2025.03.06泉港云桌面事宜

# 1. 云桌面卡顿

**故障现象：** 在办公桌面云方案的场景中，终端设备开机时，任务栏无法正常使用。具体表现为：任务栏无法点击，鼠标悬停时出现“转圈”状态，同时资源管理器（Explorer.exe）会自动重启，导致屏幕出现短暂黑屏现象。

**故障根因：** 此问题源于Windows系统环境。系统开启了“资讯和兴趣”功能组件，该组件集成在任务栏中。当用户点击任务栏或触发任务栏刷新时，系统后台尝试通过网络访问微软资讯功能服务器。然而，由于网络环境无法连接至该服务器，系统后台因长时间占用任务栏资源刷新而导致任务栏失效。如果频繁操作任务栏，例如点击任务栏图标或托盘图标，可能引发资源管理器（Explorer.exe）未响应，最终导致其重启，期间伴随屏幕黑屏的情况。

**解决方案：** 关闭“资讯和兴趣”功能组件，具体步骤如下：

1. 在任务栏上右键单击，选择“资讯和兴趣”，然后选择“关闭”。
2. 使用组策略：进入“计算机配置” -> “管理模板” -> “Windows组件”，将“资讯和兴趣”设置为禁用。
3. 重启计算机，或频繁操作任务栏以触发刷新，确认问题是否解决。

**现状：** 针对出现故障的终端设备，已采取以上禁用策略。经过系统重启后，问题未再复现，后续将持续观察设备的使用情况。

# 2. 云桌面改进建议

跟锐捷云桌面售后林工沟通中，整理了企业引入云桌面解决方案的期望点，并结合现状说明实现方案与受限因素如下：

1. 纯内网环境

* 期望点：在纯内网环境中，所有云卓仅限本地办公，无法使用联网功能（例如微信、钉钉等无法正常使用），但能有效屏蔽许多联网上传工具（如百度网盘、GitHub、OneDrive），确保数据安全。
* 实现方案：对于必须联网的软件，可通过“云应用”方式实现。具体方法是：
  + 创建一台可正常联网的云服务器
  + 在该云服务器上安装必要的联网办公软件
  + 员工通过云桌面中的“云应用”访问联网功能
* 受限点：当前云桌面部署采用了全外网方式，如果调整成纯内网环境，需要进行以下的调整：
  + 创建局域网：通过路由器划分新的局域网网段
  + 部门信息采集与模板配置：针对各部门的安全等级、业务需求以及常用软件进行全面的信息收集；在创建各部门云桌面模板时，预装各部门所需的常用软件。
  + 创建内网云桌面池
  + 要求现有云桌面的每位使用者将本地数据备份到指定存储，然后再迁移到新的云桌面。

1. 软件管控，避免自由安装软件

* 期望点：规范用户行为，防止员工在外网开放和USB未限制的情况下随意下载、安装软件，从而降低病毒风险和未经授权软件的使用。
* 实现方案：
  + 内网封闭：将云桌面改造成纯内网，并限制USB使用。这种情况下：
    - 用户无法自行下载软件或通过USB拷贝安装文件
    - 新增软件需求可通过云桌面管理平台进行推送，支持静默安装或安装包推送两种方式。
  + 黑白名单机制：定义允许安装的软件（白名单）与禁止安装的软件（黑名单）。锐捷计划在未来版本中支持该功能，据林工描述，功能有望于下半年推出。
  + 第三方管控平台：通过专业的软件管控平台（如IPGuard），强化软件管理，目前正在调研该平台。
* 受限点：黑白名单功能尚未完全上线，完全依赖第三方方案可能增加管理复杂性。

1. 文件管控

* 期望点：针对文件数据，期望具备强力的安全控制手段，防止未经授权的泄露或滥用。
* 实现方案：
  + 文件加密：在开启文件加密的云桌面使用环境中，员工通过飞书、钉钉、企业微信发送文件时将会自动加密，只有同样开启了文件加密的云桌面打开该文件时才是正常的，不然的话是乱码。
    - 缺陷点：只支持3种通讯工具；只有同样开启文件加密的云桌面打开才是正常的。
  + 文件流转审批：通过U盘或者本地盘拷贝数据时将会触发文件导出审批，员工需要提交文件审批请求。
    - 缺陷点：通讯工具文件传输时不会触发；文件审批人不能设定为部门主管这种直接领导，只有运维管理员在管理平台进行文件权限审批，加大了运维管理员的工作。
  + CMS云空间平台：可以创建云空间，每个用户拥有个人云空间，部门云空间，群组云空间。拥有群创建者可以自由拉群。并且部门空间和群组空间可以设置不同的权限。可以配置外网访问，需要申请固定IP。

1. 拓展讨论

远程办公的需求，锐捷云桌面携带了SAG安全网关平台，需要配合固定IP，然后结合SAG安全网关平台后，可以实现在家远程公司云桌面的场景。