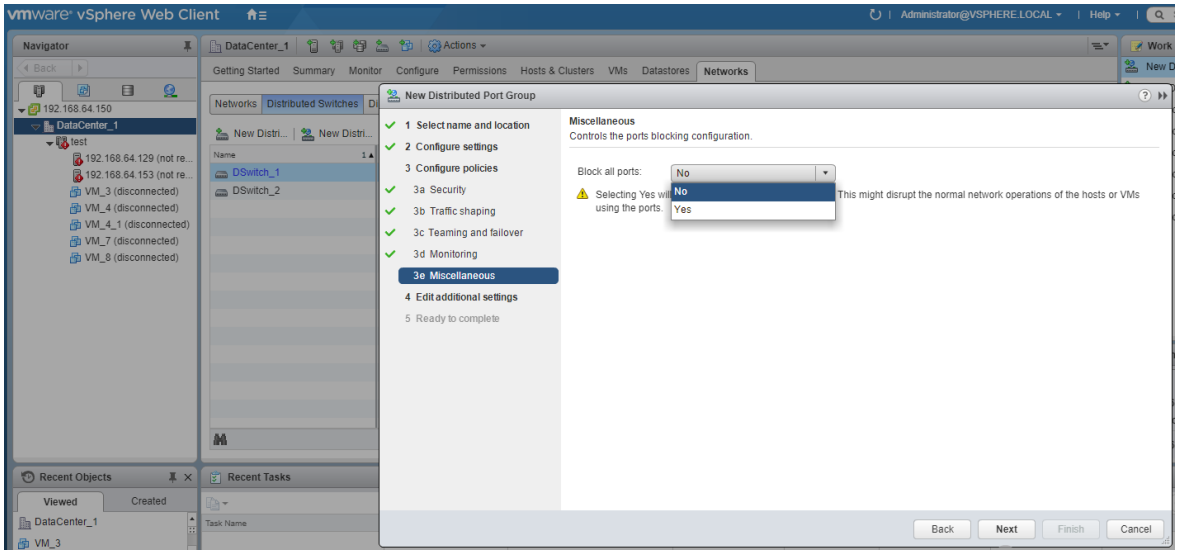
۶. در صفحه‌ی Monitoring، می‌توان NetFlow را فعال یا غیرفعال کرد (شکل ۲۰).

- Disabled: NetFlow برروی پورت‌گروه توزیع‌شده غیرفعال می‌شود.
- Enabled: NetFlow برروی پورت‌گروه توزیع‌شده فعال می‌شود. تنظیمات NetFlow در سطح سوئیچ توزیع‌شده‌ی vSphere قابل پیکربندی است.



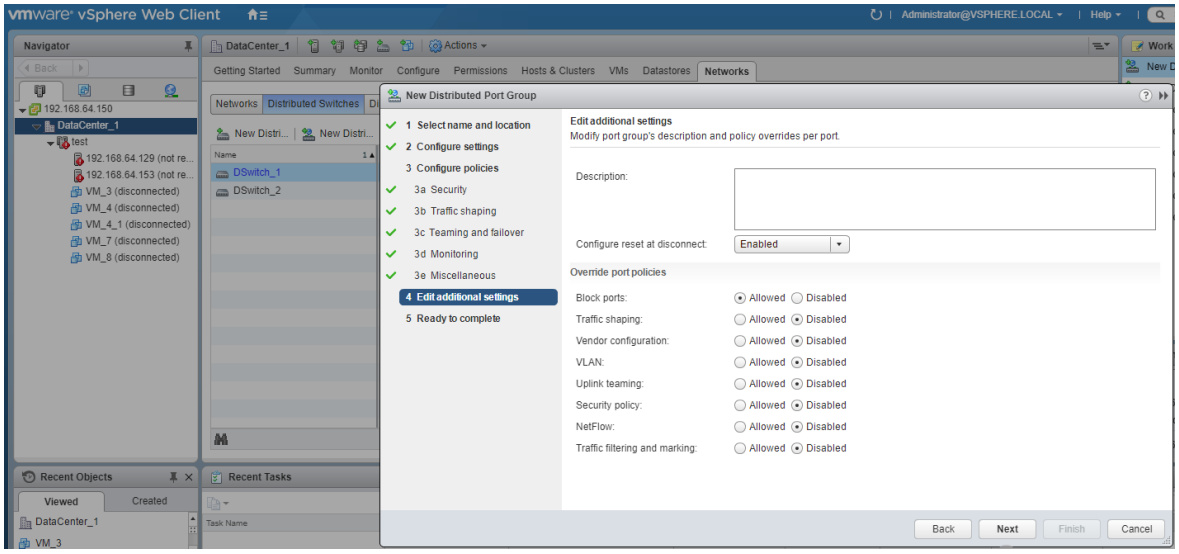
شکل ۲۰: ایجاد یک پورت‌گروه توزیع‌شده – نظارت

۷. در صفحه‌ی Miscellaneous می‌توانید Yes یا No را انتخاب کنید (شکل ۲۱). انتخاب Yes باعث می‌شود که همه‌ی پورت‌های پورت‌گروه خاموش شوند. این کار ممکن است عملکرد عادی شبکه‌ی میزبان‌ها یا ماشین‌های مجازی که به این پورت‌ها متصل هستند را مختل کند.



شکل ۲۱: ایجاد یک پورت‌گروه توزیع‌شده – سایر موارد

۸. در صفحه‌ی Edit additional settings، یک توصیف برای پورت‌گروه اضافه کنید و سیاست‌هایی که می‌خواهید به‌ازای پورت‌ها رونویسی[۲۶] کنید را مشخص کنید (شکل ۲۲).



شکل ۲۲: ایجاد یک پورت‌گروه توزیع‌شده – سایر تنظیمات

[۲۶] Override

۲-۵ رونویسی سیاست‌های شبکه در سطح پورت

به‌منظور اعمال سیاست‌های مختلف به پورت‌های توزیع‌شده، می‌توان سیاست‌هایی که در سطح پورت‌گروه پیکربندی می‌شوند را به‌ازای هر پورت رونویسی کرد (شکل ۲۳).

روش

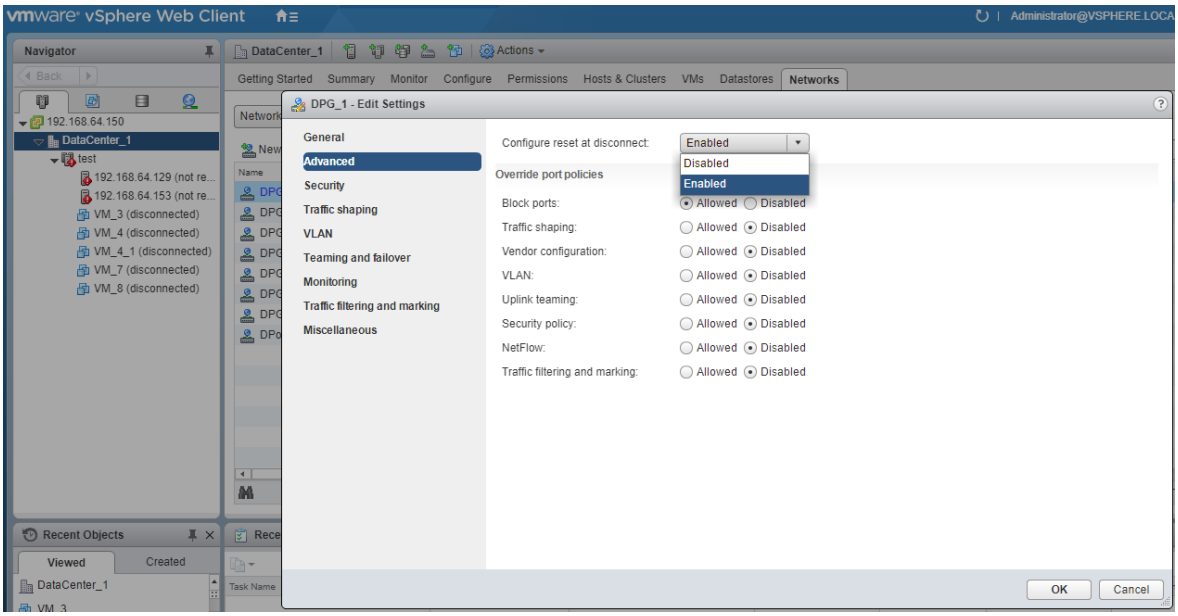
۱. پس از انتخاب سوئیچ توزیع‌شده برروی Distributed Port Groups کلیک کنید.

۲. برروی پورت‌گروه توزیع‌شده‌ی موردنظر را کلیک کرده و Edit Settings را انتخاب کنید.

۳. صفحه‌ی Advanced را انتخاب کنید.

- Configure reset at disconnect: درصورتی‌که این گزینه فعال شود، زمانی‌که یک پورت توزیع‌شده از یک ماشین مجازی جدا می‌شود، پیکربندی پورت توزیع‌شده به تنظیمات پورت‌گروه توزیع‌شده برگردانده می‌شود و رونویسی‌های سطح پورت نادیده گرفته می‌شوند.
- Override port policies: سیاست‌های پورت‌گروه توزیع‌شده، به‌منظور رونویسی در سطح پورت انتخاب می‌شوند.

٤. با استفاده از صفحات اختیاری بعدی می‌توان رونویسی‌های سطح پورت را انجام داد.



شکل ۲۳: رونویسی سیاست‌های پورت‌گروه در سطح پورت

۵-۳ نظارت بر وضعیت پورت‌های توزیع‌شده

vSphere می‌تواند بر پورت‌های توزیع‌شده نظارت داشته و در مورد وضعیت جاری و آمارهای زمان اجرای هر پورت، اطلاعاتی را ارائه دهد (شکل ۲٤).

روش

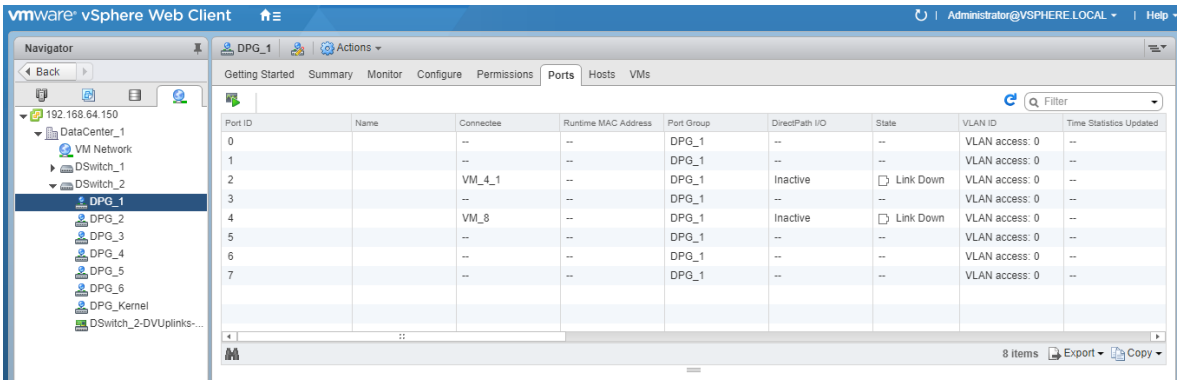
۱. پس از انتخاب سوئیچ توزیع‌شده برروی Distributed Port Groups کلیک کنید.

۲. برروی پورت‌گروه توزیع‌شده‌ی مورد نظر دابل‌کلیک کنید.

۳. سربرگ Ports را کلیک کنید. لیست پورت‌ها نشان داده می‌شود.

٤. برروی آیکون Start Monitoring Port State کلیک کنید. جدول پورت‌ها برای پورت‌گروه توزیع‌شده آمارهای زمان اجرا برای هر پورت توزیع‌شده را نشان می‌دهد. ستون State نمایش‌دهنده‌ی وضعیت فعلی هر پورت توزیع‌شده است.

- Link UP: لینک مربوط به این پورت توزیع‌شده در حال کار است.
- Link Down: لینک مربوط به این پورت توزیع‌شده از کار افتاده است.
- Blocked: پورت توزیع‌شده بلاک شده است.
- --: وضعیت پورت توزیع‌شده در حال حاضر دردسترس نیست.



شکل ۲٤: نظارت بر وضعیت پورت‌های توزیع‌شده

۵-٤ اتصال یک ماشین مجازی به یک سوئیچ توزیع‌شده‌ی vSphere

به دو روش می‌توان ماشین‌های مجازی را به سوئیچ توزیع‌شده‌ی vSphere متصل کرد: با پیکربندی یک NIC ماشین مجازی خاص، یا با مهاجرت‌دادن گروهی از ماشین‌های مجازی به/از سوئیچ توزیع‌شده‌ی vSphere.

۵-٤-۱ اتصال یک ماشین مجازی خاص به یک پورت‌گروه توزیع‌شده

یک ماشین مجازی خاص را با تغییر پیکربندی NIC آن می‌توانید به یک سوئیچ توزیع‌شده‌ی vSphere متصل کنید (شکل ۲۵).

روش

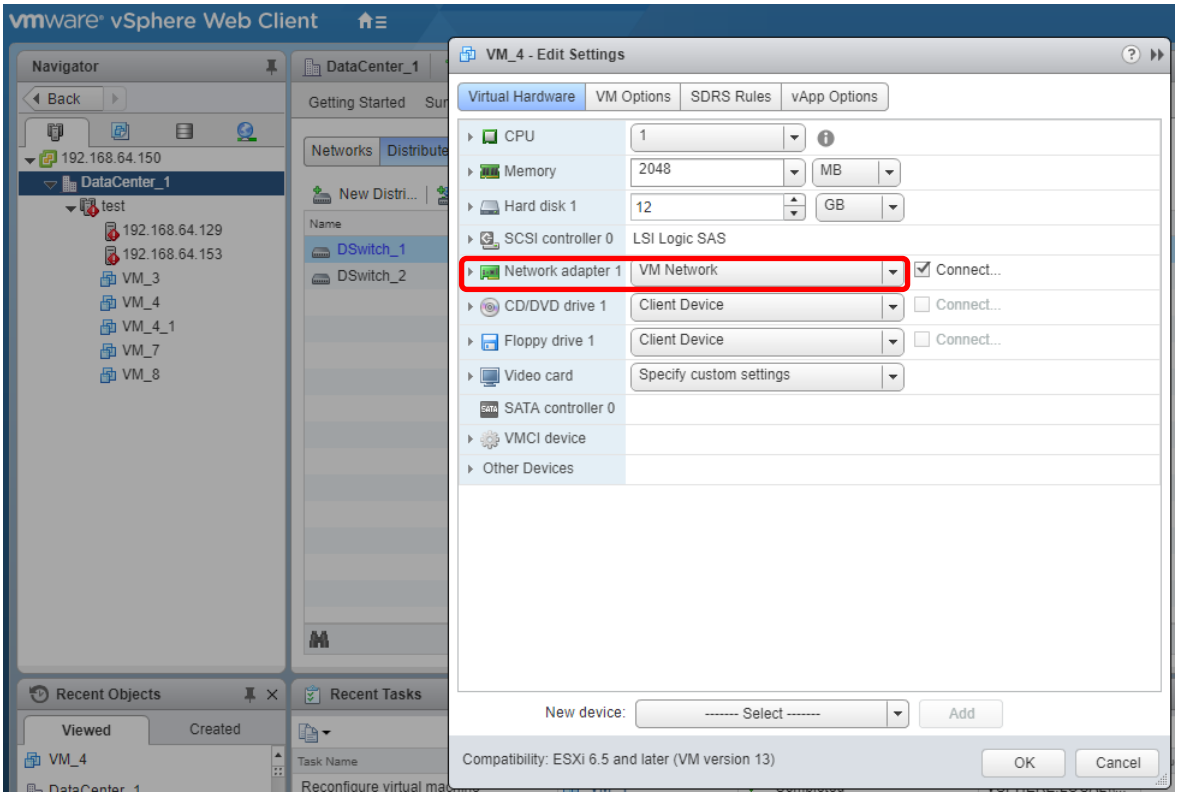
۱. با انتخاب یک میزبان و کلیک برروی سربرگ VMs می‌توانید ماشین‌های مجازی آن میزبان را مشاهده کنید.

۲. ماشین مجازی موردنظر را انتخاب کرده و در سربرگ Configure از آن ماشین مجازی، Settings و سپس VM Hardware را انتخاب کنید.

۳. Edit را کلیک کنید.

٤. قسمت Network adapter را باز کرده و از منوی Network adapter گزینه‌ی Show more networks را انتخاب کنید.

۵. پورت‌گروه توزیع‌شده‌ی مورد نظر را انتخاب کنید.



شکل ۲۵: اتصال یک ماشین مجازی خاص به یک پورت‌گروه توزیع‌شده

۵-٤-۲ مهاجرت‌دادن ماشین‌های مجازی به/از سوئیچ توزیع‌شده‌ی vSphere

علاوه بر اتصال ماشین‌های مجازی به یک سوئیچ توزیع‌شده در سطح یک ماشین مجازی خاص، می‌توانید یک گروه از ماشین‌های مجازی را بین شبکه‌ی سوئیچ توزیع‌شده‌ی vSphere و شبکه‌ی سوئیچ استاندارد vSphere مهاجرت دهید (شکل ۲٦).

روش

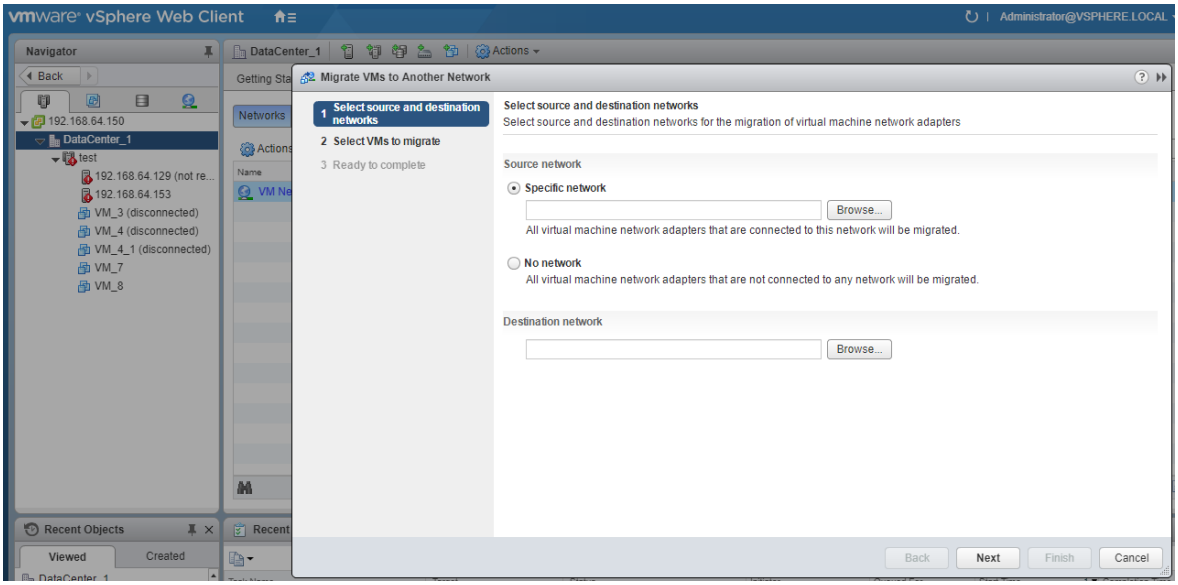
۱. در vSphere Web Client برروی مرکز داده کلیک‌راست کرده و Migrate VMs to Another Network را انتخاب کنید.

۲. یک شبکه‌ی منبع را انتخاب کنید.

- Specific network را انتخاب کرده و از دکمه‌ی Browse برای انتخاب یک شبکه‌ی منبع خاص استفاده کنید.
- No network را انتخاب کنید تا تمام آداپتورهای شبکه‌ی ماشین‌های مجازی که به هر شبکه‌ای متصل هستند، مهاجرت داده شوند.

۳. از Browse برای انتخاب شبکه‌ی مقصد استفاده کنید.

٤. از لیست نشان داده شده ماشین‌های مجازی را برای مهاجرت از شبکه‌ی منبع به شبکه‌ی مقصد انتخاب کنید.



شکل ۲٦: مهاجرت‌دادن ماشین‌های مجازی به/از سوئیچ توزیع‌شده‌ی vSphere

٦ شبکه‌های محلی مجازی خصوصی

قطعه‌بندی سیستم‌هایی که در یک دامنه همه‌پخشی (VLAN) قرار گرفته‌اند را شبکه‌های محلی مجازی خصوصی می‌گویند. این کار بدون نیاز به انجام کارهایی مانند فیلترکردن آدرس MAC انجام می‌شود. یک PVLAN را می‌توان یک VLAN داخل یک VLAN دیگر (VLAN تو در تو) در نظر گرفت. به‌عبارت دیگر VLANهای خصوصی[۲۷] برای حل محدودیت‌های مربوط به شناسه VLAN مورد استفاده قرار می‌گیرند، و این کار را با اضافه کردن قطعه‌های بیشتر به یک دامنه همه‌پخشی منطقی و تبدیل آن به چندین زیردامنه‌ی همه پخشی کوچکتر، انجام می‌دهند.

یک PVLAN شامل یک VLAN اصلی و چندین VLAN جانبی است. یک VLAN خصوصی توسط شناسه VLAN اصلی[۲۸] خود شناخته می‌شود. یک شناسه VLAN اصلی می‌تواند چندین شناسه VLAN جانبی[۲۹] را همراه با خود داشته باشد. بنابراین VLANهای جانبی قطعه‌بندی درون VLAN اصلی را انجام می‌دهند.

سه نوع VLAN جانبی وجود دارد: Promiscuous، Isolated، و Community. سیستم‌های قرارگرفته در Promiscuous VLAN می‌توانند با Isolated VLAN و Community VLANها ارتباط برقرار کنند (مانند VLAN اصلی). سیستم‌های قرارگرفته در Isolated VLAN می‌توانند تنها با سیستم‌هایی که در Promiscuous VLAN هستند ارتباط برقرار کنند، نه حتی با دیگر سیستم‌های Isolated VLAN. لازم به ذکر است که در یک PVLAN تنها یک Isolated VLAN قابل تعریف است. Isolated VLAN معمولاً برای سرویس‌دهنده‌هایی استفاده می‌شود که نیاز به ارتباط با دیگر سرویس‌دهنده‌ها ندارند و تنها با سیستم‌های معمولی شبکه باید ارتباط برقرار کنند. سیستم‌های قرار گرفته در Community VLAN می‌توانند هم با سیستم‌هایی که در Promiscuous VLAN هستند ارتباط برقرار کنند و هم با دیگر سیستم‌های Community VLAN خود. Community VLANها معمولاً برای سرویس‌دهنده‌هایی استفاده می‌شود که هم نیاز به ارتباط با دیگر سرویس‌دهنده‌ها دارند و هم نیاز به ارتباط با سیستم‌های معمولی شبکه.

---

[۲۷] Private VLANs

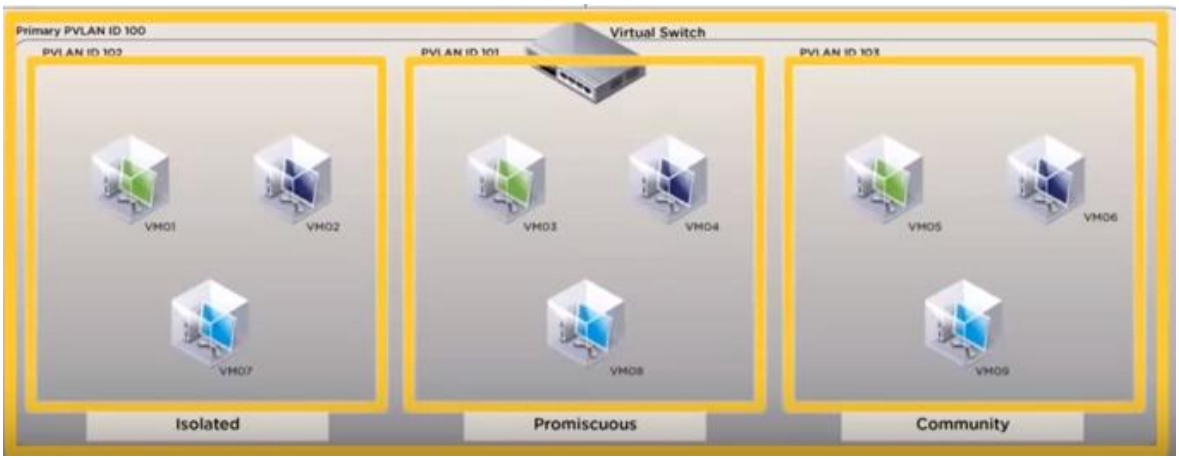
[۲۸] Primary VLAN ID

[۲۹] Secondary VLAN ID

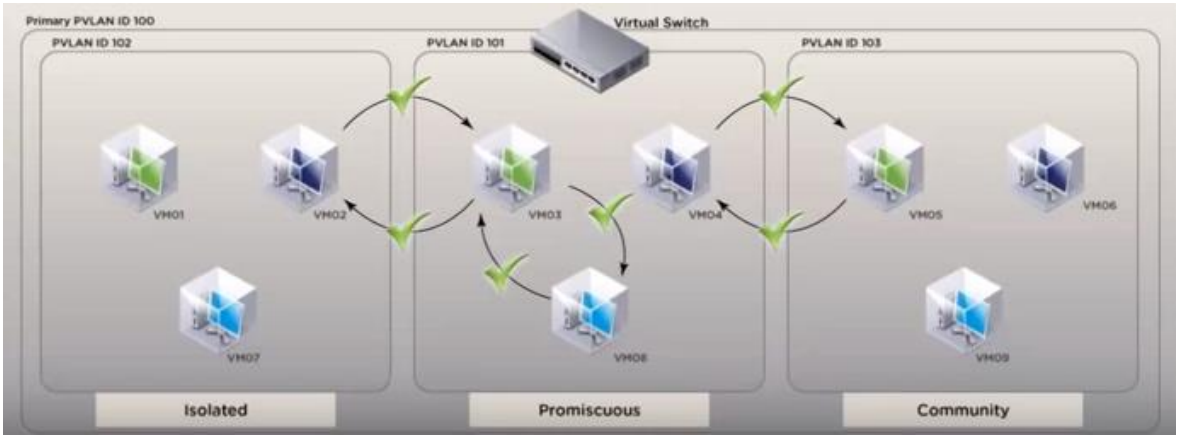
جدول ۱: انواع VLANهای جانبی قابل‌تعریف برای یک VLAN خصوصی و ویژگی‌های آن‌ها

نوع VLAN جانبی	ارتباط	کاربرد
Promiscuous	چندین Community VLAN یک Isolated VLAN	دستگاه‌هایی مانند دیواره‌های آتش (معمولاً مشابه VLAN اصلی هستند)
Isolated	دستگاه‌های روی Promiscuous VLAN با دیگر دستگاه‌های Isolated VLAN خود نمی‌توانند ارتباط برقرار کنند	سرویس‌دهنده‌هایی که نیاز به ارتباط با دیگر سرویس‌دهنده‌ها ندارند و تنها با دستگاه‌های معمولی شبکه باید ارتباط برقرار کنند
Community	دستگاه‌های روی Promiscuous VLAN دستگاه‌های روی Community VLAN خود	سرویس‌دهنده‌هایی که هم نیاز به ارتباط با دیگر سرویس‌دهنده‌ها دارند و هم نیاز به ارتباط با سیستم‌های معمولی شبکه

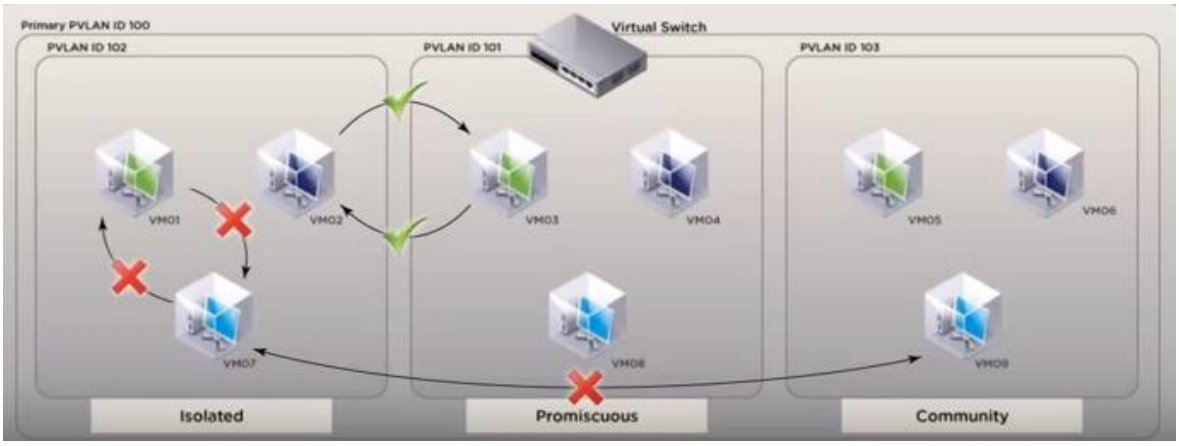
شکل ۲۷ یک VLAN خصوصی به‌همراه سه VLAN جانبی از نوع‌های Promiscuous، Isolated و Community را نشان می‌دهد. در شکل ۲۸ ارتباطات ممکن بین ماشین‌های مجازی در VLAN جانبی از نوع Promiscuous نشان داده شده است. شکل‌های ۲۹ و ۳۰ نیز ارتباطات ممکن بین ماشین‌های مجازی در VLANهای جانبی از نوع Isolated و Community را نشان می‌دهند.



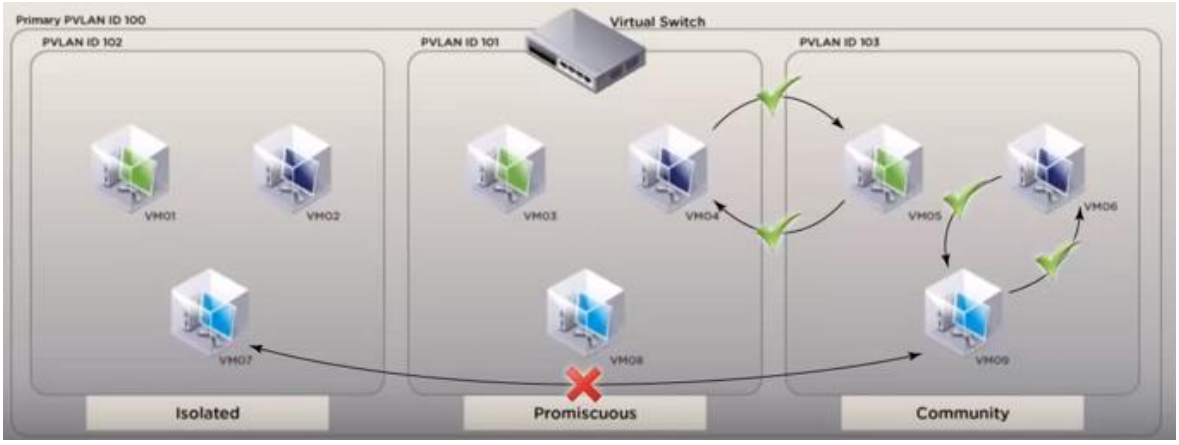
شکل ۲۷: یک VLAN خصوصی به‌همراه سه VLAN جانبی



شکل ۲۸: ارتباطات ممکن بین ماشین‌های مجازی در VLAN جانبی از نوع Promiscuous



شکل ۲۹: ارتباطات ممکن بین ماشین‌های مجازی در VLAN جانبی از نوع Isolated



شکل ۳۰: ارتباطات ممکن بین ماشین‌های مجازی در VLAN جانبی از نوع Community

نکته: برای اینکه 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 باشد.

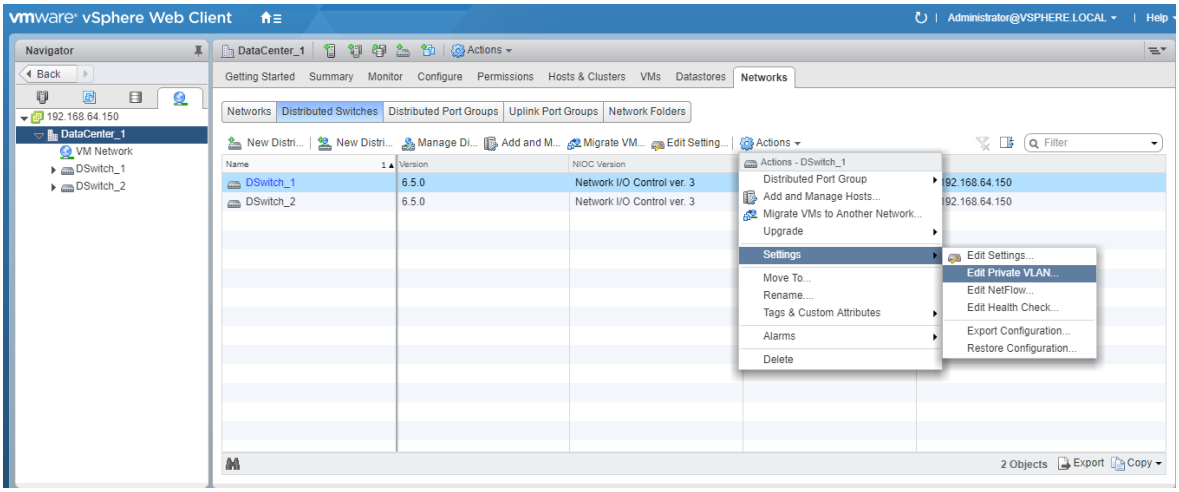
۱-۶ ایجاد یک VLAN خصوصی در محیط vSphere

VLANهای خصوصی مورد نیاز را روی سوئیچ توزیع‌شده vSphere ایجاد کنید تا بتوانید پورت‌های توزیع شده را به یک VLAN خصوصی اختصاص دهید.

روش

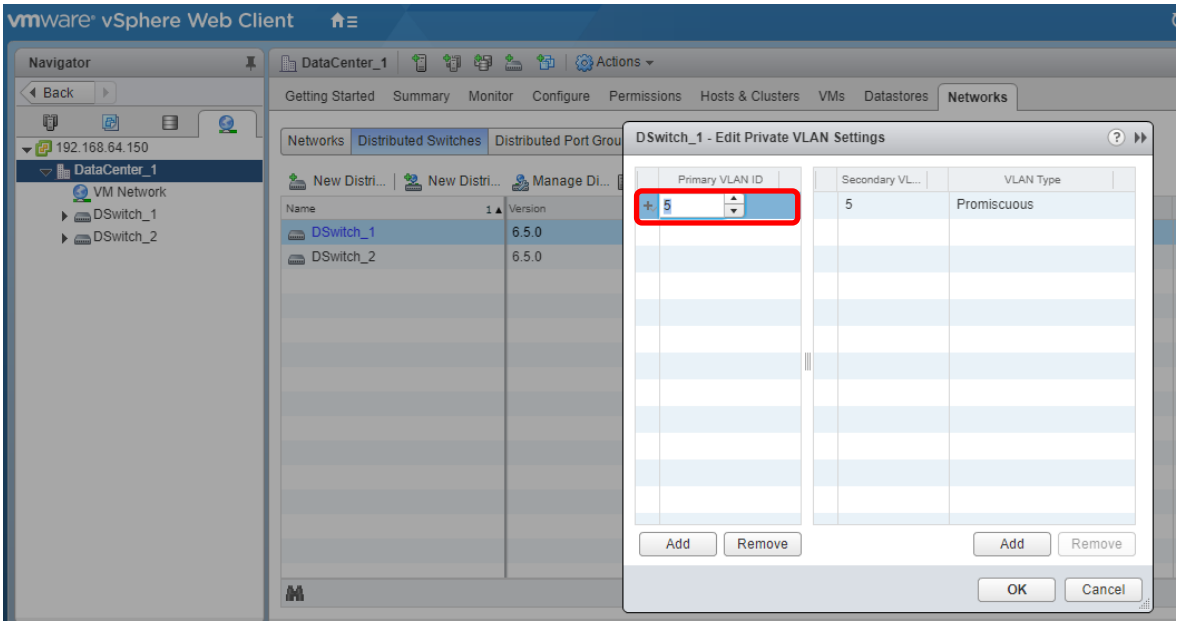
۱. در vSphere Web Client، سوئیچ توزیع‌شده را انتخاب کنید.

۲. از منوی Actions گزینه‌ی Settings را باز کرده و سپس Edit Private VLAN را انتخاب کنید (شکل ۳۱).



شکل ۳۱: ایجاد یک VLAN خصوصی

۳. برای اضافه کردن یک VLAN اصلی، زیر Primary VLAN ID بر روی Add کلیک کرده و ID یک VLAN اصلی را وارد کنید (شکل ۳۲).



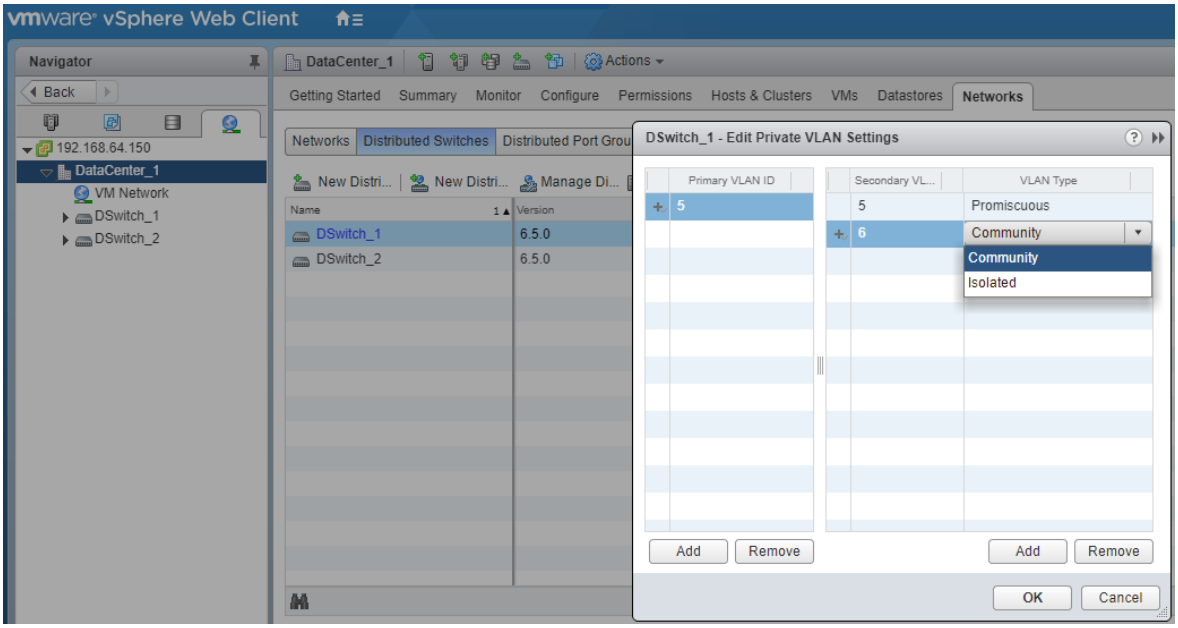
شکل ۳۲: ایجاد یک VLAN خصوصی – اضافه‌کردن VLAN اصلی

٤. 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 می‌شود.

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

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

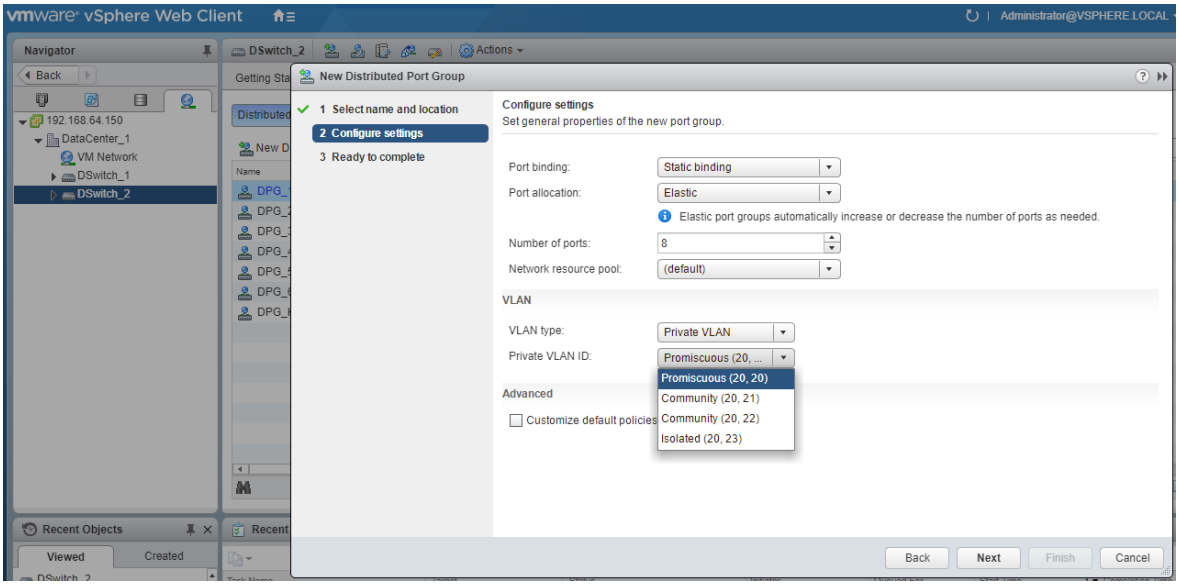
٧. از منوی کشویی ستون secondary VLAN type، یا Isolated و یا Community را انتخاب کنید (شکل ۳۳).



شکل ۳۲: ایجاد یک VLAN خصوصی – اضافه‌کردن VLAN جانبی

۲-۶ تخصیص یک VLAN خصوصی به یک پورت‌گروه

پس از ایجاد حداقل یک VLAN خصوصی برروی سوئیچ توزیع‌شده، این امکان به‌وجود می‌آید که درهنگام ایجاد یک پورت‌گروه توزیع‌شده‌ی جدید نوع VLAN را به Private VLAN تنظیم کنیم. در این‌صورت از منوی Private VLAN ID می‌توان یکی از VLANهای جانبی تعریف‌شده برای آن VLAN خصوصی را انتخاب کرد و به پورت‌گروه توزیع‌شده تخصیص داد (شکل ۳۳).



شکل ۳۳: تخصیص یک VLAN خصوصی به یک پورت‌گروه توزیع‌شده