# 排除Azure虚拟桌面连接问题

## 目录

## 问题

当用户从启用思科安全访问的办公室网络访问AVD时，Azure虚拟桌面(AVD)连接失败。观察到以下特定行为：

- 当从禁用安全访问的个人网络访问AVD时，AVD工作正常。
- AVD在未经安全访问的情况下从办公室网络访问时工作正常。
- 从启用了安全访问的任何网络访问AVD时，AVD不起作用。

这种连接故障会影响用户访问其虚拟桌面的能力并影响生产业务运营。数据包捕获分析显示，在正常运行和非正常运行情况下，双向流量没有TCP重置或其他网络级别指示安全访问正在终止AVD连接。

## 环境

- 启用零信任网络访问(ZTNA)的思科安全访问
- ZTNA配置文件配置为对所有互联网目标使用ZTA
- 通过Microsoft终端访问Azure虚拟桌面(AVD)部署
- 部署了安全访问客户端的办公室网络环境
- 从办公室网络和个人网络访问AVD的用户

## 分辨率

通过将Microsoft AVD相关域添加到ZTA例外列表，允许安全访问客户端绕过AVD流量的ZTNA，解决了此问题。

### 诊断分析

联合故障排除分析确定ZTNA配置文件配置为对所有互联网目标使用ZTA，这导致安全访问通过安全访问云代理路由AVD的连续WebSocket流量。此行为导致会话丢弃，因为Azure虚拟桌面使用复杂的、连续的流量(WebSocket)来实时传输桌面会话，并且云代理设计为检查标准网页，而不是处理流协议。

### 配置变化

以下与Microsoft AVD相关的域已添加到ZTA Exceptions列表：

```
*.wvd.microsoft.com
*.core.windows.net
*.servicebus.windows.net
*.events.data.microsoft.com
```

通过将这些域添加到ZTA例外列表，安全访问客户端被指示完全忽略特定于AVD的流量。这允许AVD流量直接进入Microsoft，完全绕过ZTNA代理，这正是Microsoft要求AVD正常运作的。

### 验证

应用ZTA Exceptions配置后，AVD连接被报告在监控期间正常运行。用户能够在启用安全访问的情况下从办公室网络成功访问其虚拟桌面。

## 原因

根本原因是ZTNA配置文件配置拦截了所有互联网绑定的流量，包括Azure虚拟桌面连接。当AVD的WebSocket流量通过安全访问云代理进行路由检查时，由于该代理不是为了处理AVD会话的持续流

性质而设计的，因此会导致连接断开。AVD需要直接连接到Microsoft终端以保持稳定的桌面流会话。

## 相关内容

- Microsoft Azure虚拟桌面所需的FQDN终结点
- 排除故障并收集思科安全访问的基本信息
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。