第 14 章 重要服务

14.1 pvedaemon – Proxmox VE API 守护进程

该守护进程在 127.0.0.1:85 上提供了 Proxmox VE API 的调用接口。该进程以 root 权限运行，能够执行所有特权操作。

- 注意

  该守护进程仅监听本地地址，外部无法直接访问。守护进程 pveproxy 负责向外部提供 API 调用接口。

14.2 pveproxy – Proxmox VE API 代理进程

该进程通过 HTTPS 在 TCP 8006 端口向外部提供 Proxmox VE API 调用接口。该进程以 www-data 权限运行，因此权限非常有限。更高权限的操作将由本地的 pvedaemon 进程执行。

指向其他节点的操作请求将自动发送到对应节点，也就是说你可以从 Proxmox VE 的一个节点管理整个集群。

14.2.1 基于主机的访问控制

可以为 pveproxy 配置类似于“apache2”的访问控制列表。相关访问控制列表保存在 /etc/default/pveproxy 中。例如：

ALLOW_FROM="10.0.0.1-10.0.0.5,192.168.0.0/22"

DENY_FROM="all"

POLICY="allow"

IP 地址可以用类似 Net::IP 的语法指定，而 all 是 0/0 的别名。

默认策略是 allow。

匹配情况	POLICY=deny	POLICY=allow
仅有 Allow 匹配上	允许访问	允许访问
仅有 Deny 匹配上	拒绝访问	拒绝访问
均未匹配上	拒绝访问	允许访问
同时匹配到 Allow 和 Deny	拒绝访问	允许访问

14.2.2 SSL 加密套件

可以在配置文件/etc/default/pveproxy 中指定加密列表。例如：

CIPHERS="HIGH:MEDIUM:!aNULL:!MD5"

以上是默认配置。可以查看 openssl 软件包中的 man 页面 ciphers(1)获取更多可用选项。

14.2.3 Diffie-Hellman 参数

可以在配置文件/etc/default/pveproxy 中指定 Diffie-Hellman 参数。只需将参数 DHPARAMS 设置为包含 DH 参数的 PEM 文件路径即可。例如：

DHPARAMS="/path/to/dhparams.pem"

如未设置该参数，将使用内置的 skip2048 参数。

- 注意

  DH 参数仅在协商使用基于 DH 密钥交换算法的加密套件时有效。

14.2.4 其他 HTTPS 证书

默认情况下，pveproxy 使用证书文件/etc/pve/local/pve-ssl.pem（以及私钥 /etc/pve/local/pve-ssl.key）进行 HTTPS 连接。该证书由集群 CA 签发，因此默认不被外部浏览器和操作系统信任。

如需使用其他证书和私钥进行 HTTPS 连接，可将服务器证书和其他所需的中间/CA 证书以 PEM 格式保存在/etc/pve/local/pveproxy-ssl.pem，同时将相关私钥以无口令的 PEM 格式文件保存在/etc/pve/local/pveproxy-ssl.key。

☒ 警告

不要用其他文件覆盖替换系统自动生成的证书/etc/pve/local/pve-ssl.pem 和私钥 /etc/pve/local/pve-ssl.key，也不要覆盖替换集群 CA 文件/etc/pve/pve-root-ca.pem 和私钥/etc/pve/priv/pve-root-ca.key。

➢ 注意

在 wiki 上有配置商业 HTTPS 证书的详细步骤。包括从免费的 Let's Encrypt 证书站点获取安装证书的具体命令。

14.3 pvestatd – Proxmox VE 监控守护进程

该守护进程定时获取虚拟机、存储和容器的状态数据。结果将自动发送到集群中的所有节点。

14.4 spiceproxy – SPICE 代理进程

SPICE（Simple Protocol for Independent Computing Environments）是一个开源远程计算解决方案，能够为远程桌面和设备（例如键盘、鼠标、音频）的提供客户端访问接口。主要使用场景是访问远程虚拟机和容器。

该守护进程监听 TCP 3128 端口，并通过 HTTP 代理将 SPICE 客户端的连接请求转发给相应的 Proxmox VE 虚拟机。该进程以 www-data 权限运行，权限非常有限。

14.4.1 基于主机的访问控制

可以为 spice 配置类似于“apache2”的访问控制列表。相关访问控制列表保存在 /etc/default/pveproxy 中。详情可查看 pveproxy 文档。