# NSX TS 笔记

## day1 - TS概览

### **Troubleshooting 方法论**

一个问题可能由以下原因引起，本TS主要讨论配置问题：

**1、配置问题**

2、资源不足（VMware自己组建占用比平时多一些）

3、网络攻击

4、软件Bug

5、硬件故障

6、不合理及未经过测试的设计

### **Troubleshooting 步骤**

**一、发现问题**

* 诊断现象 identity Symptoms
* 收集信息 Gathering Information
* 找出最近有什么变更，What Changed

**二、发现症结**

* 找出可能的原因 possible causes
* 发现根结原因 root causes
* 测试可能的原因 Testpossible causes of the problem

**三、解决方法**

* 发现解决办法
* 执行最佳解决办法
* 检查是否解决
* 记录此问题及解决办法

### 一、TS 传输网络Transport Network（先解决最基础故障）

测试物理的承载网络：

* 使用ping，vmkping测试主机之间vtep的通信。
* 检查端到端的MTU
* 检查VXLAN的端口配置正确（5.5用8472，6.x用4789，此端口可以进行修改(API)。从5.x升级到6.x后，则会保留原来的端口。如果使用了硬件VTEP，则必须修改NSX的端口和其保持一致。）
* 检查确保没有防火墙阻止通信（物理防火墙阻止了UDP 4789的通信）

### 二、确定使用了哪些服务（对症下药）

* NSX manager相关
  + NSX终端或设备的配置问题会导致和NSX manager通信异常（例如主机vsfwd进程异常，导致防火墙策略发布失败，但是6.2之后发布策略失败系统会提示）
  + identity Firewall相关问题，例如AD通信异常，安全策略配置有问题
* Contol Plane相关的服务
* 检查hybrid、Multicast模式下依赖的物理网络是否正常
* 使用的安全服务
  + DFW的策略
  + 网络和Guest Introspection相关服务
* Edge service Gateway的相关服务
  + LB配置或者故障
  + VPN（IPSec、L2VPN）
  + ESG的路由和防火墙

### 三、TS 逻辑交换 Logical Switching

* 首先检查NSX 控制层 和 管理层 的通信
* 检查ESXi主机的管理IP和管理层以及控制层的通信
  + 检查VTEP IP配置正确，状态为Connected
  + 检查VTEP和vDS端口组的MTU配置
  + 检查Logical switch的控制层面设置（controller）
* 检查主机的VXLAN设置能够从控制平面获取MAC地址。

### 关键点

* 有步骤的去进行排查
* 区分不同的现象和问题，是很重要的一步
* 一定要熟悉VMware基础架构如何工作、且对现场环境很熟悉
* 物理和逻辑网络图

## 基础架构

### Management Plane

NSX 有四个角色：NSX admin、System Admin、Enterprise Admin、Security Admin。

默认vCenter的administrator用户会成为NSX的Enterprise Admin，所以只有VC的Administrator用户可以在vCenter中管理NSX (networking & Security)

*有个第三方的软件HyTrust可以实现NSX的多级管理*

NSX manager和vCenter建立连接后，vCenter 有东西更新时才会主动发给NSX manager，NSX manager 和 vCenter 的连接状态最后更新时间指最后一次从vcenter收到更新的时间。

**NSX manager 和 vCenter连接问题：**

* NSX manager或者vcenter的DNS配置问题
* NTP 配置问题
* 连接到vCenter时使用的用户不具有vCenter的管理员权限
* NSX manager和vCenter之间网络通信有问题

在NSX manager中完成vCenter注册后，第一次需要使用进行连接的vCenter用户登陆VC才能管理NSXmanager；之后可以进入 Networking & Security >NSX Manager > {IP of manager} > Manage > Users 中将**其他用户**添加为NSX Enterprise admin；新用户需要等待几分钟才能登陆vCenter并管理NSX。

**NSX Manager和VC连接问题排查**

* 登陆NSX manager，使用show running-config 检查NSX manager的配置
* 使用 **ping x.x.x.x，show arp，show ip route** 检查网络通信情况（show arp查看当NSX manager和VC同网段时能否正常学习到VC的MAC地址，show ip route查看NSX manager和VC不同网段时，NSX manager是否有到VC网段的路由）
* **show manager log follow** ，使用此命令查看NSX manager连接到vCenter时日志，进而分析为什么注册失败。
* **debug packet display interface mgmt port\_443\_or\_port\_80**，在特权模式下执行上述命令抓取NSX manager 443和80端口的通信包。

NSX manager和Controller连接的证书为南北向证书，**不能更改**。

**NSX manager 东西向证书(对外的证书)及相关问题**

NSX manager有两种方式申请证书：

* 使用 NSX manager 生成 CSR，但是功能有限
* 使用PKSC#12，推荐用于生产环境

问题：Content Management System （CMS，比如第三方云管平台）调用NSX API失败

* CMS不信任NSX manager的证书（Root-CA不受信或者使用的是自签名证书）
* 需要在 CMS 中手动接受证书。

**NSX manager 失效：**

1、无法进行管理

2、某些依赖于NSX manager的服务（User Identity Firewall），NSX无法通过AD获取用户信息。

用户使用AD登陆虚拟机，登陆后产生Log 告诉AD用户的登陆信息。NSX Manager可以通过AD查询用户的对应IP，然后将防火墙策略应用到IP

3、基于vCenter Object的防火墙策略不可用。NSX manager失效后，vCenter正常工作，所以vSphere Admin依然可以管理vCenter的Resource Pool等对象，假如有新VM假如到Resource Pool，则防火墙策略无法应用到此新VM。

### Contrl Plane

**始终部署NSX Controller！即使某些场景下并不需要它**

netcpa 通过 management network和controller进行通信

**Control Plane**

主机进程 netcpa，Controller 与主机通过netcpa进程通信。

NSX manager 创建LSW，通知Controller，选举出LSW的master controller，然后Controller通告给主机。如果主机netcpa有问题，则无法将LSW创建到此主机，也不知道。

同一个网段，LSW上，一个VM通过Vmotion后不通，可能原因：

1、虚拟化上MTU设置错误

2、两个Uplink，但是物理交换机上MTU配置错误

3、VTEP 的Gateway配置错误，主机上所有VTEP无法正常发送

MTU 最小为1550

但是创建VTEP一般为1600，所以物理网络必须设置到最小1600。

而且，1600可以用于IPv6网络，也有50字节的预留可以在未来增加功能。1600也比较好记。

NSX 使用UDP，vSphere5.5(8472)，vSphere6.0（4789），此端口可以进行修改(API)。

如果从低版本升级到6.0，则会保留原来的端口。如果使用了硬件VTEP，则必须修改NSX的端口和其保持一致。

单个集群可以用多个VTEP IP地址段吗？两种方法：

*1、IP pool Object 是单独的一个对象，可以单独再创建一个。因此可以通过API更改IP Pool的地址，但是只能更改地址范围，不能改网关和网段。*

2、使用DHCP分配地址

### Universal 的使用注意事项

UDFW 最好使用IP地址创建防火墙规则。不能使用vCenter的Object，因为不同VC的对象使用其management object ID进行区分，而即使名称一样，ID是不一样的。