

神州云科（YK）
应用交付设备
操作手册



XXX

2020 年 03 月 24 日

目录

1. 实现功能简介.....	3
1) 负载均衡策略.....	3
2) 服务器的健康检查和监控.....	4
3) 会话保持.....	5
4) 连接复用技术.....	7
5) DDos 防护.....	8
6) 全代理安全性.....	8
2. 基础配置.....	9
1) 设备信息.....	9
2) 配置备份及恢复.....	9
3) SNMP 配置.....	13
4) 设备新账户及新分区配置.....	13
3. 网络层配置.....	14
1) 端口聚合 (Portchannel) 配置.....	14
2) 接口划分及类型配置.....	14
3) 接口 IP 配置.....	15
4) 路由配置.....	16
4. 集群配置.....	17
1) NTP 配置.....	18
2) 建立 HA 步骤.....	18
5. 应用配置.....	22
1) 配置资源池 (提供相同服务的服务器群).....	22
2) 配置虚拟服务器 (对外提供服务).....	23
6. 状态察看.....	25
1) 仪表盘.....	25
2) 性能报告.....	26
7. 故障采集.....	27
1) 寻求 YK 技术支持时, 要提供哪些信息与资料?.....	27
2) 获取 Qkview 的方式.....	27

1. 实现功能简介

1) 负载均衡策略

YK BIG-IP 利用 Virtual Server 虚拟服务器 (VS 由 IP 地址和 TCP/UDP 应用的端口组成) 来为用户的一个或多个目标服务器 (称为 Node: 目标服务器的 IP 地址和 TCP/UDP 应用的端口组成, 它可以是私网地址) 提供服务。因此, 它能够为大量的基于 TCP/IP 的网络应用提供服务器应用交付服务。根据服务类型不同分别定义服务器群组, 可以根据不同服务端口将流量导向到相应的服务器。YK BIG-IP 连续地对目标服务器进行 L4 到 L7 合理性检查, 当用户通过 VIP 请求目标服务器服务时, YK BIG-IP 根据目标服务器之间性能和网络健康情况, 选择性能最佳的服务器响应用户的请求。如果能够充分利用所有的服务器资源, 将所有流量均衡的分配到各个服务器, 我们就可以有效地避免“不平衡”现象的发生。

YK BIG-IP 是一台对流量和内容进行管理分配的设备。它提供灵活的算法将数据流有效地转发到它所连接的服务器群。而面对用户, 只是一台虚拟服务器。用户此时只须记住一台服务器, 即虚拟服务器。但他们的数据流却被 YK BIG-IP 灵活地均衡到所有的服务器。算法包括:

轮询 (Round Robin): 顺序循环将请求一次顺序循环地连接每个服务器。当其中某个服务器发生第二到第 7 层的故障, YK BIG-IP 就把其从顺序循环队列中拿出, 不参加下一次的轮询, 直到其恢复正常。

比率 (Ratio): 给每个服务器分配一个加权值为比例, 根据这个比例, 把用户的请求分配到每个服务器。当其中某个服务器发生第二到第 7 层的故障, YK BIG-IP 就把其从服务器队列中拿出, 不参加下一次的用户请求的分配, 直到其恢复正常。

优先权 (Priority): 给所有服务器分组, 给每个组定义优先权, YK BIG-IP 用户的请求, 分配给优先级最高的服务器组 (在同一组内, 采用轮询或比率算法, 分配用户的请求); 当最高优先级中所有服务器出现故障, YK BIG-IP 才将请求送给次优先级的服务器组。这种方式, 实际为用户提供一种热备份的方式。

最少的连接方式 (Least Connection): 传递新的连接给那些进行最少连接处理的服务器。当其中某个服务器发生第二到第 7 层的故障, YK BIG-IP 就把其从服务器队列中拿出, 不参加下一次的用户请求的分配, 直到其恢复正常。

最快模式 (Fastest): 传递连接给那些响应最快的服务器。当其中某个服务器发生第二到第 7 层的故障,YK BIG-IP 就把其从服务器队列中拿出,不参加下一次的用户请求的分配,直到其恢复正常。

观察模式 (Observed): 连接数目和响应时间以这两项的最佳平衡为依据为新的请求选择服务器。当其中某个服务器发生第二到第 7 层的故障, YK BIG-IP 就把其从服务器队列中拿出,不参加下一次的用户请求的分配,直到其恢复正常。

预测模式(Predictive):YK BIG-IP 利用收集到的服务器当前的性能指标,进行预测分析,选择一台服务器在下一个时间片内,其性能将达到最佳的服务器相应用户的请求。(被 YK BIG-IP 进行检测)

动态性能分配 (Dynamic Ratio-APM):YK BIG-IP 收集到的应用程序和应用服务器的各项性能参数,动态调整流量分配。

动态服务器补充 (Dynamic Server Act.):当主服务器群中因故障导致数量减少时,动态地将备份服务器补充至主服务器群。

服务质量(QoS):按不同的优先级对数据流进行分配。

服务类型(ToS):按不同的服务类型(在 Type of Field 中标识)对数据流进行分配。

规则模式:针对不同的数据流设置导向规则,用户可自行编辑流量分配规则,YK BIG-IP 利用这些规则对通过的数据流实施导向控制。

2) 服务器的健康检查和监控

YK BIG-IP LTM 提供了先进的监视器,用于检查设备、应用和内容的可用性,包括适合多种应用的专用监视器(包括多种应用服务器、SQL、SIP、LDAP、XML/SOAP、RTSP、SASP、SMB 等),以及用于检查内容和模拟应用调用的定制监视器。

服务器 (Node) - Ping (ICMP)

YK BIG-IP 可以定期的通过 ICMP 包对后台服务器的 IP 地址进行检测,如果在设定的时间内能收到该地址的 ICMP 的回应,则认为该服务器能提供服务

服务 (Port) - Connect

YK BIG-IP 可以定期的通过 TCP 包对后台服务器的服务端口进行检测,如果在设定的时间内能收到该服务器端口的回应,则认为该服务器能提供服务

扩展内容查证(ECV: Extended Content Verification)-ECV

ECV 是一种非常复杂的服务检查，主要用于确认应用程序能否对请求返回对应的数据。如果一个应用对该服务检查作出响应并返回对应的数据，则 YK BIG-IP 控制器将该服务器标识为工作良好。如果服务器不能返回相应的数据，则将该服务器标识为宕机。宕机一旦修复，YK BIG-IP 就会自动查证应用已能对客户请求作出正确响应并恢复向该服务器传送。该功能使 YK BIG-IP 可以将保护延伸到后端应用如 Web 内容及数据库。YK BIG-IP 的 ECV 功能允许您向 Web 服务器、防火墙、缓存服务器、代理服务器和其它透明设备发送查询，然后检查返回的响应。这将有助于确认您为客户提供的内容正是其所需要的。

扩展应用查证(EAV: Extended Application Verification)

EAV 是另一种服务检查，用于确认运行在某个服务器上的应用能否对客户请求作出响应。为完成这种检查，YK BIG-IP 控制器使用一个被称作外部服务检查者的客户程序，该程序为 YK BIG-IP 提供完全客户化的服务检查功能，但它位于 YK BIG-IP 控制器的外部。例如，该 外部服务检查者可以查证一个 Internet 或 Intranet 上的从后台数据库中取出数据并在 HTML 网页上显示的应用能否正常工作。EAV 是 YK BIG-IP 提供的非常独特的功能，它提供管理者 将 YK BIG-IP 客户化后访问各种各样应用的能力，该功能使 YK BIG-IP 在提供标准的可用性 查证之外能获得服务器、应用及内容可用性等最重要的反馈。

该功能对于电子商务和其它应用至关重要，它用于从客户的角度测试您的站点。例如，您可以模拟客户完成交易所需的所有步骤—连接到站点、从目录中选择项目以及验证交易使用的信用卡。一旦 YK BIG-IP 掌握了该"可用性"信息，即可利用负载平衡使资源达到最高的可用性。

3) 会话保持

当使用 YK 对服务器进行负载均衡时，就需要会话保持。如果某位客户连接到了一台服务器上，那么我们肯定希望该客户在将来再次连接时将仍可连接到该台服务器上。当该服务器存有客户相关数据，并且这些数据并不与其它服务器动态共享时，持续性就显得十分有必要了。例如，假设一位客户在某网站采购了一“购物车”的商品，然后还未结帐就离开了该网站。如果在其重新登录网站后，YK 应用交换机将客户请求路由至不同的服务器，那么新的服务器对该客户的数据和其所购买的商品将一无所知。当然，如果所有服务器都在同一个后台数据库服务器中存储客户信息及其选购商品的话，那么一切就不成问题了。但是如果网站不是这样设计的，那么具体的购物车数据就只能存储在特定的服务器上。这样，YK 应用

交换机就必需选择客户曾连接上的那台服务器，以无缝地处理客户请求。

YK 提供以下几种会话保持方法：Simple Persistence, SSL Session ID Persistence, SIP Persistence, Cookie Persistence, iMode Persistence, 目的地址归类。

Simple Persistence: 根据源地址做会话保持，即相同源地址的访问请求定位在同一台服务器上。

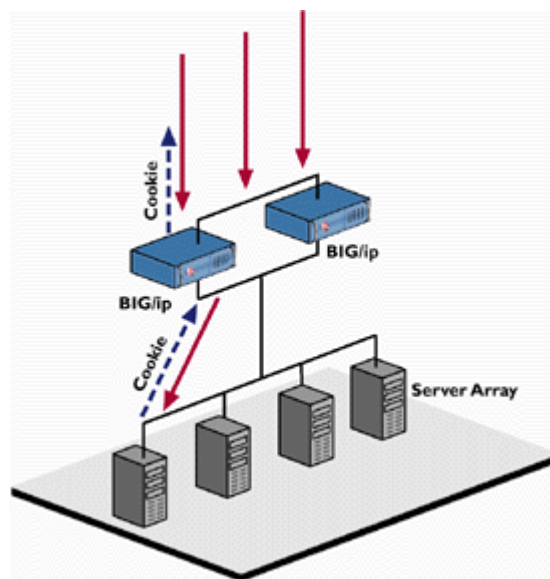
SSL Session ID Persistence: 根据 SSL 会话 ID 做会话保持。

SIP Persistence: SIP 协议会话保持技术。

HTTP Cookie Persistence: YK 支持四种 Cookie 会话保持技术，即：改写模式，插入模式，被动的 cookie，Cookie 散列：

1. Cookie 改写模式，服务器将插入一个 cookie，然后 YK 应用交换机将对其进行重写，访问流程如下：

首次命中，HTTP 请求（不带有 cookie）进入 YK 应用交换机，YK 应用交换机任选一台服务器，将请求发送至该服务器，来自该服务器的 HTTP 回复此时包括一个空白的 cookie，YK 应用交换机重写 cookie，并在粘贴一个特殊的 cookie 后将 HTTP 回复发送回去。再次命中，HTTP 请求（带有与上面同样的 cookie）进入 YK 应用交换机，YK 应用交换机借助 cookie 信息确定合适的服务器，HTTP 请求（带有与上面同样的 cookie）进入服务器，HTTP 回复（带有空白 cookie）返回 YK 应用交换机，后者将向客户机提供更新后的 cookie。如下图所示：



2. Cookie 插入模式，YK 插入一个 cookie，服务器无需作出任何修改，访问流程如下：

首次命中，HTTP 请求（不带 cookie）进入 YK 应用交换机，YK 应用交换机任选一台服

务器，将请求发送至该服务器，HTTP 回复（不带 cookie）被发回 YK 应用交换机 YK 应用交换机插入 cookie，将 HTTP 回复返回到客户机。

再次命中，HTTP 请求（带有与上面同样的 cookie）进入 YK 应用交换机，Cookie 指定合适的服务器，HTTP 请求（带有与上面同样的 cookie）进入服务器，HTTP 回复（不带 cookie）进入 YK 应用交换机，后者将为客户机提供更新后的 cookie。

3. 被动模式，服务器使用特定信息来设置 cookie，访问流程如下：

首次命中，HTTP 请求（不带有 cookie）进入 YK 应用交换机，YK 应用交换机任选一台服务器，将请求发送至该服务器，HTTP 回复（带有特定 cookie）返回至 YK 应用交换机，YK 应用交换机将 HTTP 回复（带有特定 cookie）发回客户机。

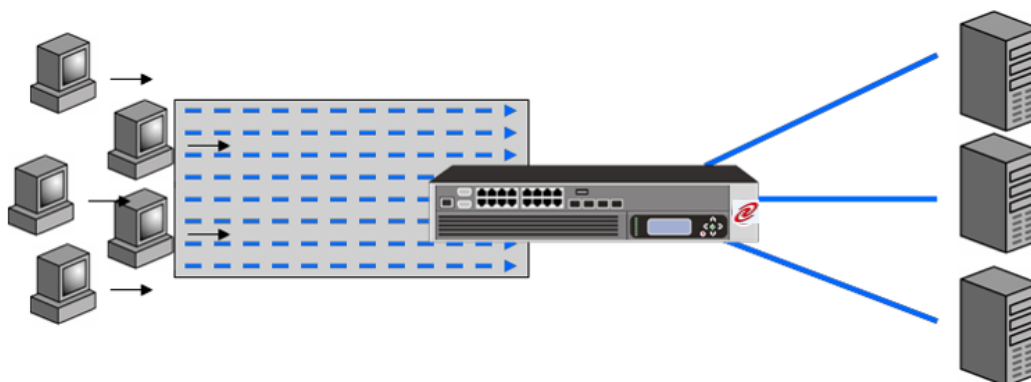
再次命中，发送 HTTP 请求（带有与上面同样的 cookie），Cookie 指定合适的服务器，HTTP 请求（带有与上面同样的 cookie）进入服务器，HTTP 回复（带有特定 cookie）返回至 YK 应用交换机，后者将 HTTP 回复（带有特定 cookie）发送回客户机。

YK 应用交换机 Cookie 持续性模式与 SSL 持续性模式之间的主要区别在于：对于 Cookie 持续性而言，数据存储是客户机上，而不是 YK 应用交换机上，因此可充分使用客户机上的无限资源。即 Cookie 持续性体现在 HTTP Cookie 上，而信息则存储于客户机的磁盘驱动器上。

4. Cookie 会话保持散列模式，该模式只能在 BIG-IP HA 控制器和企业上使用。散列模式使您可以通过设定 cookie 中一定字节数的信息来确定连接的目的地。该模式用于将 cookie 值映射到节点上，之后该值这将用于连接含该 cookie 的客户机，从而实现了节点的持续性。

4) 连接复用技术

YK BIG-IP 通过 Oneconnect 技术，将所有客户端的 TCP 连接转移至 YK BIG-IP 进行处理；而 YK BIG-IP 与服务器之间仅建立少量的、持续的 TCP 连接。使 Web 服务器从处理大量的并发 TCP 请求和 TCP 连接建立/卸载的负担中解脱出来，同时当 YK BIG-IP 收到用户请求后才发送到服务器，服务器可免于受到客户端和网络异常的影响。YK BIG-IP 还会缓存所有服务器的响应数据包，服务器以 LAN 速度发送数据到 YK BIG-IP，服务器不会受到慢速客户端连接的牵累。服务器的大量 CPU 资源被释放来提供数据，而不是管理连接。



YK BIG-IP 通过控制容量需求和访问分析优化了服务性能和带宽。企业也因为增加了更多的计算资源，减少了出口带宽需求而降低服务器和带宽投资，并且减少服务响应延迟和运营成本。

5) DDos 防护

YK BIG-IP 的全代理架构提供的功能可以在拒绝服务 (DoS) 和分散式拒绝服务 (DDoS) 攻击到达数据中心服务器之前减轻攻击的损坏，因而确保了应用的可用性。即购即用的功能包含了全方位的规则。借助这些规则，企业可以即刻跟踪、报告和防御各种知名的网络 DDoS 矢量攻击和方法，包括 flood、sweep、teardrop 和 smurf 攻击等等。

6) 全代理安全性

与传统防火墙不同，YK BIG-IP 基于全代理架构。这意味着，在将入站客户端连接转发至服务器之前，YK BIG-IP 会将这些连接完全终止，检查其是否包含可能的安全威胁。在确定不存在任何威胁后，才会将其转发至服务器。

在相反方向，服务器到客户端的通信也被代理。安装有 YK BIG-IPAFM 的 YK 应用交付 防火墙解决方案会过滤返回的数据，看是否存在敏感信息—例如会泄露网络信息进行侦查攻击的协议响应代码和私人数据（如信用卡号或社会保险号等）。

2. 基础配置

1) 设备信息

- 系统—平台
- 注意：主机名称必须为 FQDN 格式，即域名格式。由于集群配置为设备间的证书互信，故配置好集群后，尽量不更改主机名称及 root 账户以及 admin 帐户密码。

在线 (ACTIVE)
Standalone

主菜单栏 帮助 关于

统计信息
iApps
DNS
本地流量
加速
设备管理
Shared Objects
网络
系统

配置 安全

常规属性

管理端口 1 配置 ☒ 自动 (DHCP) ☐ 手动

管理端口 1

IP 地址[前缀]: 11.0.0.196

网络掩码: 255.255.255.0 /24

管理路由: 11.0.0.254

管理端口 2

IP 地址[前缀]:

网络掩码: 选择...

管理路由:

主机名: bigip1

主机 IP 地址: 使用管理端口 IP 地址

时区: America/Los Angeles

冗余设备属性

Root 文件夹设备组: 无

Root 文件夹流量组: traffic-group-1

用户管理

☐ Disable login

Root 帐户

密码:

确认:

管理员帐户

密码:

确认:

SSH 访问: ☒ 启用

SSH IP 允许: 全部地址

更新

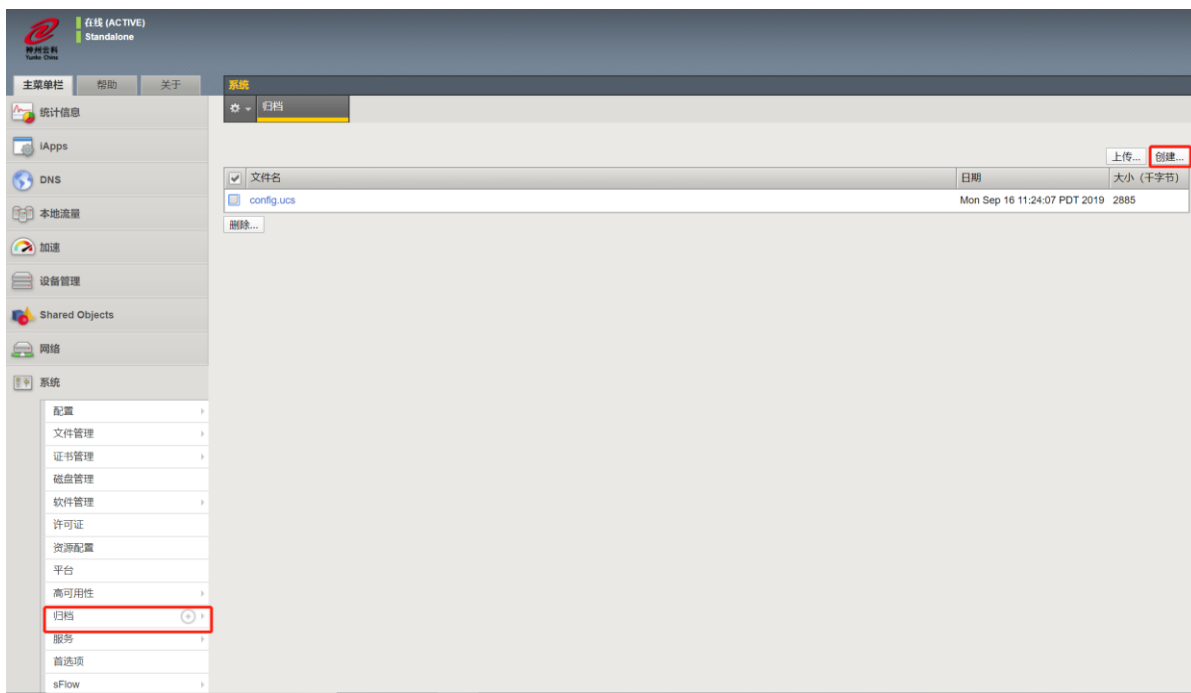
管理地址

主机名

root 和 admin 密码修改

2) 配置备份及恢复

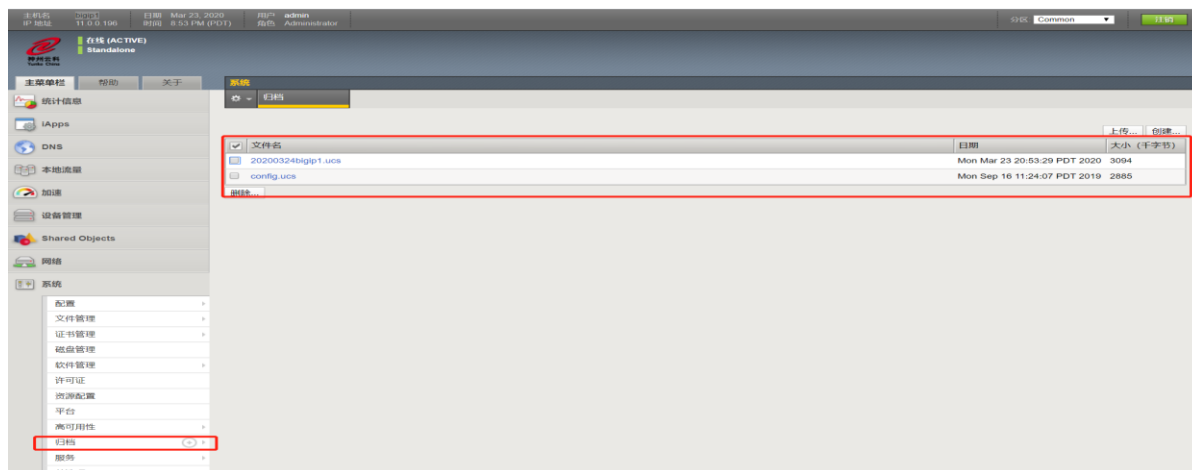
- 配置备份
- 点击 系统 选项卡中的 归档选项，在右侧菜单栏中选择 创建选项备份当前的配置。



为备份的配置文件命名并点击完成。

- 下载配置文件到本地

点击 系统 选项卡中的 归档选项，点击需要回滚的配置文件名称（并不是打勾）。



系统 >> 20200324bigip1.ucs

常规属性

文件名	20200324bigip1.ucs
版本	BIG-IP 14.1.1 Build 0.4.38
已加密	无
日期	Mon Mar 23 20:53:29 PDT 2020
大小	3094 千字节
归档配置文件	下载: 20200324bigip1.ucs

还原

删除

点击 Download，选择本地目录保存即可。

- 上传配置文件
 - 通过 web 界面上传
 - 点击 系统 选项卡中的 归档选项，在右侧菜单栏中选择上传本地 配置文件。

主机名 2020
IP 地址 11.0.0.196
日期 Mar 23, 2020
时间 8:56 PM (PDT)
用户 admin
角色 Administrator

分区 Common

注销

在线 (ACTIVE)
Standalone

主菜单栏 帮助 关于

统计信息
iApps
DNS
本地流量
加速
设备管理
Shared Objects
网络
系统

配置
文件管理
证书管理
磁盘管理
软件管理
许可证
资源配置
平台
高可用性
归档
服务

系统

归档

上传...

创建...

文件名	日期	大小 (千字节)
☒ 20200324bigip1.ucs	Mon Mar 23 20:53:29 PDT 2020	3094
☐ config.ucs	Mon Sep 16 11:24:07 PDT 2019	2885

删除...

系统 >> 上传...

上传配置归档

文件名

选择文件 未选择任何文件

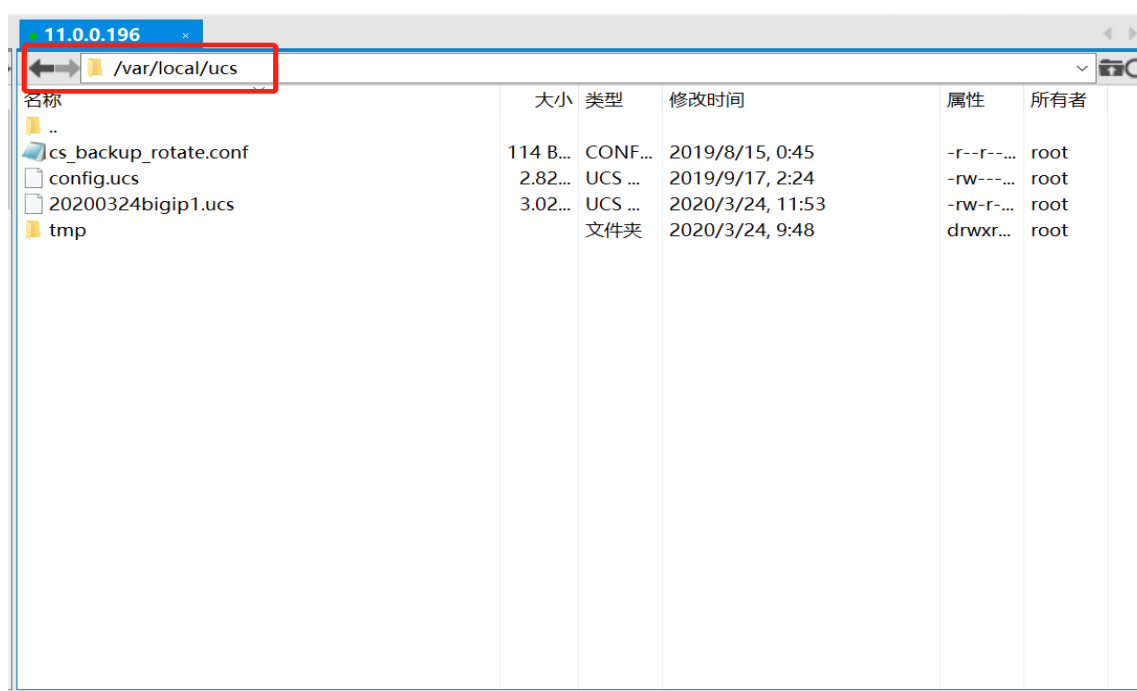
选项

☐ 覆盖现有归档文件

取消

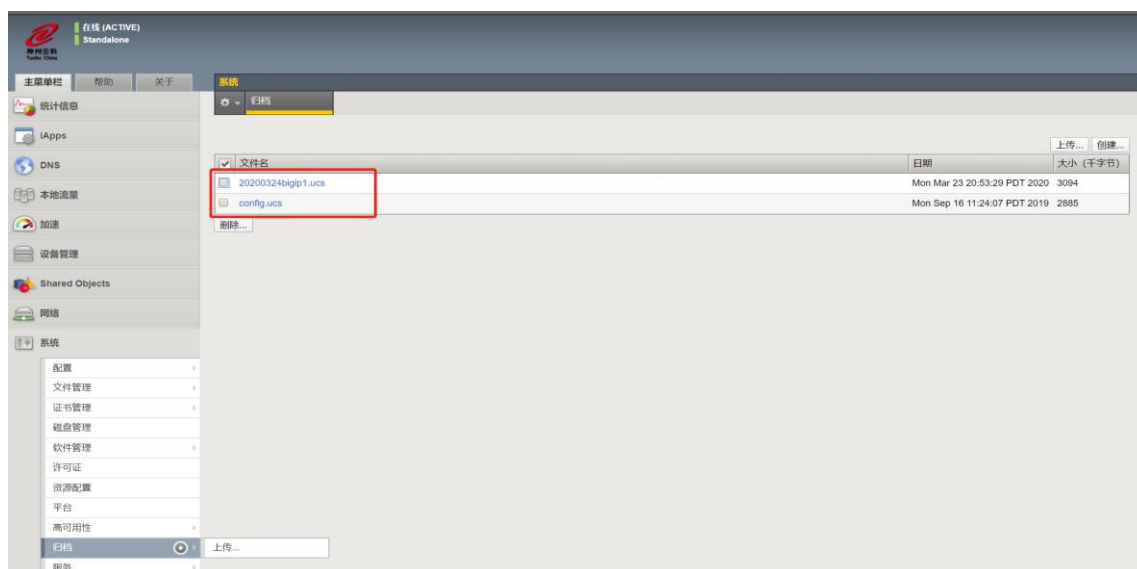
上传

➤ 通过 ftp 的方式上传到 YK 设备的 /var/local/ucs 目录下。



● 配置回滚

点击 系统 选项卡中的 归档选项，点击需要回滚的配置文件名称（并不是打勾）。



系统 » 20200324bigip1.ucs

常规属性

文件名	20200324bigip1.ucs
版本	BIG-IP 14.1.1 Build 0.4.38
已加密	无
日期	Mon Mar 23 20:53:29 PDT 2020
大小	3094 千字节
归档配置文件	下载: 20200324bigip1.ucs

还原

删除

点击 还原 回滚配置文件，待系统提示回滚完毕后再点击 OK（不可提前点击）。

3) SNMP 配置

- 系统—SNMP

4) 设备新账户及新分区配置

- 系统—用户

系统 » 用户 » 分区列表

用户列表

分区列表

认证

远端角色组

搜索

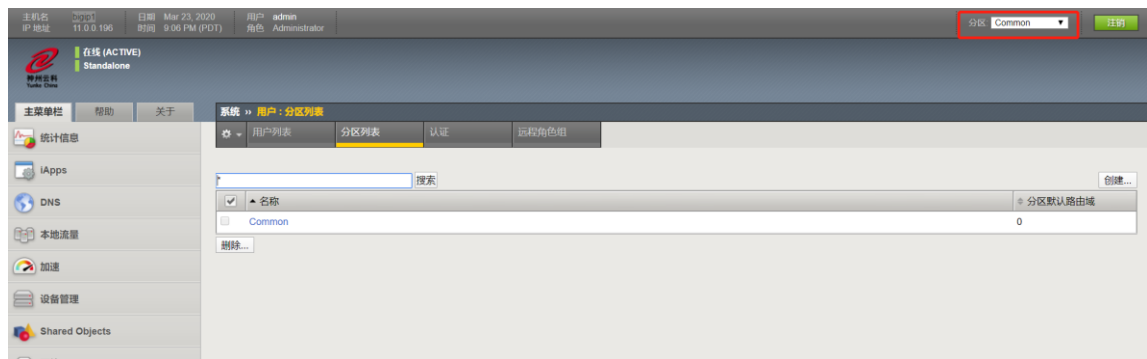
创建...

用户名	已锁定	失败登录次数	分区访问	分区	控制台
☒ admin	无	0	超级管理员 on 所有分区	Common	禁用

删除...

解锁

分区切换为右上角的下拉菜单

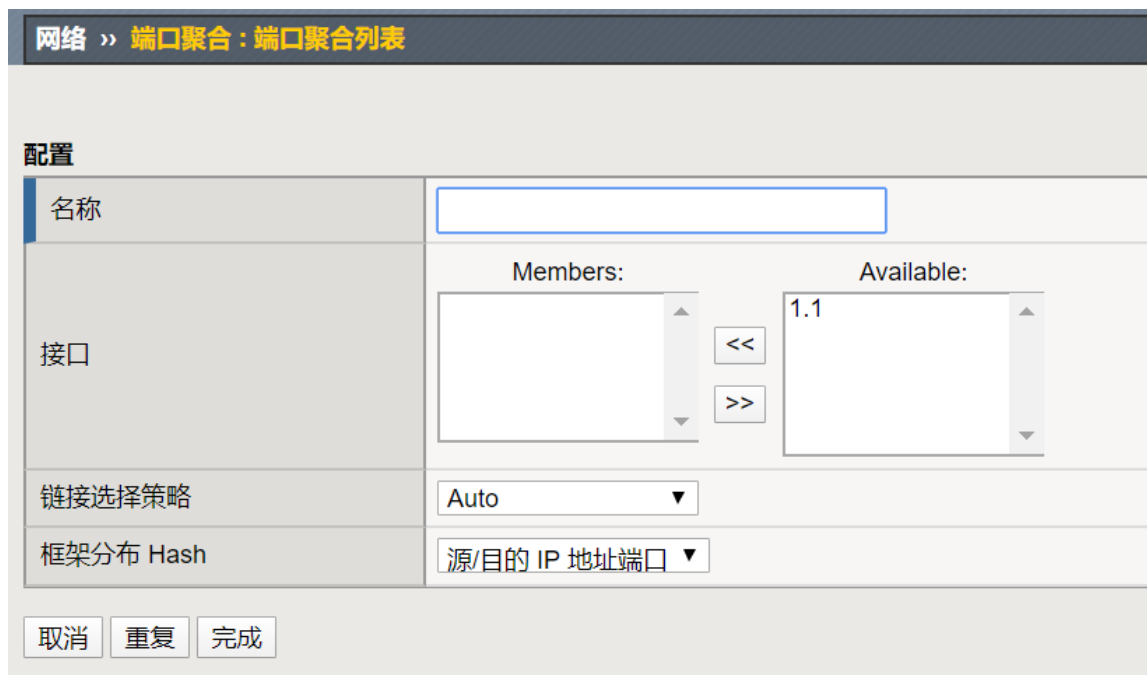


3. 网络层配置

注意：建议所有网络层配置在 Common 的分区下建立

1) 端口聚合（Portchannel）配置

- 网络—端口聚合
- 新建配置



2) 接口划分及类型配置

- 网络—VLANs
- 新建配置

网络 » VLAN : VLAN 列表 » 新建 VLAN...

常规属性	
名称	
说明	
标记	
资源	
接口	接口: 1.0 ▼ 标记: 选择... ▼ 添加 选择... ▼ 标记 未标记 编辑 删除
配置: Basic ▼	
源检查	☐
MTU	1500
sFlow	
轮询时间间隔	默认 ▼
采样率	默认 ▼
取消 重复 完成	

Vlan名称

VLAN ID

接口为access选未标记, 接口为trunk口选标记

3) 接口 IP 配置

- 网络—Self IPs
- 新建配置。若为接口的真实 IP 则选择 Traffic Group 为浮动（漂移）则选择 traffic-group-local-only(non-floating)

网络 » 新建 Self IP...

配置	
名称	
IP 地址	
网络掩码	
VLAN/通道	internal ▼
Port Lockdown	Allow None ▼
流量组	☐ 从当前分区/路径继承流量组 traffic-group-local-only (non-floating) ▼ None
服务策略	无 / Common
取消 重复 完成	

对应VLAN

4) 路由配置

- 网络—路由
- 新建配置

网络 » 路由 » 新建路由...

属性

名称		
说明		
目的	10.4.1.0	
网络掩码	255.255.255.0	
资源	使用网关...	
网关地址	IP 地址	10.4.1.22
MTU		

4. 集群配置

注意：

- 从 11.4.0 开始 BIGIP 支持在不同硬件平台之间建立 Configsync 和 Failover, 如果是 11.4.0 之前的版本则需要硬件平台一致。各硬件平台操作系统版本必须一致。
- 所有设备的 license 必须一致, 否则同步配置时会报错。
- 一定要保证设备时间尽量相同, 相差不超过 30s, 建议配置 NTP 服务器, 否则建设设备信任时可能出现问题。
- 修改设备时间方法为命令行输入: **【date 月日时分年】** (例 2015 年 12 月 18 日 11 点 12 分, date 121811122015), 修改完时间后使用 hwclock - systohc 将时间写入时钟。
- 在做基础配置时, 时区要一致。

The screenshot shows the BIGIP configuration interface. On the left is a sidebar with a menu including '统计信息', 'iApps', 'DNS', '本地流量', '加速', '设备管理', 'Shared Objects', '网络', and '系统'. The '系统' (System) menu is expanded, showing sub-items like '配置', '文件管理', '证书管理', '磁盘管理', '软件管理', '许可证', '资源配置', and '平台'. The main panel is titled '系统 >> 常规' (System >> General) and has tabs for '配置' (Configuration) and '安全' (Security). The '配置' tab is active, showing the '常规属性' (General Properties) section. This section includes fields for '管理端口 1 配置' (Management Port 1 Configuration) with radio buttons for '自动 (DHCP)' and '手动' (Manual), and input fields for 'IP 地址[前缀]', '网络掩码', and '管理路由'. Below this are fields for '管理端口 2' (Management Port 2), '主机名' (Hostname), '主机 IP 地址' (Host IP Address), and '时区' (Time Zone). The '时区' dropdown is currently set to 'America/Los Angeles' and is highlighted with a red rectangle. Below the '常规属性' section are the '冗余设备属性' (Redundancy Properties) and '用户管理' (User Management) sections. The '冗余设备属性' section includes fields for 'Root 文件夹设备组' and 'Root 文件夹流量组'. The '用户管理' section includes a checkbox for 'Disable login' and password fields for 'Root 帐户'.

1) NTP 配置

➤ 系统—配置—设备—NTP

用 ntpq -p 命令确认是否与 ntp 同步成功,如果未同步可以尝试重启 ntpd 进程(bigstart restart ntpd)

```
#####  
#####  
[root@ltn1:Active:Standalone] config # ntpq -p  
remoterefidst t when poll reach    delay    offset  jitter  
=====
```

*192.168.11.220	.CDMA.	1 u	32	64	1	0.459	2.529	0.436
172.24.1.105	192.168.11.168	3 u	31	64	1	0.248	1.980	0.344

```
#####  
#####
```

命令 nc 测试 udp 123 端口是否可达

```
#####  
#####  
[root@ltn1:Active:Standalone] config # nc -u 192.168.11.220 123  
aaa  
^C  
[root@ltn1:Active:Standalone] config #  
#####  
#####
```

2) 建立 HA 步骤

a) 完成基础网络配置, 包括 VLAN, SELF IP。Floating IP 完成 HA 配置之后再添加。我这里用的例子:

HA VLAN: 1.1.1.1(LTM1) 1.1.1.2(LTM2)

Port Lockdown 选择 allow default, traffic-group 选择 local-only

网络 » 新建 Self IP...

名称	1.1.1.1
IP 地址	1.1.1.1
网络掩码	255.255.255.0
VLAN/通道	vlan_ha
Port Lockdown	Allow Default
流量组	☐ 从当前分区/路径继承流量组 traffic-group-local-only (non-floating)
服务策略	无

取消 重复 完成

- b) 测试 NTP Server 的连通性，并添加 NTP
- c) 在 2 台设备上分别选择设备管理 » bigip1 ConfigSync 选择用来做 configsync 的地址，本例中选择 1.1.1.0/24 的 self IP。

主机名: bigip1 IP 地址: 11.0.0.196 日期: Mar 23, 2020 时间: 11:13 PM (PDT) 用户: admin 角色: Administrator 分区: Common

在线 (ACTIVE) Standalone

主菜单栏 帮助 关于

统计信息 iApps DNS 本地流量 加速 设备管理 概览 设备 设备组 设备信任 流量组 Shared Objects 网络 系统

设备管理 » bigip1

属性 ConfigSync 故障切换网络 镜像

ConfigSync 配置

本地地址: None

更新

- d) 在 2 台设备上分别选 >> 设备管理 » bigip1 故障切换选择用来做 Failover 的地址，本例中选择 1.1.1.0/24 的 self IP 和管理口地址（强烈建议把管理口加入 failover 中）

设备管理 » bigip1

属性 ConfigSync 故障切换网络 镜像

管理故障切换配置

地址系列模式: IPv4 和 IPv6

故障切换配置

本地地址	端口	VLAN
管理地址	1026	管理地址
1.1.1.1	1026	vlan_ha

删除

故障切换多播配置

使用故障切换多播地址: ☐ 启用

更新

- e) 如果有连接镜像或会话保持镜像配置 >> 设备管理 >> bigip 镜像 地址，否则跳过此步

Loading...

Receiving configuration data from your device.

设备管理 >> bigip1

属性

ConfigSync

故障切换网络

镜像

镜像配置

主本地镜像地址	1.1.1.1 (vlan_ha) ▼
次要本地镜像地址	None ▼

更新

- f) 在 2 台设备上分别选择 >>设备管理 >> 设备信任：设备信任成员,添加对端设备。

设备管理 >> 设备信任

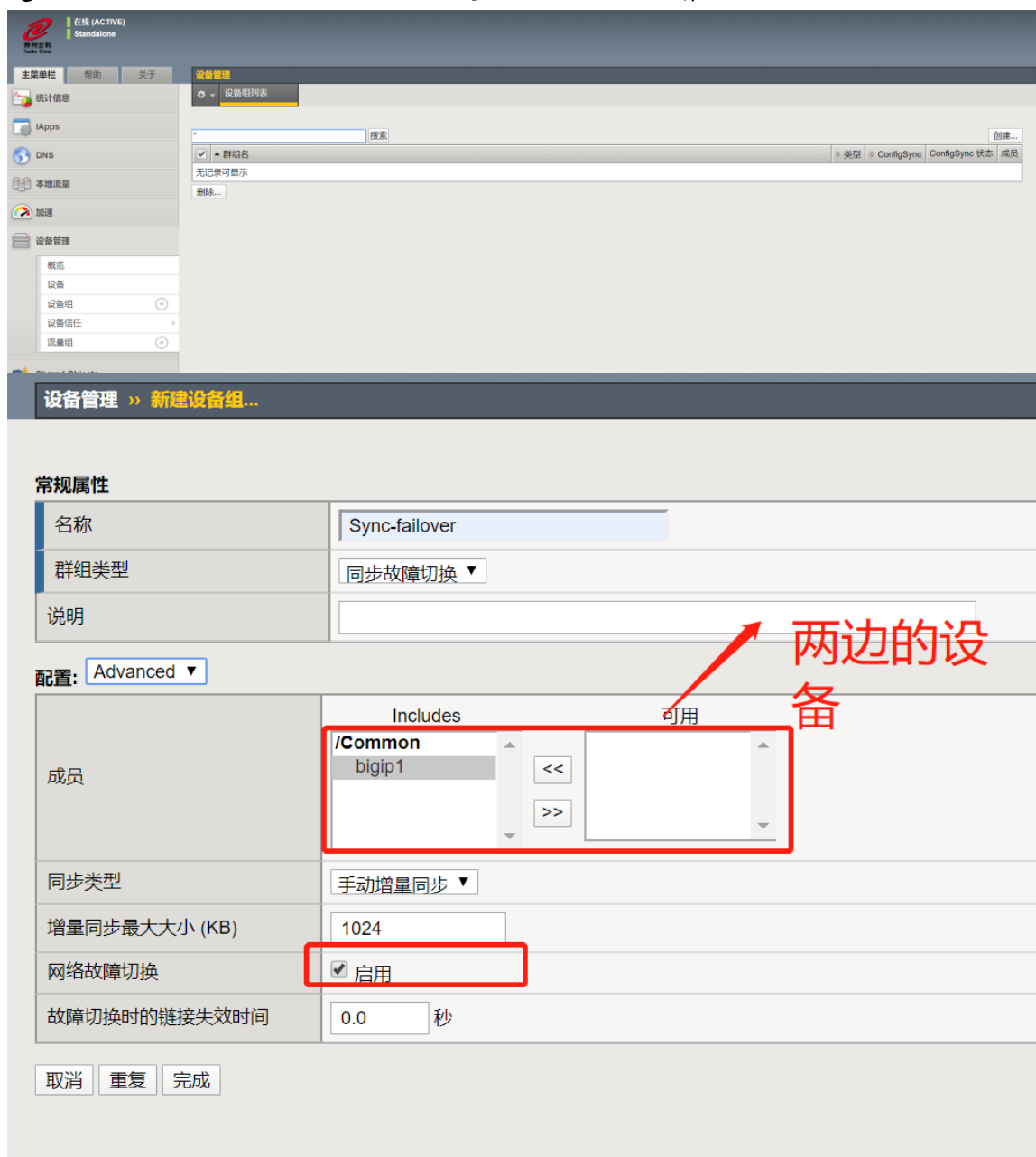
检索设备证书 (第 1 步, 共 3 步)

设备类型	对端 ▼
设备 IP 地址	1.1.1.2
超级管理员用户名	admin
超级管理员密码	

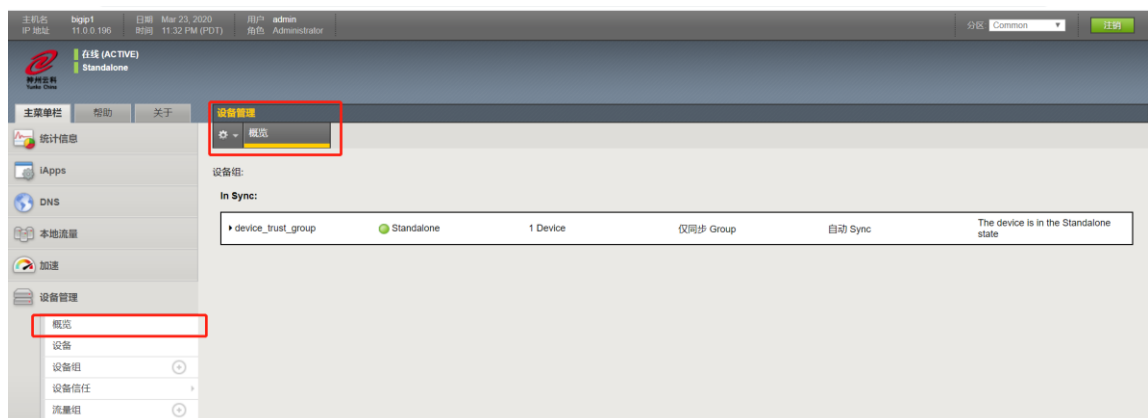
取消

检索设备信息

- g) 在 ltm1 和 ltm2 上分别查看 设备管理，要能够看 到对方的 主机名 r 和 Mac，如看不 到这些信息，可以在看不到对端信息的 设备上手动添加，或者 reset device trust 重加。
- h) 建 立 设 备 组



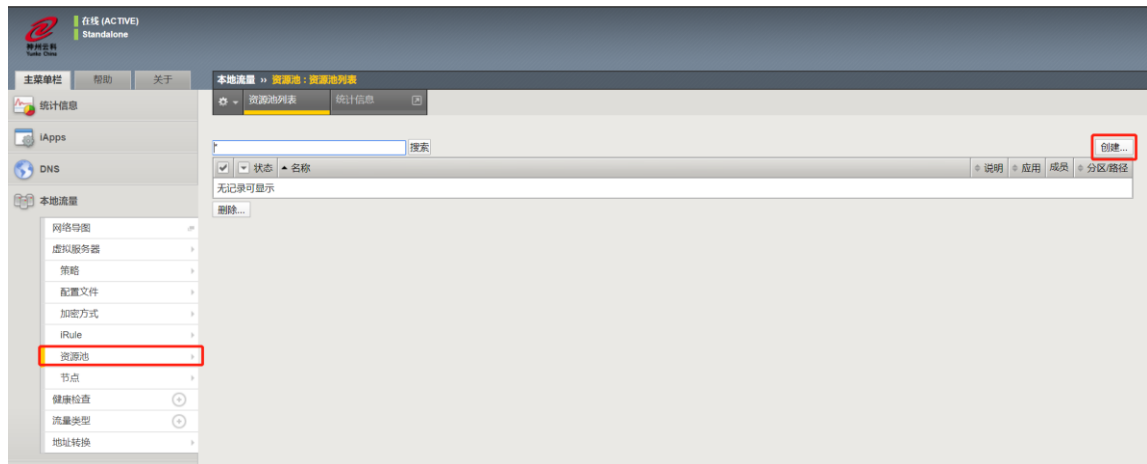
至此。HA 建立完成。在设备管理>>概览处同步主备（应该显示同步组信息）



5. 应用配置

1) 配置 资源池（提供相同服务的服务器群）

- 点击本地流量选项卡中的 资源池选项,在右侧菜单栏中选择建立新的 资源池



- 为资源池 池定义名称、健康检查方式、负载均衡算法以及成员。点击 Finished 完成

本地流量 » 资源池：资源池列表 » 新建资源池

配置: Basic

名称	
说明	
健康检查	Active 可用 << >> /Common gateway_icmp http http_head_f5 https

资源

负载均衡算法: **轮循**

优先级组激活: 禁用

新成员

☒ 新节点 ☐ 新 FQDN 节点

节点名称: (可选)
 地址:
 服务端口: 选择...

添加

节点名称	地址/FQDN	服务端口	自动填充	优先级
No members to display.				

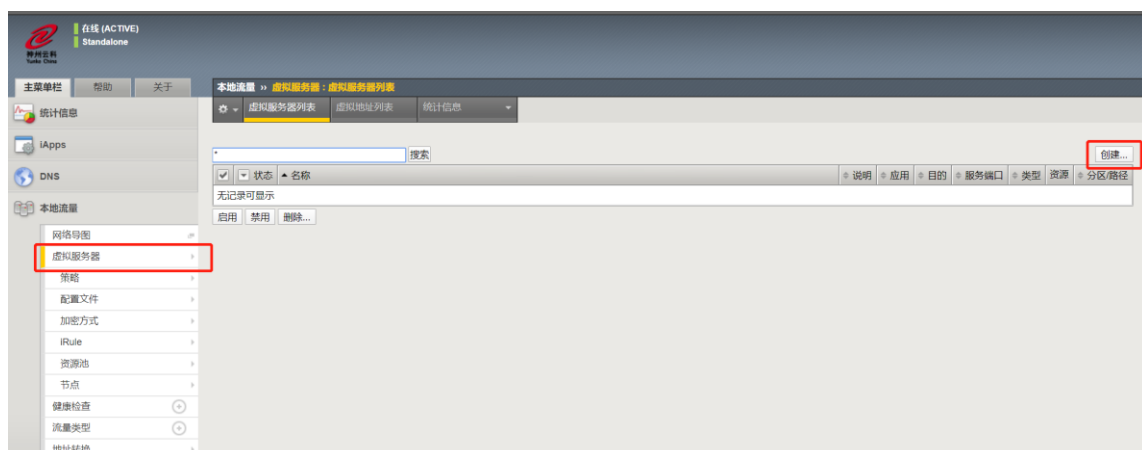
编辑 删除

取消 重复 完成

- ◆ 常用负载均衡算法：
Round Robin<轮询>:YK 将客户端请求按照轮询的方式分发到后台所有成员(服务器)
Least Connections (member) <最小连接数>: YK 监控后台所有 r 成员当前连接 数，将新的请求分配到当前连接数最小的服务器上
- ◆ 常用健康检查方式：
gateway_icmp: YK 向后端服务器发送 ping 测试，以确定服务器是否正常 tcp:
YK 与后端服务器建立三次握手，若成功则确定服务器为正常
http: YK 向后端服务器发生发送 HTTP GET 请求，根据服务器是否响应来确定服务器是否正常

2) 配置虚拟服务器（对外提供服务）

- 点击 本地流量选项卡中的虚拟服务器选项，在右侧菜单栏中选择建立新的 虚拟服务器



- 为虚拟服务器进行详细设置，点击 配置 处的下拉菜单，将 Basic 改选为 Advanced 以进行详尽的设置

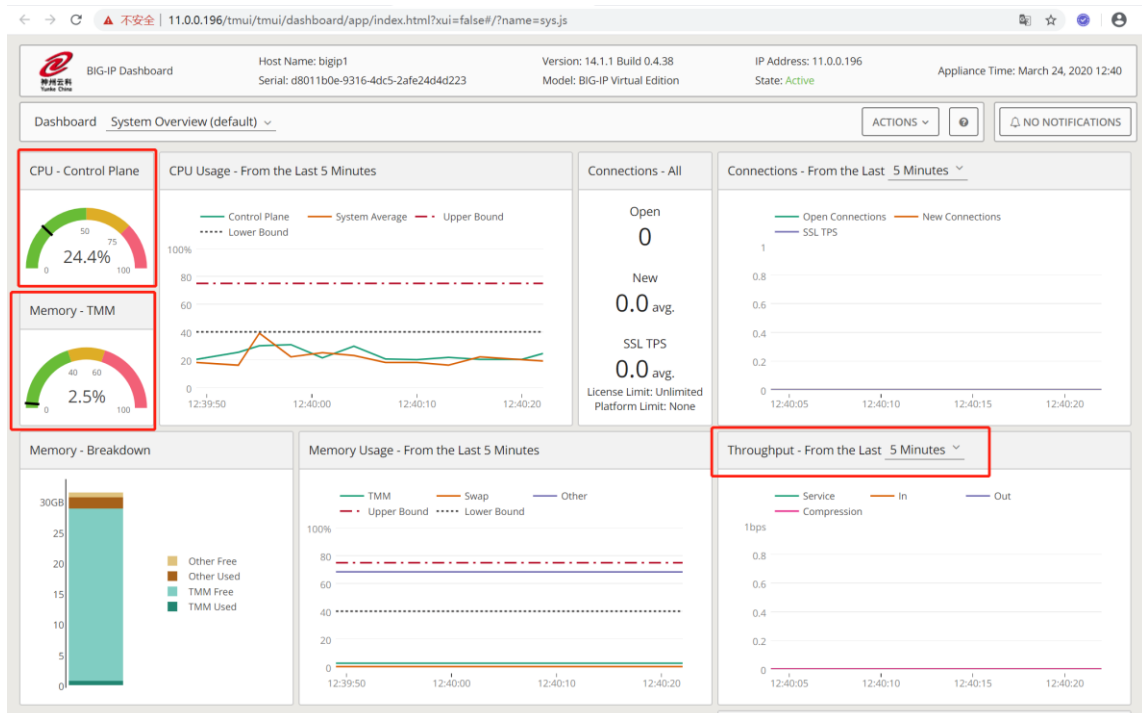
配置: **Advanced** ▼

协议	TCP ▼
协议配置文件 (客户端)	tcp ▼
协议配置文件 (服务器)	(使用客户端配置文件) ▼
HTTP 配置文件 (客户端)	无 ▼
HTTP 配置文件 (服务器)	(使用客户端配置文件) ▼
HTTP 代理连接配置文件	无 ▼
FTP 配置文件	无 ▼
RTSP 配置文件	无 ▼
SOCKS 配置文件	无 ▼
流配置文件	无 ▼
XML 配置文件	无 ▼
MQTT	☐
SSL 配置文件 (客户端)	已选 可用 << >> /Common clientssl clientssl-insecure-compatible clientssl-secure crypto-server-default-clientssl
SSL 配置文件 (服务器)	已选 可用 << >> /Common apm-default-serverssl crypto-client-default-serverssl pcoip-default-serverssl serverssl
认证配置文件	启用 可用 << >> /Common ssl_cc_idap ssl_cridp ssl_ocsp

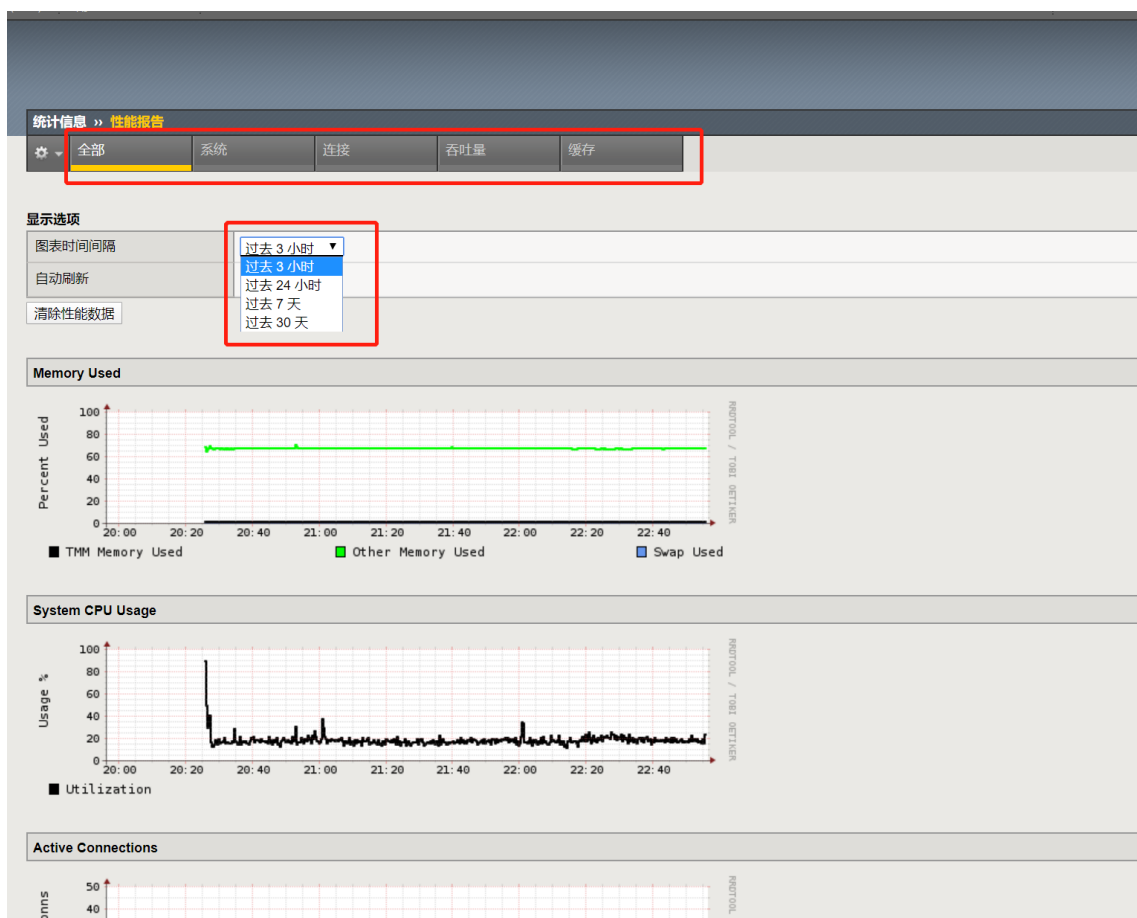
根据提供的不同应用服务而对应进行 虚拟服务器 的配置。

6. 状态察看

1) 仪表盘



2) 性能报告



7. 故障采集

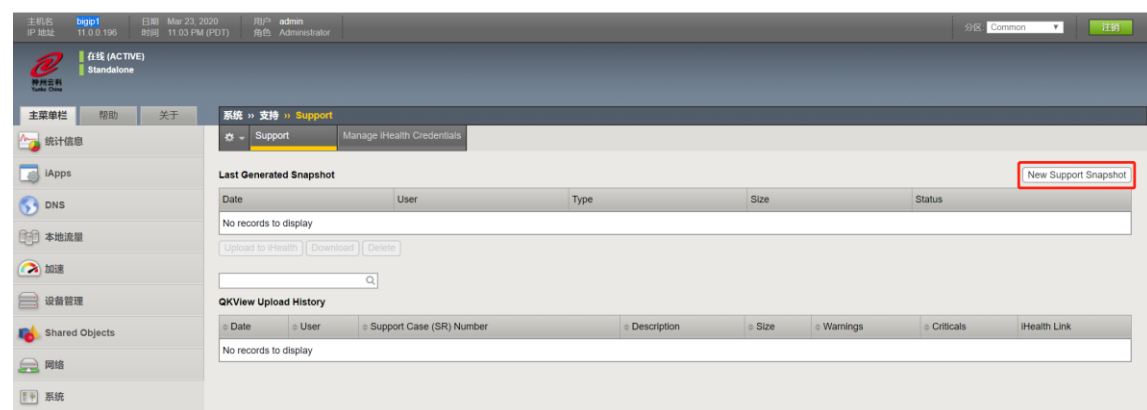
1) 寻求 YK 技术支持时，要提供哪些信息与资料？

一般来说,如果要寻求 YK 的技术支持(不论是 YK 第三方技术支持中心或 YK 全球技术支持中心),都要准备以下信息:

- 产品序列号(在 BIG-IP 机架安装耳朵的边上以 YK-开头的字符串),产品序列号是判断设备是否在 服务有效期内;
- Qkview 输出文件: 里面包含了 BIG-IP 的配置信息及日志信息。如果是双机,则两台机器的 qkview 输出文件都需要提供;
- 故障描述;
- 如果必要,还需要提供 TCPDUMP 的抓包文件,并指出数据包异常现象;
- 如条件允许,对技术支持人员开放远程访问权限。

2) 获取 Qkview 的方式

- 系统—支持



- 只勾选 QKView, 点击 Start

系统 » Support

Support

Manage iHealth Credentials

Support Snapshot

Health Utility

Generate and Upload QKView to iHealth
Generate and Upload QKView to iHealth
Generate QKView
Generate ICPDump

Upload Configuration

iHealth Credentials

☐ Use the iHealth credentials saved on this BIG-IP

☒ Use my iHealth credentials

iHealth User ID

iHealth Password

☐ Show password

QKView Options

☐ Exclude Audit Files

☐ Exclude Core Files

☐ Exclude Secure Files

☐ Exclude Bash History

☐ Unlimited snaplen

Support Case (SR) Number

Description

0/100 Characters

Cancel

Start

点击 start

系统 » Support

Support

Manage iHealth Credentials

Support Snapshot

Health Utility

Generate QKView

Upload Configuration

QKView Options

☐ Exclude Audit Files

☐ Exclude Core Files

☐ Exclude Secure Files

☐ Exclude Bash History

☐ Unlimited snaplen

Cancel

Start

●、下载到本地

主机名
IP 地址

2020
T1 0 0 196

日期
时间

Mar 23, 2020
11:07 PM (PDT)

用户
角色

admin
Administrator

分区
Common

注册

在线 (ACTIVE)
Standalone

主菜单
帮助
关于

系统
Support
Manage iHealth Credentials

统计信息
iApps
DNS
本地流量
加速
设备管理
Shared Objects
网络
系统
配置
文件管理

Complete
A QKView was successfully generated.
00:02:19 Total Elapsed Time

Last Generated Snapshot
New Support Snapshot

Date	User	Type	Size	Status
03/24/2020 2:07PM	admin	qkview	33.6 Megabytes	Generated

Upload to iHealth Download Delete

QKView Upload History

Date	User	Support Case (SR) Number	Description	Size	Warnings	Criticals	iHealth Link
No records to display							

