

# 深证云使用规范

深圳证券通信有限公司

二〇二三年十二月

## 第一章 前言

为了规范用户使用深证云相关资源，保障深证云平台系统的安全运行，根据《证券期货业网络和信息安全管理办法》、《证券投资基金经营机构信息技术管理办法》及行业相关规定，特制定本规范。

本规范适用于深证云的用户资源申请与使用，适用于 IT 基础资源外包服务、灾备服务等业务，以及可用性要求高于 99% 的业务。若用户未遵循本规范，所造成的影响自行承担。

## 第二章 云资源总体使用规范

1. 用户应负责深证云租户层面资源及操作系统的监控与日常运维，包括查看控制台、开关机、重启、监控等操作，深证通负责深证云平台层面的监控、交付等日常运维操作，不介入租户层面操作。

2. 用户负责深证云租户资源与应用系统的安全与防护。深证通负责深证云平台层面的安全与防护。

3. 用户应通过深证云运营支撑系统申请资源，此系统的账号可联系客户经理获取。

4. 用户应妥善管理云资源容量与使用率，有扩容需要时应提前申请，以避免产生负载过高或容量不足的风险。

5. 禁止工作日在深证云平台进行压力测试。其他时间段如需压测，请提前联系深证通。

6. 禁止工作日在深证云平台进行安全扫描及渗透。其他时间段如需进行，请提前联系深证通。

### 第三章 云主机使用规范

1. 用户应妥善保存好云主机密码、深证云 VPN 账户密码及 Ekey 等。

2. 不允许卸载或修改云主机内置的驱动程序。

3. 不允许修改云主机网卡的 MAC 地址。

4. 不允许使用云主机进行二次（嵌套）虚拟化。

5. 不允许修改主机默认的主网卡网络配置信息（IP、子网掩码及网关地址），否则可能会导致网络异常。

6. 不建议修改、停用云主机的远程连接服务功能，防止无法远程操作云主机。

7. 用户应自行部署监控系统对云主机、云硬盘、云网络等资源进行监控。

8. 用户应为部署核心关键业务的云主机做好定期数据备份，并将数据备份导出到云外环境，定期校验备份的有效性。

9. 用户创建云主机的最低配置是 2 CPU 核、2g 内存、50G 标准性能的云系统盘。以保障用户业务系统的正常运行。

## 第四章 Windows 操作系统使用规范

1. 用户不应强行结束系统级别的进程，否则可能会导致主机发生蓝屏、重启。

2. 用户应保留 2G 以上的空闲内存供操作系统使用，否则在使用过程中可能会出现蓝屏、卡顿、服务无法正常运行等情况。

3. 用户不应修改注册表，修改注册表可能会导致系统启动失败。

4. 用户不应关闭虚拟内存，关闭虚拟内存可能会使系统性能降低或运行异常。

5. 用户应妥善保管云主机密码，Windows 的密码无法通过后台重置。

6. 做域控、文件服务器、邮件服务器、数据库服务器的主机，应至少使用高性能云盘，专业存储盘为佳，配置不低于 16 核 32g。

## 第五章 Linux 操作系统使用规范

1. 用户不应删除系统目录或文件，否则可能导致系统无法正常运行或启动。

2. 除非确有需要且验证可行，否则请勿随意升级 Linux 操作系统的内核。

3. 不允许修改涉及/etc/fstab 相关的内容，避免导致无

法启动云主机。

4. 若加挂云硬盘（数据盘）至云主机，用户不应将云硬盘与云主机自带的系统盘整合做为同一个 LVM 卷，以避免发生异常时影响操作系统，导致无法启动。

5. 加挂数据盘的容量建议保持一致大小，以保证最优性能。

6. 不允许修改/etc/issue 文件内容，否则可能导致系统发行版本无法被识别。

7. 不允许修改系统目录的权限或名称，否则可能导致系统无法正常运行或启动，或产生大量无法找到关键系统文件的报错。

8. 使用外网或深证通 YUM 服务器升级软件包时，注意确认 YUM 提供的软件与关联依赖包的版本。

9. 进行大量文件读写任务或处理大量连接的服务器，建议将[/etc/security/limits.conf]中的 soft/hard nproc 及 soft/hard nofile 参数调到合适数值，或直接修改“max open files”、“max user processes”的数值。

## 第六章 网络使用规范

1. 深证云 Openstack 网络由深证通规划与管理，遵循以下原则：

① 每一个租户默认配置如下两个网络区域：

DMZ 区：又称互联网访问区，此区域的云主机能与互联网通信；互联网应用云主机应创建在 DMZ 区，如常见应用网站、网上交易系统等。

CORE 区：又称为核心区，此区域的云主机无法与互联网通信，可与核心机构互联；核心应用云主机应创建在 CORE 区。

②租户同一网络区域内主机默认可相互通信，不同网络区域的主机默认不可互联。如需要开通互联，请通过深证云业务支撑系统申请办理或联系我司。

2. TCE 平台的网络由用户自行规划与管理，应遵循以下原则：

①用户应根据业务系统与业务数据的安全级别，规划不同的网络安全区域进行隔离与保护。禁止将重要核心系统、关键敏感数据直接暴露于互联网。

②云主机如需与深证通网络互联，需规划专用私有网络（VPC），该 VPC 的地址由深证通分配，并禁止该 VPC 访问互联网。

③创建私有网络（vpc）网段时，应避免直接使用类似 10.0.0.0/8, 172.16.0.0/12 等大段作为子网，否则会导致该 VPC 由于地址冲突无法通信。

④如需使用云防火墙，每个 VPC 内需预留一段/28 地址，供云防火墙使用。

⑤创建专线通道时，需选为主备冗余模式，并开启 BFD 探测。对端设备需支持多跳 BFD。

⑥用户 IDC 接入 TCE PL 交换机只支持访问本地 VPC 内资源。

⑦如需开展组播业务，需选择标准型专线网关。NAT 型专线网关不支持组播。

## 第七章 云上数据安全规范

1. 用户应定期备份云上配置数据、业务数据等，另存于不同云主机或云外异构存储介质。

2. 对数据可靠性有一定要求、或产生较多数据量的应用系统，建议额外申请数据盘进行存放，并建议将数据的保存路径放在数据盘，防止抢占系统盘性能、或大量数据产生写满分区导致操作系统无法正常运行。

- 对 IO 有一定性能要求的业务场景，如 Windows 域控制器、邮件服务器、文件中转/共享服务器等，建议至少使用高性能云盘。
- 对 IO 性能有强依赖、高并发与高敏感性的使用场景，如数据库、核心业务数据处理应用、报表类应用、数据分析类应用，建议使用专业存储(iSCSI 云盘或 SAN)。
- 需要多台主机共享读写相同文件与文件夹的，建议使用 NAS 类服务。

- 有大量数据存入内存进行缓存、处理、计算的，建议使用大内存云主机。
- 对计算性能、可靠性、稳定性有较高需求的，建议使用裸金属服务器。

## 第八章 云上应用部署规范

1. 用户应向深证通金融云业务部备案其在云上部署的应用系统名称、业务功能、服务时间与服务对象。

2. 禁止在云主机上部署任何违法违规网站和应用（如色情、赌博、诈骗、宣传非法内容等）。

3. 禁止使用云资源从事、参与任何虚拟货币相关的活动，包括但不限于虚拟货币的挖矿、交易、清算、结算等。

4. 对高可用性有要求的应用系统，应采用至少两台主机进行高可用部署，避免出现单点故障。

5. 在 TCE 申请云主机时，对高可用性有要求的，建议勾选“分散放置群组”。

6. 用户应定期备份其关键应用系统配置数据、应用部署包等。

7. 所有运行于深证云主机上的重要服务，建议配置为开机自启动，以实现意外发生宕机、迁移或疏散后，应用能自动启动、恢复服务的效果。

8. 用户应自行为云主机上的应用系统部署监控系统，为

关键系统指标、业务指标做好监控、告警。

9. 重要业务系统，应根据其 SLA 级别，进行跨数据中心高可用部署。

## 第九章 NAS 使用规范

1. 深证云 Openstack 提供 NAS 服务。用户应在申请时明确指定 NFS 版本，如 4.0，防止用户端发生挂载版本问题。

2. NAS 不允许同时挂载给 Windows 与 Linux 主机，防止因协议不同使数据损坏。

3. NAS 不建议同时挂载给 DMZ、CORE 区域服务器，防止病毒或恶意软件蔓延。

## 第十章 云上安全规范

1. 用户应根据《证券期货业信息安全保障管理办法》及行业相关规定，进行安全规划与建设。

2. 用户应为云主机定期及时更新系统补丁、修补安全漏洞，做好安全加固措施。

3. 用户应定期修改深证云云主机操作系统密码，密码长度建议至少为 12 位，且应为数字、大小写字母和特殊符号中至少 3 类的组合。

4. 禁止使用云主机对底层平台或平台上的其他用户资源进行扫描、攻击与破解等行为。禁止利用云主机对外部系

统发起扫描、渗透等探测行为。

5. 禁止使用云主机提供流量穿透服务。

6. 禁止利用云主机搭建爬虫环境，对外部系统发起爬虫搜索。

7. 禁止利用云主机对外部系统发起网络攻击，如：DDoS 攻击、Web 攻击、暴力破解、传播病毒、木马等。

8. 禁止直接向互联网暴露关键端口，包括但不限于：22、23、139、445、3306、3389、1521 等。

#### **附：其他**

1. 用户应及时更新深证通统一客户专区（<https://biz.sccc.com>）和深证通业务支撑系统（<https://account.fincloud.com.cn>）中的联系方式，深证通将根据业务需要向用户联系人发送通知。

2. 根据《网络安全等级保护基本要求》，当深证通通信系统发生网络攻击等重大安全事件时，深证通可采取暂停用户网络接入、关闭用户云资源等应急手段。

3. 联系方式：

联系电话：0755-83182222（7x24 小时）

客服电话：0755-83183333

4. 本规范由深证通负责解释，自发布之日起施行。