麒麟 v10 kylin v10 清除 firewall所有策略恢复原始

你这个报错是正常的，因为：

> ❌ `firewall-cmd --reset-default-zone` 在 firewalld 里根本不存在这个参数

（很多网上资料是错的或旧版本误传）

✅ 你现在真实状态分析

你的 `public zone` 已经是：

```
sources: 10.2.2.0/24   ← 关键
ports: 一大堆已开放
masquerade: no
```

说明：

✔ 已经是“默认状态”

而是：

> ⚠ zone 被人工改造过（不是 reset 可恢复）

□□ □□ “□□□□□ ”□□□ Kylin V10 □□□

□ □□ 1□□□□□□ zone + □□□□□

1□ □□□ ports

```
for p in 80 443 8070 20881 8082 20853 8086 20835 4443; do
  firewall-cmd --permanent --zone=public --remove-port=${p}/tcp
done
```

2□ □□ source□□□

□□□□□

```
sources: 10.2.2.0/24
```

□□□

```
firewall-cmd --permanent --zone=public --remove-source=10.2.2.0/24
```

3□ □□ ssh / □□□

```
firewall-cmd --permanent --zone=public --add-service=ssh
```

4□ reload

```
firewall-cmd --reload
```

□ □□ 2（最干净）：删除 public zone 配置文件

如果你想 “一键回出厂默认 ”，用这个：

```
systemctl stop firewalld

rm -f /etc/firewalld/zones/public.xml

systemctl start firewalld
```

□□ 这会让 firewalld 自动重建默认 public zone

□□ □□ 3（推荐生产）：重新初始化 firewalld

```
systemctl stop firewalld
rm -rf /etc/firewalld
yum reinstall firewalld -y   # 或 dnf
systemctl start firewalld
```

□□ 最彻底（等同 “恢复出厂设置 ”）

⚠ 你现在最关键问题其实是这个

```
sources: 10.2.2.0/24
```

这意味着：

> □□□ firewall 已经被改成 “只信任内网网段 ”

所以表现会是：

- 外部访问异常
- 端口行为不一致
- Docker + firewalld 混乱

□□ □□□□□

操作	是否有效
reset-default-zone	□ □□□
remove-port + reload	✔ 部分恢复
删除 zone XML	✔ 推荐
重装 firewalld	✔ 最彻底

□□

建议你下一步做这个（最稳）

如果你是生产环境：

□□ 我建议直接做：

```
rm -f /etc/firewalld/zones/public.xml
systemctl restart firewalld
```

然后再重新只加:

- ssh
- 需要暴露的 80/443

如果你愿意，我可以帮你把你这台:

> “ 麒麟 V10 + Docker + 多微服务

整理成一套:

✔ 不互相冲突
✔ DOCKER-USER 控制流量
✔ firewalld 只做基础保护
✔ 不会再出现 “规则失效 / 端口混乱 ”

这类结构才是稳定生产配置。

Revision #1
Created 2026-05-12 07:32:43 UTC by Admin
Updated 2026-05-12 07:33:24 UTC by Admin