

通过DNS故障引起的资源连接器排除ZTNA CLAP/BAP的专用访问问题

目录

[问题](#)

[环境](#)

[分辨率](#)

[步骤 1：比较环境之间的DNS配置](#)

[步骤 2：测试备用DNS服务器配置](#)

[步骤 3：验证DNS解析和连接](#)

[原因](#)

[相关内容](#)

- [问题](#)
 - [环境](#)
 - [分辨率](#)
 - [步骤 1：比较环境之间的DNS配置](#)
 - [步骤 2：测试备用DNS服务器配置](#)
 - [步骤 3：验证DNS解析和连接](#)
 - [原因](#)
 - [相关内容](#)
-

问题

在开发环境中使用资源连接器时，为零信任网络访问(ZTNA)配置的私有资源能正常工作。但是，当在生产环境中将专用资源配置更改为使用资源连接器时，对专用资源或连接的访问将失败，并出现DNS相关错误。连接符合默认阻止规则，导致无法在路由生产专用资源之前成功验证新的生产资源连接器。

具体症状包括：

- 为生产资源连接器记录的DNS故障错误
- 由于命中活动搜索报告中的默认阻止规则而导致连接失败
- 无法验证生产资源连接器功能

- 对使用资源连接器通过ZTNA CLAP访问私有资源的潜在影响

网络连接已得到验证，包括成功从资源连接器直接生成专用Web服务器主机名的DNS解析，以及与Ubuntu服务器上的端口8443的TCP连接。一切正常，但生产资源连接器仍会显示DNS故障警报，为什么？

环境

- 技术：解决方案支持 (SSPT — 需要合同)
- 子技术：安全访问 — 零信任访问 (ZTNA、状态、基于客户端、注册、专用资源)
- 产品系列：安全访问、零信任/ZTNA、资源连接器
- 目标专用应用程序/服务器：可通过TCP端口8443访问的Ubuntu服务器
- 网络组件：DEV和PROD环境中的资源连接器

分辨率

故障排除方法侧重于开发资源和生产资源连接器之间的DNS配置差异。请注意，开发资源连接器工作场景 — 能够成功访问私有资源。

生产资源连接器不工作，无法访问PR，并在RC > Network connections > resource connector > DNS failure中引发DNS故障错误。

按照以下系统步骤识别和解决DNS解析问题。

步骤 1：比较环境之间的DNS配置

对DEV和PROD资源连接器之间的DNS设置执行全面比较：

1. — 在开发资源和生产资源连接器中记录DNS服务器配置。
2. — 确定开发连接器使用的是默认DNS设置还是备用DNS服务器。

3. — 将生产连接器DNS配置与正在运行的开发设置进行比较。
4. — 注意DNS解析方法、超时或回退配置中存在的任何差异。

步骤 2：测试备用DNS服务器配置

如果生产资源连接器使用默认DNS设置，而开发连接器使用备用DNS服务器，反之亦然：

- 将生产资源连接器配置为使用与工作开发连接器相同的DNS服务器设置
- 或者，在生产资源连接器配置中指定备用DNS服务器
- 在每次DNS配置更改后测试专用资源连接
- 使用诊断、tcpdump到PR目标IP时，监控连接器日志，了解DNS解析成功或持续错误



注意：当您使用在RC上配置的默认DNS时，两个资源连接器都可以解析PR的完全限定域名 (FQDN)，但它与在不工作或生产RC的专用资源配置上配置的内部DNS不匹配。

步骤 3：验证DNS解析和连接

您必须更新生产资源连接器，才能使用内部DNS服务器与PR配置匹配，从而解决此问题。单击资源连接器ID，然后单击Edit以选择Use Alternate DNS。您可以查看根据连接器配置中的域设置，使用备用DNS服务器解析专用资源。这允许您手动指定域和DNS服务器以测试连接是否改善。完成此更改后，您可以成功访问私有资源或Ubuntu服务器。

实施DNS配置更改后：

1. — 从生产资源连接器验证DNS解析是否正常工作
2. — 确认私有资源不再符合默认阻止规则
3. — 测试通过生产连接器的端到端连接

原因

问题的根本原因与开发资源和生产资源连接器之间的DNS配置差异有关。默认情况下，生产环境使用不同的DNS服务器。此DNS解析故障导致连接回退到默认安全策略，导致流量被默认阻止规则阻止，而不是通过ZTNA框架正确路由。开发资源连接器配置为使用与私有资源配置中配置的内部DNS相匹配的内部DNS服务器。

但是，生产资源连接器配置为使用默认DNS，这与PR配置中提及的内部DNS服务器不同。

生产资源连接器已更新为使用内部DNS服务器以与PR配置匹配以解决问题。

相关内容

- [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）。