

VCFC 安全纳管方案Context配置无法下发的经验案例

VCFC 安全纳管 王鹤1 2017-07-18 发表

通过云平台或者VCFC创建好Context之后，发现Context配置没有下发下去。

查看VCFC集群与Region是否正常

安全纳管方案涉及云平台、VCFC产品、硬件安全设备以及硬件交换机，Context由上层云平台下发API至VCFC，再由VCFC与设备交互。排查Context无法创建时，需要自上而下排查，从云平台开始，再到VCFC，再排查硬件安全设备，其排查思路如下：

安全纳管方案的Context配置需要控制器通过Netconf下发。确保VCFC集群和Region状态正常是排查Context无法创建问题的第一步。

如下图，在VCFC web页面的【控制器-控制器信息】内，查看各台控制器的集群状态都为active，且已选举出主Leader（集群配置角色为Leader*）。

The screenshot shows the 'Controller / Controller Information' page. Under 'Cluster Information', the 'Current Leader Controller IP' is 99.1.1.21. Under 'Controller Information', a table lists three controllers with their IP addresses, roles, and status. The controller with IP 99.1.1.21 is the Leader* and is active.

IP	控制器名称	集群配置角色	Region	Region成员...	优先级	集群网卡	主OpenFl...	总OpenFl...	集群状态	配置校验...	Region连通性	packet-in速率	备注
99.1.1.22	22	Leader	Region	Master	888888	eth0	6	8	active	true	●	○	---
99.1.1.23	23	Leader	Region	Subordinate	777777	eth0	2	8	active	true	●	○	---
99.1.1.21	21	Leader*	---	---	999999	eth0	0	0	active	true	---	○	---

如果集群状态为inactive，或无法选举出主Leader，请参考【VCFC集群无法建立问题排查云图】进行排查。

如果集群状态为active，且已选举出主Leader，则排查Region状态是否正常。

可以在控制器的[控制器-控制器信息]中，查看是否存在Region配置。

The screenshot shows the 'Controller / Controller Information' page for a specific controller. Under 'Controller Information', the 'Region' dropdown is set to 'Region1'. A table below shows the configuration for Region1, including its members and their roles.

IP	控制器名称	集群配置角色	Region	Region成员...	优先级	集群网卡	主OpenFlow...	总OpenFlow...	集群状态
99.1.1.23	23	Leader	Region1	Subordinate	23	eth0	5	12	active
99.1.1.22	22	Leader	Region1	Master	123	eth0	7	11	active
99.1.1.21	21	Leader*	---	---	999999	eth0	0	0	active

如上图，如果Region一栏中没有任何已创建的Region，则可以在[控制器-控制器配置-创建Region]路径中手工创建。

The screenshot shows the 'Controller / Controller Configuration / Create Region' page. It includes fields for 'Region Name', 'Main Controller', and 'Backup Controller', and a radio button for 'Prohibit vSwitch Access'.

* Region名称:

* 主用控制器:

* 备用控制器:

禁止vSwitch接入: 是 否

如果已创建的Region中，没有一台控制器状态为active，则请先排查控制器集群状态是否正常。

本案例中，经检查确认Region状态正常，问题仍旧无法解决，因而进入步骤二继续排查。

查看控制器上是否已经成功创建出Context

如果确认控制器集群和Region正常，下一步需要确认Context是否成功创建，需要在设备和VCFC侧都进行确认。

如下图，在控制器的【承载网络-虚拟网元-NGFW资源】内查看对应租户是否成功创建Context：

承载网络 / 虚拟网元 / NGFW资源

VNF资源 NGFW资源 VTEP地址池

所有租户 资源名称 资源ID 租户 类型 资源节点列表

资源名称	资源ID	租户	类型	资源节点列表
xxx	6fcea34-91db-471f-9230-6ef995440...	wh	vFW	VFW_5707268031

如下图，在安全设备上使用命令display context确认对应Context是否创建成功：

```
[M9K]dis context
ID      Name                Status      Location      Description
1       Admin                 active     All CPUs     DefaultContext
2       VFW_5033572236      active     5.1          ngfwm_context
4       VFW_5707268031     active     5.1          ngfwm_context

Total contexts:3
[M9K]
```

如果发现Context无法正常创建，则请参考《安全纳管方案Context无法创建问题排查云图》进行排查。

本安装中，经检查确认Context已经创建成功，但问题依旧，因而进入步骤三继续排查。

确认VCFC上是否注册了足够的License

对于安全纳管方案来说，一个Context需要占用一个虚拟服务节点License、一个OpenFlow节点License，以及BAS、Overlay等基础功能License。需要特别注意的是，安全纳管方案需要Service-Chain License可用，否则将无法创建新的Context。

请于控制器的【控制器-License管理-远端License】查看Service-Chain License是否可用。

控制器 / License管理 / 远端License

远端License 本地控制器License 本地vSwitch License

License server 信息

License server IP地址 99.1.1.21 端口号 5555 断开连接

用户名 h3c 密码 ...

连接状态: 连接成功

License状态

产品功能	已使用数/已获许可数	可用状态	申请数量
APP	...	试用(剩余167天)	all
OpenFlow节点	...	试用(剩余167天)	all
虚拟服务节点	...	试用(剩余167天)	all
vSwitch	...	试用(剩余167天)	all
ZTP	...	试用(剩余167天)	true
API	...	试用(剩余167天)	true
Overlay	...	试用(剩余167天)	true
Overlay硬件网元	...	试用(剩余167天)	all
Service-Chain	...	试用(剩余167天)	true
控制器	...	试用(剩余167天)	all

如上图，Service-Chain为试用，因而不会影响Context的创建。

如果确认缺少License，请扩容License。

如果确认License正常，而问题依旧，则进入步骤四继续排查。

登录到Context，确认管理IP是否下发

当创建Context成功后，VCFC会通过Leader*自身的IP去Telnet硬件安全设备，并且通过CLI登录到Context，下发管理IP。

如果发现Context已经创建成功，但管理IP未下发，请进入步骤五继续排查。

如果发现Context已经创建成功，且管理IP已下发，如问题依旧，则进入步骤八继续排查。

确认VCFC与硬件安全设备是否IP可达

如果管理IP未下发，需要确认VCFC的Leader*控制器，其自身的IP是否能与硬件安全设备IP可达，如果不可达，VCFC将无法登录到硬件安全设备以及对应的Context上。

本案例中，确认IP可达，因而进入步骤六继续排查。

确认硬件安全设备的Telnet账号和服务是否正常

Context创建时，VCFC的主Leader会通过自身的IP（而非集群IP）与硬件安全设备进行通信，其中最重要的一步就是通过主Leader本身的IP来Telnet到硬件安全设备，并下发CLI命令，登录到Context，配置管理IP。如果存在以下几种情况，则管理IP无法下发，某些时候Context会创建失败：

- 硬件安全设备没有开启Telnet Server服务。
- VCFC集群主Leader自身的IP与硬件安全设备不可达或Telnet端口不通。
- 在VCFC的【承载网络/NGFW Manager/设备】中添加安全设备时，填写的账号没有配置Telnet服务类型或者该账号没有admin权限，如下图，需要保证可以使用h3c账号正常Telnet登录。



本案例中，确认以上步骤无误，因而进入步骤七继续排查。

Context管理IP是否与VCFC互通

当Context管理IP成功下发后，下一步则是VCFC通过Netconf协议给Context下发配置。此时需要首先保证VCFC Leader*本身的IP能与Context的管理IP互通。

如无法互通，则需要具体排查丢包在何处，再具体排查。

如果确认以上无误之后，配置依旧无法下发，则进入步骤八继续排查。

是否将服务资源绑定至虚拟路由器

对于安全资源而言，需要将创建好的Context绑定至指定的虚拟路由器，控制器才会向虚拟路由器绑定的服务网组申请IP资源和VLAN资源。资源申请完毕后，再将资源转换为配置给Context下发。

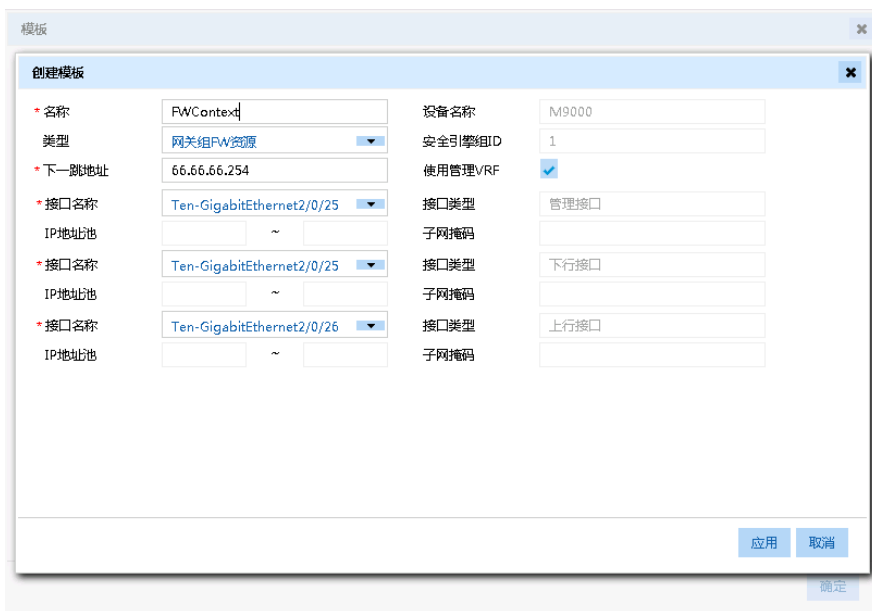
故如果Context上只有管理IP，且管理IP能与VCFC Leader*自身IP可达，则需要在VCFC的【虚拟网络-虚拟路由器-服务资源】确认，Context对应租户的虚拟路由器上，是否绑定了服务资源，如下图：



本案例中，确认虚拟路由器已绑定正确的Context服务资源，问题依旧，因而进入步骤九继续排查。

模板是否配置正确

当服务资源已经与虚拟路由器绑定，且IP可达之后，下一步则是读取模板配置，结合申请的IP资源和VLAN资源给Context下发配置。此处需要注意，模板里面的上下行口以及管理口需要提前规划好，避免由于规划错误或配置错误，导致Context下发配置的接口与规划不一致。



如上图，需要确认模板类型为网关组资源。且需要配置下一跳地址为虚拟设备管理网网关地址。上图中，66.66.66.254为虚拟设备管理网网关，该地址需要手工配置在IP GW上，Context通过在主接口下发66.66.66.0/24网段的管理IP，以及下发指向VCFC下一跳是66.66.66.254的静态路由，来使得Context与VCFC管理网互通，从而再通过Netconf给Context下发配置。

确认服务网关组的IP资源和VLAN资源是否已经用尽

Context需要使用的IP资源和VLAN资源由租户首先在服务网关组内预留，如果没有预留或资源已耗尽，则新的Context无法申请到足够的资源，会引起配置无法下发完整，某些时候还会引起创建Context失败。

可以在控制器的【承载网络-网关组-地址池】内确认预留IP资源总数：

名称	类型	网络地址	网关地址	状态	操作
租户承载网	租户承载网	66.66.67.0/24	---	In use	ⓘ ⊗
安全外网	安全外网	66.66.69.0/24	66.66.69.254	In use	ⓘ ⊗
管理网	虚拟设备管理网	66.66.66.0/24	66.66.66.254	In use	ⓘ ⊗
安全内网	安全内网	66.66.68.0/24	---	Ready	ⓘ ⊗

可以在控制器的【承载网络-网关组-地址池】内确认预留VLAN资源总数：

名称	起始值	结束值	状态	操作
VLAN_Range	300	600	In use	ⓘ ⊗

对于安全纳管方案来说，FW/LB Context都需要IP资源和VLAN资源。当租户拥有的Context情况不同时，占用的资源数不同，具体分为以下几类：

- A. 当某个租户只有一个FW Context而没有LB Context时，需要占用租户承载网两个IP资源；需要占用安全外网、虚拟设备管理网各一个IP资源，且占用一个VLAN资源。
- B. 当某个租户只有一个LB Context而没有FW Context时，需要占用租户承载网两个IP资源、虚拟设备管理网一个IP资源，且占用一个VLAN资源。
- C. 当某个租户既有FW Context也有LB Context时，需要占用租户承载网三个IP资源；需要占用安全内网和虚拟设备管理网各两个IP资源；需要占用安全外网一个IP资源；且占用两个VLAN资源。

可以进入到控制器的【承载网络-虚拟网元-NGFW资源】查看，确认使用该服务网关组的所有租户，其一共占用的IP资源数和VLAN资源数是否已经达到最大值。如果资源不足，会引起配置下发不完整。例如，虚拟资源管理网、安全内网、安全外网资源足够，而租户承载网IP资源不足，此时创建的Context无法下发租户承载网IP，但其余IP以及VLAN等配置正常下发。

如果已经达到最大值，则需要进行扩容。

本案例中，发现VLAN资源数仍旧足够，而租户承载网IP已用尽，因而租户承载网IP无法下发，从而定位问题。

安全纳管Context配置无法下发问题，大多数情况下还是配置以及资源不足造成的。遇到问题时需细心排查，建议提前规划好IP、VLAN资源，提前设计好组网连线，避免不必要的问题。