

# Troubleshoot Private Access Issue with ZTNA CLAP/BAP via Resource Connectors due to DNS Failure

## Contents

---

[Issue](#)

[Environment](#)

[Resolution](#)

[Step 1: Compare DNS Configuration Between Environments](#)

[Step 2: Test Alternate DNS Server Configuration](#)

[Step 3: Validate DNS Resolution and Connectivity](#)

[Cause](#)

[Related Content](#)

---

- [Issue](#)
  - [Environment](#)
  - [Resolution](#)
    - [Step 1: Compare DNS Configuration Between Environments](#)
    - [Step 2: Test Alternate DNS Server Configuration](#)
    - [Step 3: Validate DNS Resolution and Connectivity](#)
  - [Cause](#)
  - [Related Content](#)
- 

## Issue

A private resource configured for Zero Trust Network Access (ZTNA) functions correctly when using resource connector in the development environment. However, when the private resource configuration is changed to use the resource connector in the production environment, the access to the private resource or connection fails with DNS-related errors. The connection hits the default block rule, preventing successful validation of the new production resource connector before routing production private resources through it.

The specific symptoms include:

- DNS failure errors recorded for the production resource connector
- Connection failures due to hitting the default block rule in the activity search report
- Inability to validate the production resource connector functionality
- Potential impact to access private resource via ZTNA CLAP using Resource Connector

Network connectivity has been verified, including successful DNS resolution of the private web server hostname directly production from resource connector and TCP connectivity to port 8443 on the Ubuntu server. Everything fine, but still we get DNS failure alert in production resource connector WHY?

## Environment

- Technology: Solution Support (SSPT - contract required)
- Sub-technology: Secure Access - Zero Trust Access (ZTNA, Posture, Client-Based, Enrollment, Private Resource)
- Product Family: Secure Access, Zero Trust/ZTNA, Resource Connector
- Target Private application/Server: Ubuntu server accessible on TCP port 8443
- Network Components: Resource connectors in both DEV and PROD environments

## Resolution

The troubleshooting approach focuses on DNS configuration differences between the development and production resource connectors. Please note development resource connector is working scenario - Able to access private resource successfully.

Production resource connector is not working, PR is not accessible and throwing DNS failure error in **RC > Network connections > resource connector > DNS failure**.

Follow these systematic steps to identify and resolve the DNS resolution issues.

### Step 1: Compare DNS Configuration Between Environments

Perform a comprehensive comparison of the DNS settings between the DEV and PROD resource connectors:

- 1.- Document the DNS server configurations in both the development and production resource connectors.
- 2.- Identify whether the development connector uses default DNS settings or alternate DNS servers.
- 3.- Compare the production connector DNS configuration against the working development setup.

4.- Note any differences in DNS resolution methods, timeouts, or fallback configurations.

## Step 2: Test Alternate DNS Server Configuration

If the production resource connector is using default DNS settings and the development connector uses alternate DNS servers, or vice versa:

- Configure the production resource connector to use the same DNS server settings as the working development connector
- Alternatively, specify alternate DNS servers in the production resource connector configuration
- Test the private resource connectivity after each DNS configuration change
- Monitor the connector logs for DNS resolution success or continued errors when you use diagnostics, tcpdump to the PR destination IP



**Note:** Both resource connectors can resolve the Fully Qualified Domain Name (FQDN) of the PR when you use the default DNS configured on the RC, but it does not match with the internal DNS configured on the private resource configuration for the non-working or production RC.

---

## Step 3: Validate DNS Resolution and Connectivity

You must update the Production Resource Connector in order to use the internal DNS servers to match with the PR configuration in order to resolve the issue. Click the resource connector ID and click **Edit** in order to select **Use Alternate DNS**. You can explore the **Use alternate DNS servers to resolve private resources based on domain setting** within the connector configuration. This allows you to manually specify the domain and DNS server in order to test if the connectivity improves. After this change, you can successfully access the private resource or Ubuntu server.

After implementing DNS configuration changes:

- 1.- Verify that DNS resolution works correctly from the production resource connector
- 2.- Confirm that the private resource no longer hits the default block rule
- 3.- Test end-to-end connectivity through the production connector

## Cause

The root cause of the issue related to DNS configuration differences between the development and production resource connectors. The production environment was using different DNS servers by default. This DNS resolution failure causes the connection to fall back to default security policies, resulting in the traffic being blocked by the default block rule rather than being properly routed through the ZTNA framework. The Development Resource Connector is configured to use the internal DNS servers which matches with internal DNS configured in the private resource configuration.

The Production Resource Connector, however, is configured to use the default DNS, which differs from the internal DNS servers mentioned in the PR config.

The Production Resource Connector was updated to use the internal DNS servers to match with PR configuration to resolve the issue.

## Related Content

- [Cisco Technical Support & Downloads](#)