

DNSの障害によるリソースコネクタ経由のZTNA CLAP/BAPでのプライベートアクセス問題のトラブルシューティング

内容

[お問い合わせ内容](#)

[環境](#)

[解決策](#)

[ステップ1: 環境間のDNS設定の比較](#)

[ステップ2: 代替DNSサーバ設定のテスト](#)

[手順3:DNS解決と接続を検証する](#)

[原因](#)

[関連コンテンツ](#)

- [お問い合わせ内容](#)
 - [環境](#)
 - [解決策](#)
 - [ステップ1: 環境間のDNS設定の比較](#)
 - [ステップ2: 代替DNSサーバ設定のテスト](#)
 - [手順3:DNS解決と接続を検証する](#)
 - [原因](#)
 - [関連コンテンツ](#)
-

お問い合わせ内容

ゼロトラストネットワークアクセス(ZTNA)用に構成されたプライベートリソースは、開発環境でリソースコネクタを使用すると正しく機能します。ただし、プライベートリソースの構成が変更され、実稼働環境でリソースコネクタを使用するようになると、プライベートリソースまたは接続へのアクセスが失敗し、DNS関連のエラーが発生します。接続が既定のブロックルールに一致しているため、本番プライベートリソースをルーティングする前に新しい本番リソースコネクタの検証に失敗します。

具体的な症状は次のとおりです。

- 本番リソースコネクタに記録されたDNS障害エラー

- アクティビティ検索レポートの既定のブロックルールに一致したため、接続に失敗しました
- 本番リソースコネクタの機能を検証できない
- リソースコネクタを使用したZTNA CLAP経由でのプライベートリソースへのアクセスによる潜在的な影響

プライベートWebサーバホスト名のDNS解決がリソースコネクタから直接実行され、Ubuntuサーバのポート8443へのTCP接続が直接実行されることを含め、ネットワーク接続が確認されています。問題はありませんが、実稼働リソースコネクタにDNS障害のアラートが表示されるのはなぜですか。

環境

- テクノロジー：ソリューションサポート（SSPT – 契約が必要）
- サブテクノロジー：セキュアなアクセス：ゼロトラストアクセス（ZTNA、ポスチャ、クライアントベース、登録、プライベートリソース）
- 製品ファミリ：セキュアなアクセス、ゼロトラスト/ZTNA、リソースコネクタ
- ターゲットプライベートアプリケーション/サーバ：TCPポート8443でアクセス可能なUbuntuサーバ
- ネットワークコンポーネント：開発環境と実稼働環境の両方のリソースコネクタ

解決策

トラブルシューティングアプローチでは、開発リソースコネクタと実稼働リソースコネクタのDNS設定の違いに焦点を当てます。開発リソースコネクタが動作しているシナリオ – プライベートリソースに正常にアクセスできることに注意してください。

実稼働リソースコネクタが機能しておらず、PRにアクセスできず、「RC > Network connections > resource connector > DNS failure」でDNS障害エラーがスローされています。

DNS解決の問題を特定して解決するには、次の体系的な手順に従います。

ステップ1：環境間のDNS設定の比較

DEVリソースコネクタとPRODリソースコネクタのDNS設定を包括的に比較します。

1. – 開発と実稼働の両方のリソースコネクタでDNSサーバの設定を文書化します。
2. – 開発コネクタが既定のDNS設定を使用するか、代替DNSサーバーを使用するかを特定します。
3. – 実稼働コネクタのDNS設定を、実際の開発設定と比較します。
- 4.- DNS解決方法、タイムアウト、またはフォールバック設定の違いに注意します。

ステップ2：代替DNSサーバ設定のテスト

本番リソースコネクタがデフォルトのDNS設定を使用しており、開発コネクタが代替DNSサーバを使用している場合、またはその逆の場合は、次のようになります。

- 作業用の開発コネクタと同じDNSサーバー設定を使用するように運用リソースコネクタを構成します
- または、実稼働リソースコネクタ構成で代替DNSサーバーを指定します
- 各DNS構成を変更した後に、プライベートリソースの接続をテストします
- 診断、PR宛先IPへのtcpdumpを使用する場合は、コネクタログを監視して、DNS解決の成功または継続的なエラーを確認します



注:RCで設定されているデフォルトのDNSを使用すると、両方のリソースコネクタがPRの完全修飾ドメイン名(FQDN)を解決できますが、これは非稼働RCまたは実稼働RCのプライベートリソース設定で設定されている内部DNSと一致しません。

手順3:DNS解決と接続を検証する

問題を解決するには、内部DNSサーバを使用してPR設定と一致するように、実稼働リソースコネクタを更新する必要があります。リソースコネクタIDをクリックし、Editをクリックして、Use Alternate DNSを選択します。コネクタ設定の「代替DNSサーバを使用し、ドメイン設定に基づいてプライベートリソースを解決する」セクションを確認できます。これにより、ドメインと

DNSサーバを手動で指定して、接続が改善されるかどうかをテストできます。この変更の後、プライベートリソースまたはUbuntuサーバに正常にアクセスできます。

DNS設定の変更を実装した後：

- 1.- DNS解決が運用リソースコネクタから正しく機能することを確認します
- 2.- プライベートリソースがデフォルトブロックルールにヒットしなくなったことを確認します
- 3.- 実稼働コネクタを介したエンドツーエンド接続のテスト

原因

開発リソースコネクタと実稼働リソースコネクタ間のDNS設定の違いに関連する問題の根本原因。実稼働環境では、デフォルトで異なるDNSサーバを使用していました。このDNS解決の失敗により、接続がデフォルトのセキュリティポリシーにフォールバックし、その結果、トラフィックはZTNAフレームワークを介して適切にルーティングされるのではなく、デフォルトのブロックルールによってブロックされます。開発リソースコネクタは、プライベートリソース構成で構成された内部DNSと一致する内部DNSサーバを使用するように構成されています。

ただし、実稼働リソースコネクタは、デフォルトのDNSを使用するように設定されています。これは、PR設定に記載されている内部DNSサーバとは異なります。

この問題を解決するために、内部DNSサーバを使用してPR設定と一致するように実稼働リソースコネクタが更新されました。

関連コンテンツ

- [シスコのテクニカルサポートとダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。