セキュアアクセスにおけるプライベートアプリケーションのAPP_UNREACHABLE障害のトラブルシューティング

内容

問題

Cisco Secure Accessを介してZero Trust Network Access(ZTNA)アプリケーションにアクセスしようとすると、「Application Unreachable」というエラーメッセージが表示されます。

- コネクタがダッシュボードに正常/アクティブと表示され、アプリケーションが所有者によって実行されていることが確認されます。
- この障害は、1つのアプリケーションのすべてのユーザに影響を与える可能性がありますが、同じコネクタで処理される他のアプリケーションは正常に動作します。
- コネクタプールの導入では、障害が断続的に発生する可能性があります。プール内で選択されているコネクタによっては、セッションが成功または失敗することがあります。

環境

- ZTNAによるCisco Secure Private Accessの導入
- ZTNAアクセス用に設定されたプライベートリソース
- プライベートリソースアクセス用のリソースコネクタの導入

解決方法

ステップ 1：コネクタネットワークセグメントからの直接到達可能性のテスト

- リソースコネクタはロックダウンされたアプライアンスであり、curlやncなどのコマンドを直接実行するためのシェルアクセスは提供しません。その代わりに、Connectorと同じサブネット/VLANに配置されたテストホスト（または一時的なVM）から到達可能性テストを実行し、アプリケーションに対して同じネットワークパス、ルーティング、およびファイアウォール規則に従います。

```
curl -v http://APP_IP:PORT/health
nc -zv APP_IP PORT
```

- これが失敗すると、ネットワークパスまたはアプリケーションサーバで問題が確認されます。セキュアアクセスの設定を確認する前に、まずこれを修正してください。

注：別のサブネットからのテストでも結論は得られません。テストの発信元ではコネクタのIP配置をできる限り厳密に反映する必要があるため、ファイアウォールルールとルーティングは発信元ごとに評価されます。

ステップ 2：プライベートリソース設定の確認

- Secure Accessダッシュボードで、Resources > Private Resourcesの順に移動し、該当するプライベートリソースを開いて、設定されているIP、FQDN、およびポートの文字を、実行中のアプリケーションの実際のバインドアドレスとポートと比較します。
- 不一致（サーバ移行後の古いIP、間違ったポート、HTTP対HTTPS）があると、完全に正常なネットワークパスでもAPP_UNREACHABLEが生成されます。

ステップ 3：コネクタのDNS解決の検証

- プライベートリソースがFQDNで定義されている場合は、コネクタに割り当てられたDNSサーバーで解決できることを確認します。リソースコネクタCLI（サポートされている標準のLinuxトラブルシューティングコマンドを備えた診断CLIをVMで展開することで提供）から、次のコマンドを実行します。

```
nslookup app.internal.company.com <internal_DNS_server_IP>
```

- 正しいプライベートIPが返されることを確認します。コネクタのネットワーク構成が、プライベートアプリケーションFQDNを解決できる内部DNSサーバーを指していることを確認してください。パブリックリゾルバーで構成されたコネクタは、内部ゾーンを解決できません。

ステップ 4：ファイアウォールパスの確認

- ファイアウォールルール（ネットワークファイアウォールおよびアプリケーションサーバ上のホストファイアウォール）で、コネクタのIPアドレスから必要なポート上のアプリケーションサーバIPへのトラフィックが許可されていることを確認します。

ステップ 5：リソースコネクタのtcpdumpを使用したトラフィックのキャプチャ

- リソースコネクタでパケットキャプチャを実行し、アプリケーションへのラストマイル接続の試行を確認します。tcpdumpユーティリティはリソースコネクタで使用できます（『リソースコネクタでのtcpdumpの実行』ガイドを参照）。

ヒント：コネクタグループ配置でキャプチャを確定的なものにするには、グループで有効になっている1つのリソースコネクタだけを一時的に保持し、リソースのすべてのセッションがそのコネクタを通過するようにします。次に、アプリケーションサーバとポートでフィルタ処理されたキャプチャを実行します。

- 以下に、いくつかの例を示します。

```
tcpdump 'host x.x.x.x and tcp port 443'
```

（x.x.x.xはアプリケーションサーバのIPで、443はアプリケーションのポートです）

- 結果を解釈します。SYN-ACKを伴わない発信SYNは、ファイアウォールのドロップまたはアプリケーションがリッスンしていないことを示します。即時RSTは、ホストが到達可能でありながら、ポートに何もバインドされていないことを示します。アプリケーションへのパ

ケットは、セッションがこのコネクタに到達していないことを示し、DNSは予期しないアドレスに解決されました。

- キャプチャが完了したら、グループ内の残りのコネクタを再度有効にします。

原因

- ファイアウォールがコネクタからアプリケーションへのトラフィックをブロックする：ネットワークまたはホストベースのファイアウォールが、コネクタのホストIPとアプリケーションサーバIPの間の必要なポートをブロックします。
- Secure Accessでのプライベートリソースの設定の不一致：プライベートリソース定義(Resources > Private Resources)で設定されたIP、FQDN、またはポートが、アプリケーションが実際にリッスンする内容と一致しません（たとえば、アプリケーションが新しいIPに移動したか、8443でリッスンし、443が設定されている場合）。
- コネクタのDNS解決エラー：プライベートリソースはFQDNで定義されていますが、コネクタDNSサーバーはプライベートアプリケーションFQDNを解決していません。
- アプリケーションサーバがダウンしているか、リッスンしていない：他の方法でサーバが正常に見えるが、予期されたポートにバインドされていないか、ホストがアップ状態の間にサービスがクラッシュした。
- コネクタプールの部分的な到達可能性：プール内の1つまたは複数のコネクタが、アプリケーションに到達できないネットワークセグメントに存在するため、これらのコネクタに割り当てられたセッションだけが失敗します。

関連コンテンツ

- Cisco Secure Accessの基本情報のトラブルシューティングと収集
- 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。