XDR-Aにおけるオンプレミスデバイス、ホスト名、およびIPマッピングについて

内容

はじめに

このドキュメントでは、デバイスのホスト名とIPマッピングに関連するXDR-Analyticsの動作を理解する方法について説明します。

背景

XDRAは、時間の経過とともに論理デバイスの動作（デバイス）を追跡しようとします。

時間の経過に伴い、ネットワークトラフィックをこれらの論理デバイスに関連付けるためのさまざまな手法を使用します。

ただし、特にオンプレミス環境では、システムがトラフィックをデバイスに関連付ける方法に制限があります。

XDRAは主に、ONA、CTB、またはCisco Merakiの統合（「新しい」Meraki統合）を介してNetFlowを通じてオンプレミス環境のテレメトリを収集します。 2番目に、次の方法でホスト名解決を取得できます。

- 逆DNSルックアップによるアクティブなホスト名解決、およびONAによるオプションのSMBクエリ
- ONAを介したISE統合
- 「古い」Meraki統合
- NVMの統合、その他の注意事項

Netflowにはホスト名情報のないIPアドレスがあります。

ホスト名情報がない場合、よりインテリジェントなデバイス関連付けを行うための情報がないため、各内部IPアドレス（後述の定義を参照）がデバイスであると見なされます。

ホスト名の収集が設定されている場合、XDRAはホスト名を確認すると、それを使用してデバイスの内部表現に結び付けます。

これにより、XDRAは時間の経過とともに複数のIPアドレスを1つのデバイスにグループ化できます。

NVMテレメトリは、オプションでXDRの一部として設定できます。

このテレメトリソースは、NetFlowに似たデータフィードを提供しますが、一意のIDを持つエン

ドポイント情報も提供します。

XDRAがこの情報を利用する方法は、ONAでホスト名収集が有効になっている場合と同様に、デバイストラッキングの動作に実質的な影響があります。

これらの設定にはすべて、利用可能なテレメトリの制限に基づく制限があります。

XDRAはIPアドレスとホスト名のマッピングの性質が多対1の関係であることを前提としています（多くのIPは1つのホスト名にマッピングできます）。

1つの論理デバイスに複数のIPを同時に設定できます（たとえば、2つの物理インターフェイスまたはIPv4とIPv6など）。

モニタリングの性質により、XDRAは特定の時点で実際のネットワークのすべての関係を持っているとは決して想定できません。

重複するサブネット

単一のXDRAテナントが複数のオンプレミスサブネットを同時に監視している場合、システムは各サブネットで確認される同じIPを区別できません。

そのため、IPをデバイスに過剰に関連付けます。ホスト名を使用しても、この状況は改善されません。

これを回避する1つの方法は、複数のXDRAポータル（サブネットごとに1つ）を持つことです。もう1つの方法は、この統合によってもたらされる名前空間の分離により、「新しい」Cisco Meraki統合を使用することです。

使用可能なホスト名情報がない環境

テレメトリ情報の制限による副作用として、システムがデバイス履歴を誤って理解する可能性があります。

1つのシナリオは、IPが動的に割り当てられる場合、XDRAには、WIFIリーフのラップトップなど、基盤となる論理デバイスが変更されたことを知る方法がなく、IPは新しいラップトップに割り当てられます。

ホスト名やその他の識別情報がない場合、システムは複数の論理デバイスのアクティビティを1つのデバイスに関連付けます。これにより、デバイスプロファイル情報の混乱を招く可能性があります。

```
Actual Situation
    t0      t1      t2      t3
ip1 d1------        d2------

As seen by XDRA
    t0      t1      t2      t3
ip1 d1----------------------
```

逆に、1つの論理デバイスが複数のIPアドレスを持つ場合（2つの物理インターフェイスまたはIPv4とIPv6など）、これらを同じデバイスに確実に結び付ける情報はないため、システムは結び付けません。

```
Actual Situation
    t0      t1      t2      t3
ip1 d1--------------
ip2 d1--------------

As seen by XDRA
    t0      t1      t2      t3
ip1 d1--------------
ip2 d1--------------
```

ホスト名情報を持つ環境

XDRAがホスト名情報を参照できる場合、システムは複数のIPアドレスを1つのデバイスに関連付けることができます。ただし、データの性質を考えると、システムが確実に決定できる内容にはまだ限界があります。これにより、システム内のデバイスに対するIPの相関関係が過剰になる可能性があります。

XDRAにIPとホスト名の関連付けがあるデバイスがあり、論理デバイスがIPアドレスを変更した場合、テレメトリは最終的に新しいIPとホスト名のマッピングを反映します。

ただし、これが多対一の関係になる可能性があるため、XDRAは以前に見られたIPがホスト名（およびデバイス）に関連付けられていないと想定しても安全ではありません。

たとえば、同じ論理デバイスに対する個別の物理インターフェイスにすることができます。そのため、XDRAは、IPアドレスを別のホスト名に明確にマッピングするテレメトリが表示されるまで、直前に表示されたIPと最後に表示されたIPの両方を保持します。

この時点で、XDRはマッピングを「期限切れ」にし、以前のIPアドレスとしてリストされます。

関連付けを「早期」に解除するようにシステムに指示する方法はありません。

ホスト名の照合に関する注意

テナントが複数のドメインで設定された同じホスト名を持つ場合に、より適切に処理するために、XDRAは「柔軟な」照合を採用し、既存のデバイス（つまり、一致するIPの場合）と一致する場合は、この表に示すエントリを一致するホスト名として扱います。

```
example
example.com
example.net
example.obsrvbl.com
```

```
example.invalid.obsrvbl.com
example.example.com
```

つまり、ドメイン名の残りの部分を無視しながら、ホスト名だけを考慮します。

NVMを使用した環境

この設定は、ホスト名情報を含む「ホスト名情報を含む環境」セクションと非常によく似ていますが、いくつかの違いがあります。

このデータフィードは、一意のエンドポイントIDをユーザに提供できるという追加の利点を提供します。これらのIDにより、ホスト名の変更を受ける物理デバイスを追跡できる可能性があります（追跡できない場合は、2つの異なるデバイスを作成します）。

デバイスはエンドポイントデータフィード（一意のエンドポイントIDを持つ）に基づいて作成されますが、フローデータに基づいてエンドポイントに関する観測が行われるまで、これらのデバイスに関連付けられているホスト名またはIPはありません。

ISEを使用した環境

デバイストラッキングに対するISEの利点は、最終的にはホスト名情報を含む環境と同じになります。

ISEデータは、収集したホスト名情報をIPアドレスに関連付けるために使用されますが、新しいデバイスを作成したり、NetFlowで検出されなかったIPを追跡したりすることはありません。

Merakiを使用した環境

「旧」Meraki統合（XDRAと連携）

このMeraki統合は、Merakiデバイスからホスト名情報をプロアクティブに収集し、それらのホスト名をオンプレミスのデバイス（つまり「デフォルトの名前空間」）で通常どおりにIPにマッピングします。

デバイスが存在しない場合、このプロセスによってデバイスが作成されます。

名前空間の違いにより、他の「新しい」Cisco Meraki統合から収集したデバイスまたはIP情報を強化しません。

これにより、この設定は事実上、ホスト名情報を持つ環境のように動作します。

「新しい」Cisco Meraki統合(XDRとの統合)

この統合により、MerakiのネットワーキングデバイスからXDRデータレイクを経由して標準のXDRA NetFlowパスにNetFlowを取得します。

そのため、他のNetFlowと同様にデバイスを作成し、他のNetFlowと同様にホスト名情報を含みません。

実際には、この設定は使用可能なホスト名情報のない環境のように動作しますが、大きな例外が1つあります。

この統合では、送信された情報を利用して、異なるMeraki機器から異なる名前空間へのNetFlowにラベル付けします。

これにより、通常のサブネットの重複の問題が回避されますが、複数の統合が設定されている場合に新たな問題が発生する可能性があります。

最も明らかなケースは、「旧」と「新」の両方のMeraki統合が設定されている場合、これらの統合では同じ名前空間が使用されないことです。そのため、情報が同じ物理デバイスを表す場合でも、これらの統合では重複しないデバイスが作成されます。

つまり、2つのデバイスがあり、1つはデフォルトの名前空間にホスト名があり、トラフィックがないデバイス、もう1つは特定のMeraki名前空間にトラフィックがあり、ホスト名がないデバイスです。

同時に有効にすると、他の統合でも同様の「分割」が発生する可能性があります。

定義

1. 内部IPアドレス：XDRAはIPアドレスを内部または外部と見なします。これはサブネット設定で設定できます。オンプレミスのサブネットはデフォルトでRFC内部サブネット（RFC1918およびRFC4193）に設定されますが、サブネットの設定（追加または削除）は可能です。

2. 名前空間：異なる観測ポイントから観測されたNetFlowおよびデバイスにラベルを付けるために使用される追加情報で、IPの問題が重複することなくサブネットの重複が可能になります。

ISEホスト名データフロー

1. ONAはISEセッションデータを収集し、10分ごとにS3にアップロードします
    1. このデータには、ユーザーの<->IP情報が含まれ、ホスト名も含まれることがあります
2. IseSessionsMinerは、アップロードされたデータを解析し、可能な場合はIPをデバイスに関連付けます。デバイスが存在しない場合、デバイスは作成されません。このように、デバイスがすでに存在する場合は常に、使用可能なホスト名<->IPマッピングを収集します。
3. 次に、ONAがその逆DNSルックアップからマッピングをアップロードするのと同じ形式で、これらのマッピングを使用してs3にファイルを作成します
4. 次に、ONAホスト名をロードするのと同じように、これらのホスト名をロードするようにシステムに指示します。

FAQ

ネットワーク上のその論理デバイスに関連付けられていないIPがXDRAデバイス上に表示されるのはなぜですか。

残念ながら、私たちにできることは何もありません。

システムは、古い関連付けが無効であるか、または追加の物理ネットワークインターフェイスなどの結果であるかを認識できません。

XDRAに送信されるホスト名情報がありません。IPv4とIPv6の両方のアドレスを使用するデバイスが2つの異なるデバイスとして表示されるのはなぜですか。

ホスト名情報がないと、異なるIPがネットワーク上の同じ論理デバイスに関連付けられていることを認識できません。

異なるサブネットの複数の論理デバイスが同じXDRAデバイスに表示されるのはなぜですか。

XDRAには現在、サブネットテレメトリの由来を区別する方法がないため、同じIPは常に1つのデバイスにグループ化されます。

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。