StarVCenter

企业级部署-网络结构

-典型案例

在部署云平台时，根据企业实际网络现状与需求的不同，会采用不同的网络布线结构，下面我们将介绍StarVCenter在企业内部部署使用的几种典型的网络结构。

# 名词解释：

**管理网**：管理网是安装各节点操作系统时设置的“IP网络”，主要用于用户访问管理界面，和管控节点向计算节点发送管控指令等管理操作。

**业务网**：业务网是用于虚拟机之间、虚拟机与平台之外的计算机之间通信的网络。其物理结构由各节点的“业务网网卡及其相连的二层物理链路”构成。

**存储网**：计算节点访问存储（含虚拟机磁盘I/O）所走的“IP网络”，通常用万兆网。

# 典型案例

## 管理网与业务网合一



如上图所示，办公区的电脑同时与管理网业务网连通，借助核心交换机上的路由，可同时访问虚拟机和StarVCenter的管理界面，也能直接ssh登录到物理服务器上进行运维管理。在安全允许的情况下可将StarVCenter的管理IP地址和18080、18081、18083端口通过互联网出口路由器映射到互联网，以便能远程管理运维云平台，还可通过微信小程序“SVC助手”管理StarVCenter。

**优点：**管理网与业务网二合一结构是较常用的结构，它不仅**结构简单，使用和运维也很方便**。

**缺点：**云用户通过强制修改虚拟机IP，可能非法访问物理机，**安全性低**。另外管理网与业务网的链路和带宽是共用的，运维和管理时会**相互影响**。

这种结构中，建议虚拟子网使用vlan以确保从虚拟机内不可非法访问其它子网，需要将管理网、业务网交换机上连接服务器的端口策略设置为“trunk模式”并使用pvid来实现不带tag的管理网放行。

**企业内部用户电脑怎么访问虚拟机？虚拟子网间怎么互通？**

核心交换机充当了各子网间的直连路由，办公区子网和StarVCenter所有虚拟子网网关都配置在核心交换机上，因此办公区用户可以直接访问StarVCenter中的虚拟机，StarVCenter中多个子网间也可互通。

**虚拟机怎么访问互联网？**

互联网出口路由器所在子网与其它子网一样都是核心交换机的直连路由网络，在核心交换机上配置上网路由策略（对非直连路由转发之外的数据包，都统一转发至互联网出口路由），这样虚拟机就与办公区电脑一样，可直接通过企业互联网出口路由上网。

**从互联网上怎么访问虚拟机？**

若需从互联网上访问虚拟机，只需在互联网出口路由上做端口映射即可。

## 三网分离



这种结构下，企业内部办公电脑可直接访问StarVCenter中的虚拟机，但无法直接访问StarVCenter的管理界面。云平台管理员先通过办公区电脑远程连接到“跳板机”桌面，通过跳板机访问StarVCenter的管理界面、从跳板机上ssh登录运维物理服务器。可将跳板机的远程连接端口从路由器映射到互联网，以便能远程管理运维云平台。

**优点：**将“管理网”、“业务网”、“存储网”从链路上完全分开，可保证独立运维互不影响，**可用性高、安全性好**。

**缺点：**只能通过跳板机访问云平台，**运维管理不方便**。

## 业务网-内外网分离



某些对网络安全要求较高的企业，将企业内部的局域网进一步地分为“信息外网”和“信息内网”。其中“信息外网”是能直接通向互联网的部分，“信息内网”只能在企业内部或集团公司内部互通，不通互联网的网络。“信息外网”主要通过互联网办公或查资料用，企业内部的应用系统及重要数据传输都走“信息内网”以确保安全。

我们将企业内部的这种划分称为“内外网分离”，基于这种情况我们通常可以在信息内网和信息外网各部署一套云平台，但这种模式在管理和运维上都不方便。上图的结构描述了一种可同时服务于“信息内网”和“信息外网”的结构，在为虚拟机分配网络时，按需选择接入“信息内网”或“信息外网”均可。信息外网办公区电脑可访问接入“信息外网”的虚拟机，只有信息内网办公区的电脑才可访问“信息内网”的虚拟机。

如果一台虚拟机同时接入“信息内网”和“信息外网”，则该虚拟机可作为“信息外网”到“信息内网”的跳板机，这种情形可以管理员按需配置以确保安全。