کتاب

VMware NSX-V Network Virtualization

Fast Track

به زبان فارسی


بسم الله الرحمن الرحيم

VMware NSX-V Network Virtualization

Fast Track

مهندس ابوالفضل هاشمی

a.hashemi70@gmail.com

فهرست

Introduction – ۱

امروزه با پیشرفت تکنولوژی و پروتکل‌های شبکه، مدیران IT به سمت راه‌کارهای آسان‌تر، مطمئن‌تر و راه‌کارهایی که وابسته به سخت‌افزار نباشند، در حال حرکت هستند. مجموعه Software Defined X (SDX) یا محصولات مبتنی بر نرم‌افزار این حقیقت را به معرض نمایش گذاشته‌اند. این نرم‌افزارها باعث کاهش خطای انسانی، مدیریت آسان‌تر، سرعت بیشتر و موارد دیگر می‌شوند. نمونه‌ای از این نرم‌افزارها شامل Software Defined Storage (SDS)، Networking (SDN) و Data Center (SDDC) می‌شوند. Software Defined Networking یا شبکه مبتنی بر نرم‌افزار در واقع روشی است متمرکز برای طراحی، ساخت و مدیریت شبکه‌ها که محدوده کنترل (Control Plane) و محدوده داده (Data Plane) شبکه را جدا می‌کند. به عبارت دیگر تنظیمات و پیکربندی شبکه با نرم‌افزار تعریف می‌شود و دیگر موارد برعهده دستگاه‌های شبکه است. بطور مثال پروتکل OSPF برای مسیریابی در شبکه تعریف می‌شود. سپس دستگاه‌های شبکه با پروتکلی که تعریف شده است این عمل را اجرایی می‌کنند. این ساختار گستردگی مخصوص به خود را دارد ولی در عین حال ساده و آسان است.

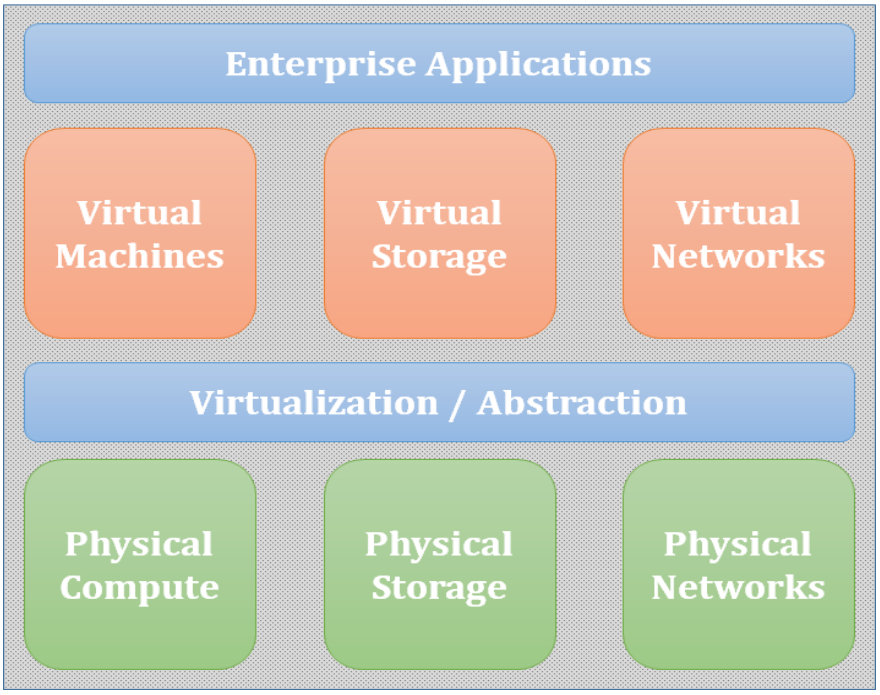
در این کتاب توضیح مختصری در رابطه با Software Defined Networking شرکت VMware به نام NSX پرداخته می‌شود. تاریخچه شبکه مبتنی بر نرم‌افزار به سال ۱۹۹۵ بر می‌گردد ولی در این چند سال اخیر موضوعی فوق العاده جذاب شده است. پس از خرید شرکت NICIRA توسط شرکت VMware به قیمت۱.۲۶ میلیارد دلار در 23 July 2012، VMware با مشارکت شرکت NICIRA شروع به کار کرد که در نتیجه محصولی به نام NVP به بازار ارائه گردید. این محصول در جهت محیط‌های غیر از VMware وارد بازار گردید. محصول VMware NSX در August 2013 بر پایه NPV برای محیط VMware ارائه شد.

در این کتاب سعی شده است علاوه بر توضیح مفاهیم کاربردی در این حوزه، نحوه پیاده‌سازی محصول VMware NSX 6.4 در بستر vSphere توضیح داده شود. هر شخص برای پیاده‌سازی و درک کافی از این مطالب، باید اطلاعاتی در مورد شبکه و مجازی‌سازی داشته باشد.

۲- Software Defined Networking

استفاده از محصولات مبتنی بر نرم‌افزار مرکز داده را به سمت Cloud نزدیک می‌کند. اصطلاح Software Defined به معنی انتقال دادن هوش یک سخت‌افزار خاص به نرم‌افزار است. بطور مثال زمانی که در مورد Distributed Firewall در NSX صحبت می‌شود، هیچ نگرانی در مورد Firewall سخت‌افزاری وجود ندارد. به عبارت دیگر فرض کنید یک Cisco ASA به یک نرم‌افزار تبدیل شده باشد. مجازی‌سازی (Virtualization) به معنای چکیده و یا جداکردن لایه‌ای از لایه دیگر است. در مراکز داده لایه‌ها و بخش‌های سخت‌افزاری متفاوتی مانند شبکه (Network)، سیستم ذخیره‌سازی(Storage)، سیستم محاسباتی (Compute) و ... وجود دارد. در بخش Physical Compute از هر سخت‌افزار و هر برندی می‌توان استفاده نمود که بستگی به سیاست‌های مرکز داده دارد. نرم‌افزارهای مجازی‌سازی در بخش Physical Compute به سخت‌افزار اهمیت زیادی نمی‌دهند، زیرا برروی سخت‌افزار لایه‌ای به نام Hypervisor قرار می‌گیرد و سخت‌افزار را مجازی‌سازی می‌کند. بطور مثال برروی سرورهای HP DL، Cisco UCS، Dell و ... می‌توان VMware ESXi نصب نمود که پس از نصب، سخت‌افزار مجازی‌سازی شده و مدیریت آن برعهده ESXi است. همچنین برای مجازی‌سازی Physical Storage می‌توان از نرم‌افزار VMware vSAN استفاده نمود. vSAN هر نوع دیسک و یا هر نوع Controller که از آن پشتیبانی می‌کند را مجازی‌سازی می‌نماید و Virtual Volumes (VVOLs) Datastore را در اختیار ماشین‌مجازی قرار می‌دهد. برای مجازی‌سازی Physical Networking می‌توان از VMware NSX استفاده نمود. بنابراین در هر بخش از مرکز داده می‌توان از محصولات مبتنی بر نرم‌افزار یا مجازی‌سازی استفاده نمود و همان قابلیت‌هایی که در لایه سخت‌افزار پیاده‌سازی و اجرا می‌شود را در لایه‌های بالایی مجازی‌سازی شده اجرا نمود.

Software Defined Data Center



در زمینه Software Defined Compute (SDC) می‌توان به محصولات VMware ESXi و Microsoft Hyper-V اشاره نمود. در زمینه Software Defined Storage (SDS) می‌توان به محصولاتی مانند VMware vSAN و EMC ViPR اشاره نمود. در زمینه Software Defined Networking (SDN) می‌توان به محصولاتی مانند VMware NSX و Juniper Contrail اشاره نمود.به گفته شرکت سیسکو نرم‌افزار Cisco ACI یک SDN است ولی این در حالی است که هنوز در ACI وابستگی به سخت‌افزار وجود دارد. در زمینه Software Defined Data Center (SDDC) یک مرکز داده تمام اتوماتیک وجود دارد که همه محصولات مبتنی بر نرم‌افزار توسط یک سیستم مرکزی مدیریت، کنترل و سیاست‌گذاری می‌شود. VMware vCenter یک نرم‌افزار SDDC است.

SDN می‌تواند به ایجاد و گسترش برنامه‌های کاربردی سرعت ببخشد. به عبارت دیگر ایجاد یک شبکه با سیاست‌های مختلف شامل قوانین Firewall، Load Balancing، Edge Services (NAT, VPN, ...) و دیگر سرویس‌های آن می‌تواند روزها و هفته‌ها به طول انجامد. این در حالی است که در صورت استفاده از SDN می‌توان شبکه را در چند ثانیه اجرا نمود. بطور مثال می‌توان Templateهایی از سیاست‌های شبکه ایجاد نمود و آن را برروی هر ماشین‌مجازی و یا سرویس دیگر بنابر سیاست مورد نیاز اعمال نمود.

شبکه‌های مبتنی بر نرم‌افزار با هدف چابکی، انعطاف‌پذیری و ارتقاء کنترل شبکه طراحی شده‌اند. ساختار SDN شامل سه جزء اصلی Controller، Southbound Application Program Interfaces (API) و Northbound Application Program Interfaces (API) می‌شود.

۲-۱- Controller

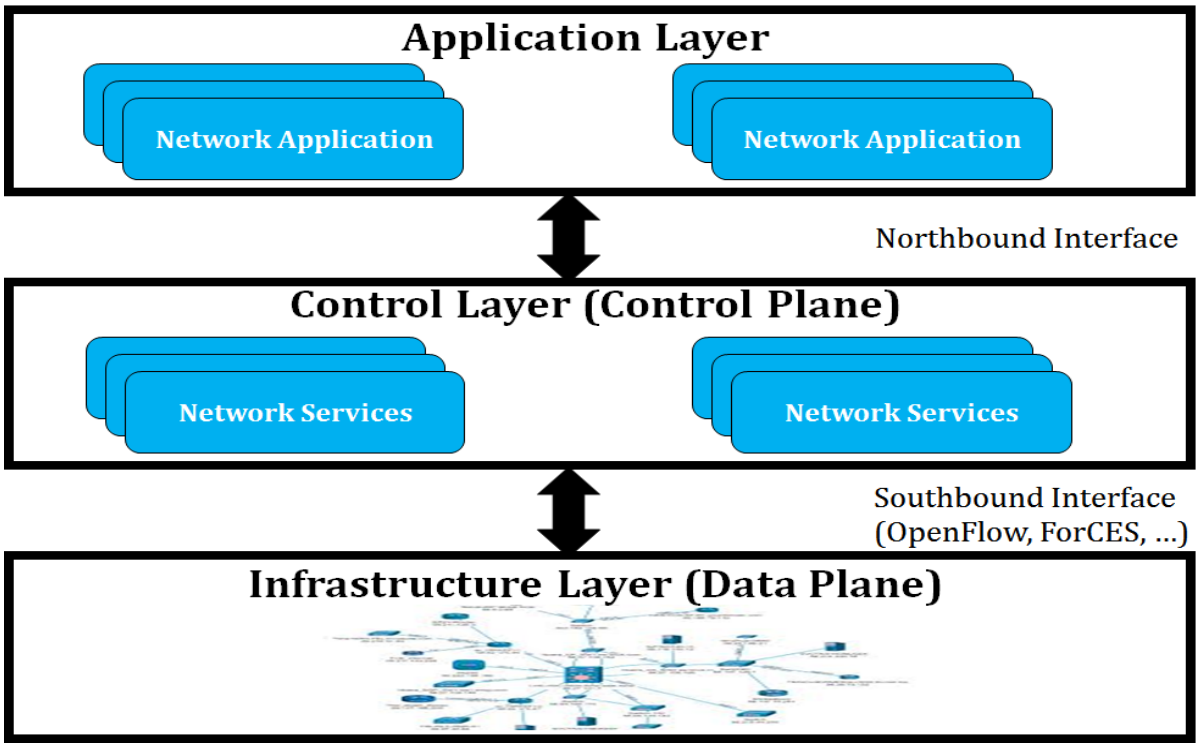
Controller به اصطلاح هسته اصلی شبکه است که یک دید متمرکز از تمامی شبکه و مدیران فعال شبکه ارائه می‌دهد. این مؤلفه تعیین می‌کند سیستم‌های لایه‌های پایین (Switch و Router) چگونه ترافیک شبکه را در محدوده Control Plane پردازش کنند. در واقع هر شبکه یک بخش Control Plane و یک بخش Data Plane دارد. در شبکه مباحث کنترلی و مدیریتی بین دستگاه‌ها مربوط به بخش Control Plane می‌شود و بخش Data Plane مربوط به ارسال بسته‌های ترافیک داده هستند.

۲-۲- Southbound APIs

SDN با استفاده از این API اطلاعات را بازنگری می‌کند و به دستگاه‌های شبکه (لایه پایین) ارسال می‌کند. OpenFlow اولین پروتکل استاندارد متن‌باز است که این عمل را انجام می‌دهد. در واقع OpenFlow یک قسمت خیلی کوچک از SDN است.

Northbound APIs -۳-۲

این API ارتباط بین SDN Controller و برنامه‌ها و سرویس‌های شبکه را فراهم می‌کند و در لایه بالای SDN است. این API به مدیران شبکه اجازه می‌دهد تا برنامه دلخواه خود را در مورد سرویس‌ها، توپولوژی شبکه و ... برنامه‌نویسی نمایند.



VMware NSX Introduction -۳

NSX محصولی از شرکت VMware است که در واقع کار نرم‌افزار Software Defined Network (SDN) را انجام می‌دهد. NSX دو محصول مختلف NSX-V برای محیط vSphere و NSX-T یا NSX-MH برای محیط‌هایی با Platformهای دیگر را ارائه می‌نماید. این نرم‌افزار شامل قابلیت‌های زیادی مانند Abstraction، Firewalling، Routing، Edge Services، Automatic، Reduce Traffic، Micro Segmentation است. Abstraction همان مجازی‌سازی در لایه شبکه است. Automatic انجام دادن تمامی کارها بصورت خودکار است که می‌توان شبکه را در چند دقیقه تنظیم نمود. برعکس تنظیم دستی که روزها طول می‌کشد که به اصطلاح Fast Provisioning گویند. Reduce Traffic به معنای کاهش بار ترافیکی شبکه است. ماشین‌ها مجازی برروی Hypervisor هستند، بنابر این ارتباطات داخلی مانند ترافیک امنیتی، مدیریتی و ... کاهش می‌یابند. در Micro Segmentation با قرار دادن NSX، ترافیک در همان Host یا Kernel Module انجام می‌شود. به عبارت دیگر شبکه را به قسمت‌هایی تکه تکه کرده و در همان تکه‌های کوچک ترافیک کنترل می‌شود.

VMware NSX Control Plane ۳-۱-

بخش مدیریتی و Control Plane مربوط به نرم‌افزار NSX بصورت Virtual Appliance است و هیچ نیازی به سرور یا دستگاه فیزیکی نیست. نسخه NSX-V برروی محیط VMware vSphere به عنوان یک ماشین‌مجازی یا VM نصب می‌گردد. پیشنها اکید می‌شود که این بخش مدیریتی و Control Plane بصورت Cluster اجرا شود و حداقل از سه NSX Manager Node استفاده گردد. در صورت استفاده از Cluster، قابلیت اطمینان و دسترسی‌پذیری افزایش می‌یابد. زمانی که NSX Manager نصب و یا Deploy می‌شود، هم‌زمان یک Kernel Module نیز برروی vSphere Host نصب می‌شود. این عملیات هیچ اختلالی ایجاد نمی‌کند و یک سرویس توزیع‌شده را فراهم می‌نماید. ابتدا Host در حالت Maintenance قرار داده می‌شود و سپس به NSX Cluster انتقال می‌یابد. در نهایت برروی آن ماژول‌های Firewall، Routing، VXLAN و ... نصب می‌شود و نیازی به Reboot شدن ندارد. در صورت استفاده از Standard Switch در محیط مجازی هیچ اختلالی در سرویس‌ها به وجود نمی‌آید ولی NSX نیاز به Distributed Switch دارد. در رابطه با زیرساخت فیزیکی باید توجه داشت که حداقل اندازه MTU 1600 برای ترافیک VXLAN نیاز است و همچنین پروتکل Internet Group Management Protocol (IGMP) Snooping باید برروی Switchهای لایه دو و Router لایه سه فعال باشد. دلایلی که از نرم‌افزار NSX استفاده می‌شود این است که مواردی همچون Network Abstraction، Automation، Distributed Logical Router (DLR)، Edge Services، Distributed Firewalling (DFW)، 3rd Party Extension را ارائه می‌نماید.

Network Abstraction ۳-۲-

یکی از دلایلی که از NSX استفاده می‌شود، Network Abstraction یا مجازی‌سازی لایه دو شبکه است. در Network Abstraction تمامی قابلیت‌های سخت‌افزاری شبکه ارائه می‌گردد و همچنین امکاناتی مانند گسترش لایه دو با استفاده از VXLAN، ایجاد Micro-Segmentation اختصاصی و عدم محدودیت در ۱۲ بیت برای VLAN وجود دارد که از شبکه فیزیکی فراتر رفته است.

Virtual Extensible LAN (VXLAN) به هدف بسته‌بندی (Encapsulation) پروتکل برای اجرا برروی زیرساخت شبکه لایه سه طراحی شده است. به عبارت دیگر به وسیله آن می‌توان شبکه لایه دو را در شبکه لایه سه توسعه داد. این امر به وسیله بسته‌بندی Frameهای لایه دو درون سرآیند VXLAN صورت می‌گیرد که به آن MAC-in-UDP نیز گفته می‌شود. VXLAN نیازی به STP ندارد و از پروتکل‌های مسیریابی پویای لایه سه برای رسیدن به بهترین مسیر استفاده می‌کند. همچنین دسترسی لایه دو بین مبدأ و مقصد را فراهم می‌کند و ترافیک مشتریان را در یک زیرساخت مشترک جداسازی و ایزوله می‌کند. از تعداد بیشتری (۲۴ بیت) برای شبکه منطقی مشابه VLAN پشتیبانی می‌کند. همانطور که گفته شد VXLAN نیاز به اندازه MTU 1600 دارد که می‌توان از Jumbo Frame استفاده نمود و حداقل نیاز به یک VLAN در زیرساخت فیزیکی دارد.

چند اصطلاح پروتکل VXLAN در زیر توضیح داده شده است.

۱. Underlay Network: به زیرساخت محیا شده برای ارسال ترافیک VXLAN گفته می‌شود که توسط Routing Protocolهای مختلف (Static Route، RIP، OSPF، EIGRP و IS-IS) مختلف انجام می‌شود.

۲. Overlay Network: شبکه‌ای‌که به کمک Underlay Network با پروتکل VXLAN ایجاد می‌شود تا شرایطی را مهیا سازد که دسترسی لایه ۲ از طریق شبکه IP برقرار شود.

۳. VXLAN Network Identifier (VNI): به منظور بالا بردن مقیاس‌پذیری و اختصاص یک شناسه به Frameهای لایه دو هنگام بسته‌بندی Ethernet Frame در داخل VXLAN استفاده می‌شود. سرآیند Dot1q که حامل VLAN TAG است پاک و در VXLAN Frame جایگزین می‌شودکه این عدد از ۱۲ بیت (VLAN) به ۲۴ بیت ارتقا یافته است.

۴. Virtual Tunnel End Points (VTEP): دستگاهی است که ترافیک ماشین‌مجازی را به پروتکل VXLAN، Encapsulate و Decapsulate می‌کند.

۵. Network Virtualization Edge (NVE): تونل ایجاد شده توسط VTEP با این نام دیده می‌شود.

۶. BUM Traffic: ترافیک‌های Broadcast، Unknown Layer-2 Unicast و Multicast هستند.

۳-۳- Edge Services

راهی برای جداسازی و تکه‌تکه کردن بخش‌های مختلف یک سازمان و یا برنامه‌های کاربردی است. اگر یک سازمان از بخش‌های مختلفی تشکیل شود، می‌توان برای هر بخش اطلاعات و دسترسی‌ها را جدا نمود و به راحتی آن را گسترش داد. به عبارت دیگر پل ارتباطی یا لبه است که کل شبکه در پشت آن قرار دارد و هر بخش از سازمان برای دسترسی به شبکه می‌تواند از سرویس‌های مختلفی مانند IPsec VPN استفاده کند. نمونه‌ای از سرویس‌هایی که در Edge ارائه می‌شود شامل Edge Firewall، Network Address Translation (NAT) و Routing Services هستند.

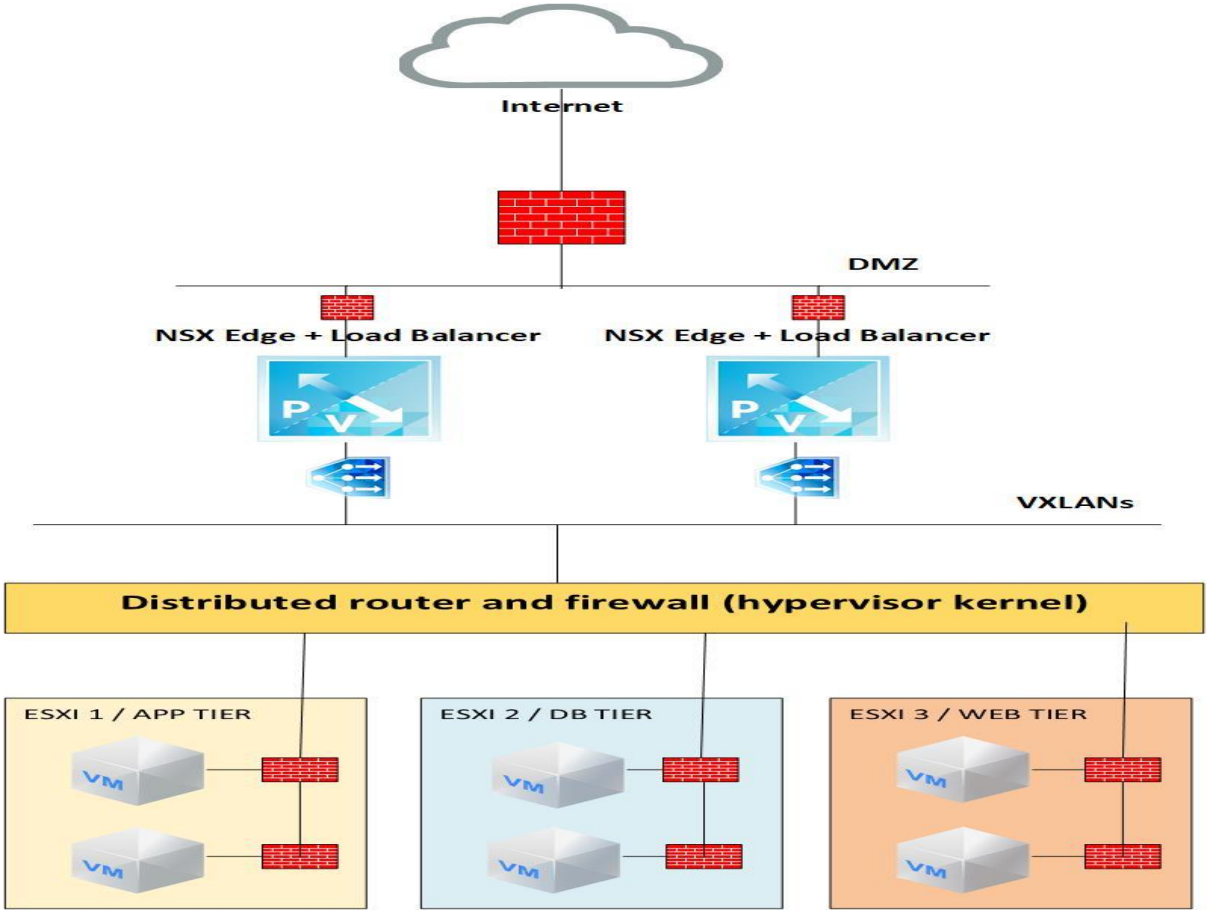
۳-٤- Distributed Firewalling and Routing

دیواره‌آتش و مسیریابی توزیع‌شده را می‌توان بهترین قابلیت NSX دانست. زمانی که در مورد ترافیک شبکه East-West صحبت می‌شود، منظور ترافیک درون مرکز داده است. بطور مثال ترافیک بین دو سرور در یک مرکز داده می‌تواند East-West باشد. زمانی که در مورد ترافیک شبکه North-South صحبت می‌شود، منظور ترافیک بین کاربر با سرور مرکز داده و یا ارتباط بین مراکز داده است. نرم‌افزار NSX بطور قابل ملاحظه‌ای

ترافیک East-West را کاهش می‌دهد. بطور مثال اگر دو ماشین‌مجازی برروی یک سرور ولی در VLANهای متفاوتی باشند، برای دسترسی به یکدیگر نیاز است بسته‌ها از Host خارج شوند و به Switch بالادستی در Rack ارسال شوند. این روند رو به بالا ادامه می‌یابد تا بسته‌ها به Router که ارتباط این دو VLAN را فراهم می‌کند ارسال شوند. بعد از پردازش Router روند رو به عقب برای ارسال به ماشین‌مجازی دیگر صورت می‌گیرد. حال اگر Distributed Routing استفاده شود و به معنای اینکه در هر Host یک مسیریاب جانمایی شود، می‌توان این ترافیک را کاهش داد. بطور مثال ابتدا بسته‌ها در Host بررسی می‌شوند و اگر ماشین مربوطه در همان Host باشد توسط این مسیریاب بسته‌ها ارسال می‌شوند. در مورد Distributed Firewall نیز به همین شکل است که ترافیک امنیتی را می‌توان کاهش داد. بنابراین با تعریف سیاست‌های امنیتی و مسیریابی برروی Host ترافیک شبکه کاهش پیدا می‌کند.

با تعریف سیاست‌های امنیتی می‌توان یک محیط Micro-Segmentation صحیح پیاده‌سازی نمود و یک فنس امنیتی بین برنامه‌های کاربردی و یا بخش‌های مختلف قرار داد. بطور مثال اگر چند VM با IP Subnet مشابه در یک Port Group باشند، می‌توان تعریف نمود که هیچ ترافیکی بین آنها جابه‌جا نشود.

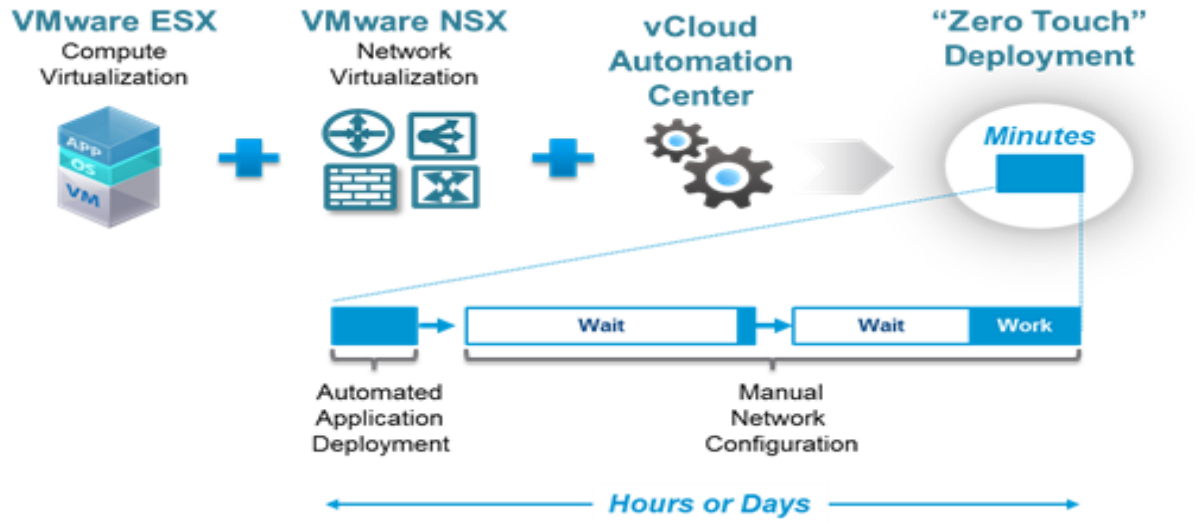
در روش Traditional Firewall یا دیوارآتش سنتی، ترافیک باید به Firewall فیزیکی ارسال و پردازش شود که این امر باعث افزایش ترافیک East-West می‌شود و سرعت پردازش بستگی به سخت‌افزار فیزیکی دارد. در روش Virtual Firewall یا دیوارآتش مجازی، ترافیک به Firewall مجازی یا Appliance ارسال



می‌شود که باز همان مشکلات در روش سنتی وجود دارد. در روش Distributed Firewall یا دیوارآتش توزیع‌شده، برروی هر Host سیاست‌های امنیتی اجرا می‌شود. این امر باعث می‌شود سرعت و عملکرد بالاتر برود زیرا وابستگی سخت‌افزاری کاهش یافته و ترافیک هنگام ورود به Host و یا خروج از Host بررسی می‌شود. اگر نیاز به Throughput بیشتری باشد مقدار RAM و CPU بیشتری مصرف می‌شود.

۳-۵- Automation

در مرحله آخر آماده‌سازی زمان بسیار کاهش می‌یابد و تغییرات در بخش کنترل و مدیریت کمتر رخ می‌دهد. پیاده‌سازی در مرحله آخر ممکن است هفته‌ها و یا ماه‌ها زمان ببرد و این در صورتی است که با استفاده از این قابلیت در چند دقیقه این کار انجام خواهد شد.



۳-۶- 3rd Party Extension

این قابلیت انعطاف‌پذیری بیشتری برای سرویس‌های اضافی فراهم می‌کند. این سرویس‌ها می‌تواند Intrusion Prevention/Detection System (IPS/IDS)، Anti-Malware، Firewall Later 7 و ... باشد. بطور مثال یک سازمان می‌تواند از محصولات شرکت Fortinet، Palo alto یا F5 استفاده نماید. در واقع این سرویس‌ها مانند یک افزونه در سطح Hypervisor نصب می‌شوند و باعث کاهش استفاده از منابع می‌شوند.

باید توجه داشت که سرویس‌های NSX توسط سرورهای مجود در Cluster پردازش می‌شوند و در صورت کمبود منابع و یا گسترش دادن محیط، می‌توان تعداد Hostهای بیشتری به Cluster اضافه نمود. پیشنهاد می‌شود که قابلیت‌های NSX برروی چند Cluster تقسیم شوند. بطور مثال Cluster مربوط به Edge Service از دیگر Clusterها جدا شود. بنابر سیاست هر سازمان می‌توان Cluster را خصوصی‌سازی نمود. بطور مثال اگر ترافیک در Edge Service بیشتر از دیگر ترافیک‌ها باشد از سرورها با کارت‌های شبکه بهتری استفاده شود.

٤- VMware NSX Components & Architecture

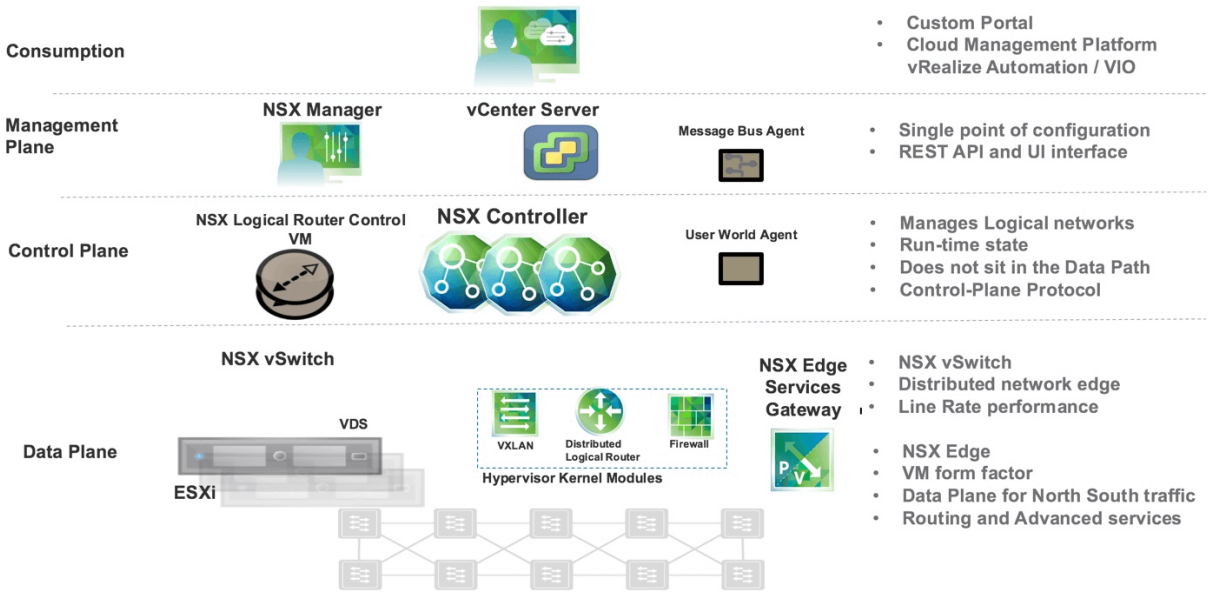
نرم‌افزار NSX از بخش‌های زیادی تشکیل نشده است و به راحتی نصب می‌شود. مدیر سیستم فقط NSX Manager را از طریق vCenter نصب یا Deploy می‌کند. پس از آن بقیه قسمت‌ها توسط NSX Manager

نصب یا Deploy می‌شوند. NSX Manager یک فایل با فرمت OVA یا Virtual Appliance است که از طریق vCenter به راحتی Deploy می‌شود. ابتدا باید NSX Manager نصب شود.

در مرحله دوم NSX Controller که مربوط به Control Plane یا بخش کنترلی است و عملیات‌های مختلف NSX را پردازش می‌کند، نصب می‌شود. تعداد NSX Controller Node باید سه Node باشد. در ادامه دلیل استفاده از این تعداد توضیح داده می‌شود. این تنظیمات برروی vCenter و از طریق NSX Manager صورت می‌گیرد.

در مرحله سوم افزونه‌ای برروی تمام vSphere Hosts نصب می‌شود. پس از ساخت Cluster در داخل vCenter و اضافه نمودن تعدادی Host به آن، نوبت به اضافه افزونه NSX به هر Host می‌رسد. این افزونه باعث برقراری ارتباط بین Host و Controller می‌شود. Host Kernel Module یا User World Agent (UWA) افزونه‌ای است که برروی vSphere Host اضافه می‌شود. برروی هر Host دو UWA به نام‌های Message Bus Client (vShield Firewall Daemon (vsfwd)) و Control Plane (netcpa) اضافه می‌شوند.

در مرحله آخر برروی محیط آماده شده، سرویس‌های شبکه مانند Edge، Distributed Router Controller و ... اجرا و تنظیم می‌شوند. باید توجه داشت که تمامی مؤلفه‌های نام برده بصورت مجازی یا Virtual هستند. پیشنهاد اکید می‌شود که بعضی از این مؤلفه‌ها بصورت Cluster یا چندتایی اجرا شوند که این امر سبب دسترسی‌پذیری و قابلیت اطمینان بالا می‌شود. در ادامه هر بخش به اختصار توضیح داده می‌شود.



Data Plane ٤-١-

در بخش Data Plane اطلاعات مربوط به NSX Virtual Switch قرار می‌گیرد. این اطلاعات بر پایه Virtual Distributed Switch (VDS) است که مؤلفه‌های اضافی برروی آن نصب می‌شوند. Kernel

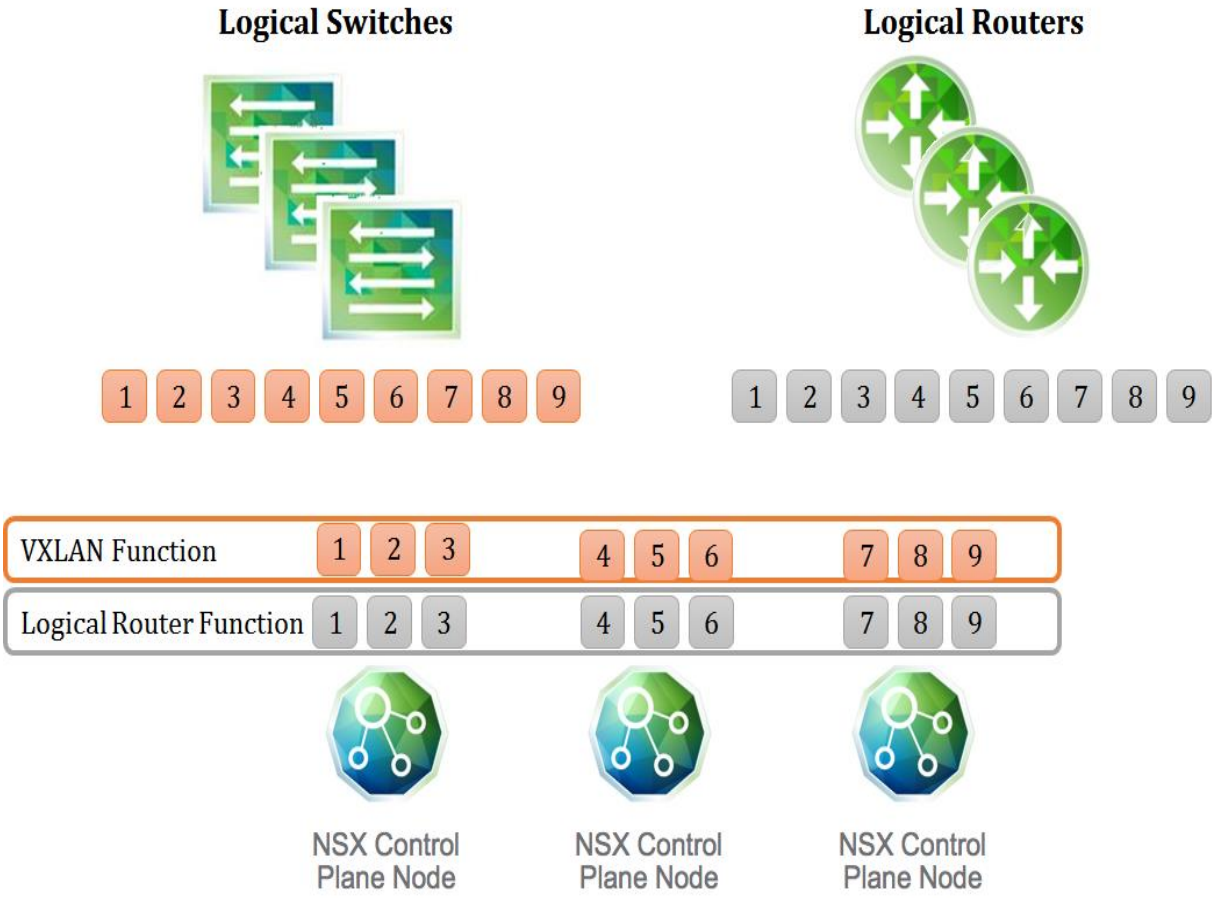
Module، Configuration/Installation Files و ... در قالب فایل‌های VIB جمع شده‌اند و اجرای آنها باعث اجرای سرویس‌هایی مانند Distributed Routing، Logical Firewall و فعال کردن VXLAN برروی Virtual Switch می‌شود. این بخش در قسمت مدیریتی قرار ندارد ولی به کار خود ادامه می‌دهد. در بخش Kernel Module مربوط به Data Plane سه مؤلفه Distributed Logical Router (DLR)، Distributed Firewall (DFW) و VXLAN جای گرفته است. همچنین VDS برای ایجاد و مدیریت Port Groupها مورد نیاز است. Edge Services نیز بصورت Virtual Appliance یا ماشین‌مجازی بصورت جداگانه نصب می‌شود که در همین بخش Data Plane قرار دارد.

٤-٢- Control Plane

این بخش داخل NSX Controller Cluster اجرا می‌شود. NSX Controller یک سیستم مدیریتی توزیع شده مرکزی پیشرفته است که عملیات Control Plane مربوط به Logical Switching و Logical Routing را فراهم می‌کند. به عبارت دیگر تنظیمات و تغییرات مدیریتی را اعمال و مشخص می‌کند که هر مؤلفه چه وظایفی را برعهده دارد. NSX Controller Cluster ماژول‌های Distributed Switching و Distributed Routing داخل Hypervisor را مدیریت می‌کند. باید توجه داشت که در هر Cluster باید سه Controller Node برای مقیاس‌پذیری و دسترسی‌پذیری وجود داشته باشد. استفاده از سه Controller باعث جلوگیری از سناریوی Split-Brain می‌شود و به معنای این است که اطلاعات در هر سه هماهنگ و Sync می‌ماند. هر خطایی برروی یک Controller Node هیچ تأثیری برروی ترافیک Data Plane ندارد ولی در صورت از بین رفتن همه Nodeها ترافیک Data Plane دچار اشکال می‌شود. با استفاده از NSX Manager می‌توان NSX Controller Nodeها را Deploy نمود. بخشی از وظایف Control Cluster ارائه API، Switch Manager، Server Directory، Logical Manager و ... است. همچنین بخش Control Plane وظیفه مدیریت UWA را برعهده دارد و به VXLAN و DLR در Kernel Module فرمان می‌دهد که چه وظایفی برعهده دارند. مدیریت DFW در Kernel Module برعهده Control Plane نیست. NSX Manager وظیفه تنظیم و مدیریت سرویس‌های مسیریابی را برعهده دارد. NSX Manager همچنین ماشین‌مجازی به نام Logical Router Control Virtual Machine را Deploy می‌کند و تنظیمات Logical Interface (LIF) را برروی هر Host که داخل Control Cluster قرار دارد، اعمال می‌کند. Logical Router Control Virtual Machine یک مؤلفه در Control Plane است که وظیفه پردازش اطلاعات مسیریابی را برعهده دارد و از BGP و OSPF پشتیبانی می‌کند. اطلاعات مسیریابی می‌تواند شامل Routing Table Update، Routing Redistribution و ... باشد. باید توجه داشت که وظیفه مسیریابی ترافیک ماشین‌های مجازی برعهده DLR Module و مدیریت آن برعهده Logical Router Control Virtual Machine است.

در بخش Control Plane در NSX Controller اطلاعات سرویس‌هایی مانند VXLAN فراهم می‌شود. این اطلاعات می‌تواند شامل MAC Table، ARP Table، VTEP Table و ... باشد تا در صورت نیاز این اطلاعات در اختیار Hostها قرار گیرد. این امر باعث انتخاب بهترین مسیر و جلوگیری از از ترافیک Broadcast می‌شود. در صورت فعال کردن VXLAN برروی شبکه فیزیکی باید IP Multicast را نیز فعال نمود و این در صورتی است که در NSX می‌توان IP Multicast را فعال نکرد و به عنوان یک پیش‌نیاز نیست. به عبارت دیگر باعث کاهش ترافیک IP Multicast می‌شود.

همانطور که گفته شد برای نصب NSX Controller حداقل و حداکثر باید از سه Node استفاده شود، البته در محیط آزمایشگاهی، یکی نیز قابل پیاده‌سازی است. NSX Controller توسط NSX Manager نصب می‌شود و از IP Pool برای آدرس‌دهی هر Node استفاده می‌شود. زمانی که NSX Controller Cluster اجرا می‌شود، فرآیندی برای انتخاب یک Node به عنوان Master رخ می‌دهد. انتخاب Master با توجه به تعداد رأی‌های Nodeهای فعال و غیرفعال صورت می‌گیرد. یکی از دلایل اینکه از سه Node استفاده می‌شود همین تعداد رأی‌ها است تا بتوان Master انتخاب شود. طی این فرآیند یک Node به عنوان Master و بقیه به عنوان Slave می‌شوند. وظیفه Master تخصیص منابع و تشخیص خطا برروی Controller Nodeها است. در صورت خطا در Master دوباره فرآیند انتخاب Master صورت می‌گیرد. همانطور که گفته شد از چند Node در Cluster برای عملکرد و دسترسی‌پذیری بالا استفاده می‌شودو Master وظیفه تخصیص منابع را برعهده



دارد. مکانیزم تخصیص منابع Slicing نام دارد. از Slicing استفاده می‌شود تا از فعال بودن هر Node در هر زمان مطمئن شد. همچنین Master از Slicing برای تخصیص منابع استفاده می‌کند تا بخشی از پردازش VXLAN و یا Logical Routing را به Nodeهای دیگر محول نماید. در تصویر زیر این تخصیص نشان داده شده است.

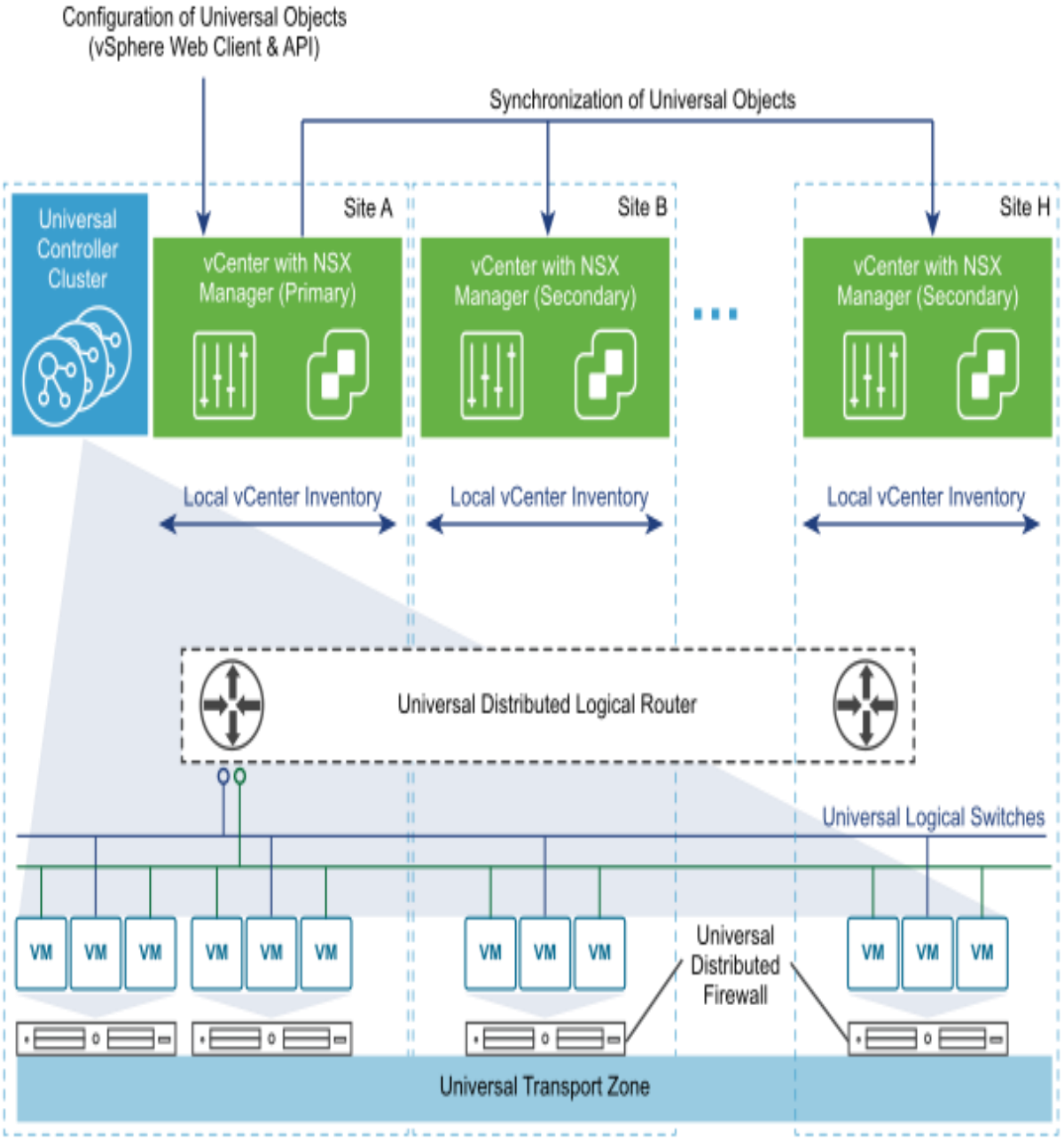
٤-٣- Management Plane

ارائه اینترفیس مدیریتی و همچنین برقراری ارتباط با بخش Control Plane یا مؤلفه‌های دیگر، برای اجرا و تغییر تنظیمات، برعهده بخش مدیریتی یا Management Plane است. vCenter Server یک محیط گرافیکی برای مدیریت مرکز داده به مدیر سیستم ارائه می‌کند. NSX Manager با برقراری ارتباط با vCenter تنهاز vSphere API برای انجام عملیات و سرویس‌های خود استفاده می‌کند. NSX Manager دستورات را از طریق vCenter، Restful APIهای قدرتمند و کامل (یک معماری نرم‌افزاری برای سرویس‌های وب است) و همچنین دیگر پلتفورم‌های مدیریتی ابر مانند vCAC دریافت می‌کند. این نرم‌افزار هیچ وظیفه‌ای در بخش Data Plane یا Control Plane ندارد. از طریق NSX Manager می‌توان با NSX Controller ارتباط برقرار نمود. در واقع تنظیمات از طریق vCenter به NSX Manager و بعد از آن به NSX Controller و در آخر به Host ارسال می‌شود و در نهایت Host تنظیمات را اعمال می‌کند. همچنین می‌توان دستورات از طریق Message Bus به مؤلفه‌ها ارسال نمود. باید توجه داشت که Message Bus یک مؤلفه است و ماشین‌مجازی نیست. Message Bus یک پروتکلی است که به فرستنده اجازه می‌دهد تا در صورت در دسترس نبود میزبان، یک پیام خصوصی را ارسال و آن را تضمین نماید. پروتکلی که NSX در این زمینه از آن استفاده می‌کند یک Advanced Message Queuing Protocol (AMQP) است که RabbitMQ نام دارد و برروی NSX Manager نصب و اجرا می‌شود. vShield Firewall Daemon (VSFWD) یک ارتباط امن برروی TCP/5671 برای اجرای دستورات Shell از NSX Manager به ESXi برقرار می‌کند.

NSX Manager به راحتی به عنوان یک Virtual Appliance برروی vCenter نصب می‌شود. برروی هر vCenter تنها یک NSX Manger تصب می‌شود. در صورت استفاده از چند vCenter در سایت‌های مختلف و یا استفاده از VMware Site Recovery Manager (SRM) می‌توان با استفاده از Cross-vCenter NSX که در نسخه 6.2 به بعد ارائه شده است، برروی هر سایت بصورت جداگانه یک NSX Manager نصب و آنها را با یکدیگر Link نمود. در صورت استفاده از چند NSX Manager یکی از آنها به عنوان Primary و بقیه به عنوان Secondary عمل می‌کنند. در واقع یک لایه یکپارچه یا Universal از شبکه مجازی بین سایت‌ها قرار می‌گیرد. در صورت از بین رفتن NSX Manager، ارتباطات و سرویس‌های شبکه برقرار هستند و فقط تغییرات برروی شبکه اعمال نمی‌شود. می‌توان با استفاده از راه‌حل‌هایی مانند vSphere HA و یا Fault Tolerance از NSX Manager محافظت نمود. پیشنهاد می‌شود که مؤلفه‌های مدیریتی برروی چند Rack

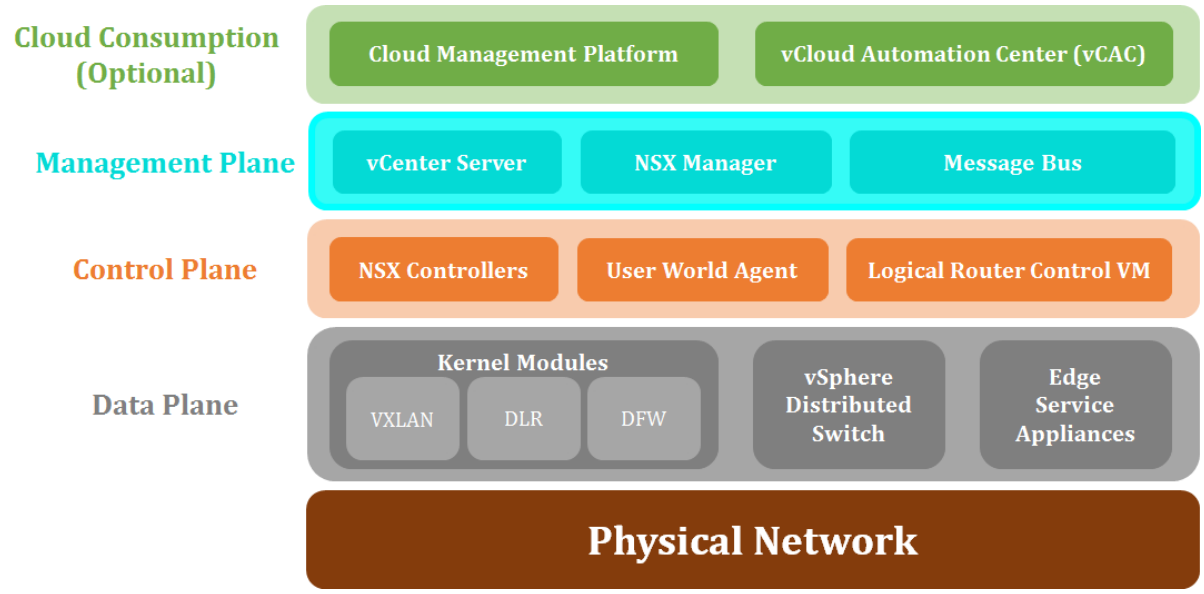
مختلف قرار گیرد تا تحمل‌پذیری در برابر خطا افزایش یابد. باید توجه داشت که NSX Cluster و vSphere Cluster قابلیت‌هاو عملکردهای متفاوتی دارند. حداکثر تأخیر در شبکه بین مؤلفه‌های مختلف در زیرساخت مجازی برای پیاده‌سازی NSX باید 150 ms باشد که در غیر اینصورت ممکن است خطا در شبکه مجازی رخ دهد. برای استفاده از Cross-vCenter NSX باید نسخه‌های زیر مورد استفاده قرار گیرد.

Component	Version
NSX Manager	6.2 or later
NSX Controller	6.2 or later
vCenter Server	6.0 or later
ESXi	ESXi 6.0 or later Host clusters prepared with NSX 6.2 or later VIBs



٤-٤- Cloud Consumption

در بالاترین لایه، بخش مدیریت ابر یا Cloud Management وجود دارد که بیشتر برای مراکز داده بزرگ استفاده می‌شود. استفاده از این بخش اختیاری است و می‌توان از پلتفورم‌های مدیریتی ابر مانند VMware vCloud Automation Center (vCAC) استفاده نمود.



٤-٥- VMware vSphere Host Components

در محیط NSX چندین مؤلفه برروی vSphere Host ESXi نصب و اجرا می‌شود. NSX Controller Cluster با استفاده از TCP SSL با مؤلفه‌های ESXi که User World Agent (UWA) نام دارند، ارتباط برقرار می‌کند. UWA اطلاعات را جمع‌آوری و دستورات را مطابق با NSX Controller Cluster اجرا می‌کند. برروی هر Host دو UWA نصب و اجرا می‌شود. Message Bus Client که با سرویسی به نام vShield Firewall Daemon (vsfwd) برروی Host قرار دارد و توسط خود NSX Manager مدیریت می‌شود. مؤلفه دیگری که توسط NSX Controller مدیریت می‌شود با سرویس netcpa شناخته می‌شود که وظیفه Switching و Routing را برعهده دارد.

Distributed Firewall Module (DFW) نیز مؤلفه‌ای است که برروی هر vSphere Host و در سطح Kernel Module قرار دارد و با توجه به قوانین و سیاست‌هایی که تعریف می‌شود امنیت محیط مجازی را در لایه‌های دو، سه و چهار فراهم می‌کند. هر DFW برروی یک vNIC ماشین‌مجازی ایجاد می‌شود. بطور مثال اگر یک ماشین‌مجازی سه کارت شبکه vNIC داشته باشد، سه DFW Instance برای ماشین‌مجازی اختصاص داده می‌شود. قوانین و سیاست‌های DFW می‌تواند در لایه دو و با استفاده از پروتکل‌های آن بر اساس آدرس MAC و یا در لایه سه و چهار بر اساس IP یا TCP/UDP تعریف شود. باید توجه داشت که ابتدا قوانین لایه دو بررسی می‌شود و در صورت Block شدن ترافیک ماشین‌مجازی، ترافیک لایه سه و چهار بررسی نمی‌شود و Block می‌شود. مؤلفه DFW ترافیک شبکه را در محیط مجازی به مجازی و مجازی به فیزیکی (East-West) کنترل

و بررسی می‌کند. قوانین و سیاست‌های DFW می‌تواند در محیط‌های vCenter، NSX Manager و یا در ESXi Host تعریف شود.

Distributed Router Module (DLR) مؤلفه دیگری در سطح vSphere Host است که وظیفه مسیریابی ترافیک ماشین‌های مجازی را برعهده دارد. DLR بهترین مسیر را با استفاده از بخش Control Plane برای ارسال ترافیک East-West ماشین‌مجازی انتخاب می‌کند. در واقع DLR از دو بخش Control Plane که برعهده NSX Controller است و بخش Data Plane که برروی Host قرار می‌گیرد، تشکیل می‌شود. DLR و DFW با همکاری یکدیگر مسیریابی و امنیت را به بهترین نحو انجام می‌دهند. DLR از دو پروتکل مسیریابی OSPF و BGP پشتیبانی می‌کند.

مؤلفه دیگری که برروی vSphere Host نصب و اجرا می‌شود VXLAN Module است. این مؤلفه وظیفه Switching را برعهده دارد.

باید توجه داشت که همه مؤلفه‌ها هنگام آماده‌سازی Host توسط NSX Manager بصورت خودکار نصب و اجرا می‌شوند و نیازی به اجرای مدیر سیستم نیست. همه مؤلفه‌ها برای امنیت در ارتباط با یکدیگر از SSL Certificate استفاده می‌کنند. SSL Certificate می‌تواند توسط خود مدیر سیستم در هنگام نصب NSX Manager نیز ایجاد شود. NSX Manager وظیفه نصب SSL Certificate را برروی vSphere Host ESXi و NSX Controller دارد.

۵- VMware vSphere Switches

شرکت VMware برای اتصال ماشین‌های مجازی و ارتباط آنها با یکدیگر از Switch مجازی استفاده می‌کند. Standard Switch یک Switch مجازی است که برروی یک ESXi بصورت جداگانه نصب و مدیریت می‌شود و هیچ ارتباطی با ESXi دیگر ندارد. ماشین‌های مجازی از طریق پورت Virtual Machine Port Group به این Switch متصل می‌شوند و با یکدیگر و یا خارج از شبکه ارتباط برقرار می‌کنند. ترافیک‌های مدیریتی و کنترلی مانند Management، vMotion و ... از طریق VMKernel Network Adapter به این Switch متصل می‌شوند. همچنین کارت‌های شبکه نیز از طریق Physical Network Adapter به این Switch متصل می‌شوند. مشکلی که در این نوع Switch وجود دارد مدیریت سخت و قابلیت‌های کم است، زیرا باید برروی هر ESXi بصورت جداگانه پورت‌ها و کارت‌های شبکه را مدیریت نمود. vSphere Distributed Switch (VDS) یک Switch مجازی است که بصورت یکپارچه همه ESXiها را پوشش می‌دهد. VDS مانند یک لایه گسترده برروی همه ESXiها قرار می‌گیرد و بصورت متمرکز آنها را مدیریت می‌کند. برروی VDS نیز می‌توان پورت‌های متفاوتی مانند Standard Switch تعریف نمود. به عبارت دیگر وظیفه VDS ارائه یک شبکه مجازی بین تمامی ESXiها است که ماشین‌های مجازی از طریق آن به شبکه مجازی متصل می‌شوند. می‌توان بعضی از قابلیت‌ها مانند vMotion، Management، iSCSI، NFS و ... را برروی

همان Standard Switch نگه‌داشت و به VDS انتقال نداد. VDS قابلیت‌هایی را ارائه می‌کند که Standard Switch نمی‌تواند. نمونه‌ای از این قابلیت‌ها به اختصار توضیح داده می‌شود.

۵-۱- Network I/O Control (NIOC)

از طریق NIOC می‌توان پهنای‌باند ترافیک‌های متفاوت را به اشتراک گذاشت و یا اینکه محدود نمود. بطور مثال هر VM یا هر سرویس از شبکه چه میزان از پهنای‌باند را می‌توانند استفاده کنند.به عبارت دیگر بسته‌های شبکه را اولویت‌بندی می‌کند.

۵-۲- Port Mirroring

با استفاده از این قابلیت می‌توان یک کپی از ترافیک پورت خاصی را به یک سیستم دیگر مانند Monitoring ارسال نمود. این قابلیت همانند Switch Port Analyzer (SPAN) و Remote Switch Port Analyzer (RSPAN) در سیستم‌های سیسکو است.

۵-۳- NetFlow

Netflow ابزار تحلیل شبکه است که با استفاده از آن می‌توان ترافیک شبکه و ماشین‌مجازی را مشاهده و بررسی نمود. آدرس IP سیستم NetFlow Collector در VDS تنظیم می‌شود و از طریق آن می‌توان ترافیک شبکه مجازی را بررسی نمود. Solar Winds یک ابزار در زمینه NetFlow است.

۵-٤- Private VLAN

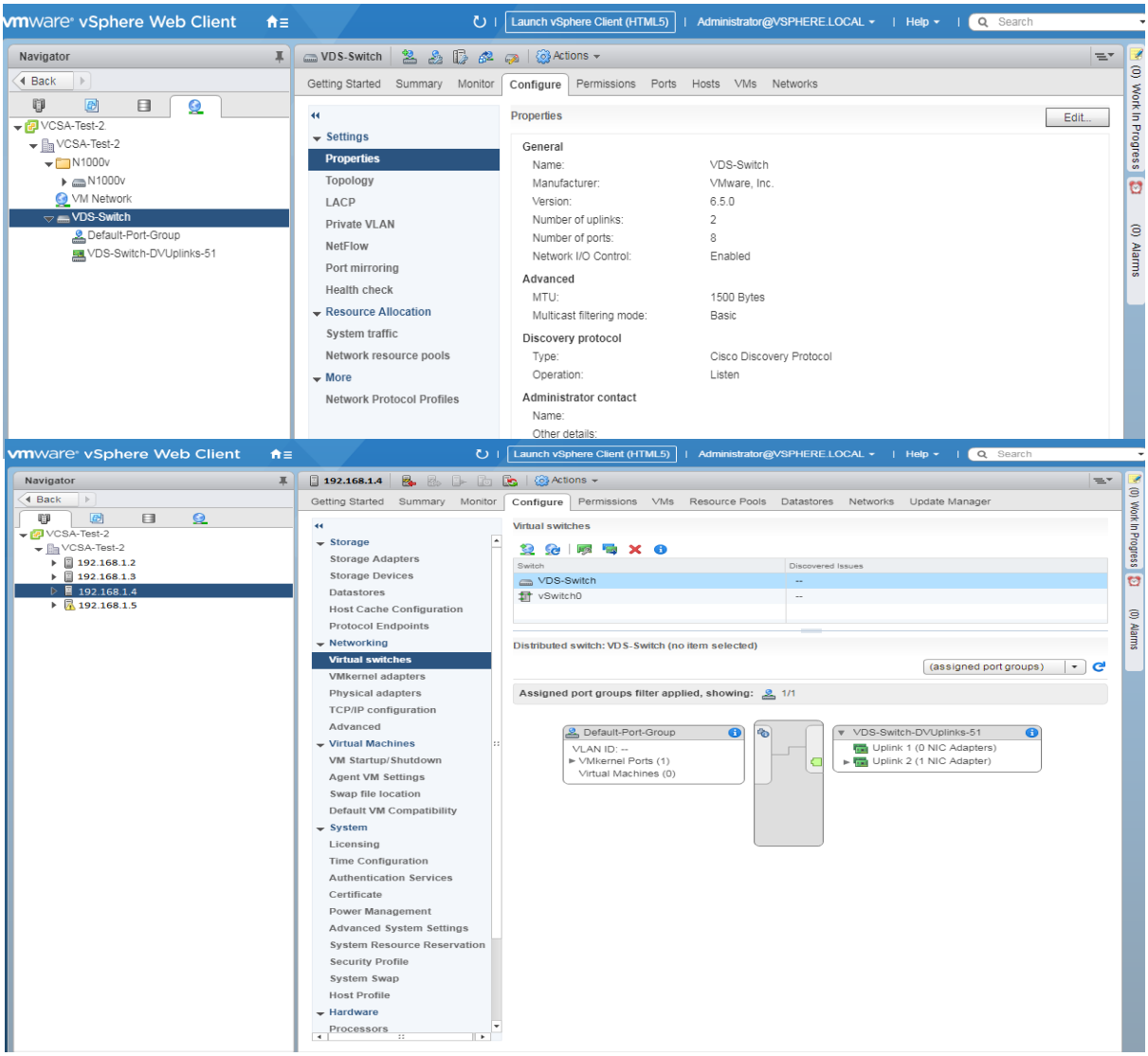
PVLAN قابلیتی است که می‌توان یک VLAN را نیز به بخش‌های کوچک‌تر تقسیم و برای هر بخش یک سیاست تعریف نمود. این سیاست مشخص می‌کند که بخش‌های کوچک‌تر چگونه با بیرو و با یکدیگر ارتباط برقرار کنند. در PVLAN یک VLAN اصلی یا Primary VLAN وجود دارد که به دو زیر مجموعه Community VLAN و Isolate VLAN تقسیم می‌شود. در یک Community VLAN، دو پورت با یکدیگر می‌توانند ارتباط برقرار کنند ولی با یک Community VLAN دیگر نمی‌توانند ارتباط برقرار کنند. در Isolate VLAN دو پورت حتی با یکدیگر نیز نمی‌توانند ارتباط برقرار کنند. باید توجه داشت که سیاست ارتباط با خارج از Primary VLAN می‌تواند برای همه بصورت یکسان باشد. به عبارت دیگر دسترسی همه به خارج از VLAN بصورت یکسان است.

۵-۵- Traffic Shaping

با استفاده از این قابلیت می‌توان ترافیک ورودی و خروجی ماشین‌مجازی را محدود نمود. این قابلیت در Standard Switch نیز وجود دارد ولی فقط ترافیک خروجی را محدود می‌کند. با استفاده از این قابلیت می‌توان پهنای‌باند ماشین‌های مجازی را بین سرورهای مختلف Load Balance نمود.

قبل از اینکه نرم‌افزار NSX تنظیم شود باید مؤلفه‌های VDS مانند Teaming and Fail Over، Security Options، Monitoring و ... بصورت صحیح و Best Practice اجرا شود. VDS نیاز به لایسنس Enterprise Plus دارد، ولی هیچ پیش‌نیاز سخت‌افزاری ندارد. VDS برای تنظیمات خود به vCenter نیاز

دارد و در صورت از بین رفتن vCenter تنظیمات آن با ریست شدن ESXi از بین می‌رود. بنابراین باید از vCenter Database نسخه پشتیبان تهیه نمود و یا از vCenter HA برا دسترسی‌پذیری بیشتر استفاده نمود. در بعضی از سازمان‌ها و یا محیطها تنظیماتی مانند VMKernel Management، iSCSI و ... برروی Standard Switch قرار می‌گیرد که این مشکلی برای VDS ایجاد نمی‌کند و می‌توان این تنظیمات را در جای خود نگه داشت. VDS از نظر ساختاری به دو مؤلفه تقسیم می‌شود. مؤلفه اول شامل بخش‌های Management و Control Plane است که هر دو از طریق vCenter تنظیم می‌شوند. مؤلفه دوم شامل بخش‌های I/O و Data Plane است که مانند یک Switch مجازی برروی هر ESXi قرار می‌گیرد و بخشی از VDS می‌شود. این Switch مجازی وظیفه پردازش ترافیک را برروی هر ESXi دارد و از طریق Control Plane که برروی vCenter قرار دارد دستورات و تغییرات را اعمال می‌کند. به همین دلیل است که با از بین رفتن vCenter در صورت ریست شدن ESXi، تنظیمات از بین می‌رود و در غیر اینصورت هنوز تنظیمات برروی ESXi وجود دارد. باید توجه داشت که VDS نیاز به نصب Module و یا Component برروی ESXi ندارد. در شکل زیر نمایی از VDS برروی vCenter نمایش داده شده است.



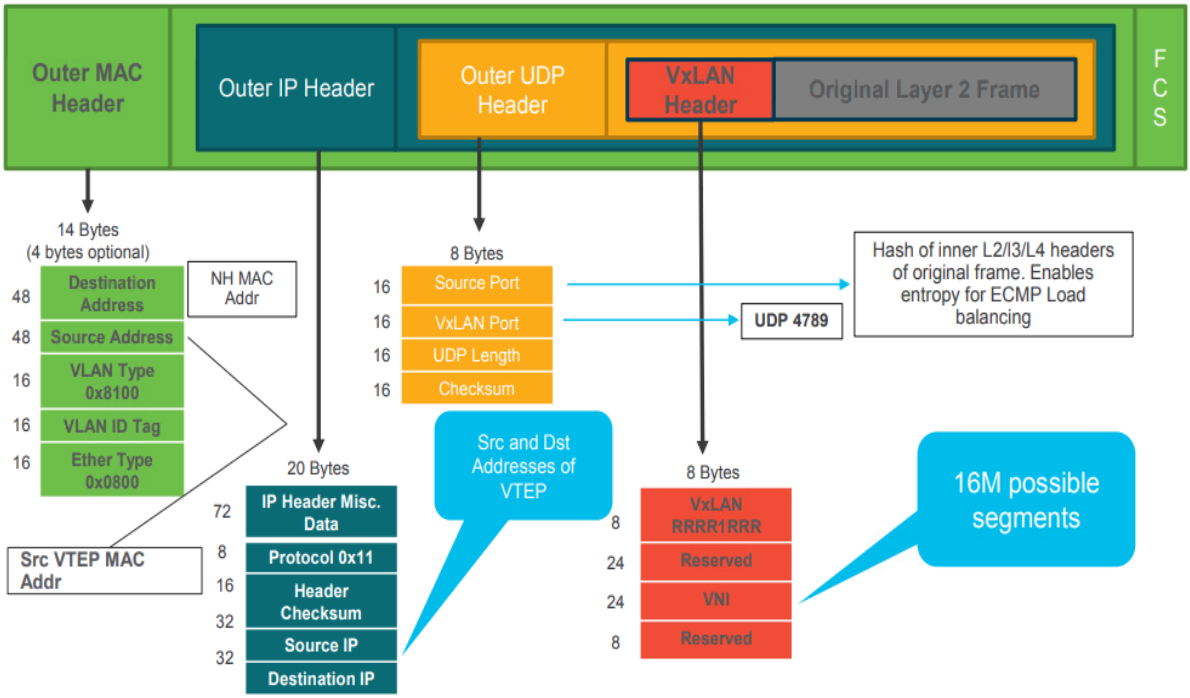
٦- VXLAN

Virtual Extensible Local Area Network (VXLAN) تکنولوژی پوششی شبکه یا Overlay Network است که توسط IETF با RFC 7348 تعریف شده است. Overlay به معنای قرار دادن یک لایه در لایه دیگر است. VXLAN یک چهارچوب برای مجازی‌سازی کردن لایه دو برروی لایه سه فراهم می‌کند. VXLAN بیشتر برای مراکز داده مجازی‌سازی شده استفاده می‌شود. در مجازی‌سازی سرور برروی هر Host تعدادی ماشین‌مجازی نصب می‌شود. که هر ماشین ماشین‌مجازی نیاز به آدرس MAC و IP دارد. همچنین هر کارت شبکه ماشین‌مجازی می‌تواند در VLAN اختصاصی مربوط به خود باشد. با توجه به اتصال ماشین‌ها به Switch مجازی نیاز به پروتکل STP نیز احساس می‌شود. با توجه به اینکه در مراکز داده تعداد بسیار زیادی ماشین‌مجازی وجود دارد و محدودیت در تعداد VLAN و مشکلات STP و زمان‌بر بودن آن باعث ایجاد دغدغه شده است، پروتکل VXLAN تعریف شده است. در پروتکل VXLAN با افزایش تعداد بیت برای شبکه منطقی به 24 Bit محدودیت در تعداد VLAN برطرف گردیده است. همچنین انتقال لایه دو برروی لایه سه و با استفاده از پروتکل‌های مسیریابی Dynamic Routing برروی لایه سه مشکل STP نیز برطرف گردیده است. در این حالت دیگر پورت‌ها به حالت Block نمی‌روند بلکهاز آنها برای Load Balancing استفاده می‌شود که این امر باعث افزایش کارایی شبکه و استفاده از حداکثر منابع است. پروتکل پوششی VXLAN ترافیک MAC هر ماشین‌مجازی را به فرمت خاصی برروی یک تونل منطقی بسته‌بندی می‌کند. اصطلاحات مربوط به VXLAN در بخش Network Abstraction توضیح داده شده است. همانطور که بیان شد به دستگاهی که از پروتکل VXLAN پشتیبانی می‌کند Virtual Tunnel End Point (VTEP) گفته می‌شود. VTEP وظیفه Encapsulate و Decapsulate کردن و یا همان بسته‌بندی بسته‌های VXLAN را برعهده دارد. VTEP برای Encapsulate کردن Ethernet Frame مقادیری قبل از Ethernet اصلی اضافه می‌کند. این مقادیر شامل موارد زیر است.

۱. VXLAN Header: این فیلد شامل چهار بخش است. بخش اول VXLAN Flag که بصورت پیش‌فرض برابر 00001000 است و به معنای این است که VNI صحیح است. بخش دوم و چهارم Reserved است. بخش سوم VXLAN Network Identifier که برابر شماره شبکه منطقی است.
۲. Outer UDP Header: این فیلد شامل چهار بخش است. بخش اول شماره پورت مبدأ (UDP Source Port) است که بر اساس عملیات Hash برروی بسته اصلی محاسبه می‌شود. بخش دوم شماره پورت مقصد که همان پورت UDP 4789 پیش‌فرض است که VTEP از آن برای ارسال بسته‌های VXLAN استفاده می‌کند. بخش سوم و چهارم UDP Length و UDP Checksum است.

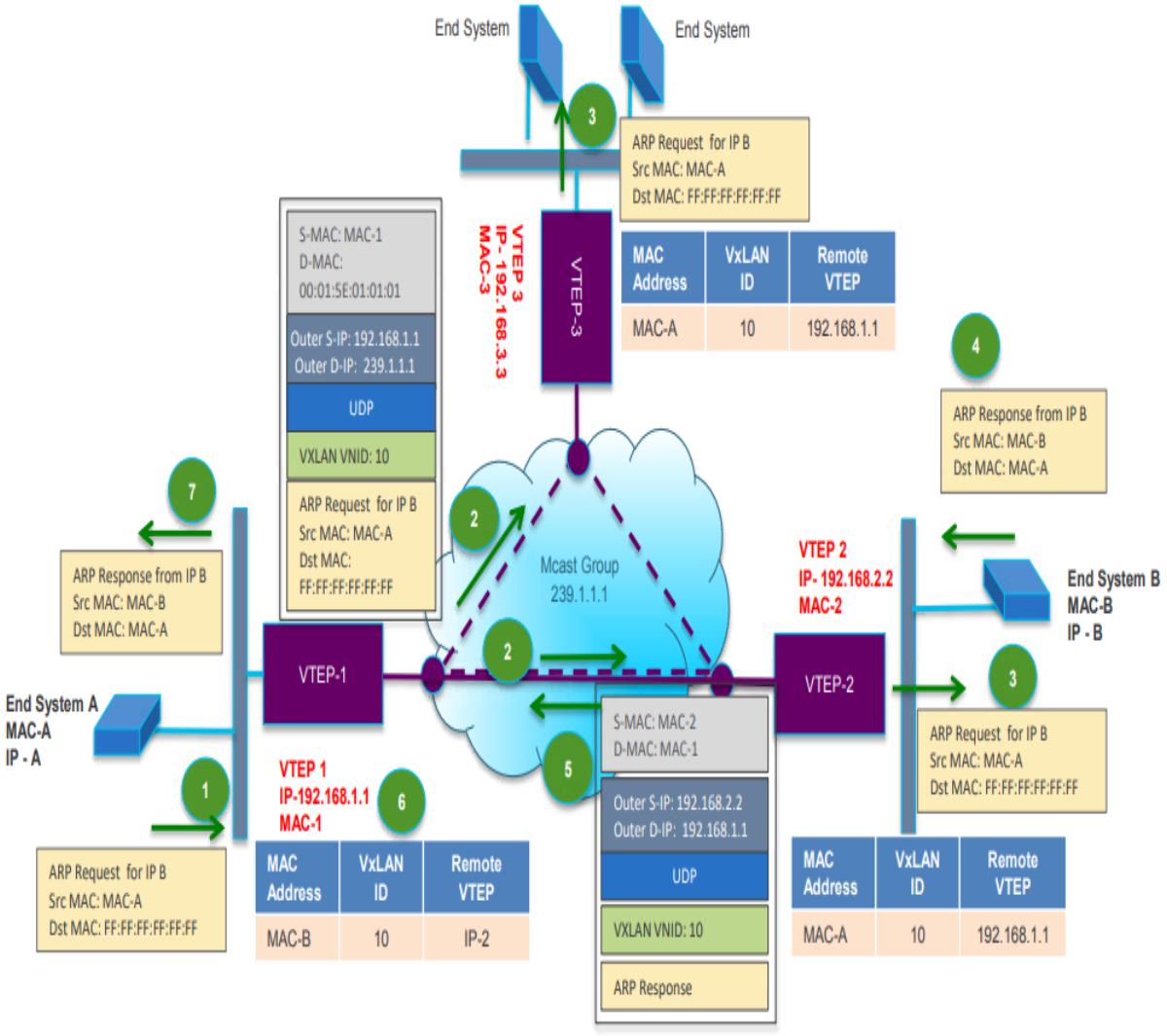
۳. Outer IP Header: این فیلد شامل پنج بخش است. بخش اول آدرس IP مقصد دستگاه VTEP است که VXLAN Tunnel را ایجاد می‌کند. به عبارت دیگر همسایه VTEP است. بخش دوم آدرس مبدأ محلی خود دستگاه VTEP است که VXLAN Tunnel را ایجاد کرد است. بخش‌های بعدی مربوط به اطلاعات پروتکل IP است که می‌تواند شامل IPv4/v6، Checksum، Time To Live و ... باشد.

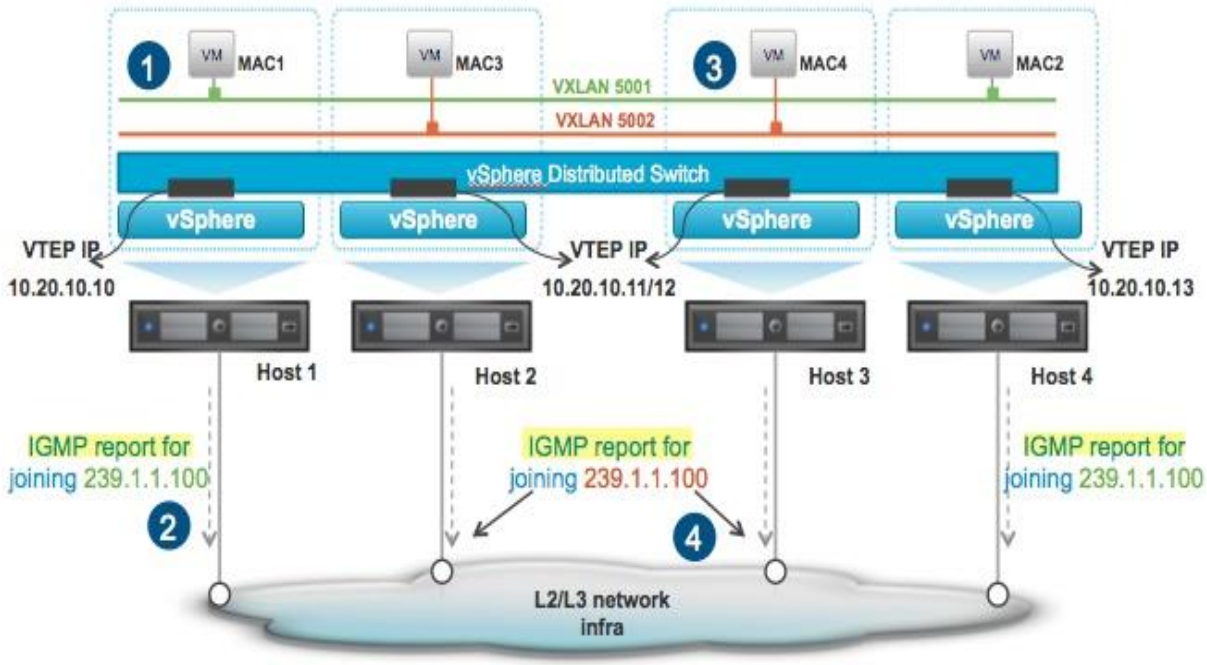
۴. Outer Ethernet Header: این فیلد شامل پنج بخش است. بخش اول Ether Type است که برای IPv4 برابر 0x0800 است. بخش دوم و سوم شامل Outer VLAN ID و VXLAN Type که اختیاری هستند. بخش چهارم آدرس MAC مبدأ یا همان VTEP MAC است. بخش پنجم آدرس MAC مقصدی است که VTEP باید بسته را به آن ارسال کند که می‌تواند Gateway یا همسایه باشد.



VXLAN از پروتکل Internet Group Membership Protocol (IGMP) استفاده می‌کند تا به گروه Multicast ملحق شود. از طریق IP Multicast یک ارتباط بین تمامی VTEPها برقرار می‌شود تا Frameهای Broadcast، Multicast و Unknown Unicast را بین یکدیگر جابه‌جا نمایند. همچنین VNIها از طریق IP Interface VTEP جابه‌جا می‌شوند.

هر ESXi از VMKernel Interface برای ارتباط با بستر VXLAN استفاده می‌کند. در واقع یک تونل مجازی بین VTEPهای هر ESXi که از آدرس VMKernel Interface خود استفاده می‌کنند، ایجاد می‌شود. هر ESXi بسته به تعداد کارت شبکه فیزیکی و NIC Teaming می‌تواند یک یا چند VTEP داشته باشد. باید توجه داشت که VMها هیچ دیدی از VXLAN و Encapsulate و Decapsulate ندارند. در تصویر بعد ارتباط بین VTEPها و نحوه ارسال بسته‌ها نمایش داده شده است.


End System
End System
3
ARP Request for IP B
Src MAC: MAC-A
Dst MAC: FF:FF:FF:FF:FF:FF
VTEP 3
IP- 192.168.3.3
MAC-3
VTEP-3
MAC Address
VxLAN ID
Remote VTEP
MAC-A
10
192.168.1.1
S-MAC: MAC-1
D-MAC:
00:01:5E:01:01:01
Outer S-IP: 192.168.1.1
Outer D-IP: 239.1.1.1
UDP
VXLAN VNID: 10
ARP Request for IP B
Src MAC: MAC-A
Dst MAC:
FF:FF:FF:FF:FF:FF
4
ARP Response from IP B
Src MAC: MAC-B
Dst MAC: MAC-A
7
ARP Response from IP B
Src MAC: MAC-B
Dst MAC: MAC-A
2
Mcast Group
239.1.1.1
VTEP 2
IP- 192.168.2.2
MAC-2
End System B
MAC-B
IP - B
VTEP-1
VTEP-2
2
3
ARP Request for IP B
Src MAC: MAC-A
Dst MAC: FF:FF:FF:FF:FF:FF
End System A
MAC-A
IP - A
S-MAC: MAC-2
D-MAC: MAC-1
5
1
VTEP 1
IP-192.168.1.1
MAC-1
6
Outer S-IP: 192.168.2.2
Outer D-IP: 192.168.1.1
UDP
VXLAN VNID: 10
ARP Response
ARP Request for IP B
Src MAC: MAC-A
Dst MAC: FF:FF:FF:FF:FF:FF
MAC Address
VxLAN ID
Remote VTEP
MAC-B
10
IP-2
MAC Address
VxLAN ID
Remote VTEP
MAC-A
10
192.168.1.1


1
VM
MAC1
VM
MAC3
3
VM
MAC4
VM
MAC2
VXLAN 5001
VXLAN 5002
vSphere Distributed Switch
vSphere
vSphere
vSphere
vSphere
VTEP IP
10.20.10.10
VTEP IP
10.20.10.11/12
VTEP IP
10.20.10.13
Host 1
Host 2
Host 3
Host 4
IGMP report for
joining 239.1.1.100
2
IGMP report for
joining 239.1.1.100
4
IGMP report for
joining 239.1.1.100
L2/L3 network
infra

پروتکل‌های دیگری نیز مانند VXALN وجود دارند که می‌توان به Network Virtualization using Generic Routing Encapsulation (NVGRE)، Stateless Transport Tunneling (STT) و Generic Network Virtualization Encapsulation (GENEVE) اشاره نمود. در NSX-T از GENEVE برای Encapsulation استفاده می‌شود.

۷- VMware NSX and vSphere Network Configuration

زمانی که برروی یک ESXi Host ماژول VTEP اجرا می‌شود، تنظیمات مربوط به NIC Teaming، Failover و Load Balancing بسیار مهم هستند. قبل از اجرای NSX باید تنظیمات مربوط به NIC Teaming، Failover و Load Balancing در vCenter بررسی شود. نرم‌افزار NSX وابسته به این تنظیمات است و قابلیت‌هایی که برروی vSphere و یا vCenter پشتیبانی نمی‌شود، در NSX پشتیبانی می‌شود. به NIC Teaming، Failover و Load Balancing به کارت‌های شبکه فیزیکی بستگی دارند که برروی VDS و VXLAN اعمال می‌شوند. باید توجه داشت که تمامی این تنظیمات به محیط و تعداد کارت شبکه بستگی دارد و باید قبل از اجرا بصورت Best Practice اجرا شوند. درباره Load Balancing هیچ قابلیت و گزینه‌ای وجود ندارد تا ارسال بسته‌ها بصورت مساوی برروی کارت‌های شبکه را تضمین کند. به عبارت دیگر توزیع بسته‌ها بر اساس الگوریتم‌های متفاوت مانند IP Hashing، MAC Hashing و ... متفاوت است که هیچ موقع نمی‌توان تضمین نمود که بسته‌ها بصورت کاملاً مساوی تقسیم و توزیع می‌شوند. در الگوریتم Round Robin که بسته‌ها یکی از کارت شبکه اول و دیگر از کارت شبکه دوم و به همین ترتیب ادامه پیدا می‌کند، مشکل رسیدن بسته‌ها به ترتیب اولویت وجود دارد که این الگوریتم آن را ضمانت نمی‌کند. زمانی که بین دو سیستم یک ارتباط برقرار می‌شود و هر سیستم چندین کارت شبکه دارد، این ارتباط فقط از یک کارت شبکه عبور داده می‌شود. به عبارت دیگر خیلی مهم نیست که از چه مکانیزمی برای Load Balancing استفاده شود. بطور مثال یک ماشین‌مجازی همیشه آدرس IP و MAC یکسانی دارد و کاربری که نیز به آن متصل می‌شود هم آدرس IP و MAC یکسانی دارد. حال هر الگوریتم Hashing که vSphere پشتیبانی می‌کند استفاده شود بازهم از یک کارت شبکه استفاده می‌شود. به عبارت ساده‌تر هیچ الگوریتم Hash وجود ندارد که بسته‌ها را در یک ارتباط بین دو کارت شبکه ارسال کند، ولی می‌توان با استفاده از الگوریتم‌های بهتر احتمال توزیع بیشتر ترافیک، بین کارت‌های شبکه فیزیکی متفاوت را افزایش داد. در نتیجه برای بهبود کیفیت و بازدهی شبکه باید کارت شبکه فیزیکی را ارتقاء داد. همچنین باید توجه داشت که ترافیک محیط مجازی (Virtual Switch) باید با ترافیک محیط فیزیکی (Physical Switch) هماهنگ باشد. در ادامه به روش‌های vSphere Load Balancing بطور مختصر پرداخته می‌شود.

Virtual Port ID -۱-۷

در این روش انتخاب مسیر یا کارت شبکه فیزیکی برای ارسال بسته‌های ماشین‌مجازی بر اساس Virtual Port ID صورت می‌گیرد. ماشین‌مجازی اول با Port ID 1 از کارت شبکه اول و ماشین‌مجازی دوم با Port ID 2 از کارت شبکه دوم و به همین ترتیب ادامه می‌یابد و دوباره از کارت شبکه اول مانند یک حلقه شروع می‌شود. این روش به عنوان روش پیش‌فرض VMware است، در همه مکان‌ها قابل پیاده‌سازی است و هیچ نیازی به اعمال تنظیمات برروی Switch فیزیکی نیست. در این روش برای تغییر مسیر می‌توان بصورت دستی Port ID ماشین‌مجازی را تغییر داد.

MAC Hash -۲-۷

این روش شبیه به Virtual Port ID است، با این تفاوت که بر اساس آدرس MAC بسته‌ها از روی کارت شبکه عبور داده می‌شوند. اگر ماشین‌مجازی چندین کارت شبکه مجازی داشته باشد بر اساس آدرس MAC آن ممکن است ترافیک از چندین کارت شبکه فیزیکی عبور داده شود. در MAC Hash نیز هیچ نیازی به اعمال تنظیمات برروی Switch فیزیکی نیست. پیشنهاد می‌شود برای ماشین‌های مجازی که بیشتر از یک کارت شبکه دارند از این روش استفاده شود.

IP Hash -۳-۷

در صورتی که Switch فیزیکی از این روش پشتیبانی کند و لایسنس vSphere Enterprise Plus موجود نباشد، IP Hash بهترین روش است. ترافیک‌های ماشین‌مجازی بر اساس آدرس HP مبدأ و مقصد Hash می‌شوند و برروی کارت‌های شبکه متفاوتی ارسال می‌شوند. به عبارت دیگر احتمال استفاده از کارت شبکه فیزیکی متفاوت افزایش می‌یابد. به عبارت دیگر ترافیک ماشین‌مجازی بر اساس آدرس IP مقصد ممکن است از چندین کارت شبکه فیزیکی متفاوت عبور داده شود. در این روش باید برروی Switch فیزیکی تنظیمات Stack و یا تکنولوژی‌های آن مانند Virtual Port Channel در Cisco Nexus و یا Virtual Switching System در Cisco Catalyst 6500 اجرا شود (برای اطلاعات بیشتر به کتاب CCNP (R&S) و CCNA (DC) نوشته مهندس ابوالفضل هاشمی مراجعه نمایید). باید توجه داشت همانطور که گفته شد هر ارتباط بین VM و Client برروی یک کارت شبکه عبور داده می‌شود. زمانی که کاربران زیادی با VM در ارتباط هستند این روش بسیار کارآمد است. در این روش نیاز به تنظیمات سخت‌افزاری مانند Port Channel و یا Ether Channel برروی Switch فیزیکی است و باید IP Hash برروی Switch فیزیکی فعال باشد.

Load Base Teaming (LBT) or Physical NIC Load -٤-۷

LBT یا Physical NIC Load بر اساس مصرف و بار کارت شبکه فیزیکی عمل می‌کند. این روش نیاز به VDS و لایسنس vSphere Enterprise Plus دارد. ESXi در هر بازه سی ثانیه (30 Sec) یکبار، وضعیت کارت‌های شبکه فیزیکی را بررسی می‌کند. در صورت بالا رفتن مصرف کارت شبکه بیشتر از هفتاد و پنج درصد (75%)، ترافیک ماشین‌مجازی را بر اساس Port ID به کارت شبکه فیزیکی دیگر اختصاص می‌دهد. در این

روش نیازی به تنظیمات برروی Switch فیزیکی نیست. این روش بسیار محبوب است ولی NSX از این روش پشتیبانی نمی‌کند.

۷-۵- Link Aggregation Control Protocol (LACP)

این روش در نسخه vSphere 5.5 به بعد ارائه شده است. LACP فقط برروی VDS قابل اجرا است. در این روش ESXi با Switch فیزیکی در ارتباط است و با یکدیگر صحبت (Negotiate) می‌کنند و یک الگوریتم Hash را برای ارسال ترافیک انتخاب می‌کنند. معمولاً از الگوریتم Source/Destination IP Hash استفاده می‌شود. vSphere در LACP از بیست روش متفاوت پشتیبانی می‌کند. برروی هر VDS حداکثر می‌توان 64 Link Aggregation و برروی هر Host حداکثر می‌توان 32 Link Aggregation ایجاد نمود. LACP نیاز به اعمال تنظیمات برروی Switch فیزیکی دارد. در صورت پشتیبانی سخت‌افزاری در شبکه فیزیکی، LACP بهترین روش است. زیرا ESXi با Switch فیزیکی در حال صحبت کردن است و از خرابی و کاهش عملکرد جلوگیری می‌کنند. در جدول زیر روش‌هایی که در vSphere پشتیبانی می‌شود آمده است.

Destination IP address	Source IP address	VLAN	Source port ID
Destination IP address and TCP/UDP port	Destination TCP/UDP port	Source TCP/UDP port	Source MAC address
Destination IP address and VLAN	Source IP address and TCP/UDP port	Source IP address and VLAN	Destination MAC address
Destination IP address, TCP/UDP port and VLAN	Source and destination IP address, TCP/UDP port and VLAN	Source and destination IP address and TCP/UDP port	Source and destination IP address
Source and destination TCP/UDP port	Source IP address, TCP/UDP port and VLAN	Source and destination IP address and VLAN	Source and destination MAC address

۷-۶- Explicit Failover

در صورتی که Host چندین کارت شبکه داشته باشد، می‌توان کارت‌های شبکه را در حالت Active، Standby و Unused قرار داد. حالت Unused به معنای عدم استفاده از کارت شبکه است که به ندرت اتفاق می‌افتد. حالت Active و Standby معمولاً برای جداسازی ترافیک شبکه استفاده می‌شود که در صورت خرابی در کارت شبکه Active از کارت شبکه Standby استفاده می‌شود. بطور مثال در یک طرف تنظیمات پورت از کارت شبکه Active برای ترافیک iSCSI و از کارت شبکه Standby برای Management استفاده می‌شود. در طرف دیگر بر عکس است و از کارت شبکه Active برای ترافیک Management و از کارت شبکه Standby برای iSCSI استفاده می‌شود. در صورت خرابی هر یک از کارت شبکه‌ها از کارت شبکه دیگر استفاده می‌شود و دیگر جداسازی کارت‌های شبکه در اولویت نیست.

با توجه به مطالب گفته شده، قابلیت‌های نرم‌افزار NSX به نوع به NIC Teaming، Failover و Load Balancing بستگی دارد. پروتکل VXLAN برای ارسال بسته‌ها سه حالت دارد. در حالت Unicast همه VTEPها بصورت Unicast با یکدیگر در ارتباط هستند و بسته‌های Ethernet Frame را ارسال می‌کنند. در این حالت اگر یک بخش لایه سه (Layer 3 Segment) بخواهد با چندین بخش لایه سه دیگر ارتباط برقرار کند، باید به همه آنها بسته‌های Unicast ارسال نماید. در حالت Multicast بسته‌ها به Switch فیزیکی ارسال می‌شود و از طریق آن ترافیک Multicast به Hostهایی که عضو گروه هستند، ارسال می‌شود. در حالت Hybrid ابتدا یک بسته به یک Host مشخص ارسال می‌شود و سپس از طریق آن ترافیک به دیگر Hostها ارسال می‌شود. در جدول زیر پشتیبانی نرم‌افزار NSX، VTEP و VXLAN بر اساس NIC Teaming، Failover و Load Balancing توضیح داده شده است. Multi-VTEP به معنای داشتن یک VTEP برروی هر کارت شبکه فیزیکی است.

Teaming Type	NSX Support	Multiple VTEP Support	VXLAN Mode
Originating Port ID	Yes	Yes	All
Source MAC Hash	Yes	Yes	All
IP Hash	Yes	No	Hybrid & Multicast
Explicit Failover	Yes	No	Hybrid & Multicast
LACP	Yes	No	All
Physical NIC Load (LBT)	No	N/A	N/A

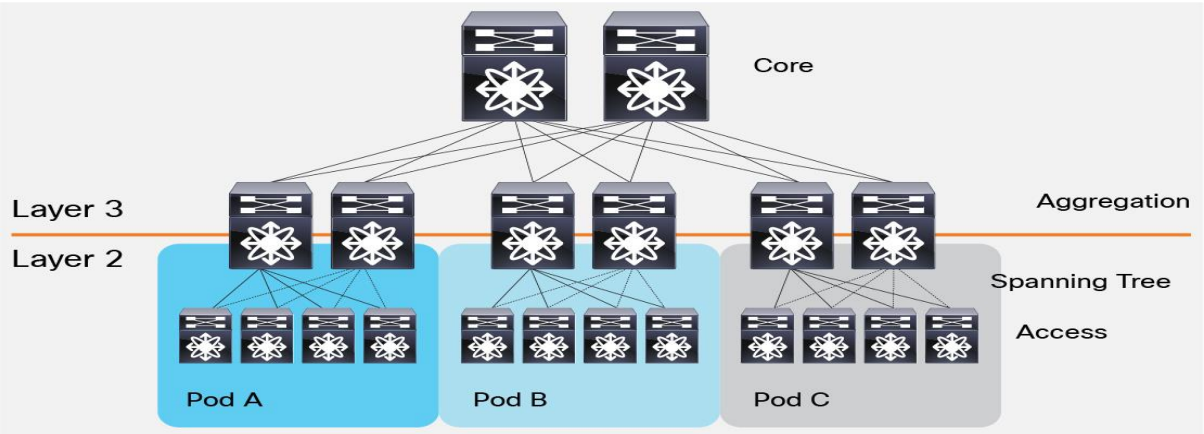
۸- VMware NSX and Physical Networking

برای برقراری ارتباط بین Hostها به بستر شبکه فیزیکی نیاز است و شبکه مجازی باید با شبکه فیزیکی ارتباط برقرار نماید. طراحی شبکه فیزیکی بسیار وابسته به سیاست‌های سازمان است. به عبارت دیگر هر سازمان طراحی شبکه مخصوص به خود را دارد. زمانی که ترافیک شبکه NSX نیاز داشته باشد تا از شبکه فیزیکی عبور کند، شبکه فیزیکی باید نیازهای NSX را برطرف نماید. همچنین در طراحی شبکه فیزیکی اگر قابلیت اطمینان (Reliability)، عملکرد (Performance)، سرعت (Speed) و تأخیر (Delay) مناسبی وجود نداشته باشد، نرم‌افزار NSX قادر به اصلاح آن نیست. بطور مثال اگر یک شبکه فیزیکی تأخیر بسیار زیادی داشته باشد، نرم‌افزار NSX قادر به کاهش آن نیست. اگر شبکه فیزیکی سرعت مناسبی ندارد بطور مثال به جای 10G از سرعت 1G پشتیبانی شود، نرم‌افزار NSX قادر به افزایش سرعت شبکه فیزیکی نیست. بنابر این باید در طراحی شبکه فیزیکی دقت زیادی داشت. باید توجه داشت که در صورت استفاده از نرم‌افزار NSX، مدیریت آسان‌تر و پیچیدگی کمتر می‌شود. نرم‌افزار NSX نیاز به سخت‌افزار فیزیکی شبکه و برند خاصی و یا خرید تجهیزات با قابلیت‌های بسیار زیاد را ندارد. ولی نیازمند قابلیت‌هایی مانند پشتیبانی از 1600 Byte MTU و چند پخشی لایه دو و سه (Layer 2,3 Multicast) است. بعضی از سخت‌افزارها بطور مثال Arista با VMware NSX هماهنگ می‌شوند. در

طراحی شبکه مراکز داده، دو نوع معماری اصلی سنتی سه لایه‌ای (Traditional Three-Layer) و شاخه و برگ (Spine and Leaf) وجود دارد. در معماری Traditional Three-Layer مقیاس‌پذیری و مدیریت سخت‌تر است ولی در Spine and Leaf انعطاف‌پذیری و مقیاس‌پذیری بیشتری وجود دارد.

۸-۱- Traditional Three-Layer

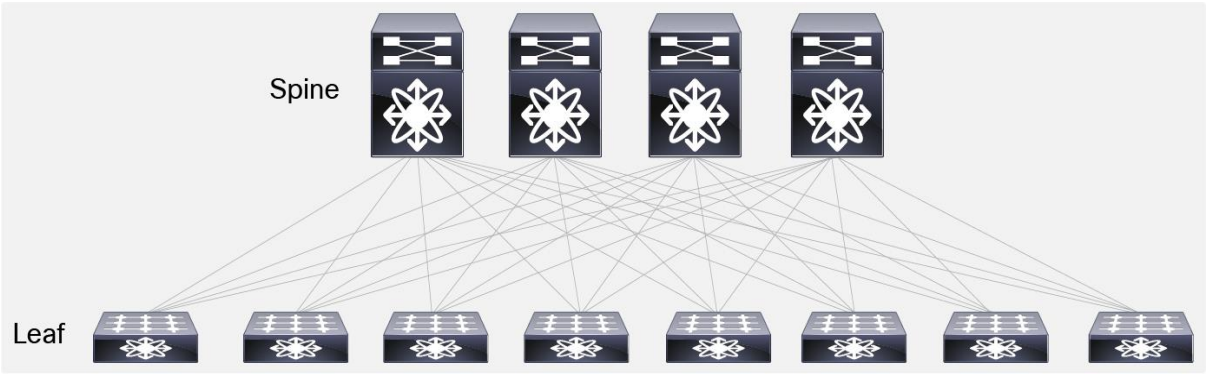
مراکز داده سنتی، معماری سه لایه‌ای را به کار می‌برند که در آن سرورها مبتنی بر مکان، درون pod تقسیم می شوند. این معماری شامل تجهیزات Core، تجهیزات Aggregation (Distribution) و تجهیزات Access میشود. بین تجهیزات Aggregation و Access از پروتکل STP برای جلوگیری از ایجاد حلقه در لایه دو شبکه استفاده می‌شود. VLANها درون هر pod توسعه داده می‌شوند و بدون اینکه نیازی به تغییر آدرس IP و تنظیمات Default Gateway باشد، مکان سرورها آزادانه درون podها تغییر می کند. با این حال STP نمی تواند از مسیرهای ارسال موازی استفاده کند و همیشه مسیرهای افزونه در یک VLAN را مسدود می کند. در سال ۲۰۱۰ شرکت سیسکو تکنولوژی Virtual Port Channel (vPC) را برای غلبه بر محدودیت STP عرضه نمود. vPC ویژگی است که امکان تنظیم چندین مسیر را میان چند Switch فراهم می کند. vPC مدیریت پورت ها را از STP گرفته و خود مدیریت می کند و مسیرهای Uplink Active/Active را از Access Switch به Aggregation فراهم می کند و از پهنای باند موجود بهره بیشتری می‌برد. با استفاده از تکنولوژی vPC پروتکل STP همچنان به عنوان مکانیزمی برای Fail-Safe استفاده می‌شود. از سال ۲۰۰۳ با ارائه تکنولوژی مجازی‌سازی محاسباتی، شبکه و ذخیره‌سازی که قبل از آن در طراحی مرکز داده، درون podها در لایه دو قرار می گرفتند، حال می‌توانند یکپارچه شوند. این تکنولوژی نیاز به دامنه لایه دوی بزرگتری را از لایه Access تا لایه Core به وجود آورد. مدیر مرکز داده می‌تواند یک pool مرکزی از منابع با قابلیت تغییرپذیری بیشتر را ایجاد نماید که بر اساس نیازها دوباره تخصیص دهی شوند. مجموعه ای از VMها بر روی سرورها قرار دارند که آزادانه از سروری به سرور دیگر قابل جابجایی هستند بدون اینکه به تغییری در مؤلفه‌های عملیاتی خود نیاز داشته باشند. با استفاده از سرورهای مجازی‌سازی شده، برنامه‌های کاربردی بگونه‌ای در میان سرورها توزیع می شوند که منجر به افزایش ترافیک East-West می‌شود. چنین ترافیکی به مدیریتی موثر به همراه تأخیری کم و قابل پیش‌بینی نیاز خواهد



داشت و این در در صورتی است که vPC تنها از فعال بودن حداکثر دو uplink موازی پشتیبانی می‌کند. بنابراین در معماری مراکز داده سه لایه‌ای پهنای باند به یک گلوگاه تبدیل می‌شود. مشکل دیگری که در معماری سه لایه‌ای وجود دارد، تأخیر بین سرورها است که بسته به مسیر ترافیکی استفاده شده تغییر می‌کند.

۸-۲- Spine and Leaf (Leaf-Spine)

همانطور که گفته شد در طراحی معماری سه‌لایه‌ای مشکل گلوگاه و تأخیر بین سرورها وجود دارد. در طراحی مراکز داده مدرن با نام معماری Leaf-Spine که مبتنی بر شبکه Clos است برای غلبه بر این محدودیت‌ها عمومیت یافته است. این معماری تأخیر کمتر و مقیاس‌پذیری و پهنای باند بیشتر را فراهم می‌کند. در معماری دو لایه‌ای Clos، هر تجهیز موجود در لایه پایین‌تر (Leaf) به هر یک از تجهیزات لایه بالاتر (Spine) می‌تواند از طریق توپولوژی Full-Mesh متصل شود و هیچ اتصال مستقیمی از نوع Spine-Spine و Leaf-Leaf وجود نداشته باشد. لایه Leaf شامل تجهیزات Access می‌شود که به دستگاه‌هایی همچون سرورها متصل می‌شوند. لایه Spine به عنوان ستون فقرات یا شاخه شبکه عمل می‌کند و در برابر اتصال داخلی میان تمامی تجهیزات لایه Leaf مسئول است و بار ترافیک به صورت یکنواخت میان تجهیزات لایه بالاتر توزیع می‌شود. اگر یکی از تجهیزات لایه بالاتر معیوب شود، تنها درصد اندکی از کارایی شبکه در سراسر مرکز داده کاهش می یابد. اگر بار قرار گرفته بر روی لینک بیش از ظرفیت آن باشد (یعنی ترافیک تولید شده بیش از حدی باشد که توسط یک لینک فعال در یک زمان تجمیع شود)، فرآیند افزایش ظرفیت ساده است. یک تجهیز Spine دیگر افزوده شده و در نتیجه تعداد Uplinkها افزایش می‌یابد که منجر به افزایش پهنای باند میان لایه‌ها و کاهش رخداد باری بیش از ظرفیت لینک (oversubscription) می‌شود. اگر ظرفیت پورت‌های دستگاه مورد توجه باشد، می‌توان یک تجهیز Leaf از طریق اتصال به هر تجهیز Spine اضافه نمود و تنظیمات شبکه را به آن اعمال نمود. سادگی در توسعه و گسترش این معماری، فرآیند ارتقای شبکه را بهینه می‌سازد. همانطور که گفته شد طراحی معماری سه لایه‌ای سنتی از پروتکل STP برای پیشگیری از حلقه استفاده می‌شود. پروتکل STP بر اساس شناسایی حلقه در شبکه، لینک های افزونه را مسدود می‌کند. در نتیجه یک تجهیز Access که دارای دو Uplink است تنها از یکی از آنها استفاده می‌کند. معماری Leaf-Spine پروتکل‌های جایگزینی مانند Shortest Path Bridging (SPB) که از پروتکل مسیریابی IS-IS در لایه دو برای جلوگیری از حلقه که دیگر پورت را مسدود نمی‌کند،

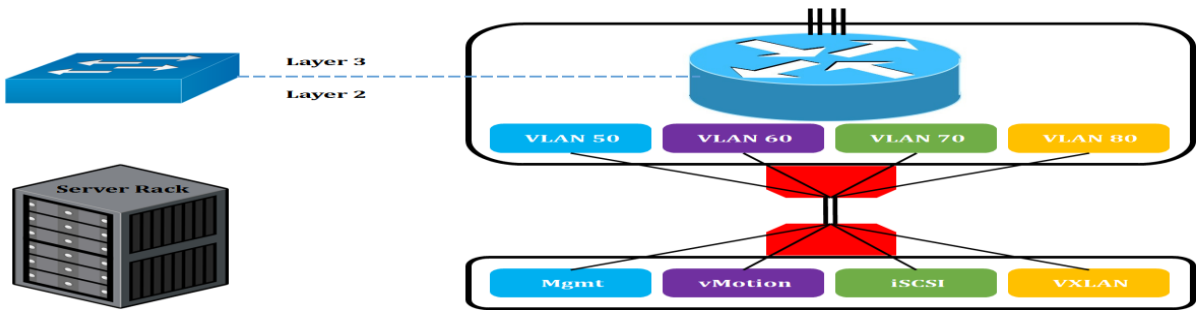


استفاده می‌کند. Transparent Interconnection of Lots of Links (TRILL) نمونه دیگری از پروتکل جیگزین STP است. پروتکل‌های SPB و TRILL با به کارگیری پروتکل‌های مسیریابی خودکار لایه سه برای دستگاه‌های لایه دو مشکلات STP را رفع می‌نماید. این پروتکل‌ها به دستگاه‌های لایه دو اجازه خواهند داد که Ethernet Frameها را مسیریابی نمایند.

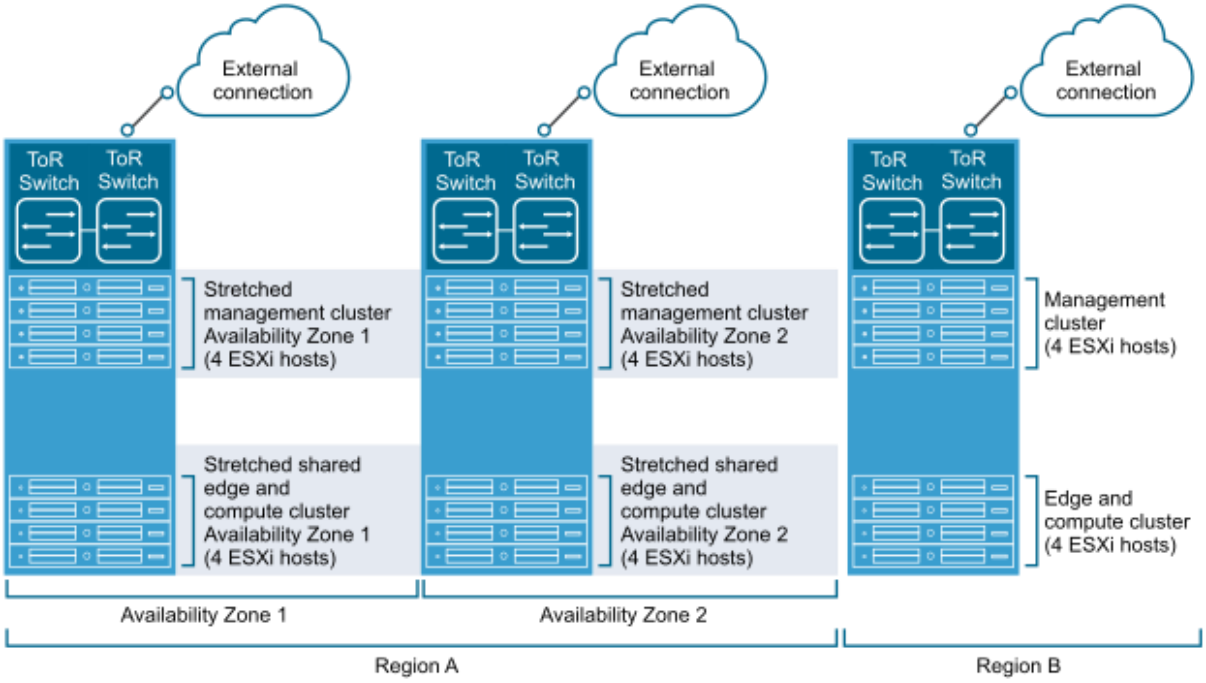
با توجه به مطالب گفته شده، در نرم‌افزار NSX اجباری به استفاده از معماری Leaf-Spine نیست.

۸-۳- Rack Design

برای جانمایی و طراحی سرورها در داخل Rackها قوانین و توصیه‌هایی وجود دارد. بطور مثال همه سرورها نباید در داخل یک Rack قرار گیرند، بلکه باید بصورت توزیع شده بین Rackها تقسیم شوند تا در صورت از بین رفتن و قطعی یک Rack فقط تعدادی از منابع از دسترس خارج شوند. به عبارت دیگر باید Single Point Of Failure وجود نداشته باشد. همچنین برای برقراری ارتباط سرورها با شبکه فیزیکی باید دقت نمود که نیازمندی‌های سرعت و تأخیر ماشین‌ها و کلاسترهای مجازی برروی سرور رعایت شود. بطور مثال سرورهای مربوط به Edge Cluster نیاز به I/O بیشتری نسبت به Workload Cluster دارند. در طراحی NSX Rack باید بخش Management، Edge و Work برروی Rackها توزیع و پخش شوند. بصورت یک نمای کلی از مرکز داده می‌توان این گونه بیان نمود که؛ Hostها باید از طریق Uplinkها به Switch بالا دستی در Rack یا همان Top Of Rack (TOR) متصل شوند. در Switch TOR بستگی به نوع Switch و برند آن باید از تکنولوژی‌های Port Channel (LACP, VSS, vPC) برای ارتباط Host به Switch استفاده نمود. همچنین TOR Switchها باید با یکدیگر در ارتباط و از تکنولوژی‌های Stack استفاده کنند. نوع لینک بین Host و Switch باید Trunk باشد تا اطلاعات VLANهای ماشین‌های مجازی و مدیریتی را بتوانند جابه‌جا نمایند. Hostهایی که در Rack قرار دارند به Switchهای لایه Leaf متصل هستند. حال TOR Switch برای ارتباط با Core Switch یا لایه Spine باید از لینک‌های لایه سه استفاده نمایند. باید توجه داشت که در تمامی مراحل باید Redundancy رعایت شود. در پیاده‌سازی NSX علاوه بر اینکه تمامی VLANهای مربوط به vMotion، Management و ... توصیه می‌شود که جدا باشند، در تمامی Rackها نیز باید تعریف شوند. همچنین توصیه می‌شود که از گسترش VLANهای اضافی و غیر قابل استفاده در Rackها جلوگیری نمود. نکته قابل تأملی که در اینجا وجود دارد این است که ترافیک vMotion نیز می‌تواند برروی لایه سه عبور داده شود. بطور مثال



ماشین‌مجازی از یک سایت در یک شهر به سایت دیگر در شهر دیگر انتقال یابد و این در صورتی است که زیرساخت شبکه فیزیکی جوابگوی ارسال ترافیک vMotion باشد. باید توجه داشت که برای نرم‌افزار NSX توصیه می‌شود NSX Controller در چند Rack توزیع و بین همه Rackها ارتباط لایه دو برقرار شود. همچنین در یک نگاه کلی می‌توان VLANهای داخل یک Rack و نحوه مسیریابی آنها را در تصاویر زیر مشاهده نمود. بطور مثال برای هر ترافیک می‌توان یک VLAN تعریف و آن را از دیگر ترافیک‌ها جدا نمود.



۸-٤- VTEP IP Addressing

برای آدرس‌دهی IP در شبکه‌مجازی بیشتر مواقع از حالت دستی (Manually) استفاده می‌شود. بطور مثال برای آدرس‌دهی VMKernel بیشتر مدیران شبکه ازآدرس‌دهی IP دستی استفاده می‌کنند. آدرس‌دهی IP برای VTEP کمی متفاوت است. در VTEP می‌توان از IP Pool، DHCP و Manually استفاده نمود. با توجه به گفته‌های گذشته عملیات ساخت و اجرای VTEP بصورت خودکار توسط NSX Manager انجام می‌شود. پس آدرس‌دهی حالت دستی در VTEP کمی بی‌معنا به نظر می‌رسد. ولی با این حال اگر مدیر شبکه در مواقعی نیاز به آدرس‌دهی دستی داشته باشد این امر امکان‌پذیر است. در IP Pool یک بازه از آدرس‌های IP به عنوان آدرس‌های VTEP رزرو شده و مدیریت و نگاشت آدرس‌ها بر عهده NSX Manager است. همچنین برای آدرس‌های NSX Controller نیز می‌توان آدرس‌دهی IP Pool استفاده نمود. در IP Pool اشکالی که وجود دارد عدم استفاده از آدرس‌های متفاوت برای VLANهای متفاوت است. با استفاده از آدرس‌دهی DHCP می‌توان برای هر VLAN یک بازه IP مشخص نمود که برروی دستگاه‌های شبکه مانند Switch یا Router قابل اجرا است. حال برای آدرس‌دهی Manually باید از DHCP استفاده نمود ولی از DHCP Server استفاده نکرد. این امر باعث می‌شود که بعد از مدت زمان مشخصی Host آدرس نگیرد و بعد از آن می‌توان با استفاده از

دستورات خط فرمان به vSphere VTEP آدرس IP نگاشت نمود. به عبارت دیگر از طریق User Interface (UI) نمی‌توان آدرس‌دهی دستی انجام داد.

۹- VMware NSX Installation Step By Step

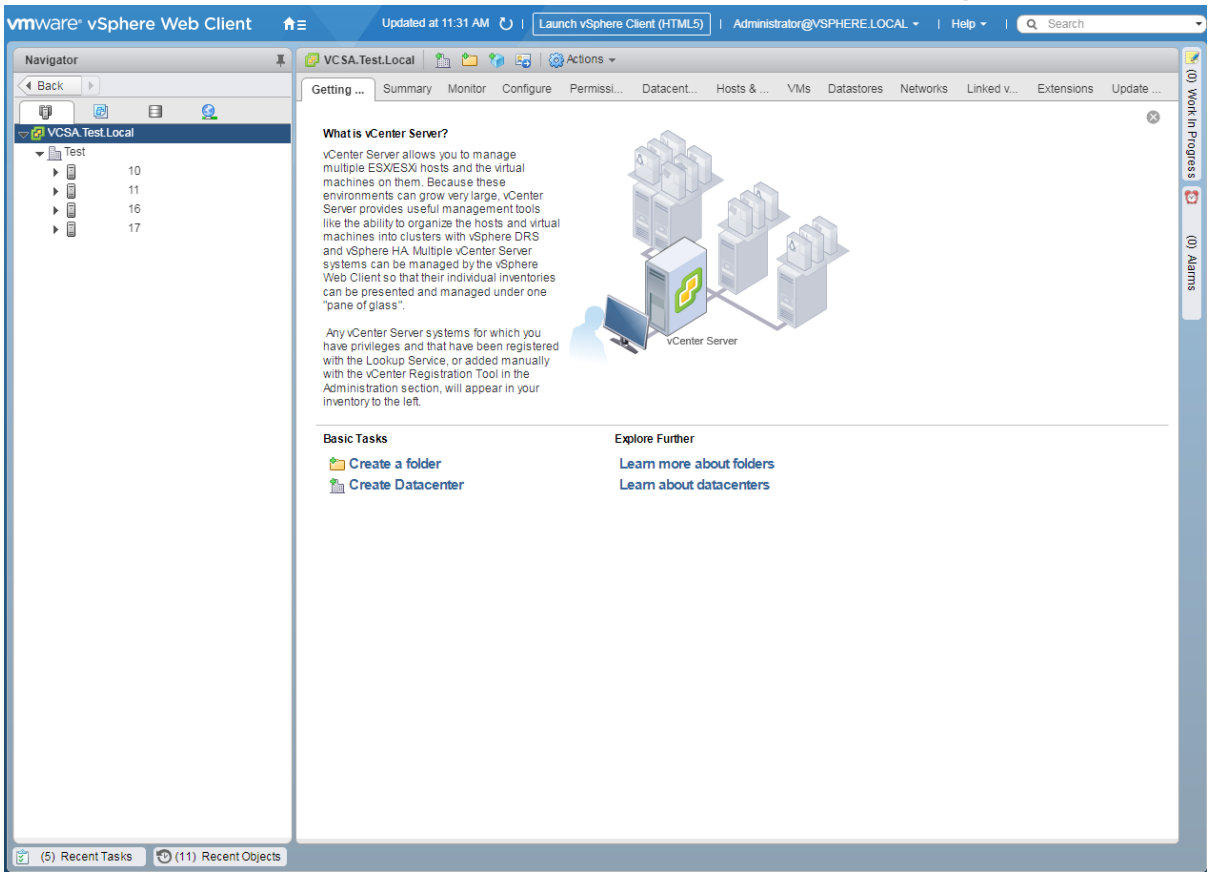
قبل از این که به نصب مؤلفه‌های مختلف نرم‌افزار NSX پرداخته شود، نیاز است تا پیش‌نیازهای آن بررسی گردد. همانطور که توضیح داده شده است، ابتدا باید قسمت مدیریتی نرم‌افزار NSX نصب شود. قسمت مدیریتی یا همان NSX Manager یک فایل OVA تقریباً 2.5GB است مه باید داخل vCenter، Deploy شود. پس از نصب NSX Manager باید Host Modules برروی هسته ESXi یا همان VMKernel نصب شوند تا خود را برای اعمال دستورات NSX Controller آماده کنند. این مؤلفه‌ها همانطور که گفته شده شامل UWA، Kernel Module و ... هستند. پس از آماده شدن ESXi باید NSX Controller نصب گردد تا ارتباط بین Data Plane و Management Plane برقرار شود. این امر توسط NSX Manager صورت می‌گیرد. چک لیست قبل از نصب مؤلفه‌های NSX در جدول زیر به ترتیب آمده است.

	Need These Information
1	Name and login to vCenter Server (5.5 or Later)
2	vSphere Host (ESXi 5.0 or later) (Highly recommend for VXLAN Unicast Support 5.5 or later)
3	VMware Tools installed in all VMs (Need for Endpoint and Data Security)
4	IP information for NSX Manager
5	IP information for NSX Controllers
6	IP information for vSphere Host VTEPs
7	One or more Transport VLANs
8	Data Stores for NSX Manager and Controllers

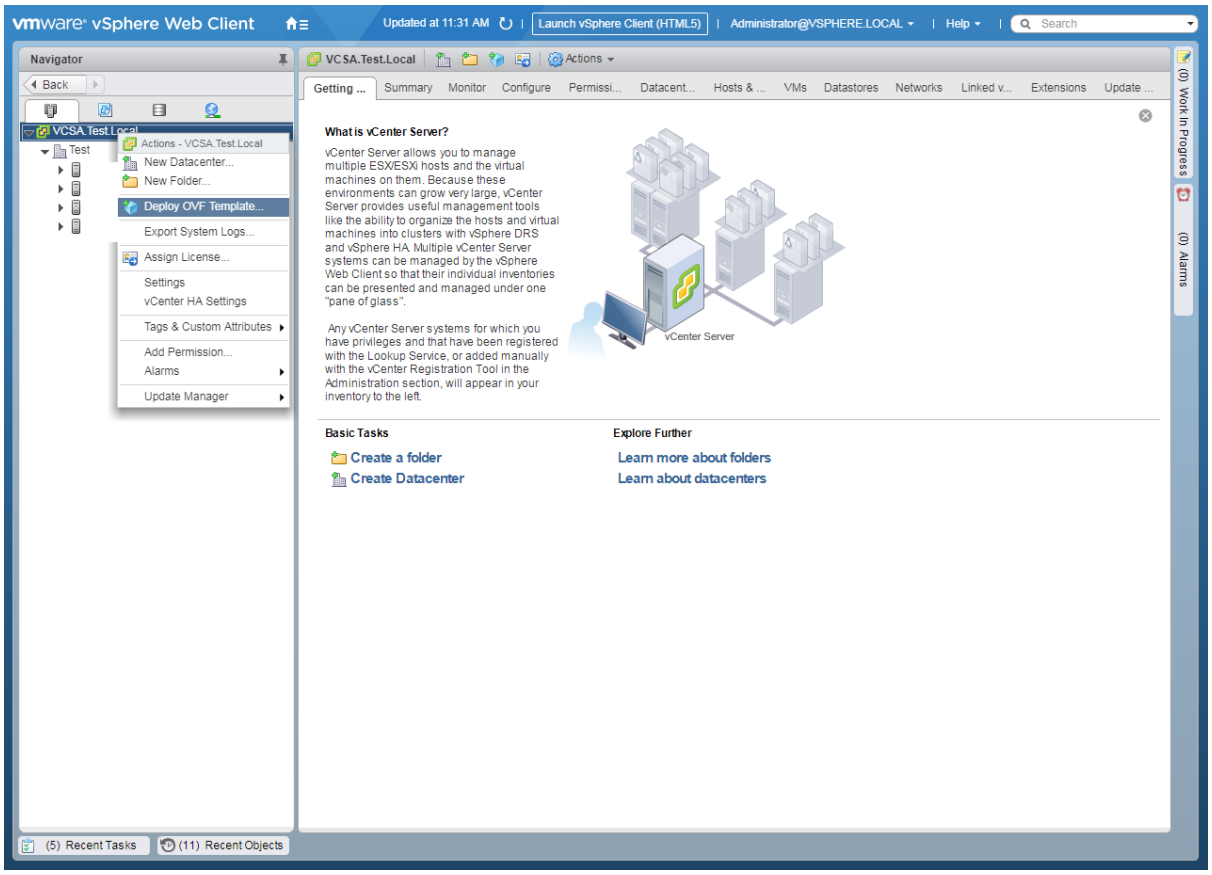
در جدول زیر پیش‌نیازهای سخت‌افزاری مؤلفه‌های مختلف برای نرم‌افزار VMware NSX-V 6.4 شرح داده شده است. در صورتی از NSX Manager با Memory و CPU بیشتری استفاده می‌شود که مرکز داده بیشتر از Hypervisor 256 و یا بیشتر از VM 2000 داشته باشد.

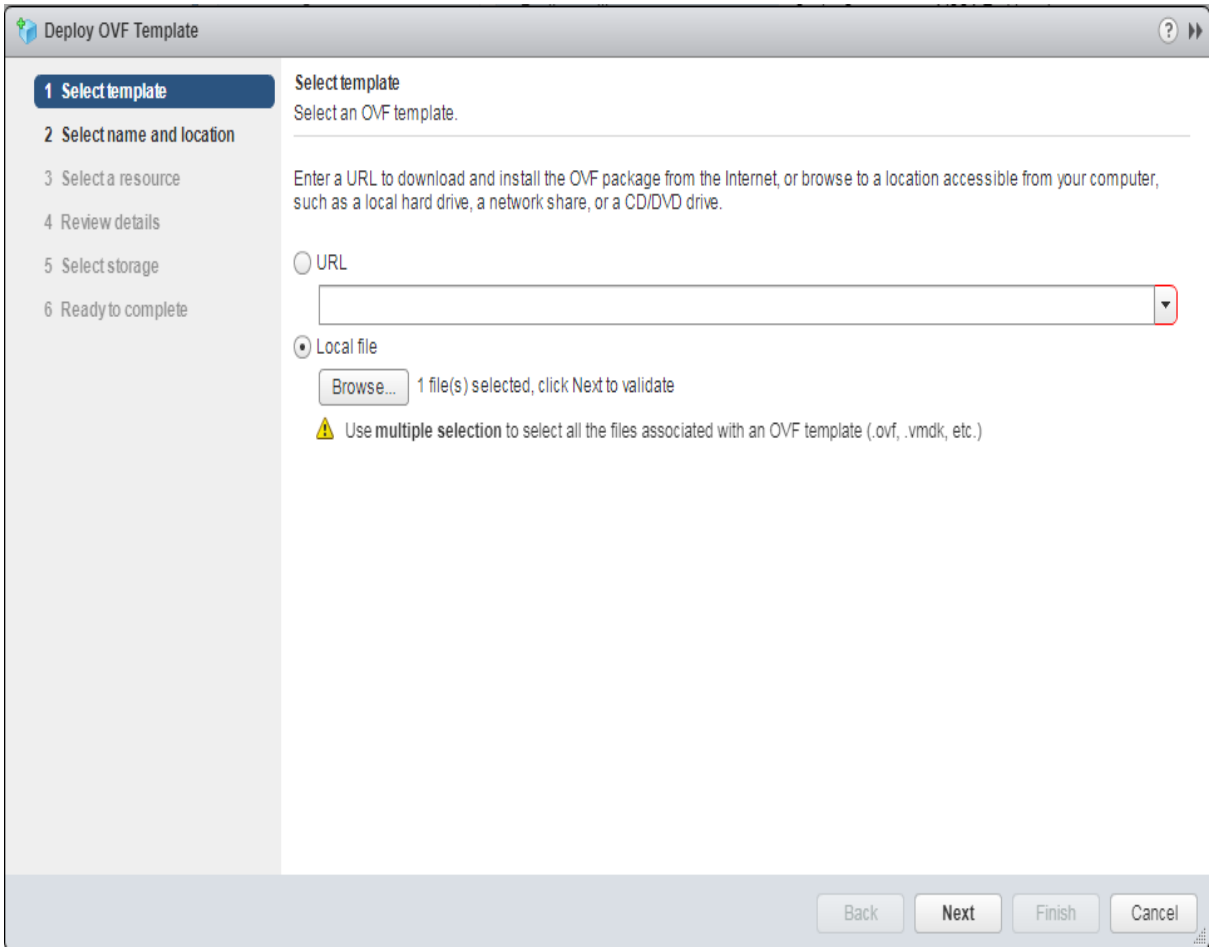
Appliance	Memory	vCPU	Disk Space
NSX Manager	16 GB (24 GB for larger NSX Data Center for vSphere deployments)	4 (8 for larger NSX Data Center for vSphere deployments)	60 GB
NSX Controller	4 GB	4	28 GB
NSX Edge (Distributed logical router is deployed as compact appliance)	Compact: 512 MB Large: 1 GB Quad Large: 2 GB X-Large: 8 GB	Compact: 1 Large: 2 Quad Large: 4 X-Large: 6	**Compact, Large:** 1 disk 584 MB + 1 disk 512 MB **Quad Large:** 1 disk 584 MB + 2 disks 512 MB **X-Large:** 1 disk 584 MB + 1 disk 2 GB + 1 disk 512 MB
Guest Introspection	2 GB	2	5 GB (Provisioned space is 6.26 GB)

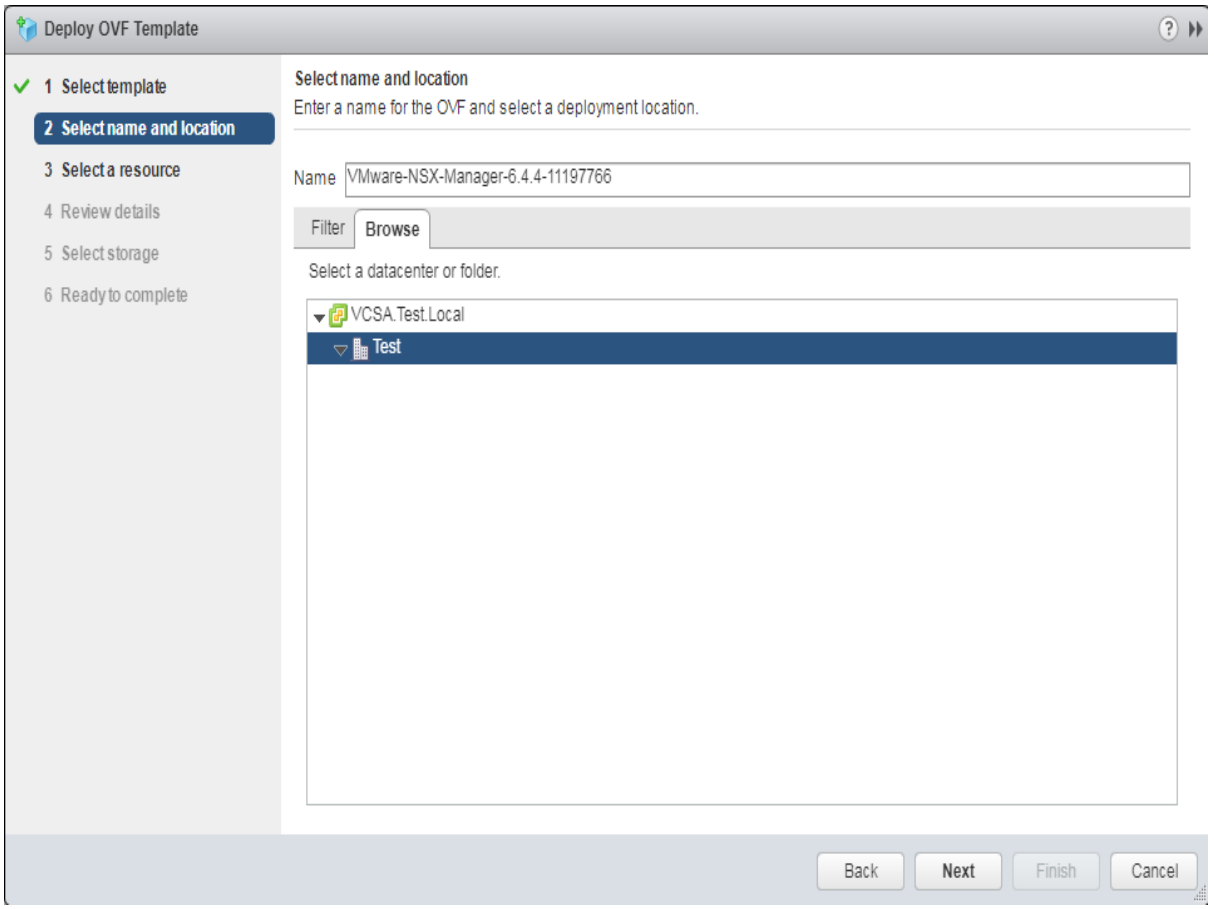
Install NSX Manager ۹-۱-

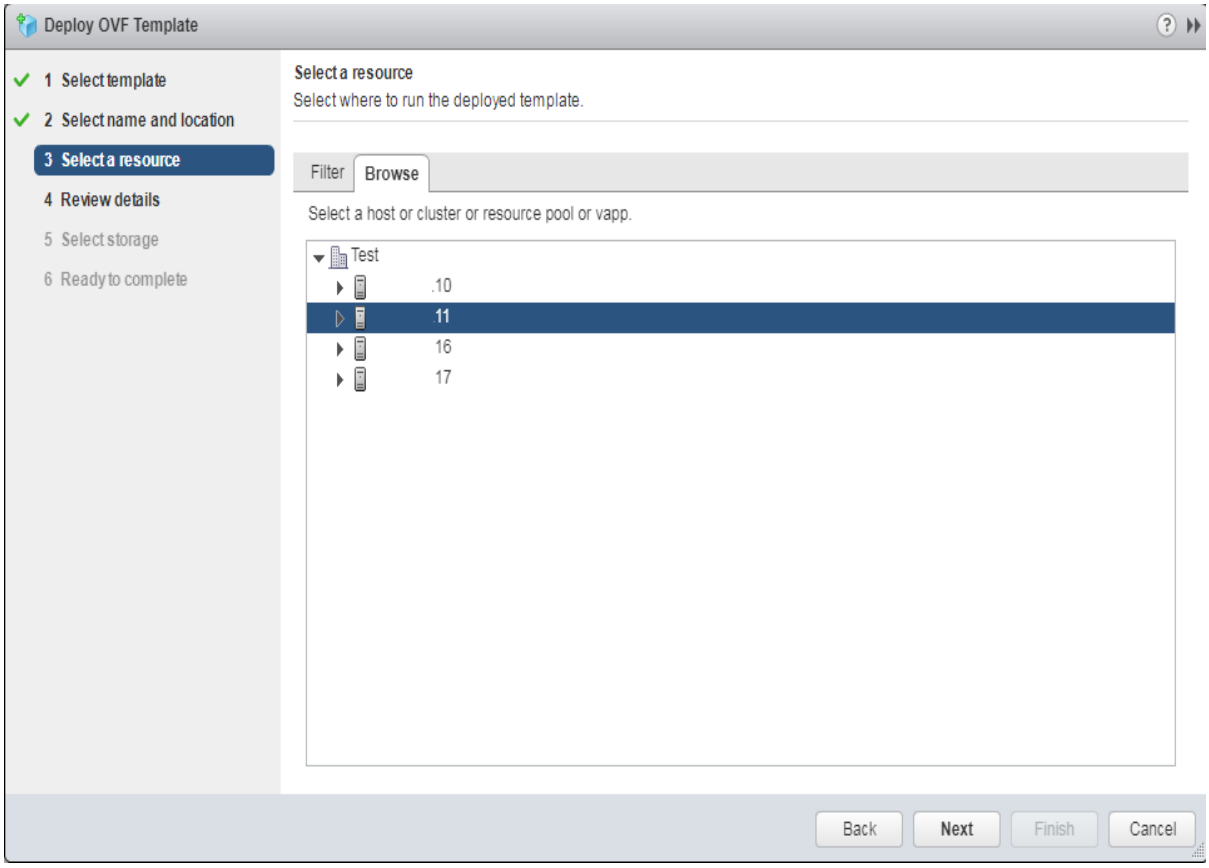


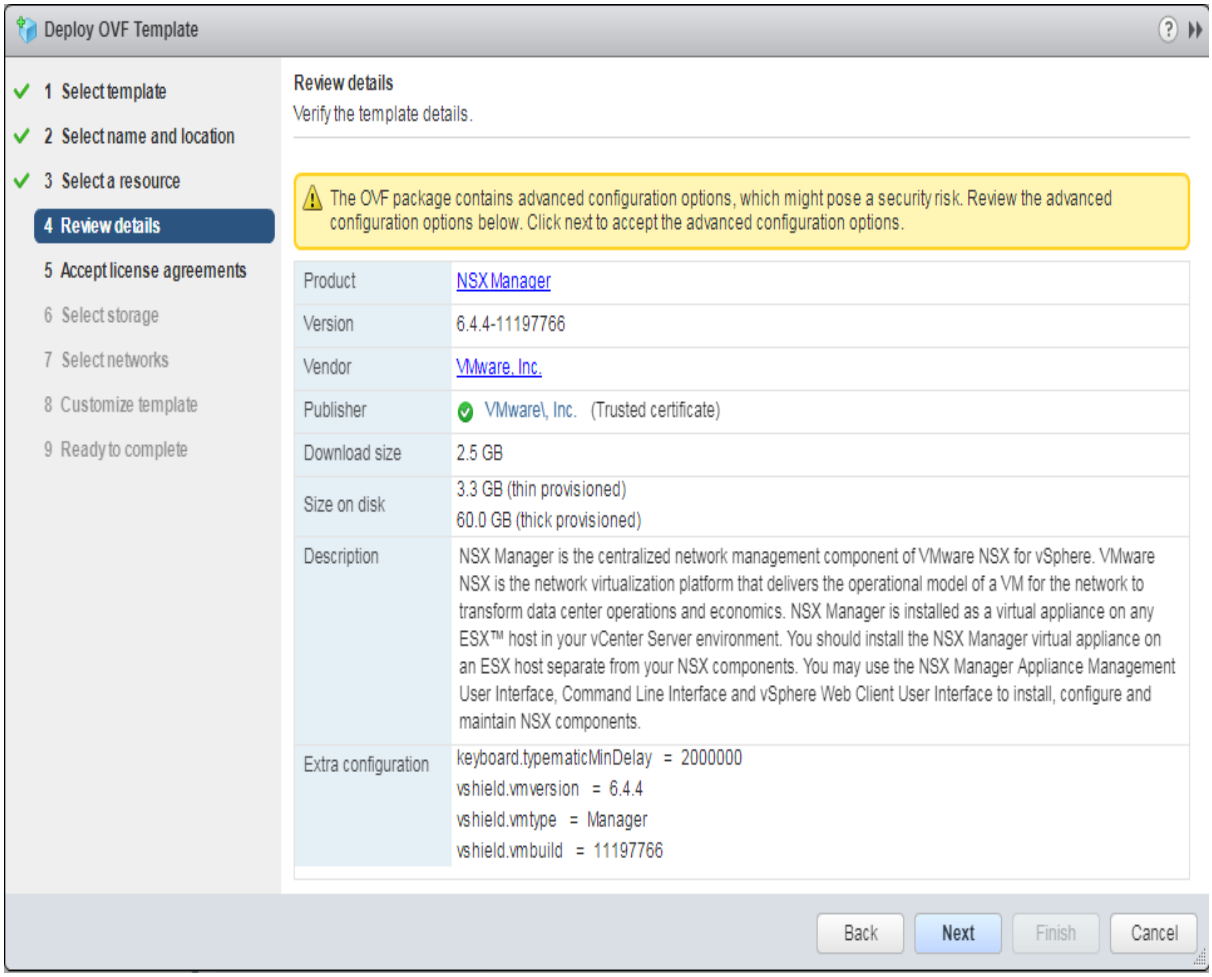
ابتدا باید فایل OVA را Deploy نمود.

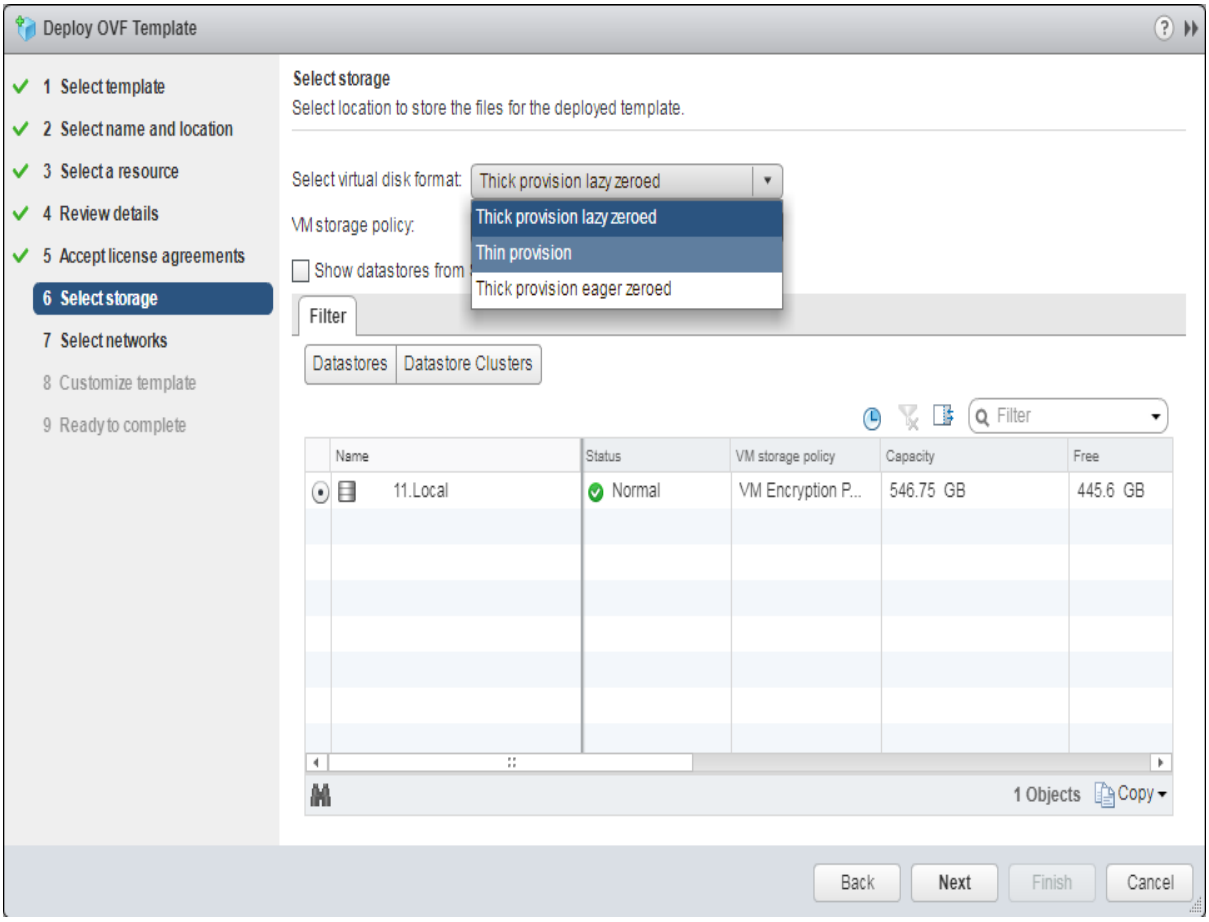


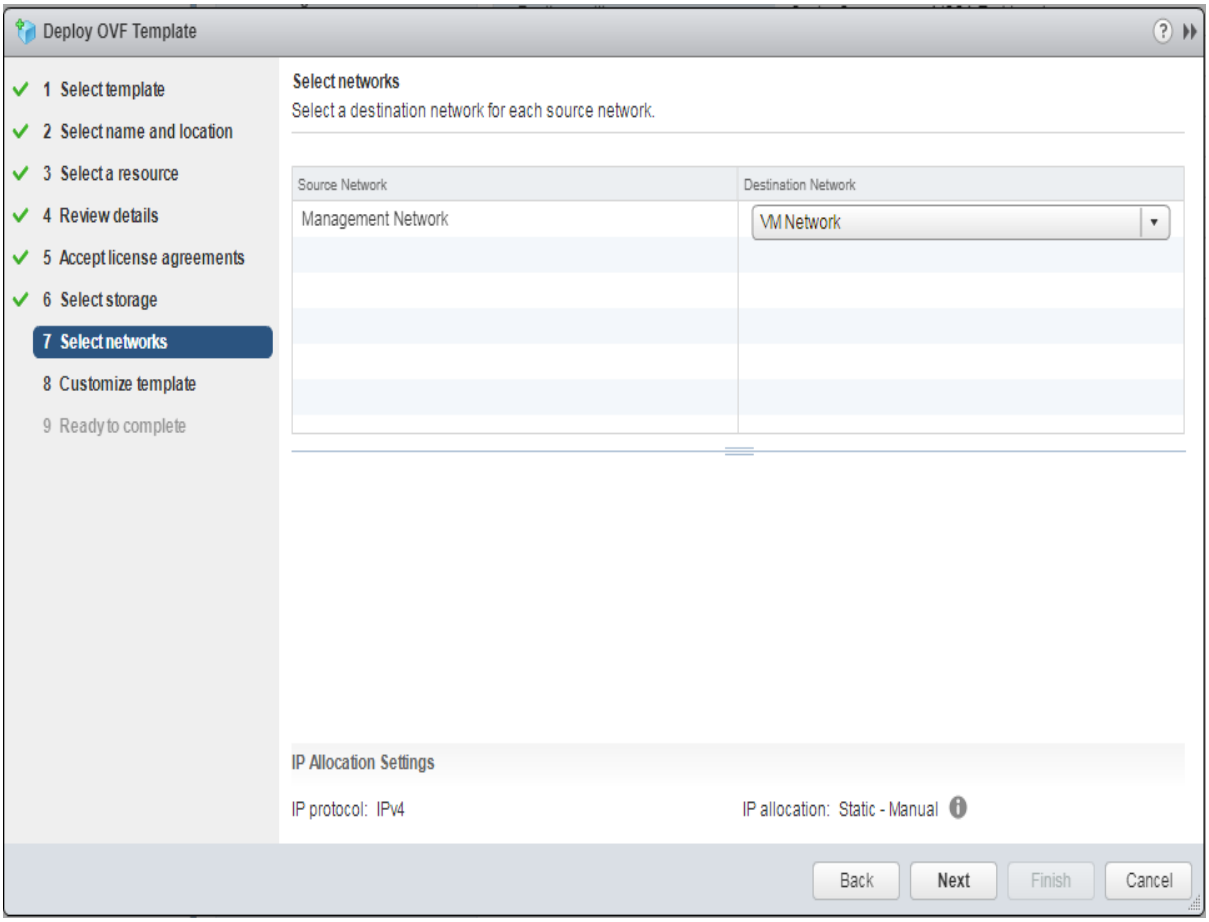

Deploy OVF Template
1 Select template
2 Select name and location
3 Select a resource
4 Review details
5 Select storage
6 Ready to complete
Select template
Select an OVF template.
Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.
URL
Local file
Browse...
1 file(s) selected, click Next to validate
Use multiple selection to select all the files associated with an OVF template (.ovf, .vmdk, etc.)
Back
Next
Finish
Cancel

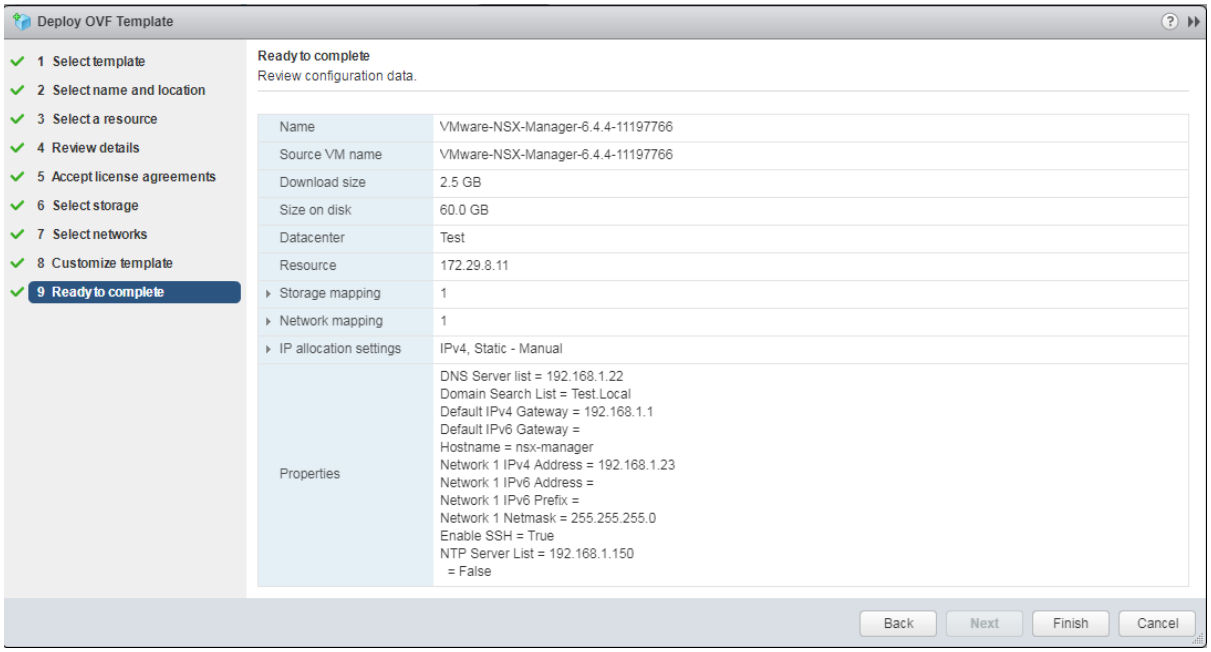

Deploy OVF Template
1 Select template
2 Select name and location
3 Select a resource
4 Review details
5 Select storage
6 Ready to complete
Select name and location
Enter a name for the OVF and select a deployment location.
Name
VMware-NSX-Manager-6.4.4-11197766
Filter
Browse
Select a datacenter or folder.
VCSA.Test.Local
Test
Back
Next
Finish
Cancel


Deploy OVF Template
1 Select template
2 Select name and location
3 Select a resource
4 Review details
5 Select storage
6 Ready to complete
Select a resource
Select where to run the deployed template.
Filter
Browse
Select a host or cluster or resource pool or vapp.
Test
.10
11
16
17
Back
Next
Finish
Cancel

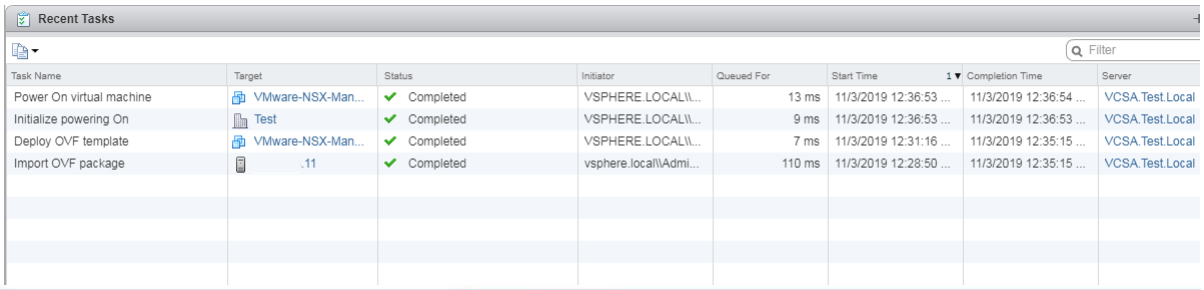

Deploy OVF Template
1 Select template
2 Select name and location
3 Select a resource
4 Review details
5 Accept license agreements
6 Select storage
7 Select networks
8 Customize template
9 Ready to complete
Review details
Verify the template details.
The OVF package contains advanced configuration options, which might pose a security risk. Review the advanced configuration options below. Click next to accept the advanced configuration options.
Product
NSX Manager
Version
6.4.4-11197766
Vendor
VMware, Inc.
Publisher
VMware\, Inc. (Trusted certificate)
Download size
2.5 GB
Size on disk
3.3 GB (thin provisioned)
60.0 GB (thick provisioned)
Description
NSX Manager is the centralized network management component of VMware NSX for vSphere. VMware NSX is the network virtualization platform that delivers the operational model of a VM for the network to transform data center operations and economics. NSX Manager is installed as a virtual appliance on any ESX™ host in your vCenter Server environment. You should install the NSX Manager virtual appliance on an ESX host separate from your NSX components. You may use the NSX Manager Appliance Management User Interface, Command Line Interface and vSphere Web Client User Interface to install, configure and maintain NSX components.
Extra configuration
keyboard.typematicMinDelay = 2000000
vshield.vmversion = 6.4.4
vshield.vmtype = Manager
vshield.vmbuild = 11197766
Back
Next
Finish
Cancel

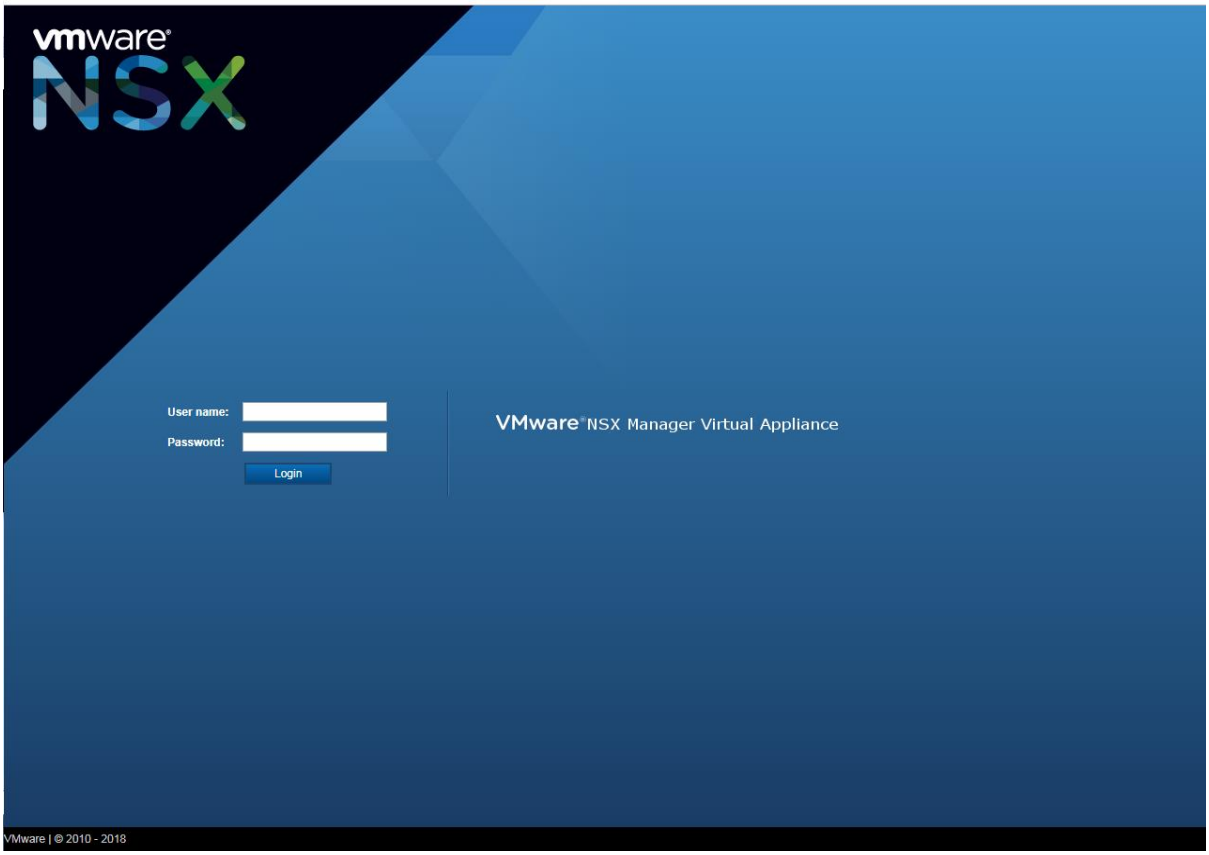

Deploy OVF Template
1 Select template
2 Select name and location
3 Select a resource
4 Review details
5 Accept license agreements
6 Select storage
7 Select networks
8 Customize template
9 Ready to complete
Select storage
Select location to store the files for the deployed template.
Select virtual disk format:
Thick provision lazy zeroed
VM storage policy:
Thick provision lazy zeroed
Thin provision
Thick provision eager zeroed
Show datastores from
Filter
Datastores
Datastore Clusters
Filter
Name
Status
VM storage policy
Capacity
Free
11.Local
Normal
VM Encryption P...
546.75 GB
445.6 GB
1 Objects
Copy
Back
Next
Finish
Cancel


Deploy OVF Template
1 Select template
2 Select name and location
3 Select a resource
4 Review details
5 Accept license agreements
6 Select storage
7 Select networks
8 Customize template
9 Ready to complete
Select networks
Select a destination network for each source network.
Source Network
Destination Network
Management Network
VM Network
IP Allocation Settings
IP protocol: IPv4
IP allocation: Static - Manual
Back
Next
Finish
Cancel



در قسمت بالا باید IP NSX Manager، IP DNS Server و Password برای Admin وارد شود.

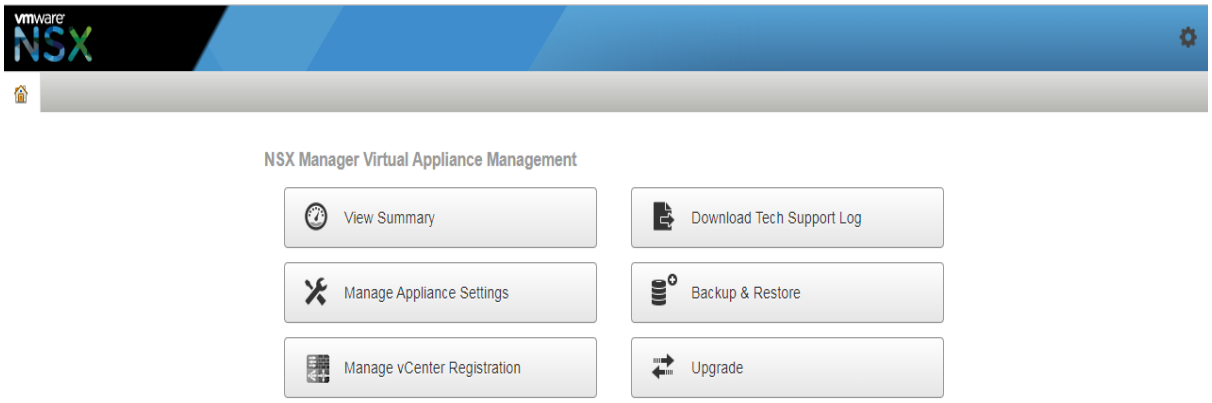


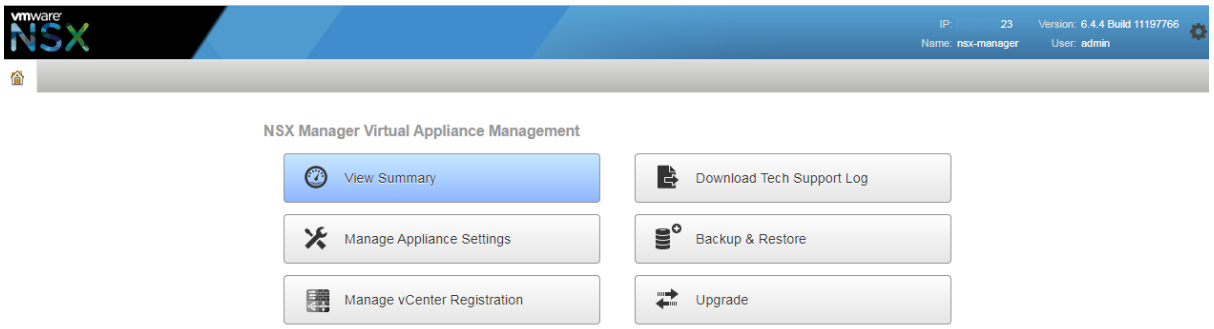


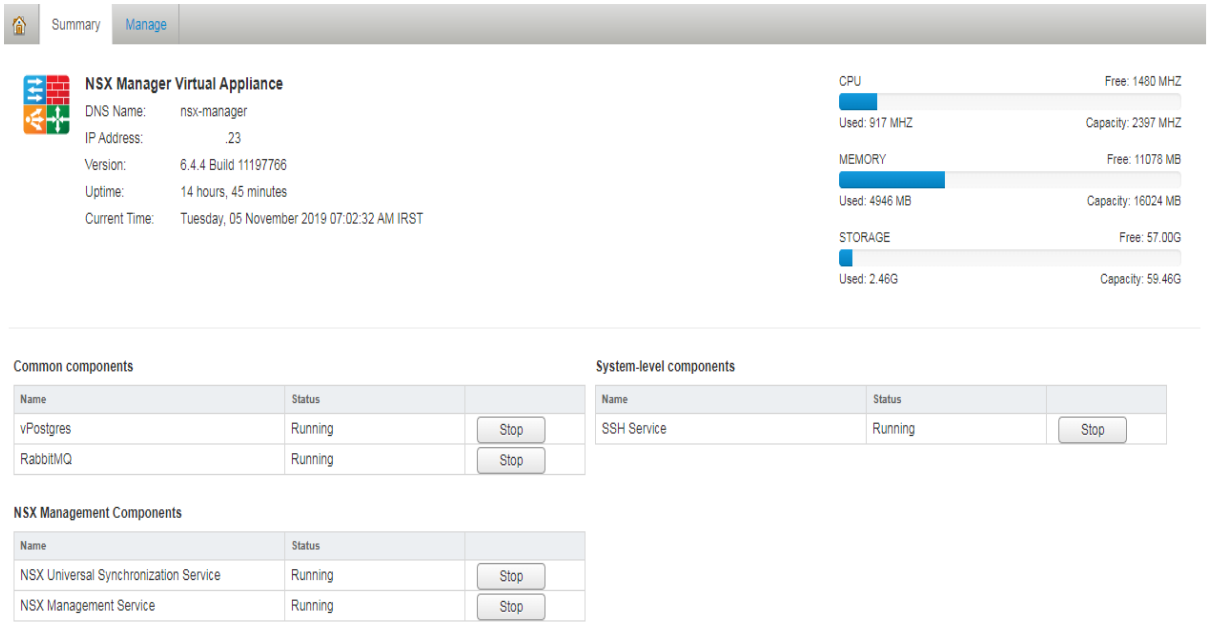
```
login as: admin
admin@         23's password:
nsx-manager>
  debug       Debug Host Connection
  enable      Turn on privileged mode command
  exit        Exit current mode and down to previous mode
  get         get host event notification status
  list        Print command list
  ping        Send echo messages
  quit        Exit current mode and down to previous mode
  reset       Reset terminal settings
  set         set host event notification [enable/disable]
  show        Show running system information
  traceroute  Trace route to destination
nsx-manager> enable
Password:
nsx-manager#
  clear       Clear system configuration
  configure   Configuration from vty interface
  copy        Copy from one file to another
  debug       Debug Host Connection
  delete      Show running system information
  disable     Turn off privileged mode command
  end         End current mode and change to enable mode
  exit        Exit current mode and down to previous mode
  export      Export to a remote system
  list        Print command list
  no          Negate a command or set its defaults
  ping        Send echo messages
  purge       Log commands
  quit        Exit current mode and down to previous mode
  reboot      Reboot the system
  reset       Reset terminal settings
  set         Set parameters
  setup       Launch the setup wizard to configure required settings
  show        Show running system information
  shutdown    Shutdown the system after confirmation
  ssh         Start/Stop SSH service
  start
  traceroute  Trace route to destination
  write       Write running configuration to memory, network, or terminal
nsx-manager#
```

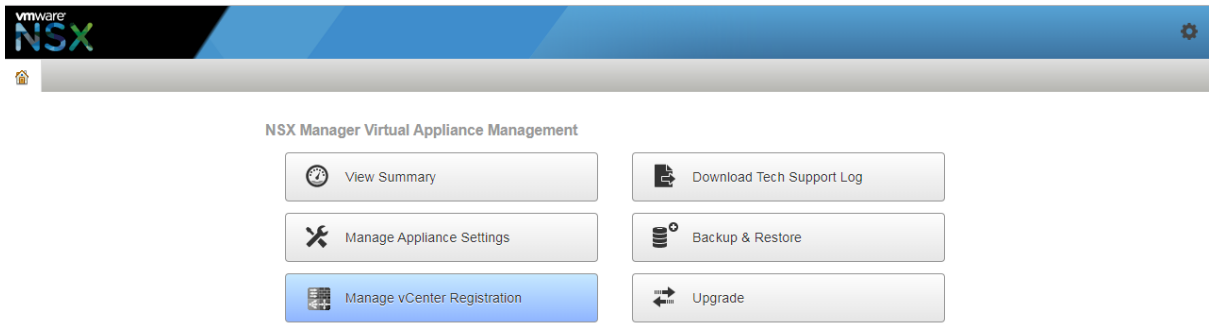
VMware NSX Configuration ۹-۲-

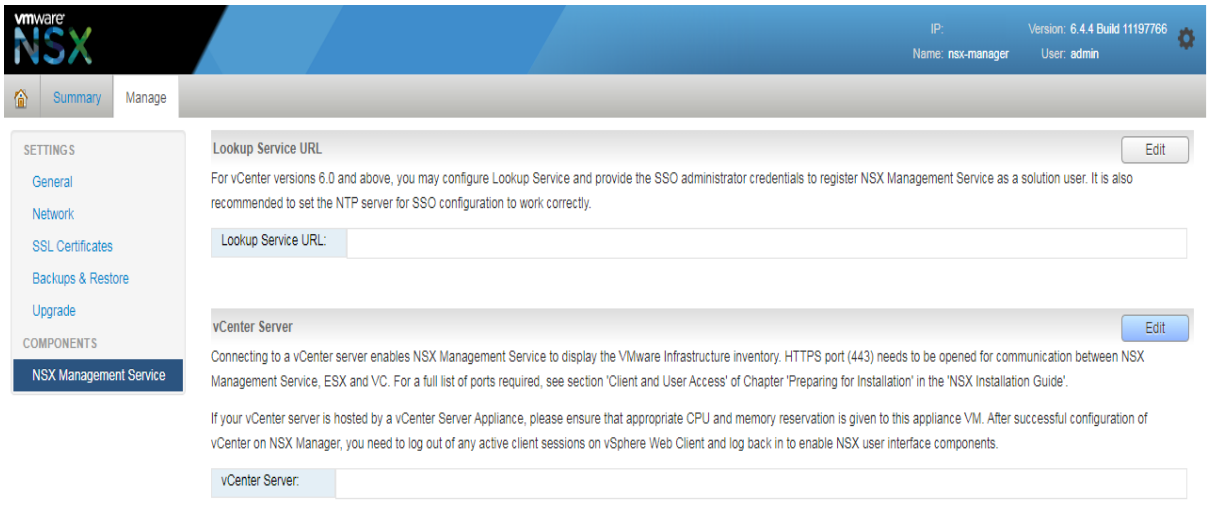
زمانی که IP NSX Manager را در صفحه WEB و پسورد Admin را وارد می‌کنید، با صفحه زیر برخورد می‌کنید.

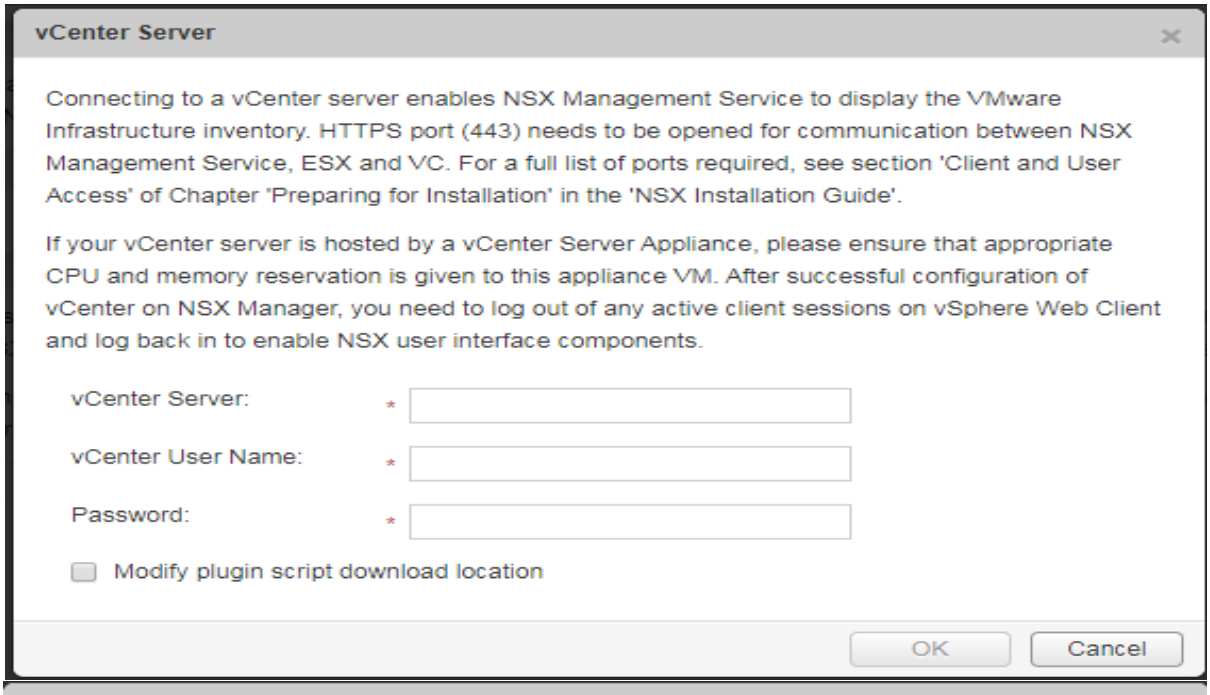


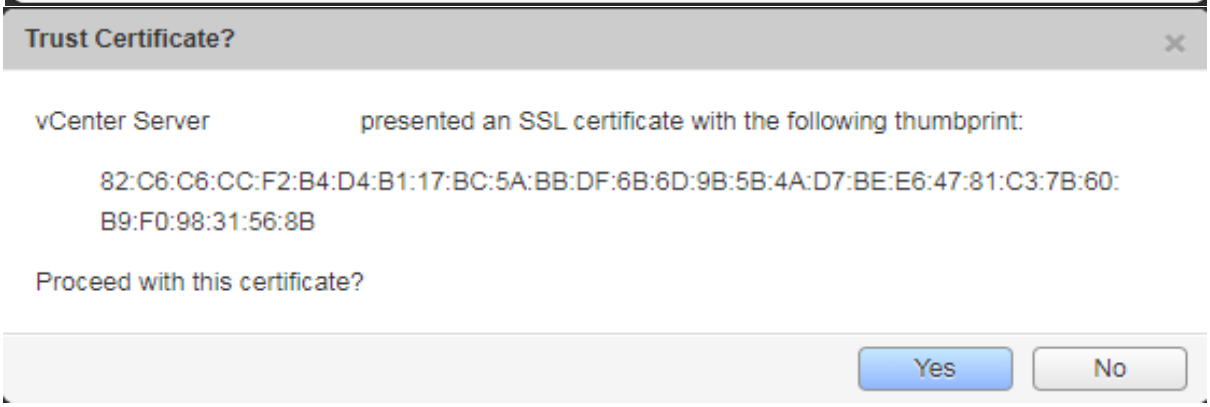

vmware NSX
IP: 23
Version: 6.4.4 Build 11197766
Name: nsx-manager
User: admin
NSX Manager Virtual Appliance Management
View Summary
Download Tech Support Log
Manage Appliance Settings
Backup & Restore
Manage vCenter Registration
Upgrade

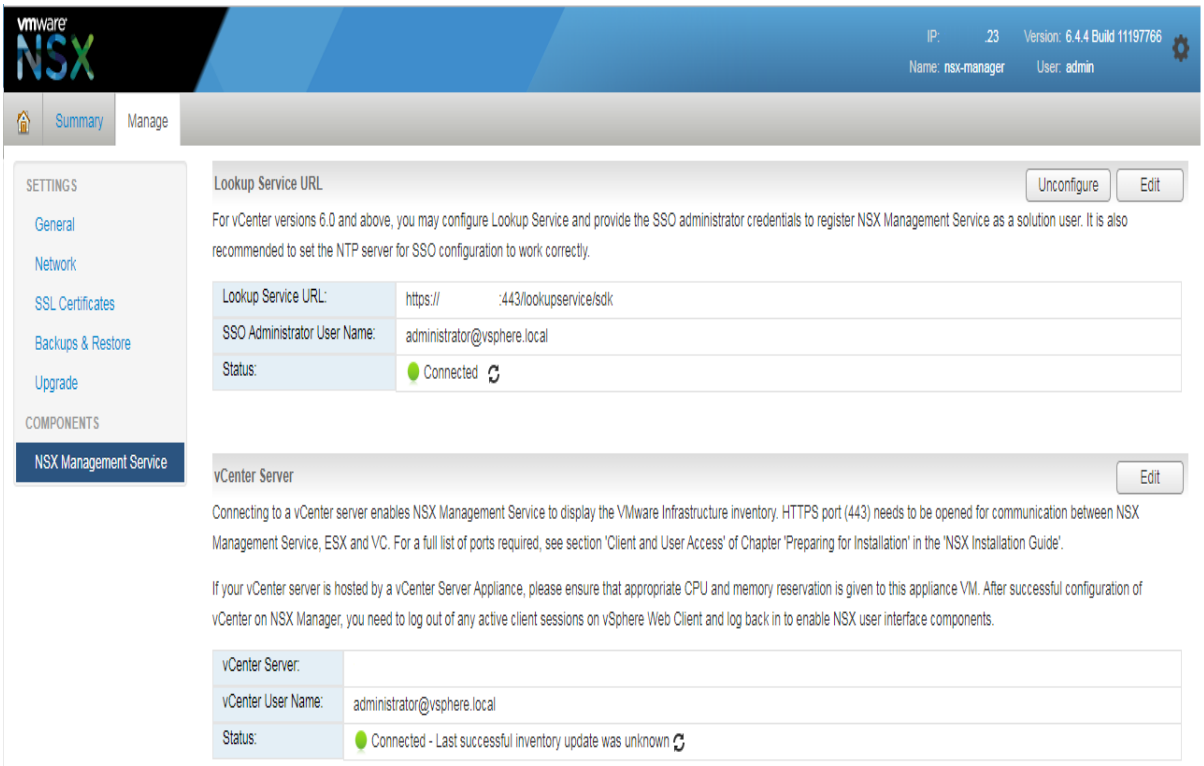

Summary
Manage
NSX Manager Virtual Appliance
DNS Name: nsx-manager
IP Address: .23
Version: 6.4.4 Build 11197766
Uptime: 14 hours, 45 minutes
Current Time: Tuesday, 05 November 2019 07:02:32 AM IRST
CPU
Free: 1480 MHZ
Used: 917 MHZ
Capacity: 2397 MHZ
MEMORY
Free: 11078 MB
Used: 4946 MB
Capacity: 16024 MB
STORAGE
Free: 57.00G
Used: 2.46G
Capacity: 59.46G
Common components
Name
Status
vPostgres
Running
Stop
RabbitMQ
Running
Stop
System-level components
Name
Status
SSH Service
Running
Stop
NSX Management Components
Name
Status
NSX Universal Synchronization Service
Running
Stop
NSX Management Service
Running
Stop

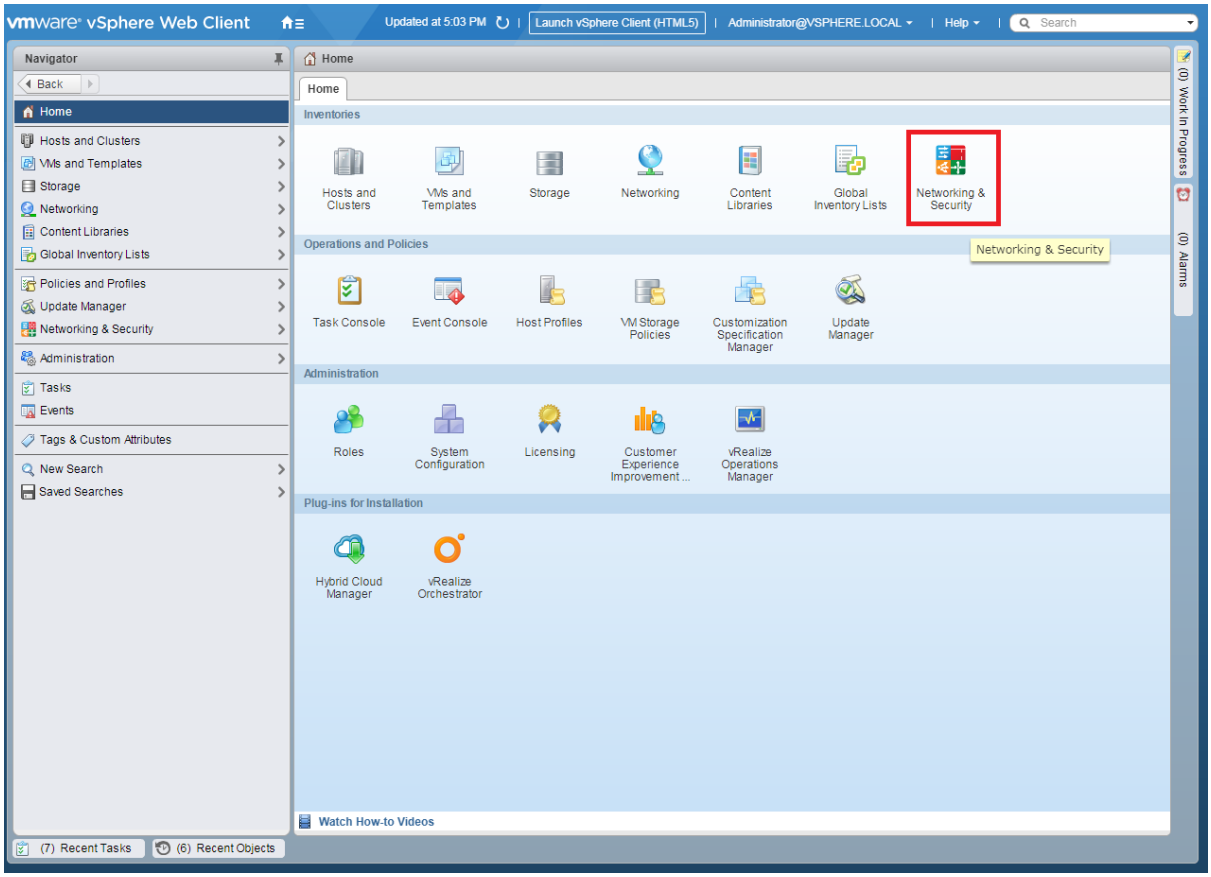

vmware NSX
NSX Manager Virtual Appliance Management
View Summary
Download Tech Support Log
Manage Appliance Settings
Backup & Restore
Manage vCenter Registration
Upgrade

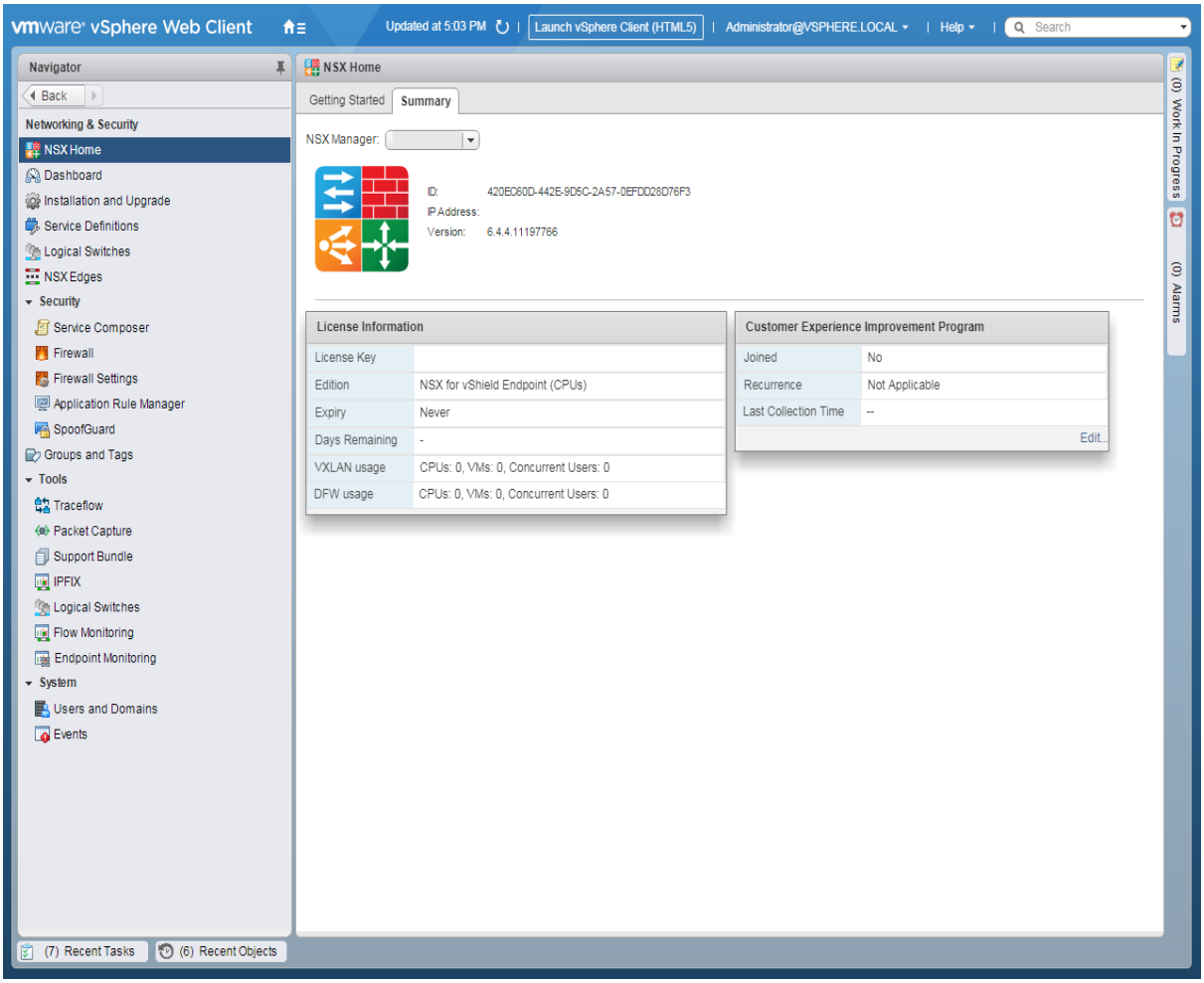

vmware NSX
IP:
Version: 6.4.4 Build 11197766
Name: nsx-manager
User: admin
Summary
Manage
SETTINGS
General
Network
SSL Certificates
Backups & Restore
Upgrade
COMPONENTS
NSX Management Service
Lookup Service URL
Edit
For vCenter versions 6.0 and above, you may configure Lookup Service and provide the SSO administrator credentials to register NSX Management Service as a solution user. It is also recommended to set the NTP server for SSO configuration to work correctly.
Lookup Service URL:
vCenter Server
Edit
Connecting to a vCenter server enables NSX Management Service to display the VMware Infrastructure inventory. HTTPS port (443) needs to be opened for communication between NSX Management Service, ESX and VC. For a full list of ports required, see section 'Client and User Access' of Chapter 'Preparing for Installation' in the 'NSX Installation Guide'.
If your vCenter server is hosted by a vCenter Server Appliance, please ensure that appropriate CPU and memory reservation is given to this appliance VM. After successful configuration of vCenter on NSX Manager, you need to log out of any active client sessions on vSphere Web Client and log back in to enable NSX user interface components.
vCenter Server:

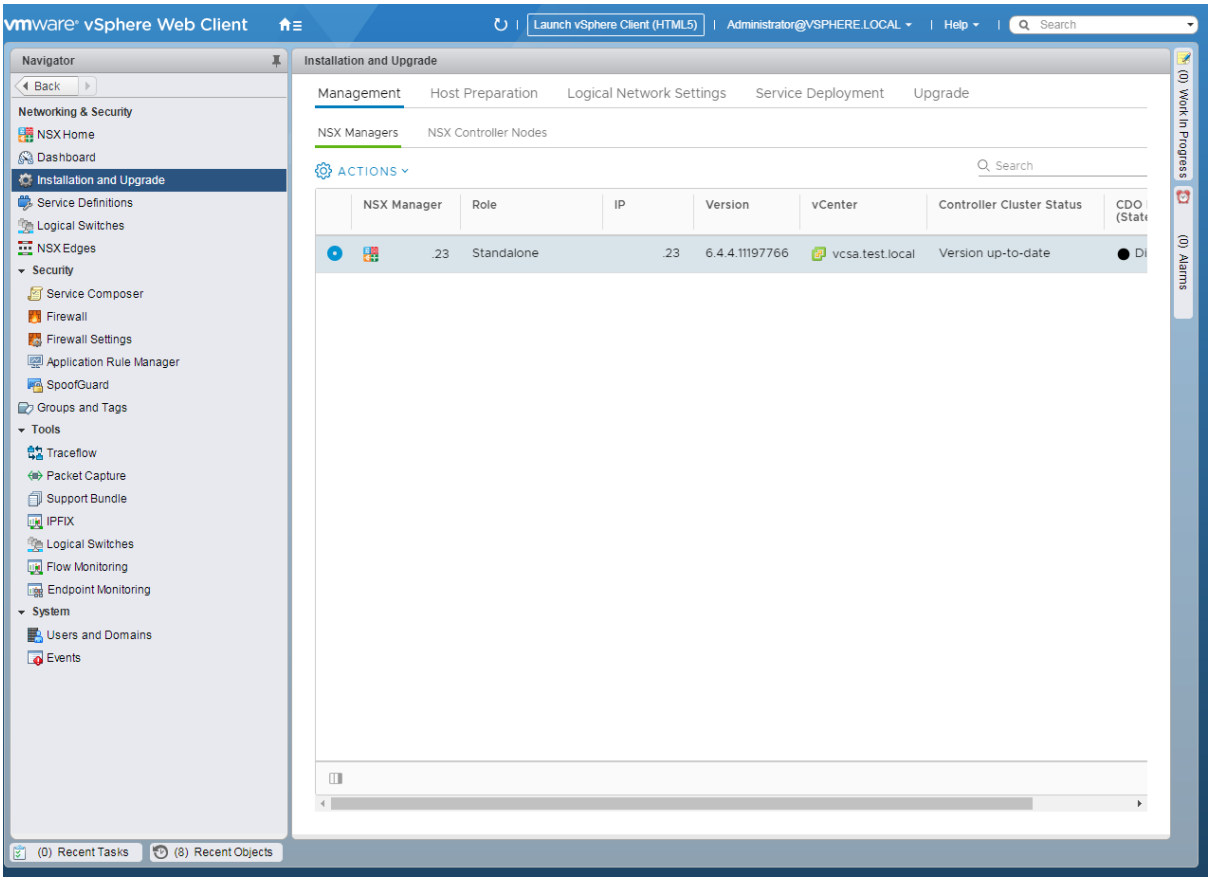

vCenter Server
Connecting to a vCenter server enables NSX Management Service to display the VMware Infrastructure inventory. HTTPS port (443) needs to be opened for communication between NSX Management Service, ESX and VC. For a full list of ports required, see section 'Client and User Access' of Chapter 'Preparing for Installation' in the 'NSX Installation Guide'.
If your vCenter server is hosted by a vCenter Server Appliance, please ensure that appropriate CPU and memory reservation is given to this appliance VM. After successful configuration of vCenter on NSX Manager, you need to log out of any active client sessions on vSphere Web Client and log back in to enable NSX user interface components.
vCenter Server: *
vCenter User Name: *
Password: *
Modify plugin script download location
OK
Cancel

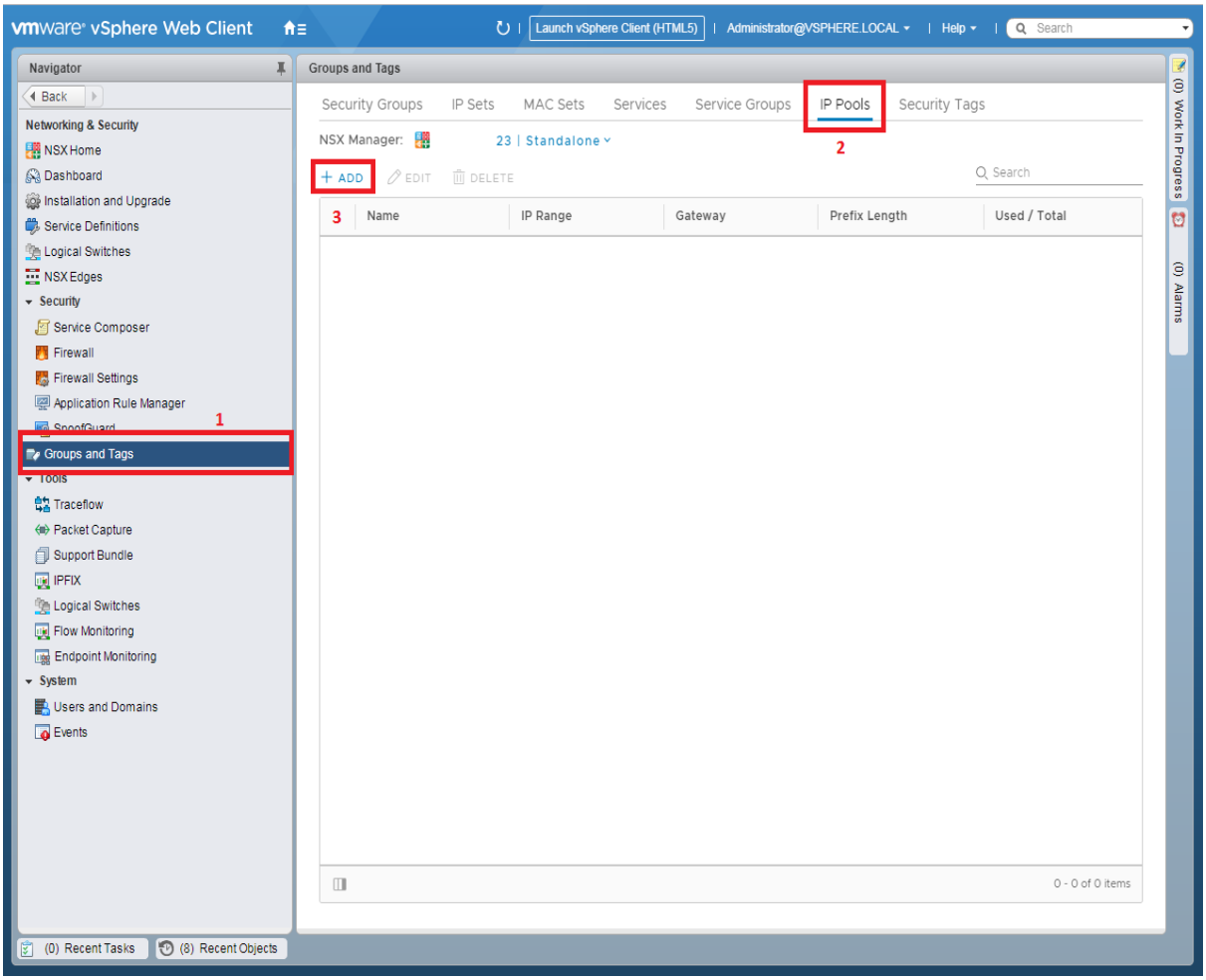

Trust Certificate?
vCenter Server presented an SSL certificate with the following thumbprint:
82:C6:C6:CC:F2:B4:D4:B1:17:BC:5A:BB:DF:6B:6D:9B:5B:4A:D7:BE:E6:47:81:C3:7B:60:
B9:F0:98:31:56:8B
Proceed with this certificate?
Yes
No

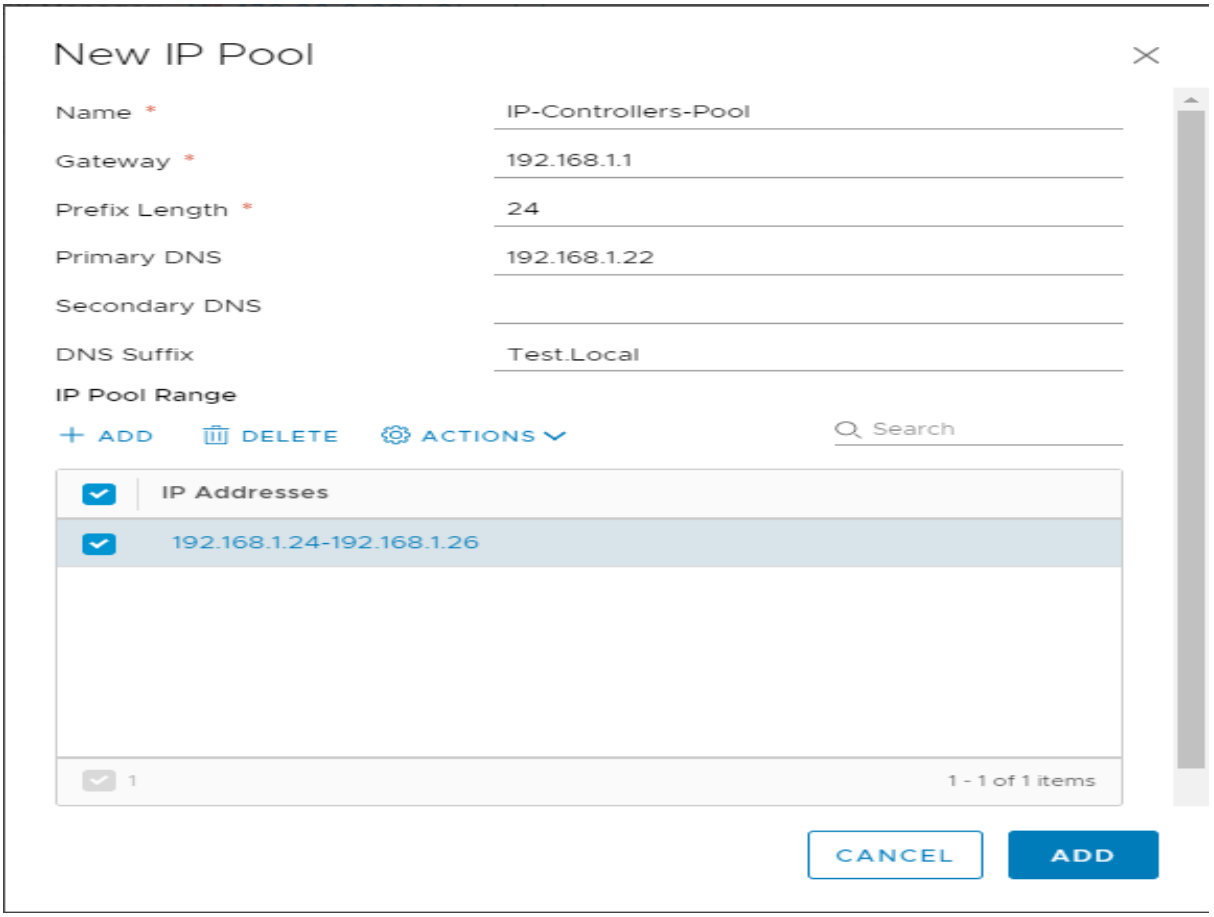

vmware NSX
IP: .23 Version: 6.4.4 Build 11197766
Name: nsx-manager User: admin
Summary
Manage
SETTINGS
General
Network
SSL Certificates
Backups & Restore
Upgrade
COMPONENTS
NSX Management Service
Lookup Service URL
Unconfigure
Edit
For vCenter versions 6.0 and above, you may configure Lookup Service and provide the SSO administrator credentials to register NSX Management Service as a solution user. It is also recommended to set the NTP server for SSO configuration to work correctly.
Lookup Service URL: https:// :443/lookupservice/sdk
SSO Administrator User Name: administrator@vsphere.local
Status: Connected
vCenter Server
Edit
Connecting to a vCenter server enables NSX Management Service to display the VMware Infrastructure inventory. HTTPS port (443) needs to be opened for communication between NSX Management Service, ESX and VC. For a full list of ports required, see section 'Client and User Access' of Chapter 'Preparing for Installation' in the 'NSX Installation Guide'.
If your vCenter server is hosted by a vCenter Server Appliance, please ensure that appropriate CPU and memory reservation is given to this appliance VM. After successful configuration of vCenter on NSX Manager, you need to log out of any active client sessions on vSphere Web Client and log back in to enable NSX user interface components.
vCenter Server:
vCenter User Name: administrator@vsphere.local
Status: Connected - Last successful inventory update was unknown


vmware vSphere Web Client
Updated at 5:03 PM
Launch vSphere Client (HTML5)
Administrator@VSPHERE.LOCAL
Help
Search
Navigator
Back
Home
Hosts and Clusters
VMs and Templates
Storage
Networking
Content Libraries
Global Inventory Lists
Policies and Profiles
Update Manager
Networking & Security
Administration
Tasks
Events
Tags & Custom Attributes
New Search
Saved Searches
Home
Inventories
Hosts and Clusters
VMs and Templates
Storage
Networking
Content Libraries
Global Inventory Lists
Networking & Security
Networking & Security
Operations and Policies
Task Console
Event Console
Host Profiles
VM Storage Policies
Customization Specification Manager
Update Manager
Administration
Roles
System Configuration
Licensing
Customer Experience Improvement ...
vRealize Operations Manager
Plug-ins for Installation
Hybrid Cloud Manager
vRealize Orchestrator
Watch How-to Videos
(7) Recent Tasks
(6) Recent Objects
(0) Work in Progress
(0) Alarms

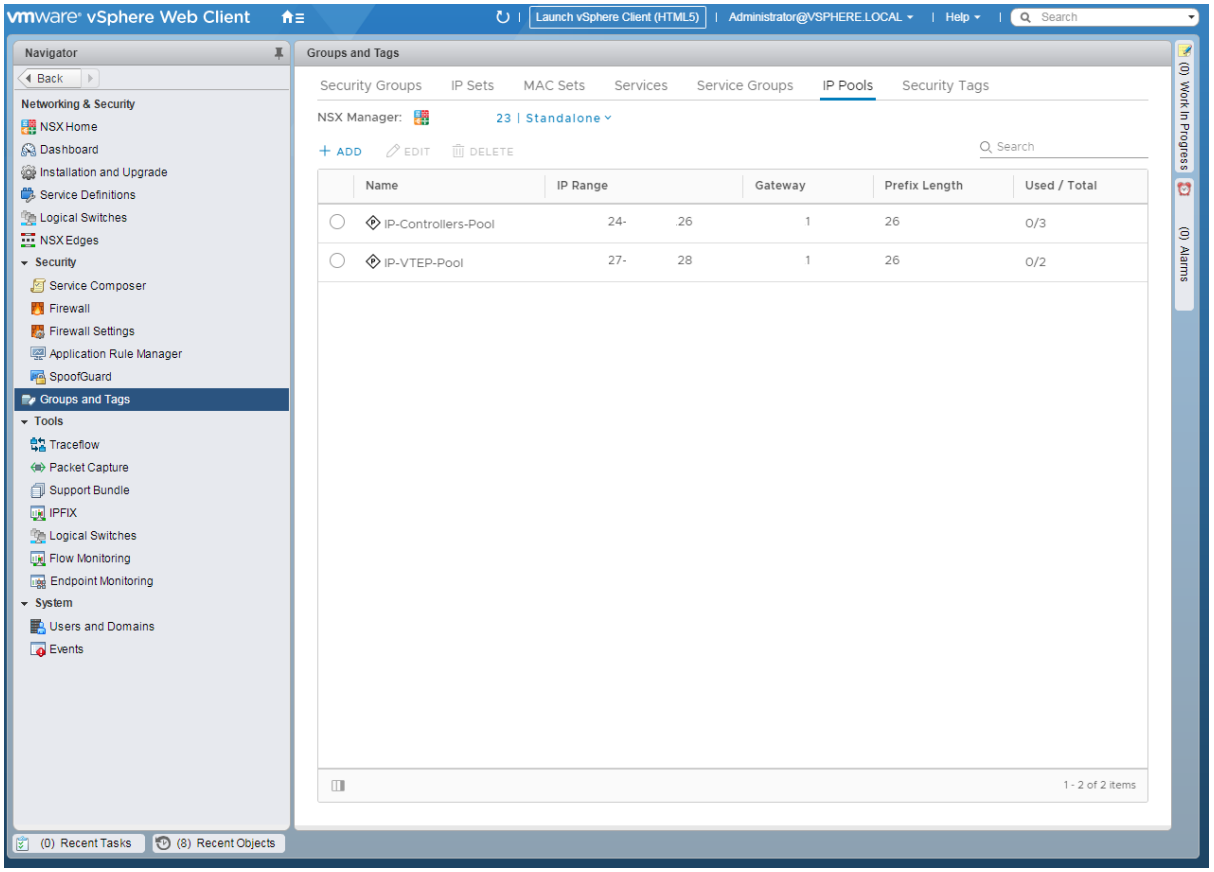

vmware vSphere Web Client
Updated at 5:03 PM
Launch vSphere Client (HTML5)
Administrator@VSPHERE.LOCAL
Help
Search
Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation and Upgrade
Service Definitions
Logical Switches
NSX Edges
Security
Service Composer
Firewall
Firewall Settings
Application Rule Manager
SpoofGuard
Groups and Tags
Tools
Traceflow
Packet Capture
Support Bundle
IPFIX
Logical Switches
Flow Monitoring
Endpoint Monitoring
System
Users and Domains
Events
NSX Home
Getting Started
Summary
NSX Manager:
ID: 420E060D-442E-9D5C-2A57-0EFDD28D76F3
IP Address:
Version: 6.4.4.11197766
License Information
License Key
Edition
NSX for vShield Endpoint (CPUs)
Expiry
Never
Days Remaining
-
VXLAN usage
CPUs: 0, VMs: 0, Concurrent Users: 0
DFW usage
CPUs: 0, VMs: 0, Concurrent Users: 0
Customer Experience Improvement Program
Joined
No
Recurrence
Not Applicable
Last Collection Time
--
Edit...
(7) Recent Tasks
(6) Recent Objects
(0) Work in Progress
(0) Alarms

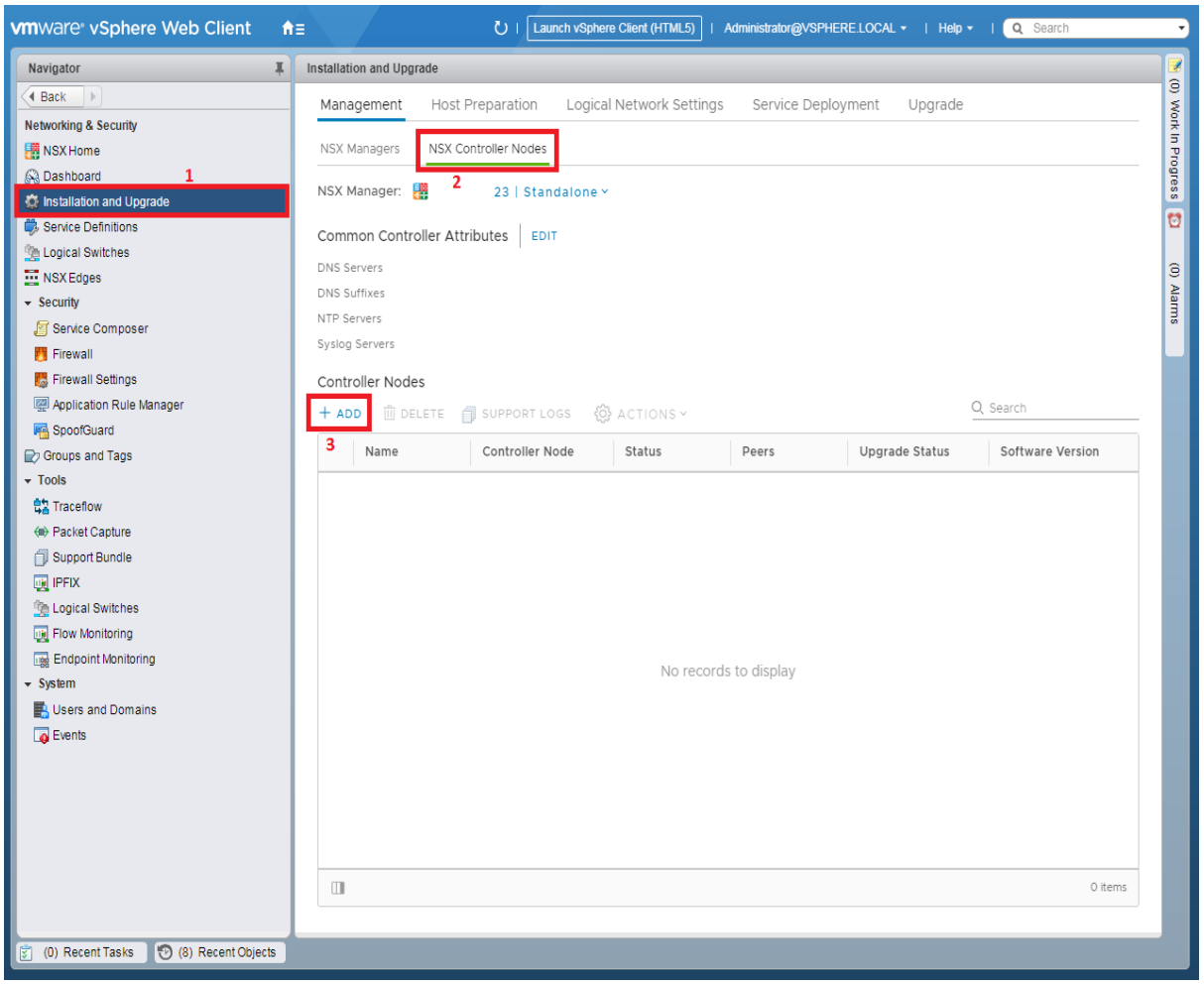

vmware vSphere Web Client
Launch vSphere Client (HTML5)
Administrator@VSPHERE.LOCAL
Help
Search
Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation and Upgrade
Service Definitions
Logical Switches
NSX Edges
Security
Service Composer
Firewall
Firewall Settings
Application Rule Manager
SpoofGuard
Groups and Tags
Tools
Traceflow
Packet Capture
Support Bundle
IPFIX
Logical Switches
Flow Monitoring
Endpoint Monitoring
System
Users and Domains
Events
Installation and Upgrade
Management
Host Preparation
Logical Network Settings
Service Deployment
Upgrade
NSX Managers
NSX Controller Nodes
ACTIONS
Search
NSX Manager
Role
IP
Version
vCenter
Controller Cluster Status
.23
Standalone
.23
6.4.4.11197766
vcsa.test.local
Version up-to-date
(0) Work in Progress
(0) Alarms
(0) Recent Tasks
(8) Recent Objects

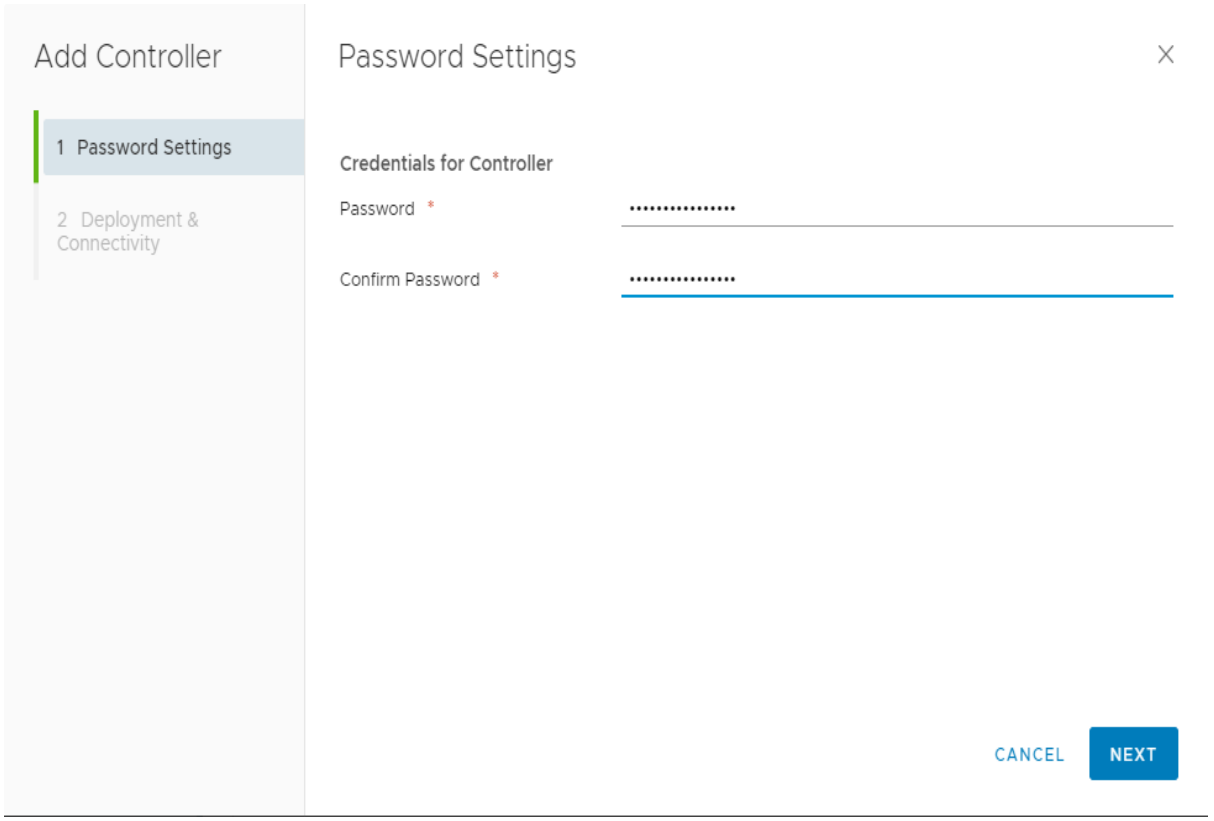

vmware vSphere Web Client
Launch vSphere Client (HTML5)
Administrator@VSPHERE.LOCAL
Help
Search
Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation and Upgrade
Service Definitions
Logical Switches
NSX Edges
Security
Service Composer
Firewall
Firewall Settings
Application Rule Manager
SpoofGuard
1
Groups and Tags
Tools
Traceflow
Packet Capture
Support Bundle
IPFIX
Logical Switches
Flow Monitoring
Endpoint Monitoring
System
Users and Domains
Events
Groups and Tags
Security Groups
IP Sets
MAC Sets
Services
Service Groups
IP Pools
Security Tags
2
NSX Manager:
23 | Standalone
+ ADD
EDIT
DELETE
Search
3
Name
IP Range
Gateway
Prefix Length
Used / Total
0 - 0 of 0 items
(0) Work in Progress
(0) Alarms
(0) Recent Tasks
(8) Recent Objects

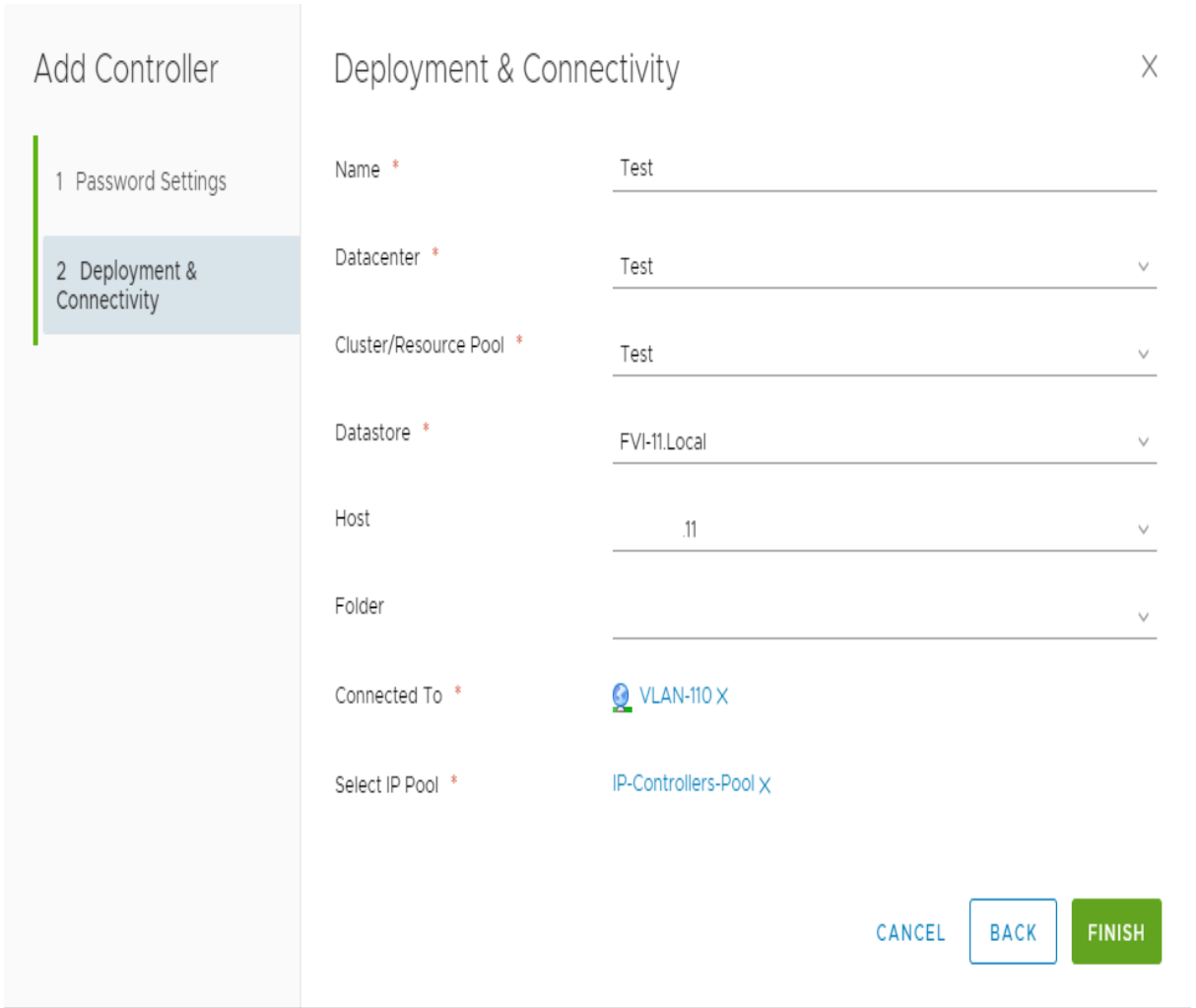

New IP Pool
Name *
IP-Controllers-Pool
Gateway *
192.168.1.1
Prefix Length *
24
Primary DNS
192.168.1.22
Secondary DNS
DNS Suffix
Test.Local
IP Pool Range
ADD
DELETE
ACTIONS
Search
IP Addresses
192.168.1.24-192.168.1.26
1 - 1 of 1 items
CANCEL
ADD

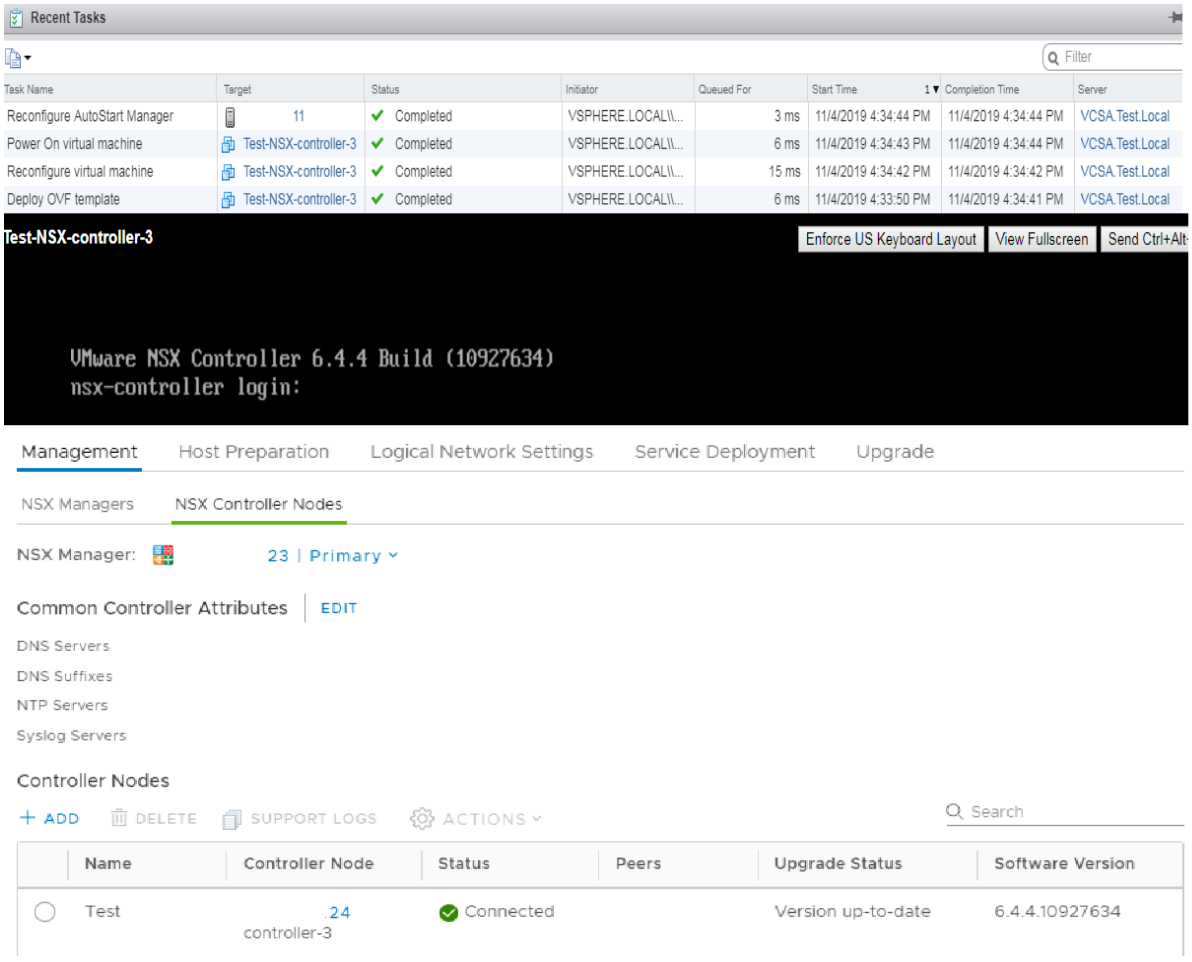

New IP Pool
Name *
IP-VTEP-Pool
Gateway *
192.168.1.1
Prefix Length *
24
Primary DNS
192.168.1.22
Secondary DNS
DNS Suffix
Test.Local
IP Pool Range
ADD
DELETE
ACTIONS
Search
IP Addresses
192.168.1.27-192.168.1.28
1 - 1 of 1 items
CANCEL
ADD


vmware vSphere Web Client
Launch vSphere Client (HTML5)
Administrator@VSPHERE.LOCAL
Help
Search
Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation and Upgrade
Service Definitions
Logical Switches
NSX Edges
Security
Service Composer
Firewall
Firewall Settings
Application Rule Manager
SpoofGuard
Groups and Tags
Tools
Traceflow
Packet Capture
Support Bundle
IPFIX
Logical Switches
Flow Monitoring
Endpoint Monitoring
System
Users and Domains
Events
(0) Recent Tasks
(8) Recent Objects
Groups and Tags
Security Groups
IP Sets
MAC Sets
Services
Service Groups
IP Pools
Security Tags
NSX Manager:
23 | Standalone
+ ADD
EDIT
DELETE
Search
Name
IP Range
Gateway
Prefix Length
Used / Total
IP-Controllers-Pool
24-
.26
1
26
0/3
IP-VTEP-Pool
27-
28
1
26
0/2
1 - 2 of 2 items
(0) Work In Progress
(0) Alarms

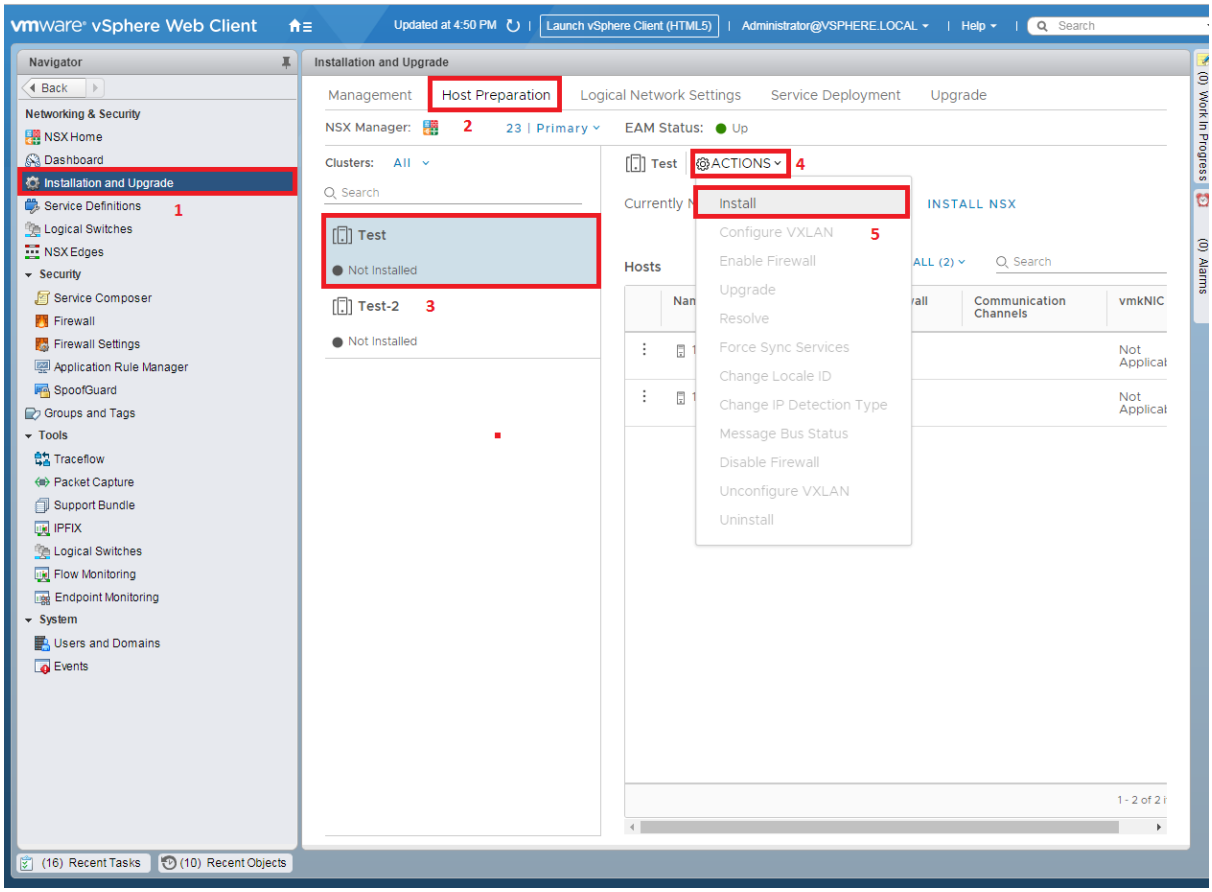

vmware vSphere Web Client
Launch vSphere Client (HTML5)
Administrator@VSPHERE.LOCAL
Help
Search
Navigator
Back
Networking & Security
NSX Home
Dashboard
1
Installation and Upgrade
Service Definitions
Logical Switches
NSX Edges
Security
Service Composer
Firewall
Firewall Settings
Application Rule Manager
SpoofGuard
Groups and Tags
Tools
Traceflow
Packet Capture
Support Bundle
IPFIX
Logical Switches
Flow Monitoring
Endpoint Monitoring
System
Users and Domains
Events
(0) Recent Tasks
(8) Recent Objects
Installation and Upgrade
Management
Host Preparation
Logical Network Settings
Service Deployment
Upgrade
NSX Managers
NSX Controller Nodes
2
NSX Manager:
23 | Standalone
Common Controller Attributes
EDIT
DNS Servers
DNS Suffixes
NTP Servers
Syslog Servers
Controller Nodes
+ ADD
DELETE
SUPPORT LOGS
ACTIONS
Search
3
Name
Controller Node
Status
Peers
Upgrade Status
Software Version
No records to display
0 items
(0) Work In Progress
(0) Alarms

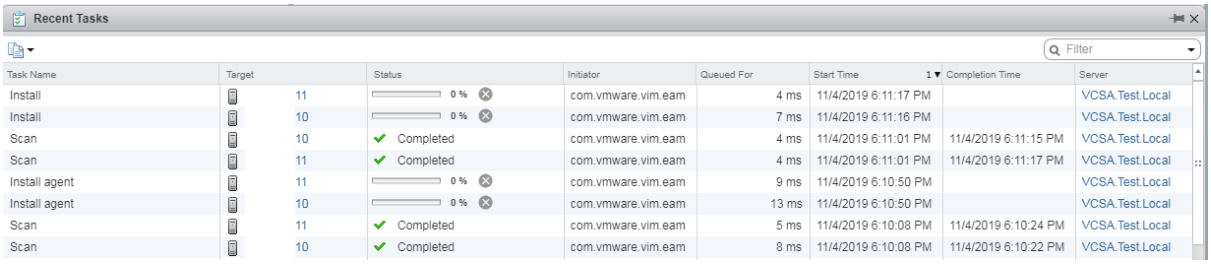

Add Controller
1 Password Settings
2 Deployment & Connectivity
Password Settings
Credentials for Controller
Password *
Confirm Password *
CANCEL
NEXT

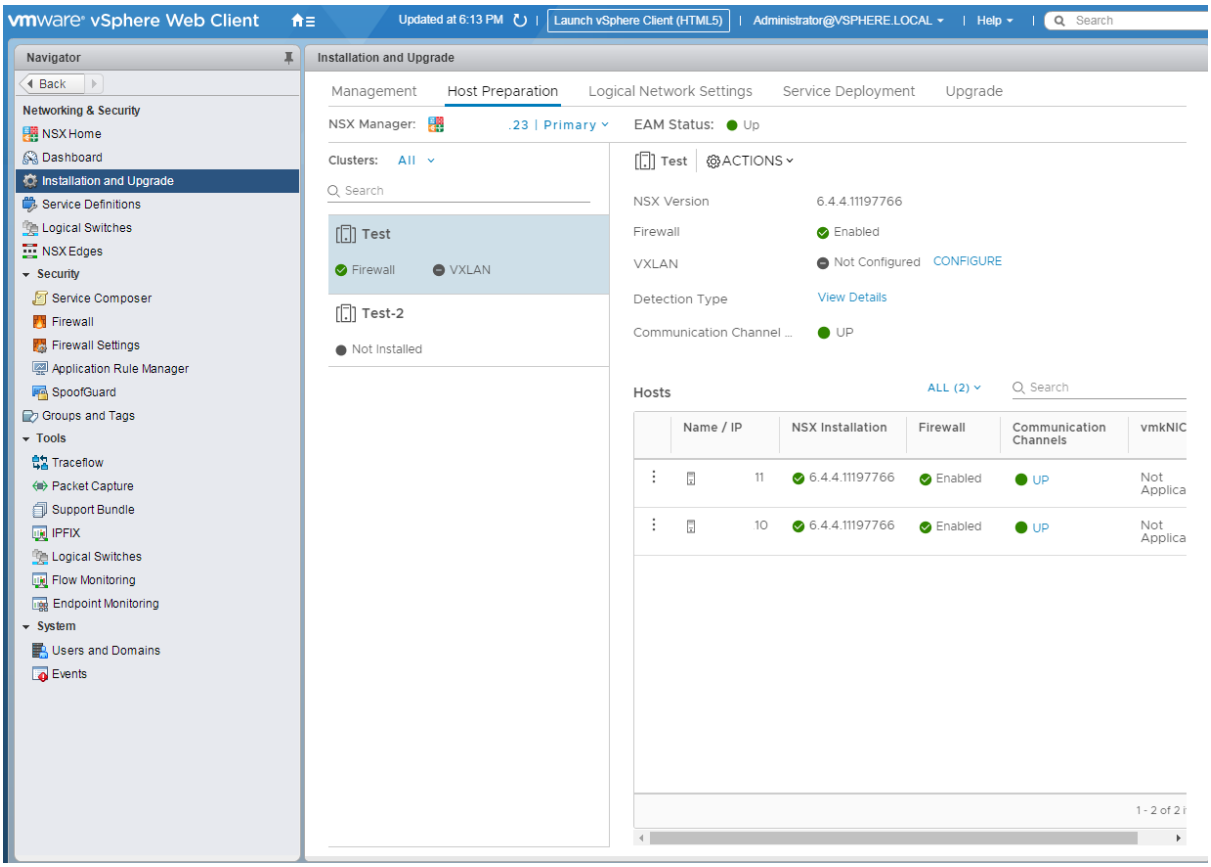

Add Controller
1 Password Settings
2 Deployment & Connectivity
Deployment & Connectivity
Name *
Test
Datacenter *
Test
Cluster/Resource Pool *
Test
Datastore *
FVI-11.Local
Host
.11
Folder
Connected To *
VLAN-110 X
Select IP Pool *
IP-Controllers-Pool X
CANCEL
BACK
FINISH

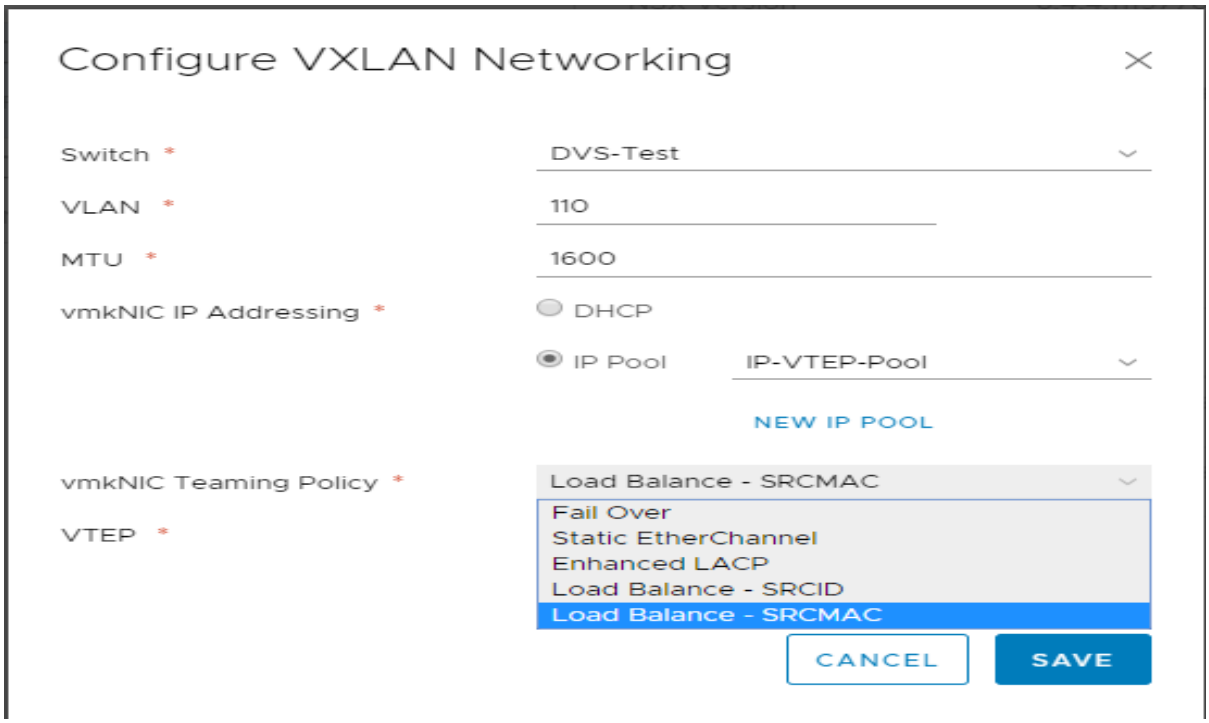

Recent Tasks
Filter
Task Name | Target | Status | Initiator | Queued For | Start Time | Completion Time | Server
Reconfigure AutoStart Manager | 11 | Completed | VSPHERE.LOCAL\\... | 3 ms | 11/4/2019 4:34:44 PM | 11/4/2019 4:34:44 PM | VCSA.Test.Local
Power On virtual machine | Test-NSX-controller-3 | Completed | VSPHERE.LOCAL\\... | 6 ms | 11/4/2019 4:34:43 PM | 11/4/2019 4:34:44 PM | VCSA.Test.Local
Reconfigure virtual machine | Test-NSX-controller-3 | Completed | VSPHERE.LOCAL\\... | 15 ms | 11/4/2019 4:34:42 PM | 11/4/2019 4:34:42 PM | VCSA.Test.Local
Deploy OVF template | Test-NSX-controller-3 | Completed | VSPHERE.LOCAL\\... | 6 ms | 11/4/2019 4:33:50 PM | 11/4/2019 4:34:41 PM | VCSA.Test.Local
Test-NSX-controller-3
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt
VMware NSX Controller 6.4.4 Build (10927634)
nsx-controller login:

Management
Host Preparation
Logical Network Settings
Service Deployment
Upgrade
NSX Managers
NSX Controller Nodes
NSX Manager: 23 | Primary
Common Controller Attributes
EDIT
DNS Servers
DNS Suffixes
NTP Servers
Syslog Servers
Controller Nodes
ADD
DELETE
SUPPORT LOGS
ACTIONS
Search
Name | Controller Node | Status | Peers | Upgrade Status | Software Version
Test | .24 controller-3 | Connected | | Version up-to-date | 6.4.4.10927634

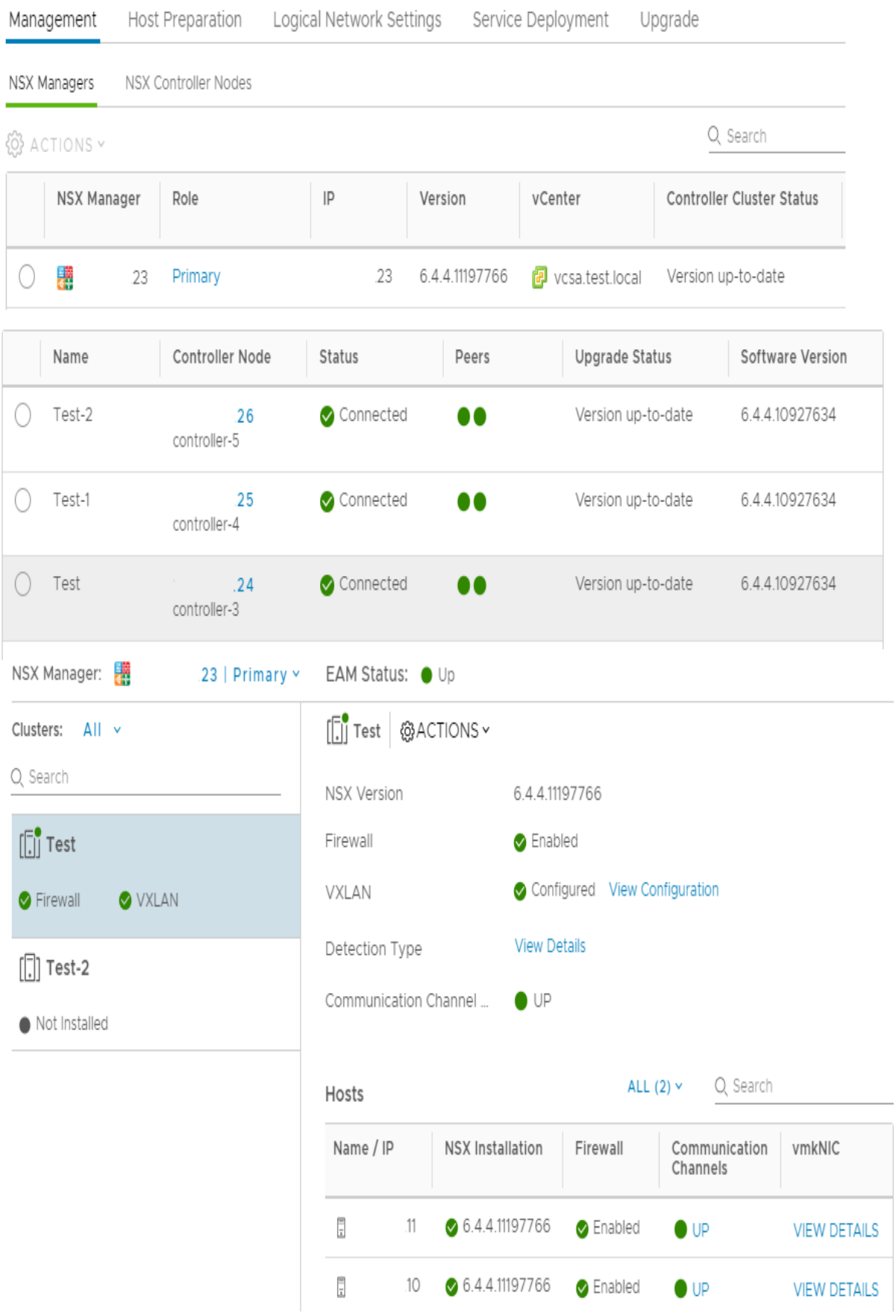

vmware vSphere Web Client
Updated at 4:50 PM
Launch vSphere Client (HTML5)
Administrator@VSPHERE.LOCAL
Help
Search
Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation and Upgrade
Service Definitions
Logical Switches
NSX Edges
Security
Service Composer
Firewall
Firewall Settings
Application Rule Manager
SpoofGuard
Groups and Tags
Tools
Traceflow
Packet Capture
Support Bundle
IPFIX
Logical Switches
Flow Monitoring
Endpoint Monitoring
System
Users and Domains
Events
1
Installation and Upgrade
Management
Host Preparation
Logical Network Settings
Service Deployment
Upgrade
NSX Manager: 2 23 | Primary
EAM Status: Up
Clusters: All
Search
Test
Not Installed
Test-2 3
Not Installed
Test
ACTIONS 4
Install
Configure VXLAN 5
Enable Firewall
Upgrade
Resolve
Force Sync Services
Change Locale ID
Change IP Detection Type
Message Bus Status
Disable Firewall
Unconfigure VXLAN
Uninstall
INSTALL NSX
Hosts
ALL (2)
Search
Communication Channels
vmkNIC
Not Applicat
Not Applicat
1 - 2 of 2
(16) Recent Tasks
(10) Recent Objects
(0) Work in Progress
(0) Alarms


Recent Tasks
Filter
Task Name | Target | Status | Initiator | Queued For | Start Time | Completion Time | Server
Install | 11 | 0 % | com.vmware.vim.eam | 4 ms | 11/4/2019 6:11:17 PM | | VCSA.Test.Local
Install | 10 | 0 % | com.vmware.vim.eam | 7 ms | 11/4/2019 6:11:16 PM | | VCSA.Test.Local
Scan | 10 | Completed | com.vmware.vim.eam | 4 ms | 11/4/2019 6:11:01 PM | 11/4/2019 6:11:15 PM | VCSA.Test.Local
Scan | 11 | Completed | com.vmware.vim.eam | 4 ms | 11/4/2019 6:11:01 PM | 11/4/2019 6:11:17 PM | VCSA.Test.Local
Install agent | 11 | 0 % | com.vmware.vim.eam | 9 ms | 11/4/2019 6:10:50 PM | | VCSA.Test.Local
Install agent | 10 | 0 % | com.vmware.vim.eam | 13 ms | 11/4/2019 6:10:50 PM | | VCSA.Test.Local
Scan | 11 | Completed | com.vmware.vim.eam | 5 ms | 11/4/2019 6:10:08 PM | 11/4/2019 6:10:24 PM | VCSA.Test.Local
Scan | 10 | Completed | com.vmware.vim.eam | 8 ms | 11/4/2019 6:10:08 PM | 11/4/2019 6:10:22 PM | VCSA.Test.Local

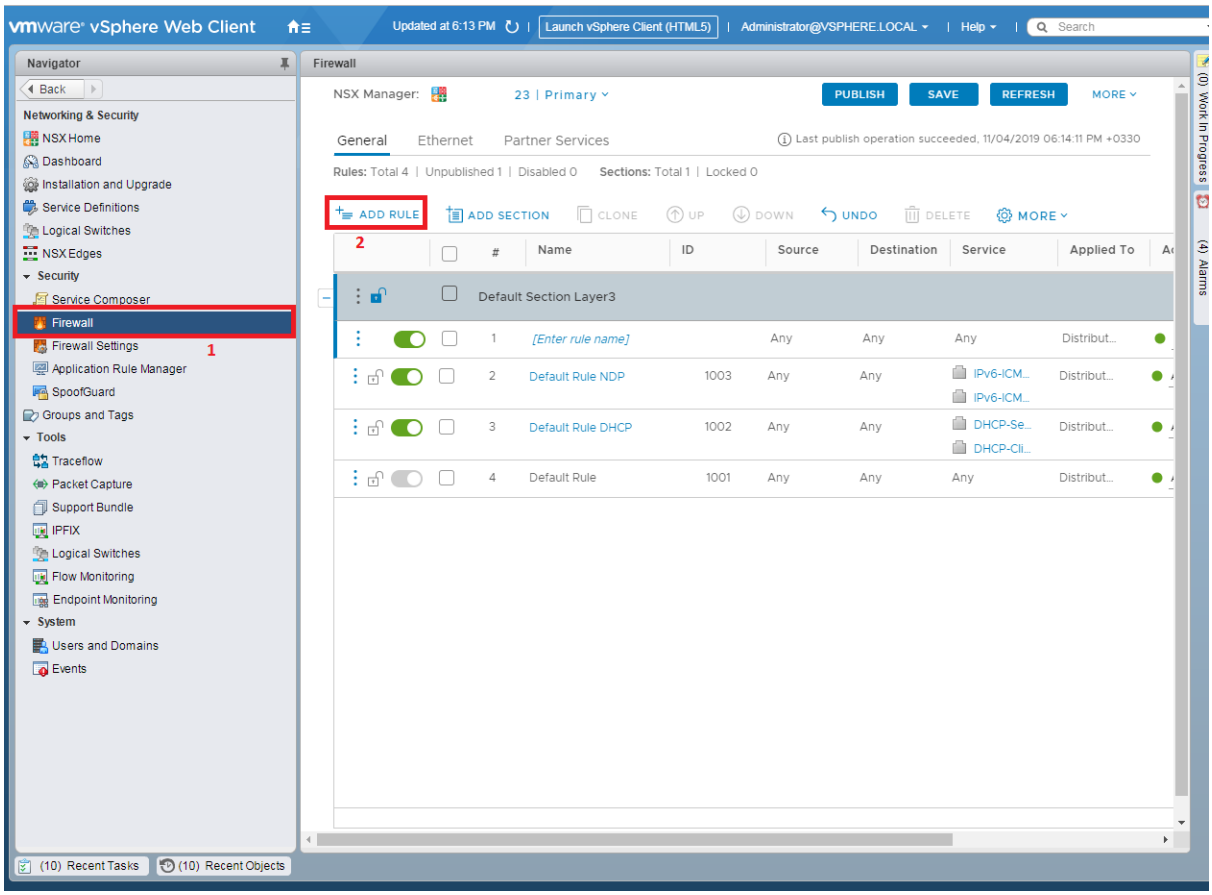

vmware vSphere Web Client
Updated at 6:13 PM
Launch vSphere Client (HTML5)
Administrator@VSPHERE.LOCAL
Help
Search
Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation and Upgrade
Service Definitions
Logical Switches
NSX Edges
Security
Service Composer
Firewall
Firewall Settings
Application Rule Manager
SpoofGuard
Groups and Tags
Tools
Traceflow
Packet Capture
Support Bundle
IPFIX
Logical Switches
Flow Monitoring
Endpoint Monitoring
System
Users and Domains
Events
Installation and Upgrade
Management
Host Preparation
Logical Network Settings
Service Deployment
Upgrade
NSX Manager:
.23 | Primary
EAM Status: Up
Clusters: All
Search
Test
Firewall
VXLAN
Test-2
Not Installed
Test
ACTIONS
NSX Version 6.4.4.11197766
Firewall Enabled
VXLAN Not Configured CONFIGURE
Detection Type View Details
Communication Channel ... UP
Hosts
ALL (2)
Search
Name / IP | NSX Installation | Firewall | Communication Channels | vmkNIC
11 | 6.4.4.11197766 | Enabled | UP | Not Applica
10 | 6.4.4.11197766 | Enabled | UP | Not Applica
1 - 2 of 2


Configure VXLAN Networking
Switch *
DVS-Test
VLAN *
110
MTU *
1600
vmkNIC IP Addressing *
DHCP
IP Pool
IP-VTEP-Pool
NEW IP POOL
vmkNIC Teaming Policy *
Load Balance - SRCMAC
VTEP *
Fail Over
Static EtherChannel
Enhanced LACP
Load Balance - SRCID
Load Balance - SRCMAC
CANCEL
SAVE

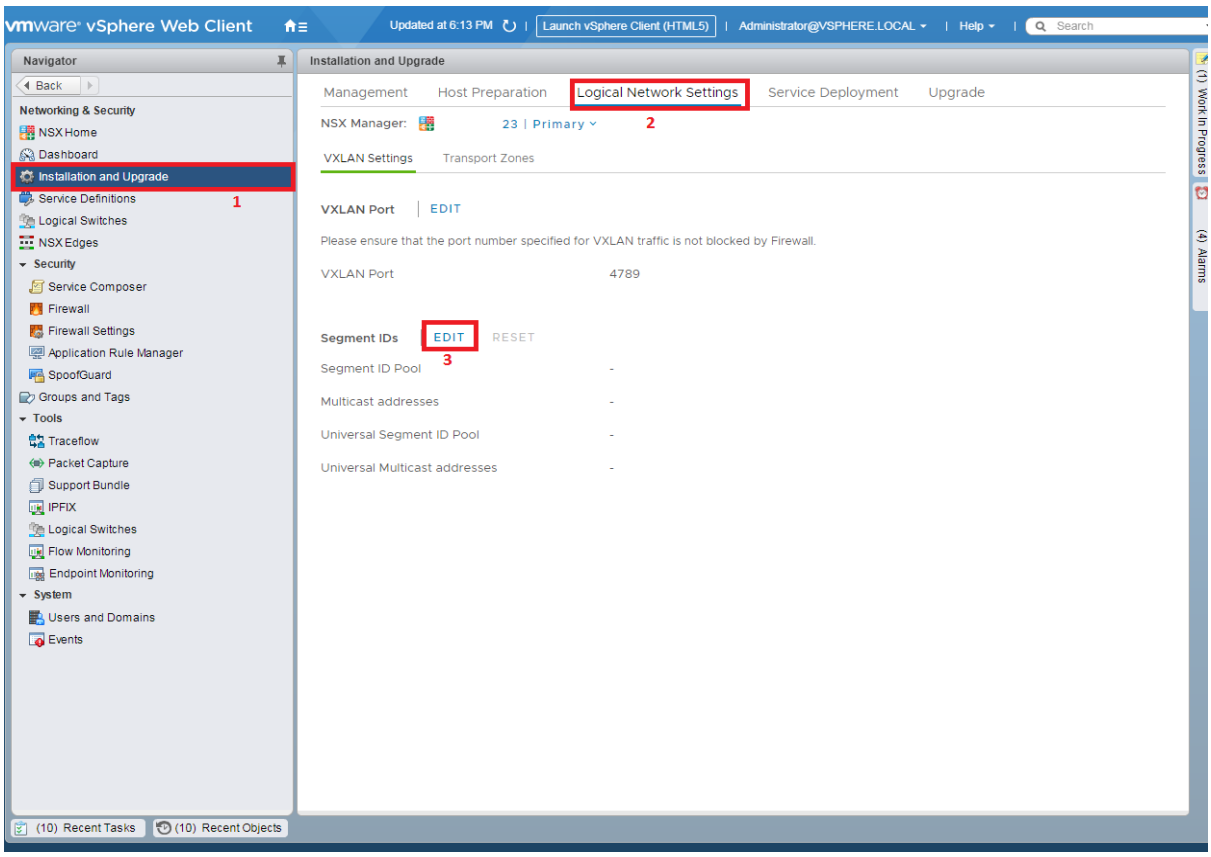
خلاصه‌ای از تنظیمات به شرح زیر است.

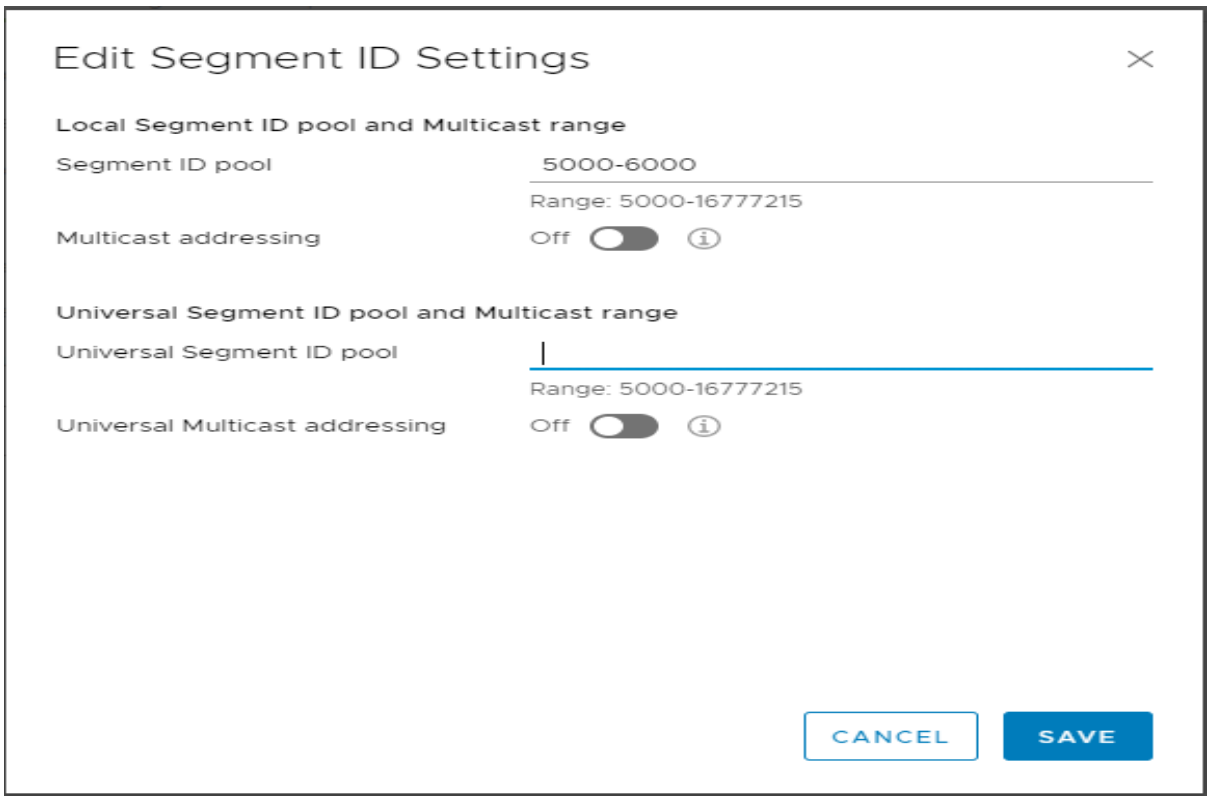


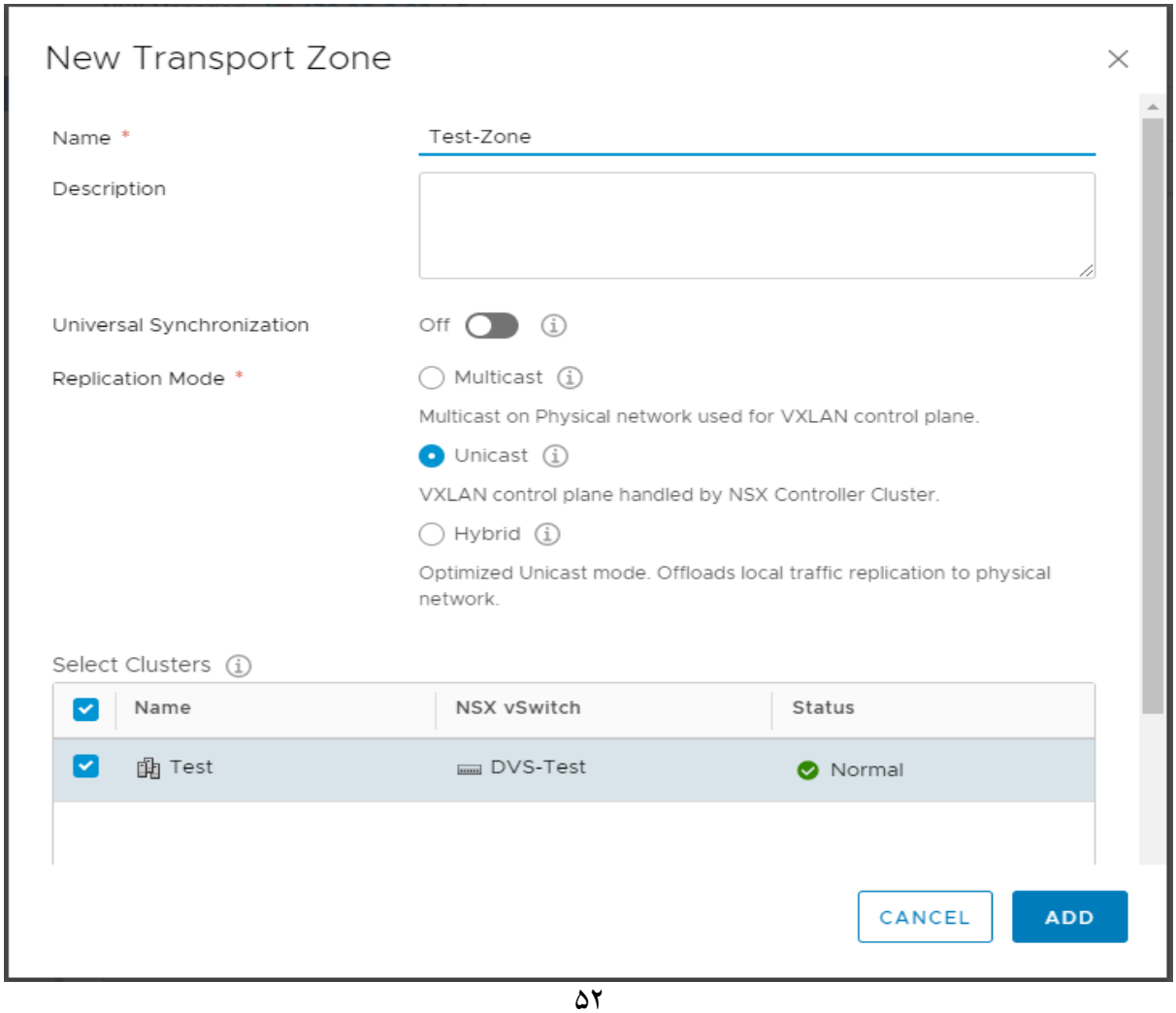
VMware NSX Distributed Firewall Rule ٩-٣-

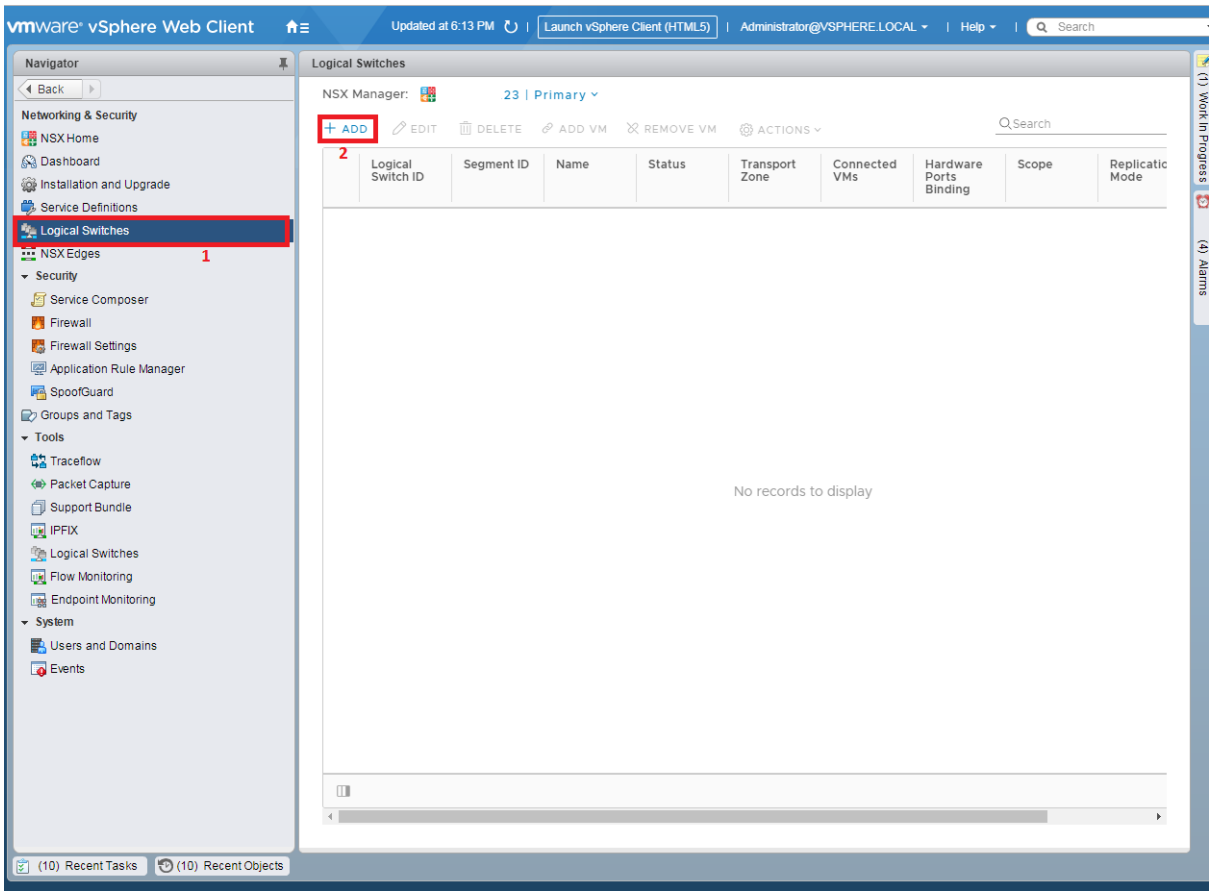


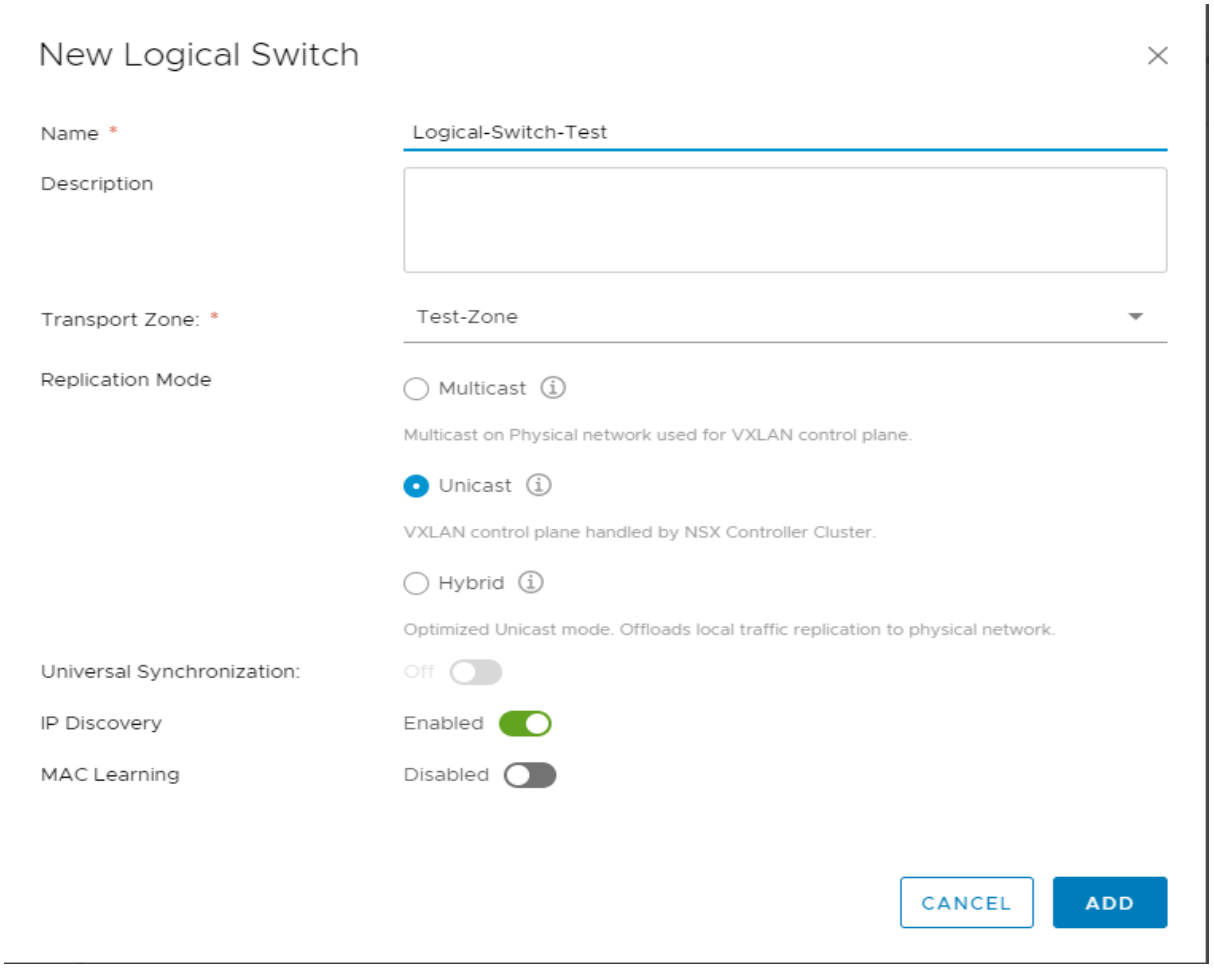
VMware NSX Logical Switch ٩-٤-

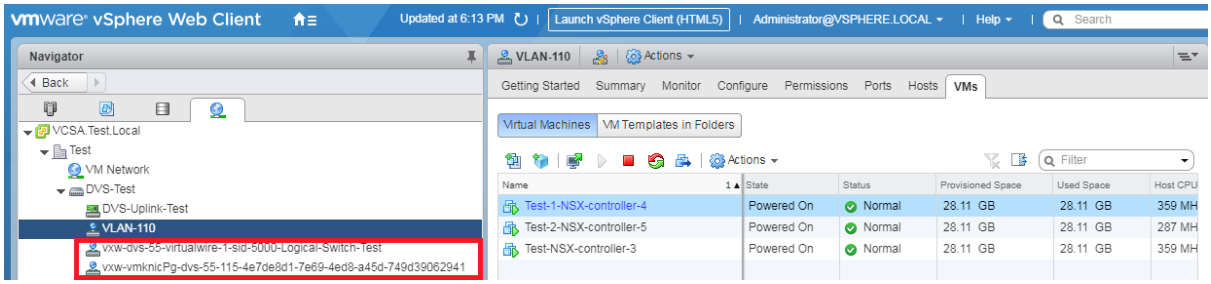



Edit Segment ID Settings
Local Segment ID pool and Multicast range
Segment ID pool
5000-6000
Range: 5000-16777215
Multicast addressing
Off
Universal Segment ID pool and Multicast range
Universal Segment ID pool
Range: 5000-16777215
Universal Multicast addressing
Off
CANCEL
SAVE

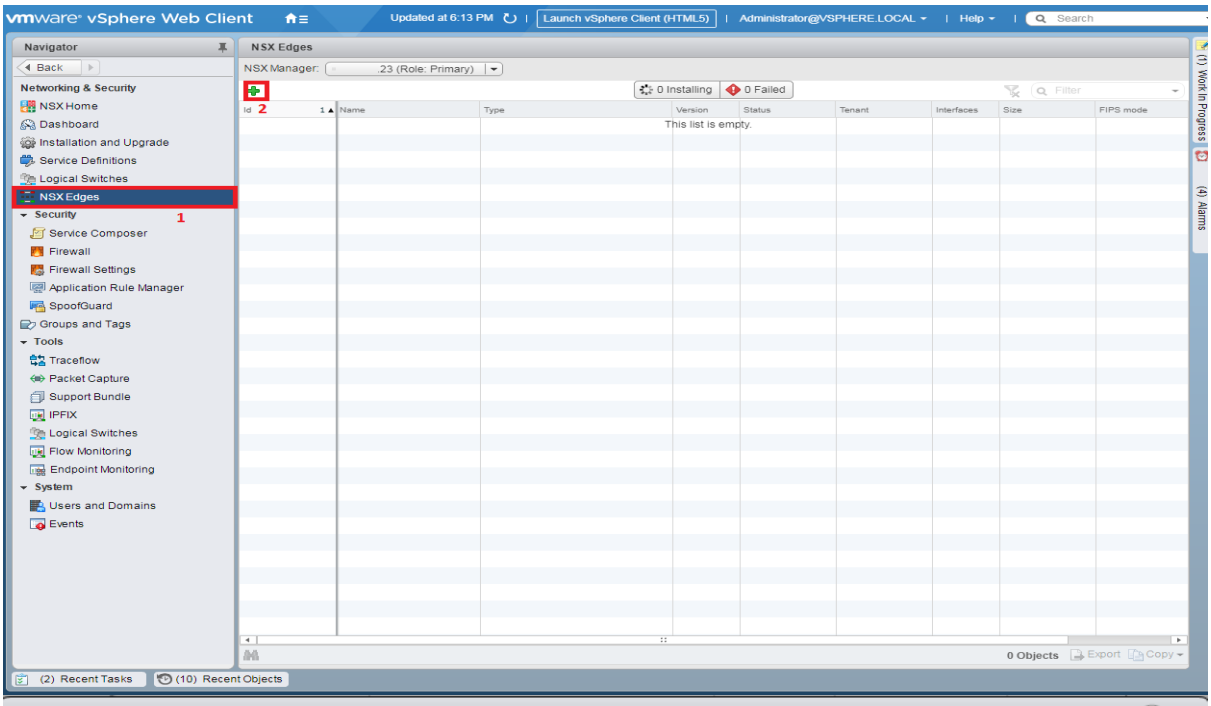

New Transport Zone
Name *
Test-Zone
Description
Universal Synchronization
Off
Replication Mode *
Multicast
Multicast on Physical network used for VXLAN control plane.
Unicast
VXLAN control plane handled by NSX Controller Cluster.
Hybrid
Optimized Unicast mode. Offloads local traffic replication to physical network.
Select Clusters
Name
NSX vSwitch
Status
Test
DVS-Test
Normal
CANCEL
ADD

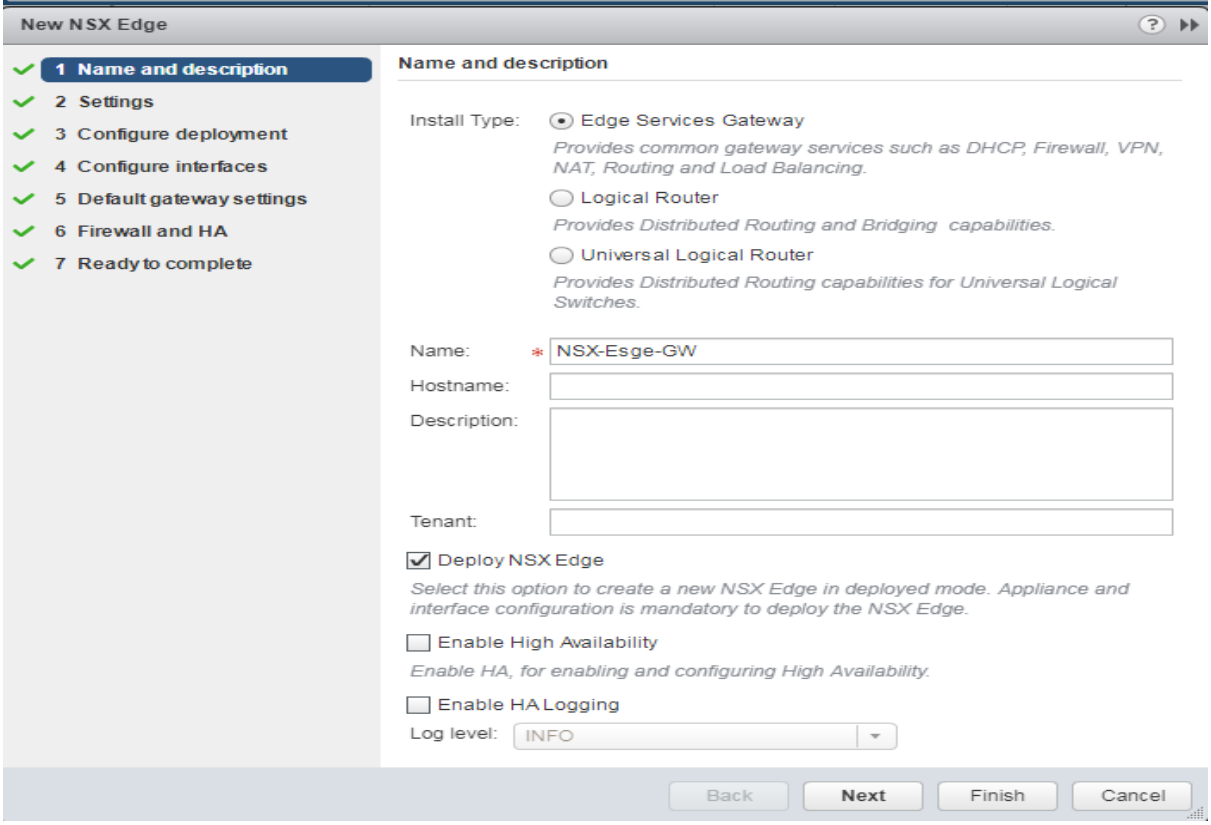

vmware vSphere Web Client
Updated at 6:13 PM
Launch vSphere Client (HTML5)
Administrator@VSPHERE.LOCAL
Help
Search
Navigator
Back
Networking & Security
NSX Home
Dashboard
Installation and Upgrade
Service Definitions
Logical Switches
NSX Edges
1
Security
Service Composer
Firewall
Firewall Settings
Application Rule Manager
SpoofGuard
Groups and Tags
Tools
Traceflow
Packet Capture
Support Bundle
IPFIX
Logical Switches
Flow Monitoring
Endpoint Monitoring
System
Users and Domains
Events
Logical Switches
NSX Manager:
23 | Primary
+ ADD
2
EDIT
DELETE
ADD VM
REMOVE VM
ACTIONS
Search
Logical Switch ID
Segment ID
Name
Status
Transport Zone
Connected VMs
Hardware Ports Binding
Scope
Replicatic Mode
No records to display
(10) Recent Tasks
(10) Recent Objects
(1) Work in Progress
(4) Alarms

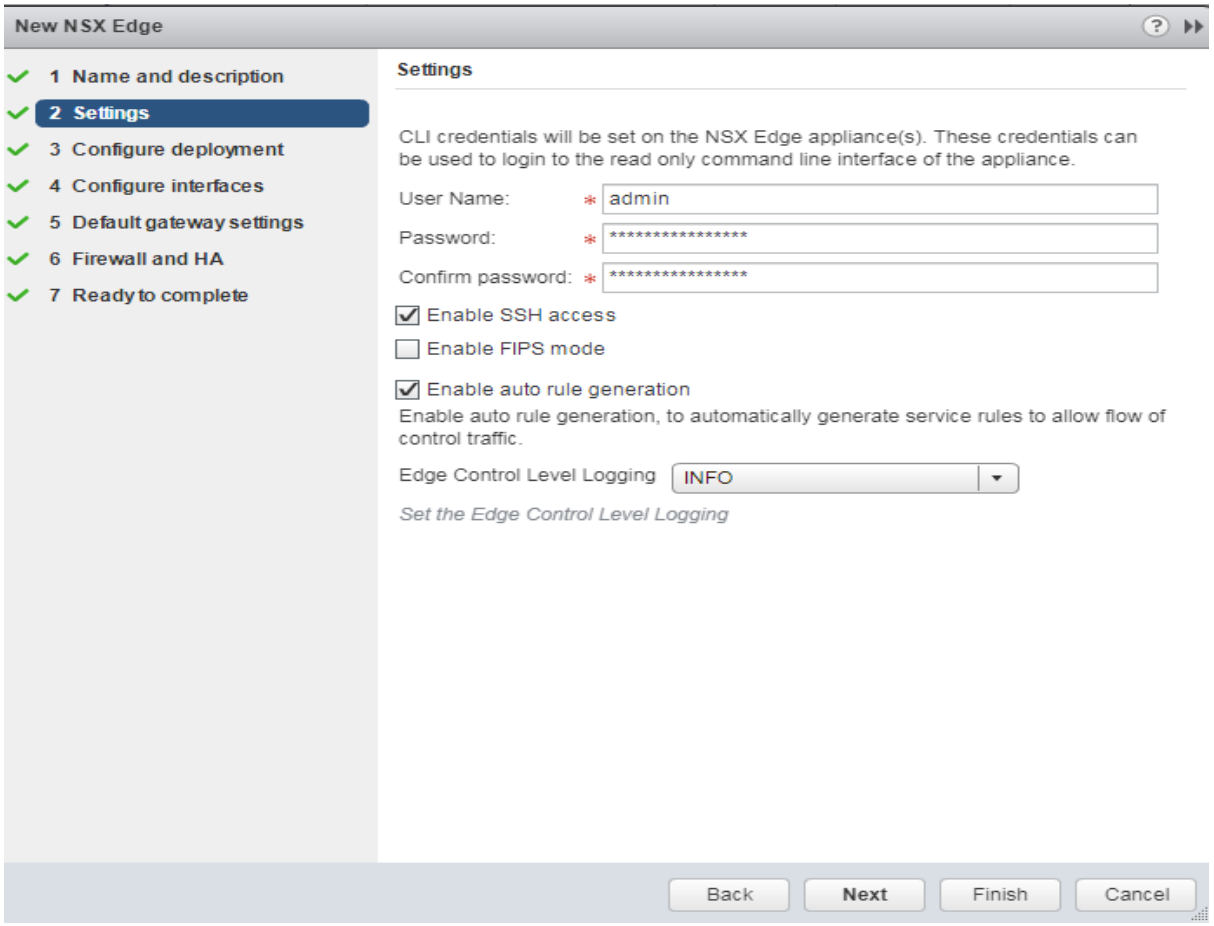

New Logical Switch
Name *
Logical-Switch-Test
Description
Transport Zone: *
Test-Zone
Replication Mode
Multicast
Multicast on Physical network used for VXLAN control plane.
Unicast
VXLAN control plane handled by NSX Controller Cluster.
Hybrid
Optimized Unicast mode. Offloads local traffic replication to physical network.
Universal Synchronization:
Off
IP Discovery
Enabled
MAC Learning
Disabled
CANCEL
ADD

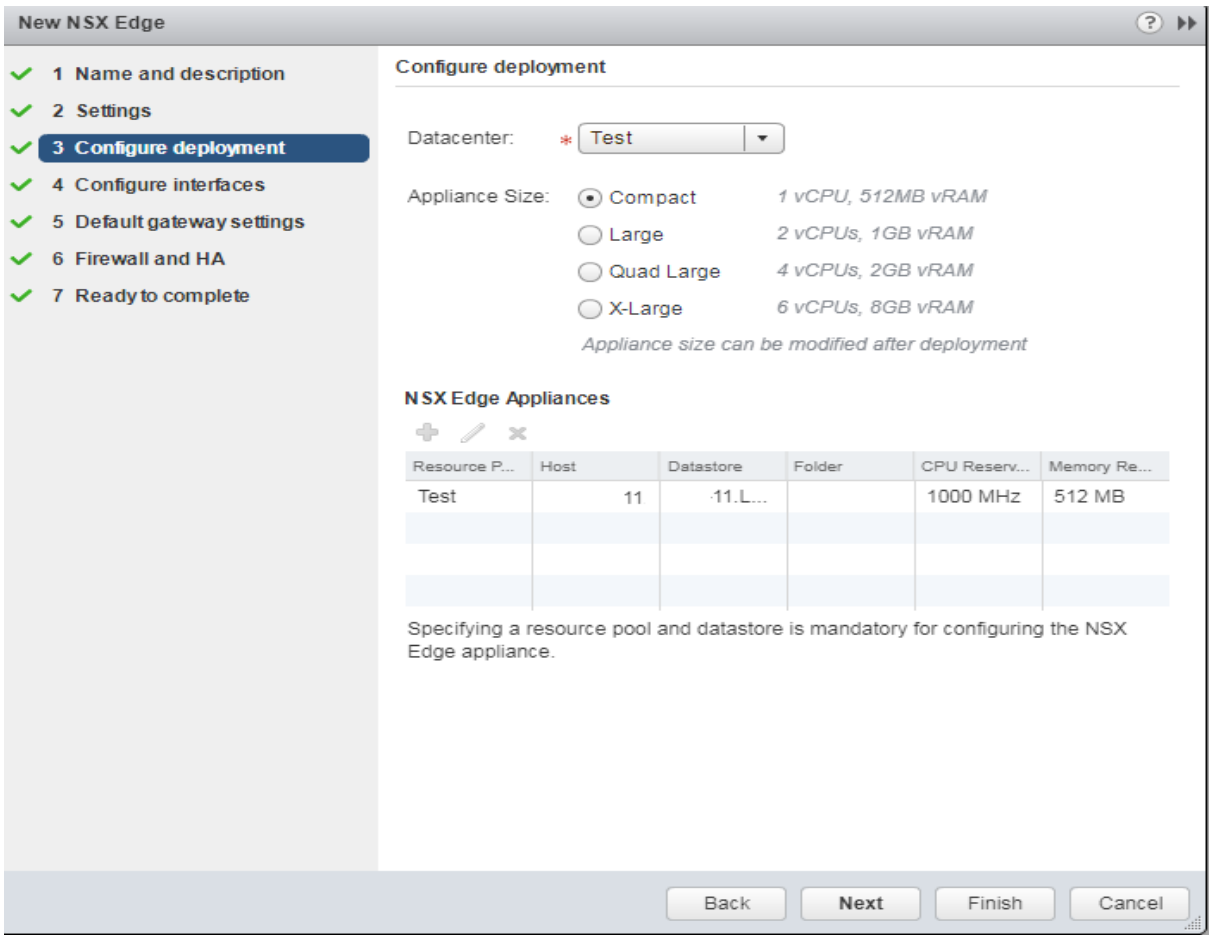


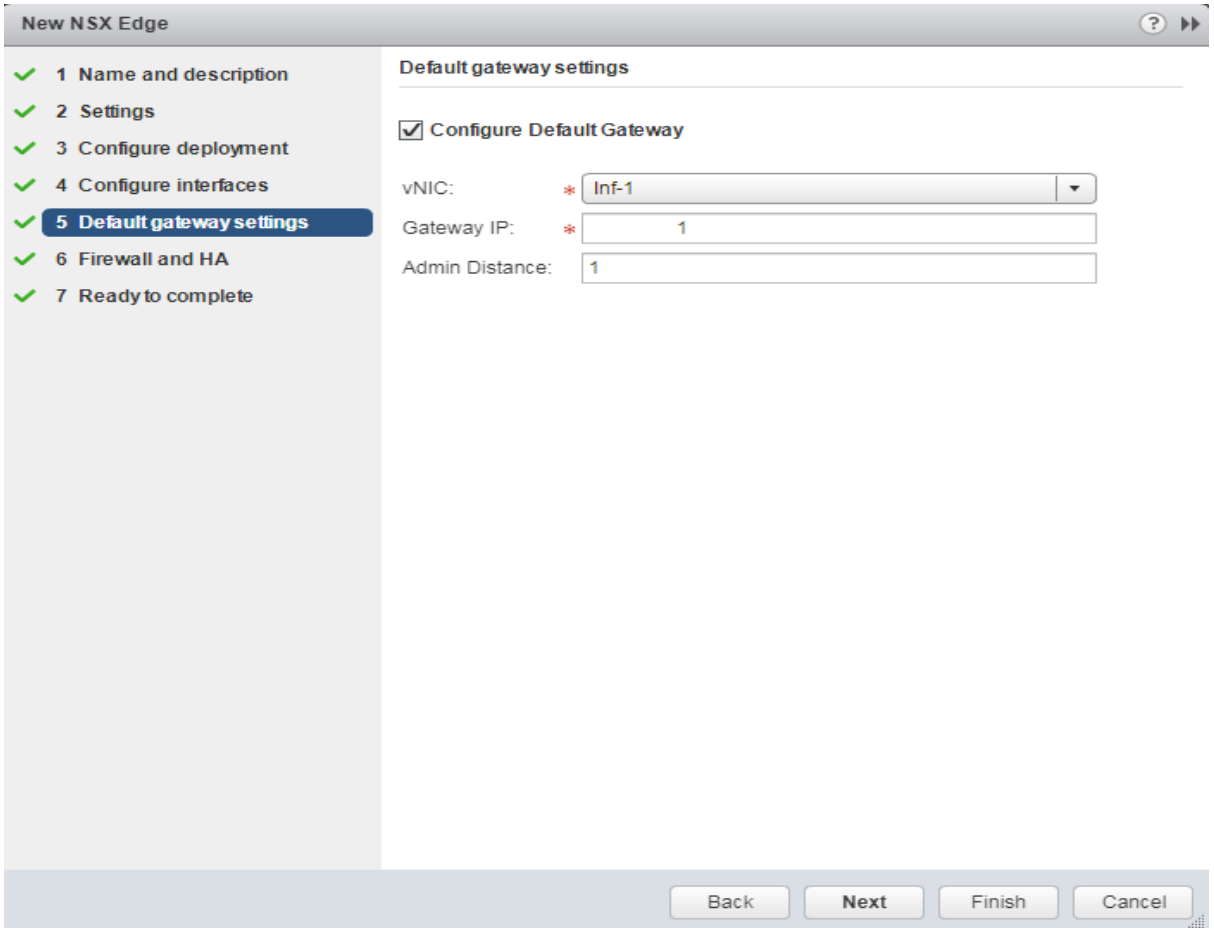
VMware NSX Edge ۹-۵-

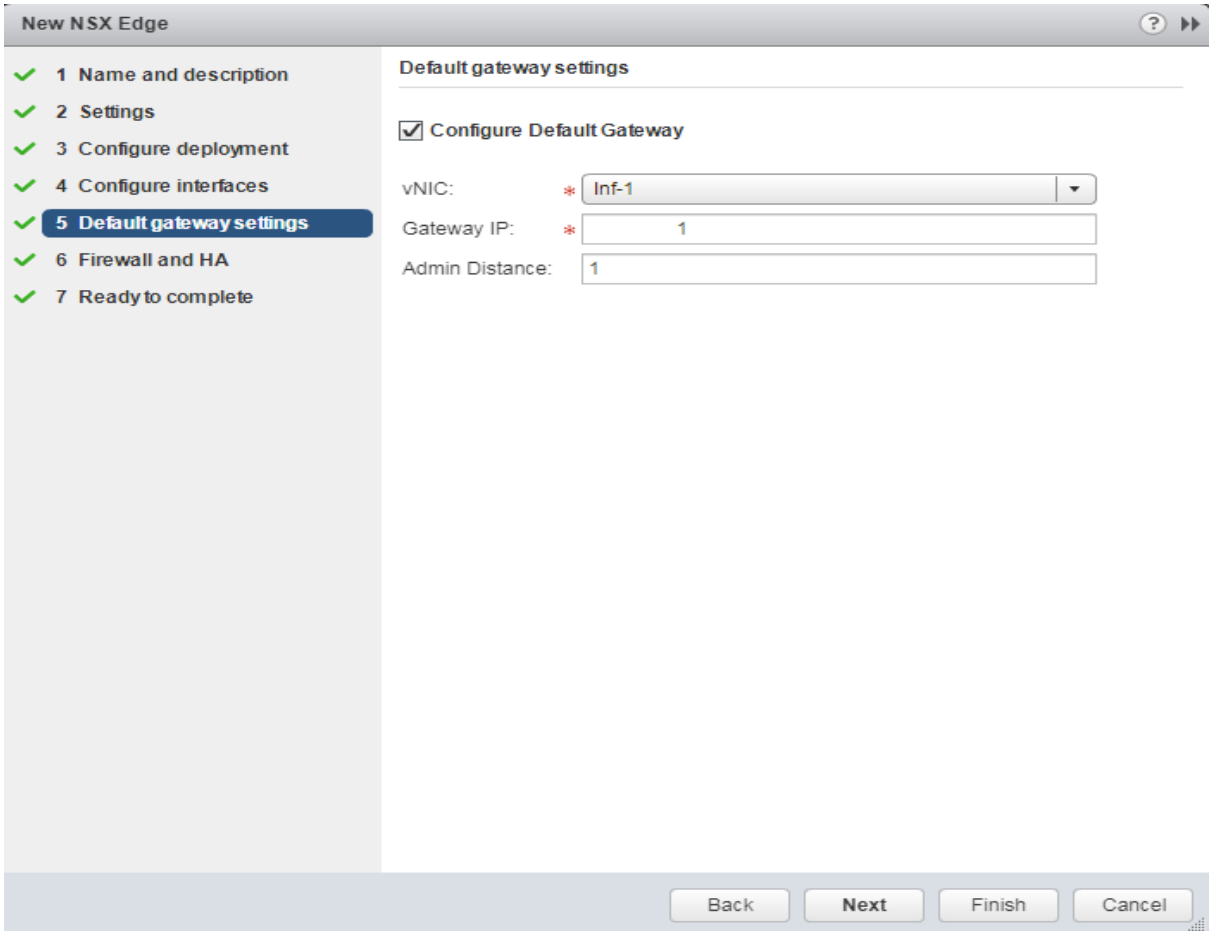


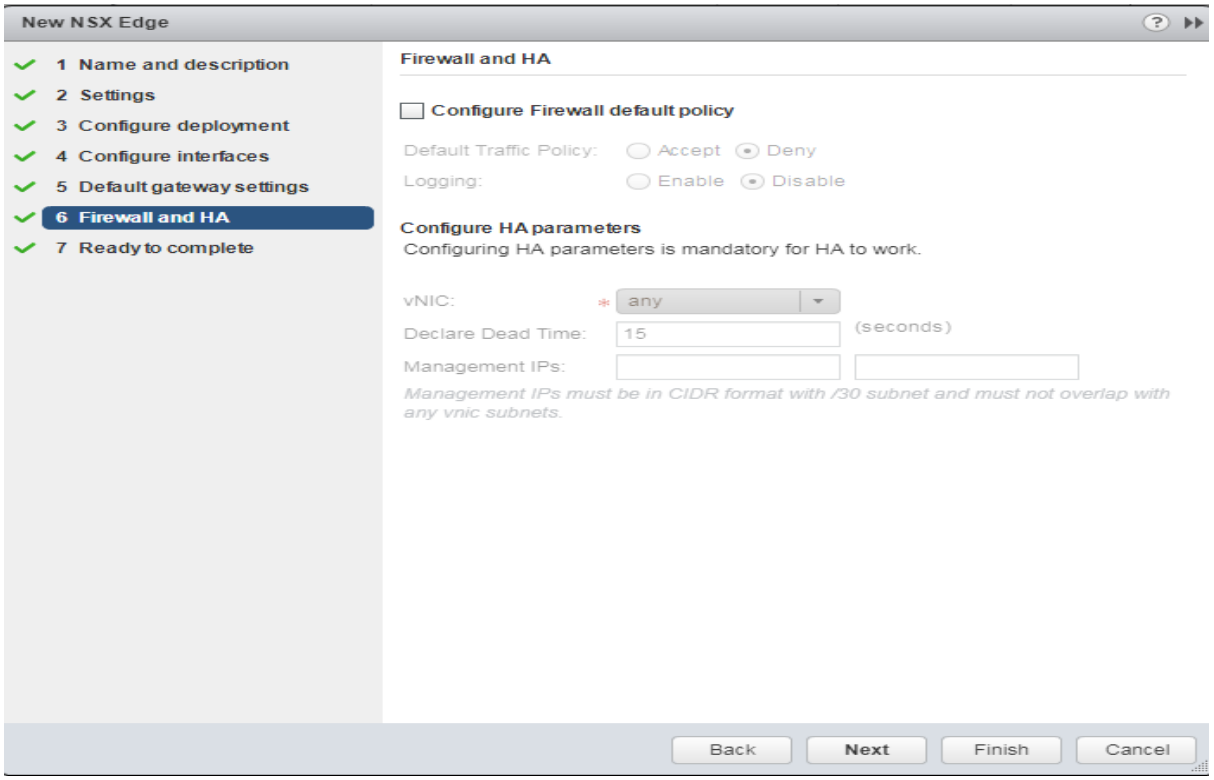


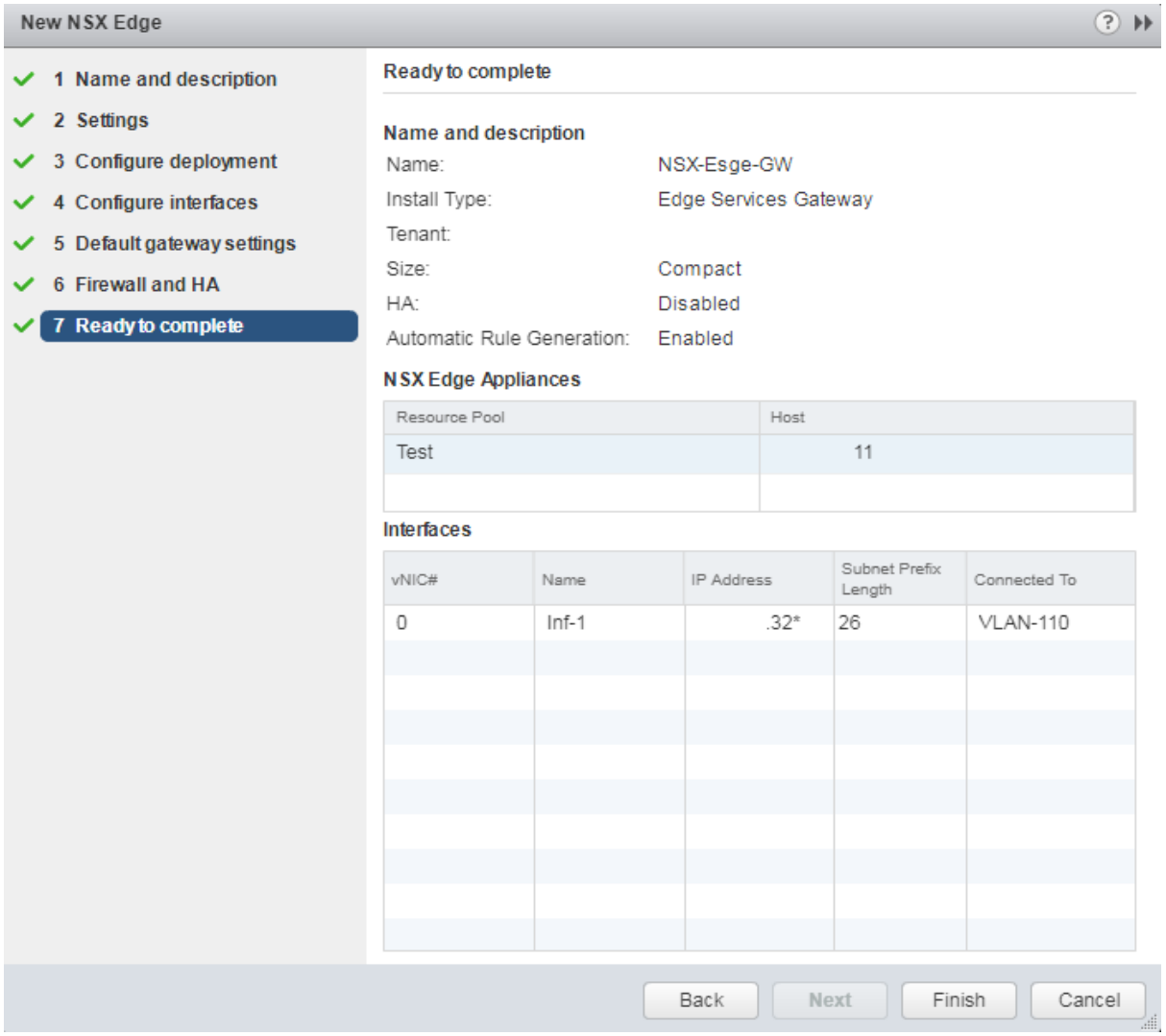

New NSX Edge
1 Name and description
2 Settings
3 Configure deployment
4 Configure interfaces
5 Default gateway settings
6 Firewall and HA
7 Ready to complete
Settings
CLI credentials will be set on the NSX Edge appliance(s). These credentials can be used to login to the read only command line interface of the appliance.
User Name: * admin
Password: * **********
Confirm password: * **********
Enable SSH access
Enable FIPS mode
Enable auto rule generation
Enable auto rule generation, to automatically generate service rules to allow flow of control traffic.
Edge Control Level Logging INFO
Set the Edge Control Level Logging
Back
Next
Finish
Cancel

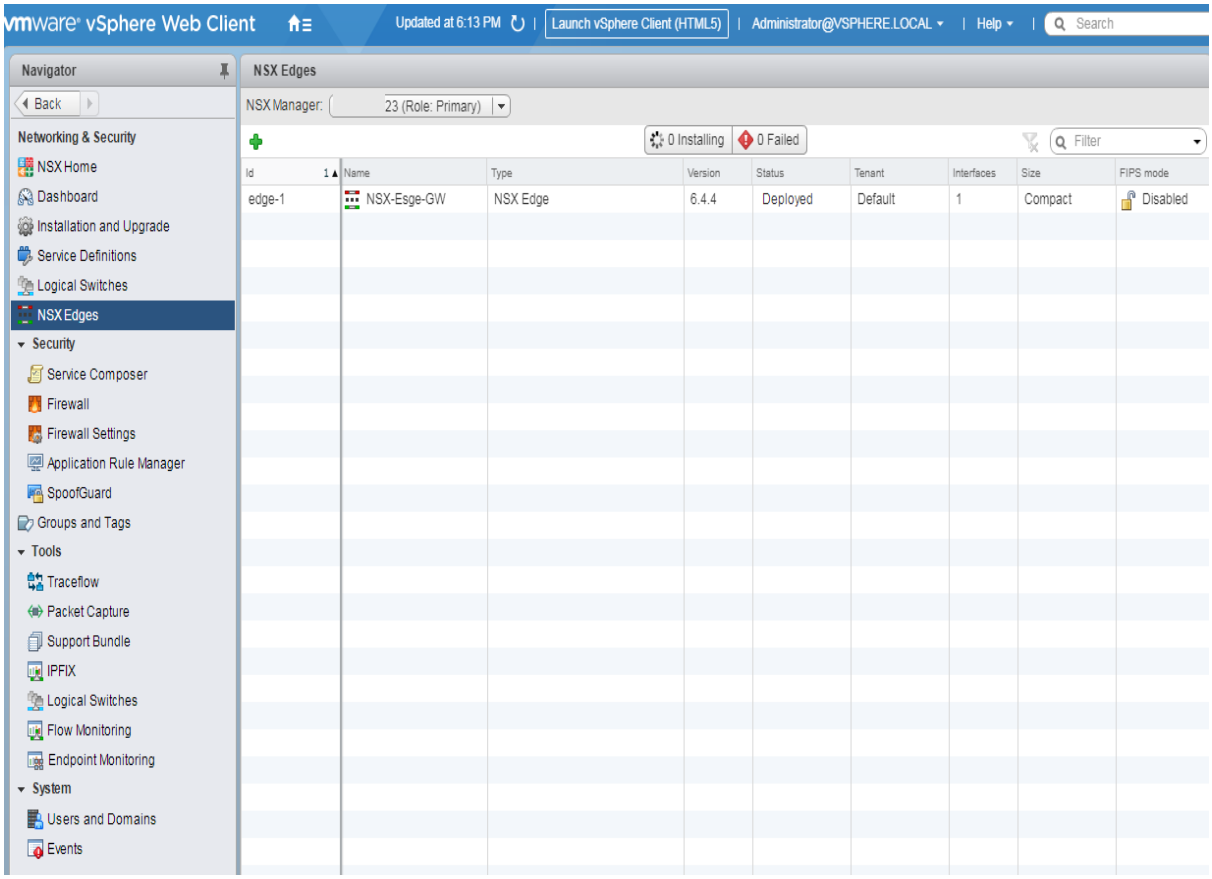

New NSX Edge
1 Name and description
2 Settings
3 Configure deployment
4 Configure interfaces
5 Default gateway settings
6 Firewall and HA
7 Ready to complete
Configure deployment
Datacenter: * Test
Appliance Size:
Compact 1 vCPU, 512MB vRAM
Large 2 vCPUs, 1GB vRAM
Quad Large 4 vCPUs, 2GB vRAM
X-Large 6 vCPUs, 8GB vRAM
Appliance size can be modified after deployment
NSX Edge Appliances
Resource P... Host Datastore Folder CPU Reserv... Memory Re...
Test 11 11.L... 1000 MHz 512 MB
Specifying a resource pool and datastore is mandatory for configuring the NSX Edge appliance.
Back
Next
Finish
Cancel


New NSX Edge
1 Name and description
2 Settings
3 Configure deployment
4 Configure interfaces
5 Default gateway settings
6 Firewall and HA
7 Ready to complete
Default gateway settings
Configure Default Gateway
vNIC:
Inf-1
Gateway IP:
1
Admin Distance:
1
Back
Next
Finish
Cancel


New NSX Edge
1 Name and description
2 Settings
3 Configure deployment
4 Configure interfaces
5 Default gateway settings
6 Firewall and HA
7 Ready to complete
Default gateway settings
Configure Default Gateway
vNIC:
Inf-1
Gateway IP:
1
Admin Distance:
1
Back
Next
Finish
Cancel


New NSX Edge
1 Name and description
2 Settings
3 Configure deployment
4 Configure interfaces
5 Default gateway settings
6 Firewall and HA
7 Ready to complete
Firewall and HA
Configure Firewall default policy
Default Traffic Policy: Accept Deny
Logging: Enable Disable
Configure HA parameters
Configuring HA parameters is mandatory for HA to work.
vNIC: * any
Declare Dead Time: 15 (seconds)
Management IPs:
Management IPs must be in CIDR format with /30 subnet and must not overlap with any vnic subnets.
Back
Next
Finish
Cancel


New NSX Edge
1 Name and description
2 Settings
3 Configure deployment
4 Configure interfaces
5 Default gateway settings
6 Firewall and HA
7 Ready to complete
Ready to complete
Name and description
Name: NSX-Esge-GW
Install Type: Edge Services Gateway
Tenant:
Size: Compact
HA: Disabled
Automatic Rule Generation: Enabled
NSX Edge Appliances
Resource Pool
Host
Test
11
Interfaces
vNIC#
Name
IP Address
Subnet Prefix Length
Connected To
0
Inf-1
.32*
26
VLAN-110
Back
Next
Finish
Cancel



۱۰- VMware NSX-T Overview

همانطور که گفته شد پس از خرید شرکت NICIRA توسط شرکت VMware به قیمت۱.۲۶ میلیارد دلار در 23 July 2012، VMware با مشارکت شرکت NICIRA شروع به کار کرد که در نتیجه محصولی به نام NVP به بازار ارائه گردید. این محصول در جهت محیط‌های غیر از VMware وارد بازار گردید. محصول NSX VMware در August 2013 بر پایه NPV برای محیط VMware ارائه شد. نرم‌افزار NSX-MH یا NSX-T بر پایه همان NVP است و قابل استفاده در محیط‌های غیر vSphere و یا Hypervisorهای مختلف است. در این قسمت سعی شده است که توضیح مختصری در رابطه با NSX-T ارائه شود. نرم‌افزار NSX-V فقط برروی محیط vSphere قابل پیاده‌سازی است و این در صورتی است که نرم‌افزار NSX-T برای محیط‌های غیر vSphere مانند KVM، RedHat، OpenStack و ... است. همانطور که گفته شد نرم‌افزار NSX-V قابلیت‌های بسیاری دارد که با به‌روزرسانی محیط vSphere نرم‌افزار NSX-V نیز به‌روزرسانی می‌شود ولی در NSX-T قابلیت‌های آن وابسته به استانداردها و پیاده‌سازی‌های پروژه‌های متن‌باز یا Open Source است. در صورتیکه محیط کاملاً مبتنی بر vSphere است باید از NSX-V استفاده شود و در صورت استفاده از Hypervisorهای دیگر می‌توان برای SDN از نرم‌افزار NSX-T استفاده نمود. در نرم‌افزار NSX-T مؤلفه‌هایی مشابه NSX-V وجود دارد. که در ادامه به توضیح مختصری از آن پرداخته می‌شود. موارد گفته شده بر اساس NSX-T 2.5 است.

۵. NSX-T Manager: دارای یک رابط کاربری مدیریتی و یک API برای محیط است و تفاوت‌های بسیاری با NSX-V دارد. با vCenter هماهنگ نمی‌شود و می‌توان تنظیمات را بصورت دستی و از طریق APIهای تعریف شده تنظیم و اجرا نمود. این مؤلفه بصورت Bare Metal یا VM برروی ESXi و KVM قابل نصب است.

Appliance Size	Memory	vCPU	Disk Space	VM Hardware Version
NSX Manager Extra Small	8 GB	2	200 GB	10 or later
NSX Manager Small VM	16 GB	4	200 GB	10 or later
NSX Manager Medium VM	24 GB	6	200 GB	10 or later
NSX Manager Large VM	48 GB	12	200 GB	10 or later

Hypervisor	Version	CPU Cores	Memory
vSphere	-	4	16 GB
CentOS Linux KVM	7.5, 7.4	4	16 GB
Red Hat Enterprise Linux (RHEL) KVM	7.6, 7.5, and 7.4	4	16 GB
SUSE Linux Enterprise Server KVM	12 SP3	4	16 GB
Ubuntu KVM	18.04.2 LTS	4	16 GB

Browser	Ubuntu 18.04	Mac OS X 10.13, 10.14	Windows 10
Google Chrome 76	Yes	Yes	Yes
Mozilla Firefox 68	Yes	Yes	Yes
Microsoft Edge 44			Yes
Apple Safari 12		Yes	

Appliance Size	Memory	vCPU	Disk Space	VM Hardware Version
NSX Edge Small	4 GB	2	200 GB	11 or later (vSphere 6.0 or later)
NSX Edge Medium	8 GB	4	200 GB	11 or later (vSphere 6.0 or later)
NSX Edge Large	32 GB	8	200 GB	11 or later (vSphere 6.0 or later)

NSX-T Controller: این مؤلفه نیز بسیار شبیه به NSX-V است و همان عملکرد را دارد.

NSX-T vSwitch: نرم‌افزار NSX-T با استفاده از Open vSwitch (OVS) که پروژه متن‌باز است یک Virtual Distributed Switch را فراهم می‌کند. OVS می‌تواند برروی سیستم‌عامل‌ها و Hypervisorهای مختلف نصب و اجرا شود.

Communication: در رابطه با برقراری ارتباط بین NSX-T Controller و OVS باید به دو مورد توجه داشت. یکی اینکه تنظیمات برروی پایگاه داده‌ای به نام OVSDB ذخیره می‌شود و دو اینکه تنظیمات از طریق پروتکلی به نام OpenFlow از بخش Control Plane به بخش Data Plane ارسال می‌شود که این تنظیمات

شامل تنظیمات Switch، Router و ... است. در واقع OVS با استفاده از OpenFlow و Open vSwitch Database Management Protocol (OVSDB) تنظیمات را ذخیره و اجرا می‌نماید.

Service Nodes: این مؤلفه برای ارسال ترافیک‌های Unicast، Multicast و Broadcast است استفاده می‌شود.