了解XDR-A中的本地设备、主机名和IP映射

目录

简介

本文档介绍如何理解与设备主机名和IP映射相关的XDR-Analytics行为。

背景

XDRA会尝试跟踪一段时间的逻辑设备行为，称为设备。

它使用各种技术将网络流量随着时间的推移关联到这些逻辑设备。

但是，特别是在内部部署环境中，系统可以将流量关联到设备的性能存在限制。

XDRA主要通过Netflow通过ONA、CTB或Cisco Meraki集成（“新的”Meraki集成）收集现场环境的遥感勘测。 其次，它可以通过以下方式获得主机名解析：

- 通过反向DNS查找进行活动主机名解析，或者通过ONA进行SMB查询
- 通过ONA集成ISE
- “旧”Meraki集成
- NVM集成，附带其他警告

Netflow的IP地址没有主机名信息。

如果没有主机名信息，它会假设看到的每个内部IP地址（请参阅下面的定义）都是设备，因为它没有进一步的信息来实现更智能的设备关联。

在配置主机名集合的情况下，XDRA使用主机名（如果看到）将其与设备的内部表示相关联。

这允许XDRA在一段时间内将多个IP地址分组到一台设备。

可以选择将NVM遥测配置为XDR的一部分。

此遥测源提供类似Netflow的数据馈送，但也提供具有唯一标识符的终端信息。

XDRA利用此信息的方式具有设备跟踪的净效应，这与在ONA上启用主机名收集的情况类似。

所有这些设置都有限制，具体取决于可用遥测的限制。

请注意，XDRA假定IP地址和主机名映射的性质为多对一关系（多个IP可以映射到一个主机名）。

一个逻辑设备可以同时拥有多个IP（例如，两个物理接口或IPv4和IPv6）。

由于监控的性质，XDRA永远不能假定在任意给定时间拥有实际网络的所有关系。

子网重叠

如果单个XDRA租户同时监控多个内部部署子网，则系统无法区分每个子网中看到的相同IP。

因此，它将IP与设备过度关联。主机名可用性并不能改善这种情况。

解决此问题的一种方法是拥有多个XDRA门户（每个子网一个）。 另一种方法是使用"新"Cisco Meraki集成，因为此集成带来的命名空间隔离。

没有可用主机名信息的环境

由于遥测信息有限，系统可能会对设备历史记录产生不正确的了解。

一种情况是IP是动态分配的，XDRA无法知道底层逻辑设备已更改（例如WIFI上的笔记本电脑），并且IP已分配给新的笔记本电脑。

如果没有主机名或其他标识信息，系统将多个逻辑设备的活动关联到一台设备。这会导致设备配置文件信息混乱。

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

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

相反，如果一个逻辑设备具有多个IP地址（例如，两个物理接口或IPv4和IPv6），则没有信息可以可靠地将这些地址绑定到同一设备，因此系统不会这样做。

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

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

包含主机名信息的环境

其中XDRA可以看到主机名信息，系统能够将多个IP地址关联到一个设备。然而，鉴于数据的性质，系统能够可靠地确定的数据仍有局限性。这会导致IP与系统中的设备过度关联。

如果XDRA中具有IP与主机名关联的设备，然后逻辑设备更改IP地址，则遥测最终会反映新的IP到主机名的映射。

但是，由于这可能是一个多对一关系，XDRA无法安全地假设先前看到的IP不再与主机名（进而与设备）相关联。

例如，它可以是连接到同一逻辑设备的单独物理接口。因此，XDRA将之前看到的IP与最近看到的IP一起保留，直到发现遥测时，该IP地址会正映射到不同的主机名。

此时，XDR“过期”映射并将其列为前一个IP地址。

没办法告诉系统“早期”中断关联。

主机名匹配注意事项

为了更好地处理租户在多个域中配置了相同主机名的情况，XDRA采用“灵活的”匹配，并在查找匹配现有设备（即匹配的IP）时将表中显示的条目视为匹配的主机名：

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

换句话说，它只考虑主机名，而忽略域名的其余部分。

使用NVM的环境

此设置与主机名信息部分的Environment with hostname information非常相似，但存在一些差异。

此数据馈送提供额外的优势，即能够为用户提供一些唯一的终端标识符，这些ID可能允许我们跟踪主机名发生变化的物理设备（否则无法跟踪，我们将创建2个不同的设备）。

虽然根据终端数据馈送（具有唯一终端ID）创建设备，但在根据流数据观察该终端之前，没有与这些设备关联的主机名或IP。

使用ISE的环境

ISE到设备跟踪的优势最终与使用主机名信息的环境相同。

ISE数据用于将其收集的主机名信息与IP地址关联，但它不会创建新设备或跟踪netflow中未检测到的IP。

使用Meraki的环境

“旧”Meraki集成（与XDRA集成）

此Meraki集成主动从Meraki设备收集主机名信息，将这些主机名映射至内部设备（即“默认命名空间”）的IP。

如果设备尚不存在，此过程将创建设备。

由于命名空间差异，它不会增加从其他“新”Cisco Meraki集成收集的设备或IP信息。

实际上，这会导致此配置的行为类似于包含主机名信息的环境。

“新”Cisco Meraki集成(与XDR集成)

此集成可将Meraki网络设备的Netflow通过XDR数据湖连接到标准XDRA Netflow路径。

因此，它像任何其他netflow一样创建设备；与任何其他netflow一样，它不包含主机名信息。

实际上，此配置的工作方式与没有可用主机名信息的Environment类似，但有一个主要例外。

此集成利用发送的信息将来自不同Meraki设备的Netflow标记到不同的名称空间。

这避免了通常的重叠子网问题，但如果设置多个集成，则可能会带来新的困难。

最明显的是，如果同时设置“旧”和“新”Meraki集成，它们不会使用相同的命名空间，因此它们会创建非重叠设备，即使在信息表示同一物理设备的情况下也是如此。

也就是说，您有2台设备，其中一台位于默认名称空间中，具有主机名且无流量，另一台位于特定Meraki名称空间中，且无主机名。

如果同时启用，其他集成可能会出现类似的“拆分”。

定义

1. 内部 IP 地址:XDRA考虑IP地址是内部地址还是外部地址，可通过子网设置进行配置。内部子网的默认子网为RFC内部子网（RFC1918和RFC4193），但可以配置（添加或删除）子网。
2. 命名空间：用于标记从不同观察点看到的netflow和设备的其他信息，允许重叠子网而不出现重叠IP问题。

ISE主机名数据流

1. ONA收集ISE会话数据，每10分钟上传至S3
    1. 此数据包含用户<->IP信息，有时也包含主机名
2. IseSessionsMiner解析上传的数据，并在可能的情况下将IP与设备相关联。如果设备尚不存在

，则不会创建设备。这样，只要我们已有设备，它就会收集可用的主机名<->IP映射。

3. 然后，它会在s3中创建与这些映射相同的文件，格式与ONA从其反向DNS查找上传的格式相同

4. 然后通知系统加载这些主机名，就像加载ONA主机名一样。

常见问题

为什么在XDRA设备上看到不再与网络上的该逻辑设备关联的IP?

不幸的是，我们对此无能为力。

系统无法知道旧关联是否无效或是由其他物理网络接口导致的。

我没有任何主机名信息发送到XDRA，为什么同时使用IPv4和IPv6地址的设备会显示为2个不同的设备？

如果没有主机名信息，我们就无法知道不同的IP与网络上的同一逻辑设备相关联。

为什么在同一个XDRA设备中会出现来自不同子网的多个逻辑设备？

XDRA目前无法区分来自哪个子网遥感勘测，因此相同的IP始终被分组到一个设备中。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。