

## به نام خدا

اسماعیل زارع

### مجازی سازی دسکتاپ (VDI) چیست؟

عبارت **VDI مخفف Virtual Desktop Infrastructure** به معنای زیرساخت دسکتاپ مجازی یا به بیان ساده تر، به اجرای نرم افزارهای دسکتاپ های کاربران بصورت مجازی بر روی پلتفرم های مجازی گفته می شود

مجازی سازی دسکتاپ (VDI) روشی جدید برای مدیریت محیط کاربران ارائه می دهد. VDI این امکان را برای مدیران شبکه فراهم می آورد تا کامپیوتر کاربران را در زیرساختی مجازی، واقع در مرکز داده میزبانی و مدیریت کنند.

این روش، سیستم عامل کامپیوترهای شخصی را از ماشین فیزیکی جدا می کند و ماشین مجازی حاصل را، به جای اینکه روی هارد دیسک کامپیوتر کاربر ذخیره کند، روی یک سرور مرکزی ذخیره می کند بنابراین وقتی کاربران در حال کار با ماشین خودشان هستند، همه برنامه ها و عملیات پردازشی و داده های استفاده شده توسط آنان روی سرور مرکزی اجرا و نگهداری می شود. کاربران با استفاده از پروتکل های PCoverIP به کامپیوتر خود دسترسی خواهند داشت. VDI با ارائه تمام قابلیت های موجود در یک کامپیوتر، مزایای جدید و قابل قبولی ارائه می دهد که با آن می توان قابلیت مدیریت کردن، کارایی و امنیت کامپیوترهای شخصی کاربران را افزایش داد. VDI بیش از اینکه یک محصول باشد، یک فن آوری است.

اصل و اساس این نرم افزار در جهت ارائه خدمات مجازی سازی دسکتاپ (Desktop Virtualization) بنا نهاده شده است. به واسطه پیاده سازی این نرم افزار در سازمان عملاً وابستگی مجموعه به سخت افزار قطع می شود. به واسطه استفاده از نرم افزار VMware View 6.0 شما دیگر دغدغه نگهداری سخت افزار را نداشته و هزینه های نگهداری آن به شدت کاهش خواهد یافت. همچنین به واسطه پیاده سازی VDI در سازمان می توانید به راحتی در هر زمانی به سیستم عامل های جدید مثل Windows 7 یا Windows 8 مهاجرت نمایید. این روند با کاربران امکان دسترسی به کامپیوترهایشان با هر وسیله ای از قبیل کامپیوترهای شخصی، نوت بوک، Smart Phone یا Thin Client را می دهد. کاربران نیز رضایت بیشتری دارند، زیرا به برنامه ها و تنظیماتی که برای کارشان نیاز دارند، دسترسی آسان تری دارند. ایده این کار بسیار ساده است به جای اینکه روی کامپیوتر کاربران به صورت محلی، نسخه ای از سیستم عامل ویندوز اجرا شود، شما در مرکز داده خود، نسخه ویندوز را نصب می کنید. سپس کاربران شما به صورت Remote به کامپیوتر خود واقع در سرور وصل می شوند و سیستم عامل ویندوز ماشین خود (Windows XP)، Vista، 7 و یا هر سیستم عامل دیگر را اجرا می کنند. با استفاده از این تکنولوژی کاربران می توانند از هر کلاینتی برای دسترسی به کامپیوتر خود استفاده کنند.

### چرا از مجازی سازی دسکتاپ استفاده کنیم؟

قبل از مجازی سازی دسکتاپ کاربران برای استفاده از کامپیوتر شخصی خود می بایست از یکی از دو روش زیر استفاده می کردند:

1. روش قدیمی که روی کامپیوتر یا لپ تاپ هر کاربر یک نسخه محلی از ویندوز اجرا می شد (Local Desktop).

2. روش مبتنی بر سرور، که هر کاربر به صورت Remote به یک سرور مایکروسافت و یا Citrix متصل می گردید (SBC Desktop).

VDI گزینه سوم می دهد. بوسیله VDI عمل پردازش را از سمت کاربران گرفته و بر روی یک سرور می آورد. در VDI برخلاف روش استفاده از تکنولوژی ترمینال سرویس، کامپیوتر مجازی به یک کاربر اختصاص داده شده و محدودیت های پیشین حذف شده است.

در این قسمت سعی بر آن داریم که یکی از پرکاربردترین نرم افزارهای شرکت VMware را تحت عنوان VMware View معرفی نماییم اصل و اساس این نرم افزار در جهت ارائه خدمات مجازی سازی دسکتاپ (Desktop Virtualization) بنا نهاده شده است. به واسطه پیاده سازی این نرم افزار در سازمان عملاً وابستگی مجموعه به سخت افزار قطع می شود. به واسطه استفاده از نرم افزار VMware View شما دیگر دغدغه نگهداری سخت افزار را نداشته و هزینه های نگهداری آن به شدت کاهش خواهد یافت. همچنین به واسطه پیاده سازی VDI در سازمان می توانید به راحتی در هر زمانی به سیستم عامل های جدید مثل Windows 7 یا Windows 8 مهاجرت نمایید...

VMware View با در اختیار گذاشتن میزکار (Desktop) از طریق فضای ابری (Cloud) کاربران نهایی آزادی عمل و به مدیران توانایی کنترل را می دهد. ساده سازی و خودکار سازی مدیریت هزاران میزکار (Desktop) را برای واحد IT امکان پذیر می سازد. همچنین این نرم افزار به واحد IT اجازه می دهد، تا با کامپیوترهای قدیمی به میزکار (Desktop)، با سطوح دسترسی و با قابلیت اطمینان منحصر به فرد، به طور امن دست یابند. با امن کردن مسیر دسترسی هر دستگاه به نرم افزارها و داده ها، نرم افزار VMware View در هر زمان و مکانی، دسترسی به اطلاعات را با سطح بالایی از جابجایی و انعطاف پذیری در اختیار کاربر نهایی قرار می دهد.

## چيست؟ VMware NSX

شرکت VMware راه کاری جدید را در مجازی سازی ارایه نموده است که انقلاب بزرگی در شبکه میباشد، آن هم مجازی کردن بستر و تجهیزات شبکه از قبیل روتر ها ، سویچ ها و فایروال ها در بستر NSX میباشد که نرم افزاری است مانند SDN ها که شرکت vmware با سرمایه گذاری هنگفت توانست پروژه شرکت Nicira را خریداری نماید و آن را بست و گسترش دهد. در واقع VMware ESXI منابع شبکه را مجازی سازی میکند همانند CPU و RAM و کارت های شبکه، ولی در مقایسه NSX یک هایپروایزور است که بستر شبکه مثل کابل ها ، سویچ ها ، روترها و فایروال ها را مجازی میکند .

این پلتفرم یکی از پلتفرم های پیشرو برای مجازی سازی شبکه به شمار میرود که مدل عملیاتی یک ماشین مجازی را برای شبکه ارائه مینماید. شبکه های مجازی همچون ماشین های مجازی Computing از لحاظ برنامه ای به صورت مستقل از سخت

افزارهای اصلی، آماده سازی و مدیریت می شوند NSX. مدل شبکه را به طور کامل در نرم افزار بازآفرینی نموده و امکان ایجاد و آماده سازی هرگونه توپولوژی را از شبکه های ساده تا شبکه های پیچیده ی Multi-Tier میسر میسازد. این تکنولوژی یک مجموعه از سرویس ها و فاکتورهای منطقی شبکه مانند فایروال ها، LoadBalancer ها، VPN، سوئیچ ها، روترهای منطقی و همچنین امنیت بار کاری یا Workload را فعال می نماید. علاوه بر آن کاربران می توانند شبکه های مجازی جداگانه ای را از طریق ترکیب سفارشی این قابلیت ها ایجاد کنند .

VMware NSX حرکتی از سوی شرکت VMware برای مجازی سازی شبکه های فیزیکی است. در واقع SDN شرکت VMware برای ورود به این عرصه است، حرکتی که شرکت های دیگر هر چند محدود بر روی ساختار VMware vSphere به آن پرداخته اند مانند Cisco v1000 که سوییچ ها را در محیط VMware vSphere مجازی می نمود NSX. محصول شبکه و امنیت شرکت VMware است که در سال 2012 با خریداری شرکت Nicira به سبد محصولات این شرکت افزوده شد. این محصول یکی از پرکاربردترین محصولات مجموعه VMware vSphere است که بر پایه سه مفهوم مهم زیر میباشند :

### **: Network Virtualization**

در این تکنولوژی با استفاده از پروتکل های Overlay Networking بدون تغییر در زیرساخت فعلی شبکه، بستر جدیدی با ایجاد لایه 2 بر روی لایه 3 فراهم می شود. فراهم آورنده NV پروتکل مورد استفاده محصول NSX، یعنی پروتکل VXLAN می باشد .

### **: Network Function Virtualization**

در این تکنولوژی تمرکز بر تفکیک فانکشن های مورد استفاده در تجهیزات است، بدین ترتیب که اگر مثلاً ما نیاز به یک قابلیت به نام IPS یا Intrusion Prevention System داریم، تنها این قابلیت را در زیرساخت به کار گیریم و نیازی به تهیه ی تجهیزات همه منظوره ای مانند فایروال ها یا اپلاینس های دیگر نداشته باشیم. این نوع فانکشن ها معمولاً از طریق یک VM Appliance در محیط مجازی قرار میگیرند و به وسیله هایپروایزر کنترل می شوند که به اختصار NFV نام دارد .

### **:Software Defined Networking**

در تکنولوژی SDN که در آن با تفکیک اجزای تجهیزات ، شبکه را چابک تر میکنند، معماری شبکه به بخشهای مدیریت یا Management plane و بخش کنترل یا Control plane و بخش انتقال داده یا Data plane تقسیم می شود .

با این تفاسیر VMware NSX یک مجموعه کامل از سرویس ها و فاکتورهای منطقی و ساده شده ی شبکه بندی را ارائه مینماید که شامل روترها، فایروال ها، LoadBalancer ها، VPN، QoS، مانیتورینگ، امنیت و سوئیچ های منطقی می باشد. این سرویس ها در شبکه های مجازی و از طریق هر یک از پلتفرم های مدیریت کلود که از NSX API ها استفاده می کنند، آماده سازی شده و در هر نوع توپولوژی به صورت مجزا و Multi-Tenancy ارائه می گردند. همچنین شبکه های مجازی را میتوان بدون قطعی در هر یک از شبکه های موجود و Hypervisor ها به کار گرفت. بطور کلی کاربرانی که قصد تجربه کار با نرم افزار های مجازی سازی و رایانش ابری را در زیرساخت شبکه ای داشته باشند، ساختاری شبیه مجازی سازی سرور ها اما برای شبکه می خواهند و شرکت VMware اعلام نموده که NSX قابلیت انجام این پروسه ها را برای شبکه به همراه دارد .

با توجه به توضیحاتی که ارائه گردید، مجموع قابلیت و ویژگی های NSX را میتوانیم به این گونه تشریح نماییم :

• **سوئیچینگ منطقی** : عملکرد کامل L2 و L3 را در یک فضای مجازی بازآفرینی کرده و از سخت افزارهای اصلی جدا مینماید. محیطی ایده آل برای ایجاد بستری چابک بین دیتاسنترهای مختلف که هم اکنون بستر لایه 3 بین آنها وجود دارد به دور از مشکلاتی از قبیل loop در شبکه

• **NSX Gateway** : از L2 Gateway برای اتصال بدون محدودیت به بارکاری فیزیکی و VLAN های قدیمی استفاده میشود .  
• **مسیریابی منطقی** : مسیریابی بین سوئیچ های منطقی که قابلیت مسیریابی پویا در شبکه های مجازی مختلف را میسر میسازد .

• **فایروال منطقی** : فایروال توزیعی عملکرد Line Rate فعال شده با Kernel، مجازی سازی و اطلاع از هویت Identity Aware با نظارت بر فعالیت ها صورت میگیرد .

• **Load Balancer منطقی** : یک Load Balancer با تمام ویژگی ها به همراه SSL Termination

• **VPN منطقی** : دسترسی Site-to-Site و راه دور VPN در نرم افزار میباشد .

• **NSX API** : قابلیت استفاده از RESTful API جهت ادغام با هر یک از پلتفرم های مدیریت Cloud

• **عدم وابستگی شبکه به سخت افزار** : مجازی سازی شبکه به عنوان یک لایه بالای لایه ی فیزیکی قرار دارد و بر روی یک پلتفرم hypervisor کار می کند. تنها لازمه ی شبکه فیزیکی این است که قابلیت حمل بسته های IP را داشته باشد. به طور کلی هیچ وابستگی سخت افزاری نیاز نیست .

• **شفاف نمودن شبکه برای نرم افزار ها NSX** : کل شبکه را در نرم افزارهای موجود در هر شبکه مجازی تولید می کند. این یک معماری منطقی توزیع شده برای سرویس های L2-7 شامل، سوئیچ منطقی، روتر، فایروال، بالانس کننده بار و VPN ارائه می دهد. این سرویس های منطقی شبکه همراه با ماشین های مجازی در vMotion به صورت برنامه ای ارائه می شوند. و هیچ تفاوتی بین یک شبکه مجازی و یک اتصال شبکه فیزیکی وجود ندارد .

• **توسعه پذیری** : یکی دیگر از قابلیت های خوب NSX این است که امکان پشتیبانی از سرویس های مختلف سازمان ها و نهادهای متفاوت را می دهد NSX. کمک می کند تا خدمات مناسب در مسیرهای ترافیکی مناسب قرار گیرند و می تواند به شما در ساخت شبکه های پیچیده در یک میزبان ESXi یا در چندین میزبان ESXi برای اهداف تولید ، آزمایش یا توسعه کمک کند .  
• **فراهم آوری زیرساخت قابل توسعه شبکه** : استفاده از نرم افزار های جانبی Third-party به عنوان راه کارهای مورد نیاز است .

• **پیاده سازی سرویس های اصلی** : با استفاده از NAT، VPN، DHCP، DNS محلی سازی یا Localize کردن سرویس های مهم لایه شبکه برای ادمین مجازی ایجاد ارتباط های امن بین دیتاسنترها با استفاده از L2 VPN میباشد .

• **ایجاد فایروال توزیع شده** : پیاده سازی فایروال های مجزا به ازای هر کارت شبکه ماشین مجازی، استفاده از تکنولوژی Micro segmentation و کنترل دقیق کوچکترین workload ها به صورت مجزا در شبکه در لایه های 2 و 7 انجام میشود .

• **قابلیت ایجاد perimeter firewall** : فایروال مرکزی با امکان کنترل ترافیک در لایه های 2 و 7 انجام میشود .

• **قابلیت Automatic Rule Generation** : ایجاد سهولت و دقت در امر ایجاد قوانین و پالیسی ها با ایجاد اتوماتیک rule ها

• **پایین آوردن هزینه** : کاهش چشم گیر هزینه های سازمانی برای خدمات به کاربرها و خرید تجهیزات شبکه و امنیت

• **قابلیت identity based firewall** : ایجاد پالیسی به ازای کاربران مختلف سازمان

• **Service defined firewall** : ایجاد پالیسی و rule های مورد نیاز اپلیکیشن ها و سرویس های شناخته شده مانند

SAP و ERP به صورت اتوماتیک

• **NSX در CLOUD** : محصول NSX در هر دو نسخه nsx-v و nsx-T به راحتی از طریق API قابلیت استفاده در زیرساخت های

رایانش ابری همچون open stack را دارد و کلیه سرویس های ذکر شده می توانند به صورت اتوماتیک و بسته به نیاز ایجاد و یا حذف گردند .

NSX، یک RESTful API را ارائه نموده و این امکان را برای پلتفرم های مدیریت Cloud فراهم میکند تا فرآیند ارائه سرویس های شبکه، خودکار گردد. آماده سازی شبکه که ممکن بود چندین روز یا هفته به طول بیانجامد، هم اکنون در مدت چند ثانیه قابل انجام است. با توجه به اینکه در حال حاضر سرویس های شبکه از طریق شبکه های مجازی برای برنامه ها ارائه میگردند، نیازی به پیگیری مجدد شبکه فیزیکی به صورت دستی نمی باشد .

NSX Service Composer، شیوه ای را برای خودکار سازی روند مصرف سرویس ها و طراحی آنها برای ماشین های مجازی با استفاده از Policy منطقی ارائه مینماید. مشتریان میتوانند Policy هایی را به گروهی از ماشین های مجازی اختصاص دهند و در صورت اضافه شدن ماشین های مجازی دیگری به این گروه، این Policy به صورت خودکار بر روی ماشین های مجازی جدید اعمال میگردد. کاربران میتوانند جریان های کاری پیشرفته ای را ارائه نمایند که امنیت، سازگاری و آماده سازی شبکه شامل قواعد فایروال و Load Balancing را خودکار می سازد .

NSX پلتفرمی را برای ورود سایر سرویس های Vendor ارائه مینماید. ترکیب محصولات نرم افزاری و سخت افزاری میتواند در محدوده سرویس های Gateway شبکه، سرویس های ارائه برنامه و پلتفرم های امنیت شبکه تا سرویس های امنیتی قرار گیرد. این تکنولوژی یک پلتفرم کامل مجازی سازی شبکه ی Multi-Hypervisor و Multi-Cloud می باشد. مجازی سازی شبکه ی لایه 2 و 3 با ماژول های نرم افزار Add-On برای سرویس های شبکه لایه 4-7 نظیر فایروال، Load Balancer و VPN، توسط پلتفرم NSX ارائه میشود .

نرم افزارهای سازگار با NSX:

- VMware vSphere
- KVM
- Xen Citrix
- OpenStack
- CloudStack
- vCAC | VMware vCloud Automation Center
- vCD | VMware vCloud Director

NSX به عنوان محصول SDN در معماری SDDC به کار میرود و می بایست بتواند به عنوان یک محصول، SDN لایه های سنتی شبکه را به لایه های مبتنی نرم افزار تبدیل کند که این امر در شکل زیر قابل مشاهده است. محصول NSX با تفکیک لایه های تجهیزات شبکه و متمرکز کردن آنها در 3 لایه Management plane، Control Plane و Data plane معماری و شکل جدیدی به شبکه تحت مدیریت ما خواهد داد که در ذیل به صورت مختصر به هر کدام از آنها اشاره می کنیم :

#### **: Management plane**

در این لایه نرم افزار NSX manager قرار میگیرد که به عنوان پنل مدیریتی NSX از آن استفاده میشود. این نرم افزار به صورت یک فایل OVA ارائه میشود که پس از دیپلوی کردن در زیرساخت مجازی، پلاگینی را روی وی سنتر ایجاد می نماید. از وظایف NSX Manager میتوان به ایجاد لایه Control plane به وسیله دیپلوی کردن کنترلرها و همچنین ایجاد لایه Data plane آماده سازی هاست ها برای مجازی سازی شبکه اشاره کرد .

#### **: Control Plane**

در این لایه با دیپلوی کردن کنترلرها که به صورت ماشین مجازی خواهند بود و توصیه می شود که حداقل 3 عدد از آنها برای ایجاد HA و پخش کردن وظایف لایه کنترلی بین آنها، وجود داشته باشد، قرار خواهند گرفت . لایه کنترلی در NSX وظیفه نگهداری MAC Table، ARP Table، VTEP Table و شرکت در ایجاد Dynamic Routing ها را بر عهده دارد که در پست های بعدی به تفصیل به آنها خواهیم پرداخت .

#### **: Data plane**

این لایه با نصب VIB هایی از طریق NSX Manager، بر روی هاست های درون یک کلاستر ایجاد خواهد شد که توسط این VIB ها پکیج های VXLAN لایه سویچینگ، DLR روتینگ در سطح هاست و DFW فایروال توزیع شده به صورت مستقیم بر روی هاست نصب می شوند.