

由于内部DNS配置，通过Azure中的安全访问虚拟设备无法访问专用链接资源

目录

问题

当流量通过部署在Azure中的思科安全访问虚拟设备(VA)路由时，无法从Azure工作空间和工作负载访问Azure专用链接资源。尽管已配置流量引导例外以绕过Azure专用域的安全访问、启用DNS回退以及在VA上配置专用DNS，但此问题依然存在。

尝试从Secure Access VA后面的Azure工作负载访问Azure专用链接终端会导致解决和连接失败。

环境

- 在Azure中部署的思科安全访问虚拟设备(VA)
- Azure工作空间和Azure托管的工作负载
- 为专用Azure资源连接启用Azure专用链接
- 配置为绕过Azure私有域安全访问的流量引导异常
- 在安全访问VA内启用DNS回退
- 在安全访问VA中配置的专用DNS区域
- 软件版本:ALL (问题与版本无关)

分辨率

解决方法涉及更新Cisco安全访问VA中的DNS配置，以包含能够解析Azure专用链接域的内部DNS服务器条目。这些步骤详细说明了所执行的故障排除和更正操作：

诊断安全访问VA上的本地DNS配置

1. 要检查现有DNS配置并确认是否设置了内部DNS服务器，请在安全访问VA上使用此命令：

```
config localdns show
```

1. 输出示例 (替换了设备名称)：

```
device# config localdns show
No internal DNS servers configured.
Conditional forwarders present for Azure private domains.
```

将内部DNS服务器条目添加到安全访问VA

1. 要启用Azure专用链接域的正确解析，请使用此命令添加适当的内部DNS服务器IP地址：

```
config localdns add <internal-DNS-server-IP>
```

1. 用可解析Azure专用链接域的内部DNS服务器的实际IP地址替换<internal-DNS-server-IP>。

验证Azure专用链接域的DNS解析

1. 更新DNS配置后，请验证是否可以通过安全访问VA解析Azure专用链接域。使用此命令确认DNS服务器配置：

```
config localdns show
```

1. 输出示例（替换设备名称）：

```
device# config localdns show
Internal DNS servers configured:
- x.x.x.x
Conditional forwarders present for Azure private domains.
```

1. 未找到CLI命令，该命令显示从config localdns show（没有DNS服务器）到解析确认的工作状态的更改。

验证与Azure专用链接资源的连接

一旦DNS正确解析，请测试从Secure Access VA后面的Azure工作负载到目标Azure专用链接终端的连接，以确保正确的访问。

原因

问题的根本原因是思科安全访问VA内没有内部DNS服务器配置。VA配置有Azure私有域条件转发器，但缺少对Azure私有链接域进行正确DNS解析所需的内部DNS服务器。添加内部DNS服务器条目解决了问题。

相关内容

- [思技术支持和下载](#)

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）。