瞭解XDR-A中的本地裝置、主機名和IP對映

目錄

簡介

本文檔介紹如何理解與裝置主機名和IP對映相關的XDR-Analytics行為。

背景

XDRA試圖跟蹤一段時間的邏輯裝置行為，稱為裝置。

它使用各種技術將網路流量隨著時間的推移關聯到這些邏輯裝置。

但是，特別是在內部部署環境中，系統可以將流量關聯到裝置的能力存在限制。

XDRA主要通過Netflow通過ONA、CTB或Cisco Meraki整合（「新的」Meraki整合）收集本地環境的遙感勘測。 其次，可以通過以下方式獲得主機名解析：

- 通過反向DNS查詢和通過ONA的SMB查詢進行活動主機名解析（可選）
- 通過ONA整合ISE
- 「舊」Meraki整合
- NVM整合，附帶其他警告

Netflow的IP地址沒有主機名資訊。

如果沒有主機名資訊，它將假定看到的每個內部IP地址（請參閱下面的定義）都是裝置，因為它沒有進一步的資訊來實現更智慧的裝置關聯。

在配置了主機名集合的情況下，XDRA使用主機名（如果看到），將其與裝置的內部表示形式相關聯。

這允許XDRA在一段時間內將多個IP地址分組到一個裝置。

NVM遙測可作為XDR的一部分進行可選配置。

此遙測源提供類似netflow的資料饋送，但也提供具有唯一識別符號的終端資訊。

XDRA利用此資訊的方式具有裝置跟蹤的淨效果，與在ONA上啟用主機名收集的情況類似。

所有這些設定都存在限制（基於可用遙測的限制）。

請注意，XDRA假定IP地址與主機名對映的性質為多對一關係（許多IP可以對映到一個主機名）。

一個邏輯裝置可以同時具有多個IP（例如，兩個物理介面或IPv4和IPv6）。

由於監控的性質，XDRA永遠不能假定在任何給定的時間擁有實際網路的所有關係。

重疊的子網

如果單個XDRA租戶同時監視多個本地子網，則系統無法區分其中每個子網中看到的同一IP。

因此，它將IP與裝置過度關聯。主機名可用性不能改善這種情況。

解決此問題的一種方法是擁有多個XDRA門戶（每個子網一個）。 另一種方法是使用「新」Cisco Meraki整合，因為此整合帶來的名稱空間隔離。

沒有可用主機名資訊的環境

作為有限的遙測資訊的一個副作用，系統可能會對裝置歷史記錄產生不正確的理解。

一種情況是IP是動態分配的，XDRA無法知道底層邏輯裝置已更改（例如WIFI上的筆記型電腦離開），並且IP已分配給新的筆記型電腦。

在沒有主機名或其他標識資訊的情況下，系統將多個邏輯裝置的活動關聯到一個裝置。這會導致裝置配置檔案資訊混亂。

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

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

反之，如果一個邏輯裝置具有多個IP地址（例如，兩個物理介面或IPv4和IPv6），則沒有資訊可以可靠地將這些地址關聯到同一裝置，因此系統沒有此功能。

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

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

包含主機名資訊的環境

其中XDRA可以看到主機名資訊，系統能夠將多個IP地址與一個裝置相關聯。然而，鑑於資料的性

質，系統能夠可靠地確定的資料仍有侷限性。這會導致IP與系統中的裝置過度關聯。

如果在XDRA中具有IP與主機名關聯的裝置，然後邏輯裝置更改IP地址，則遙測最終會反映新的IP與主機名的對映。

但是，由於這可能是一個多對一關係，因此XDRA無法安全地假設以前看到的IP不再與主機名（從而與裝置）相關聯。

例如，它可以是連線到同一邏輯裝置的單獨物理介面。因此，XDRA將以前看到的IP與最近看到的IP一起保留，直到發現遙測時，該遙測會將IP地址正對映到不同的主機名。

此時，XDR「過期」對映並將其列為前一個IP地址。

沒有辦法告訴系統「早期」中斷關聯。

有關主機名匹配的註釋

為了更好地處理租戶在多個域中配置了相同主機名的情況，XDRA採用「靈活」匹配方法，並在查詢匹配現有裝置（即匹配IP）時將表中顯示的條目視為匹配的主機名：

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

換句話說，它只考慮主機名，而忽略域名的其餘部分。

使用NVM的環境

此設定與「包含主機名資訊的環境」部分非常相似，但存在一些差異。

此資料饋送提供了額外的優勢，即能夠為使用者提供一些獨特的端點識別符號，這些ID可能允許我們跟蹤主機名發生變化的物理裝置（如果不進行跟蹤，我們將建立2個不同的裝置）。

儘管根據終端資料饋送（具有唯一終端ID）建立裝置，但在根據流資料對該終端進行觀察之前，沒有與這些裝置關聯的主機名或IP。

使用ISE的環境

ISE到裝置跟蹤的優勢最終與具有主機名信息的環境完全相同。

ISE資料用於將其收集的主機名資訊與IP地址相關聯，但不會建立新裝置或跟蹤Netflow中未檢測到的IP。

使用Meraki的環境

「舊」Meraki整合（即與XDRA整合）

此Meraki整合可主動從Meraki裝置收集主機名資訊，並按照常規方式將這些主機名對映到本地裝置（即「預設名稱空間」）中的IP。

如果裝置尚不存在，此過程將建立裝置。

由於名稱空間差異，它不會增加從其他「新」Cisco Meraki整合收集的裝置或IP資訊。

實際上，這會導致此配置的行為與包含主機名資訊的環境類似。

「全新」Cisco Meraki整合(即與XDR)

此整合將netflow從Meraki網路裝置通過XDR資料湖連線到標準XDRA netflow路徑。

因此，它會像任何其他netflow一樣建立Devices;此外，與任何其他netflow一樣，它不包含主機名資訊。

實際上，此配置的行為與沒有可用主機名資訊的環境類似，只有一個主要例外。

此整合利用傳送的資訊將來自不同Meraki裝置的netflow標籤到不同的名稱空間。

這避免了通常的子網重疊問題，但是如果設定多個整合，則可能會帶來新的困難。

最明顯的是，如果同時設定了「舊」和「新」Meraki整合，則它們不使用相同的名稱空間，因而建立了非重疊的裝置，即使在資訊表示同一物理裝置的情況下也是如此。

也就是說，您有2個裝置，其中一個位於預設名稱空間中，具有主機名且無流量，另一個位於特定Meraki名稱空間中，且無主機名。

如果同時啟用，則其他整合可能會發生類似的「拆分」。

定義

1. 內部IP地址：XDRA考慮IP地址是內部地址還是外部地址，可以通過子網設定進行配置。內部子網的預設子網為RFC內部子網（RFC1918和RFC4193），但可以配置（新增或刪除）子網。
2. 名稱空間：用於標籤從不同觀察點看到的netflow和裝置的其他資訊，允許子網重疊而不出現重疊IP問題。

ISE主機名資料流

1. ONA收集ISE會話資料，每10分鐘上傳至S3
    1. 此資料包含使用者<->IP資訊，有時還包含主機名

2. IseSessionsMiner分析上傳的資料，並在可能的情況下將IP與裝置關聯。如果裝置不存在，則不會建立裝置。這樣，只要我們已有裝置，它就會收集可用的主機名<->IP對映。

3. 然後，它會在s3中建立一個檔案，其中的對映格式與ONA從其反向DNS查詢上傳的對映格式相同

4. 然後通知系統載入這些主機名，就像載入ONA主機名一樣。

常見問題

為什麼在XDRA裝置上看到不再與我的網路上的該邏輯裝置關聯的IP?

不幸的是，我們對此無能為力。

系統無法知道舊關聯是否無效，或者是否由其他物理網路介面導致。

我沒有任何主機名資訊被傳送到XDRA，為什麼同時使用IPv4和IPv6地址的裝置顯示為2個不同的裝置？

如果沒有主機名資訊，我們就無法知道不同的IP與網路上的同一邏輯裝置相關聯。

為什麼在同一個XDRA裝置中會出現來自不同子網的多個邏輯裝置？

XDRA目前無法區分來自哪個子網遙測，因此相同的IP總是被分組到一個裝置中。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。