Descripción del dispositivo en las instalaciones, nombre de host y asignación de IP en XDR-A

Contenido

Introducción

Este documento describe cómo entender el comportamiento de XDR-Analytics en relación con el nombre de host del dispositivo y la asignación de IP.

Background

XDRA intenta realizar un seguimiento del comportamiento de un dispositivo lógico a lo largo del tiempo, conocido como dispositivo.

Utiliza diversas técnicas para correlacionar el tráfico de red con estos dispositivos lógicos a lo largo del tiempo.

Sin embargo, especialmente en un entorno in situ, existen límites en cuanto a la capacidad del sistema para asociar el tráfico a un dispositivo.

XDRA recopila principalmente telemetría para entornos in situ a través de netflow mediante la integración de ONA, CTB o Cisco Meraki (la "nueva" integración de Meraki). En segundo lugar, puede obtener la resolución del nombre de host mediante:

- Resolución activa de nombres de host mediante búsquedas de DNS inversas y, opcionalmente, consultas SMB a través de ONA
- Integración de ISE a través de ONA
- La "antigua" integración con Meraki
- Integración de NVM, con advertencias adicionales

Netflow tiene direcciones IP sin información de nombre de host.

Sin la información del nombre de host, asume que cada dirección IP interna (ver definición a continuación) vista es un Dispositivo, ya que no tiene más información para hacer una asociación de Dispositivo más inteligente.

En un caso en el que se configura la recopilación de nombres de host, XDRA utiliza los nombres de host, cuando se ven, para vincularlos a una representación interna de Device.

Esto permite a XDRA agrupar varias direcciones IP en un único dispositivo a lo largo del tiempo.

La telemetría de NVM se puede configurar opcionalmente como parte de XDR.

Este origen de telemetría proporciona una fuente de datos similar a NetFlow, pero también proporciona información de terminales con identificadores únicos.

La forma en que XDRA utiliza esta información tiene el efecto neto de que el seguimiento de dispositivos se comporte de forma similar al caso en el que la recopilación de nombres de host está habilitada en la ONA.

Todas estas configuraciones tienen limitaciones basadas en las limitaciones de la telemetría disponible.

Tenga en cuenta que XDRA supone que la naturaleza de las asignaciones de direcciones IP y nombres de host es una relación de varios a uno (muchas IP se pueden asignar a un nombre de host).

Un dispositivo lógico puede tener varias IP simultáneamente (por ejemplo, dos interfaces físicas o IPv4 e IPv6).

Debido a la naturaleza de la monitorización, XDCAM nunca puede suponer que tiene todas las relaciones de la red en un momento dado.

Superposición de subredes

En el caso de que un único arrendatario XDRA esté monitorizando varias subredes en las instalaciones de forma simultánea, el sistema no puede distinguir entre la misma IP que se ve en cada una de ellas.

Como tal, correlaciona excesivamente las IP con los dispositivos. La disponibilidad del nombre de host no mejora esta situación.

Una forma de evitarlo es tener más de un portal XDRA (uno por subred). Otra es utilizar la "nueva" integración de Cisco Meraki debido al aislamiento del espacio de nombres que conlleva.

Entorno sin información de nombre de host disponible

Como efecto secundario de la información de telemetría limitada, el sistema puede llegar a una comprensión incorrecta del historial de dispositivos.

Una de ellas es cuando las IP se asignan de forma dinámica, XDRA no tiene forma de saber que el dispositivo lógico subyacente ha cambiado, por ejemplo, cuando un ordenador portátil deja WIFI, y la IP se asigna a un nuevo ordenador portátil.

En ausencia de nombre de host u otra información de identificación, el sistema asocia las actividades de varios dispositivos lógicos a un dispositivo. Esto puede llevar a confundir la información del perfil del dispositivo.

```
Actual Situation
    t0      t1      t2      t3
```

```
ip1 d1------        d2------

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

Por el contrario, en los casos en los que un dispositivo lógico tiene más de una dirección IP (por ejemplo, dos interfaces físicas o IPv4 e IPv6), no hay información con la que podamos vincularlos de forma fiable al mismo dispositivo, por lo que el sistema no lo hace.

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

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

Entorno con información de nombre de host

Si XDRA puede ver la información del nombre de host, el sistema puede asociar más de una dirección IP a un dispositivo. Sin embargo, dada la naturaleza de los datos, todavía existen límites a lo que el sistema puede determinar de manera fiable. Esto puede llevar a una correlación excesiva de IP con los dispositivos del sistema.

Si un dispositivo tiene una asociación de IP a nombre de host en XDRA y, a continuación, el dispositivo lógico cambia la dirección IP, la telemetría refleja finalmente la nueva asignación de IP a nombre de host.

Sin embargo, debido a la posibilidad de que se trate de una relación de varios a uno, XDRA NO puede asumir de forma segura que la IP previamente vista ya no esté asociada al nombre de host (y, por tanto, al dispositivo).

Podría ser, por ejemplo, una interfaz física independiente para el mismo dispositivo lógico. Así pues, XDRA mantiene las dos IP anteriores junto con la IP más reciente, hasta que se descubra la telemetría que asigna positivamente la dirección IP a un nombre de host diferente.

En este momento, XDR 'caduca' la asignación y se mostrará como una dirección IP anterior.

No hay manera de decirle al sistema que interrumpa una asociación "temprano".

Nota sobre coincidencia de nombre de host

Para tratar de gestionar mejor los casos en los que un arrendatario tiene el mismo nombre de host configurado en varios dominios, XDRA emplea una coincidencia "flexible" y trata las entradas

que se muestran en esta tabla como nombres de host coincidentes cuando busca coincidir con un dispositivo existente (es decir, en el caso de una IP coincidente):

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

En otras palabras, considera solamente el nombre de host mientras ignora el resto del nombre de dominio.

Entorno con NVM

Esta configuración se comporta de manera muy similar a la sección Entorno con información de nombre de host con información de nombre de host, pero hay algunas diferencias.

Esta fuente de datos proporciona las ventajas añadidas de poder proporcionar algunos identificadores de terminales únicos al usuario, y estas ID nos permiten potencialmente realizar un seguimiento de un dispositivo físico que sufre un cambio de nombre de host (que no es posible realizar un seguimiento de lo contrario, crearíamos 2 dispositivos diferentes).

Mientras que los dispositivos se crean en función de la fuente de datos del terminal (con ID de terminal únicos), no hay ningún nombre de host ni IP asociados con estos dispositivos hasta que se realice una observación sobre ese terminal basada en los datos de flujo.

Entornos con ISE

Las ventajas del seguimiento de ISE a dispositivo acaban siendo idénticas a las del entorno con información de nombre de host.

Los datos de ISE se utilizan para asociar la información de nombre de host que recopila con las direcciones IP, pero no crean un nuevo dispositivo ni realizan un seguimiento de las IP que no se han visto en netflow.

Entornos con Meraki

Integración con Meraki "antigua" (es decir, con XDRA)

Esta integración de Meraki recopila de forma proactiva la información del nombre de host de los dispositivos Meraki, asignando dichos nombres de host a las IP de la forma habitual para los dispositivos in situ (es decir, el "espacio de nombres predeterminado").

Este proceso crea Dispositivos si aún no existen.

No aumenta la información de IP o de dispositivos recopilada de la otra "nueva" integración de Cisco Meraki debido a las diferencias de espacio de nombres.

En efecto, esto hace que esta configuración se comporte como un entorno con información de nombre de host.

"Nueva" integración de Cisco Meraki (es decir, con XDR)

Esta integración permite que el flujo de red de los equipos de red Meraki, a través del lago de datos XDR, entre en la ruta de NetFlow estándar de XDRA.

Como tal, crea Dispositivos como cualquier otro Netflow; al igual que cualquier otro netflow, no contiene información de nombre de host.

En efecto, esta configuración se comporta como Entorno sin información de nombre de host disponible, con una excepción importante.

Esta integración aprovecha la información enviada para etiquetar el flujo de red de diferentes equipos Meraki en diferentes espacios de nombres.

Esto evita los problemas habituales de superposición de subredes, pero puede introducir nuevas dificultades si se configura más de una integración.

Obviamente, si se configuran las integraciones Meraki "antigua" y "nueva", no se utilizan los mismos espacios de nombres y, por tanto, se crean dispositivos que no se solapan, incluso en aquellos casos en los que la información representa el mismo dispositivo físico.

Es decir, tiene 2 dispositivos, uno en el espacio de nombres predeterminado con un nombre de host y sin tráfico, otro con tráfico en un espacio de nombres Meraki específico y sin nombre de host.

Pueden producirse "divisiones" similares con otras integraciones si se habilitan simultáneamente.

Definiciones

1. Dirección IP interna: XDRA tiene en cuenta las direcciones IP internas o externas, y esto se puede configurar a través de los parámetros de subred. Las subredes para las subredes en las instalaciones tienen de forma predeterminada las subredes internas RFC (RFC1918 y RFC4193), pero las subredes se pueden configurar (agregar o quitar).
2. Espacio de nombres: Información adicional que se utiliza para etiquetar netflow y Devices vistos desde diferentes puntos de observación, lo que permite superponer subredes sin problemas de IP superpuestos.

Flujo de datos de ISE Hostname

1. ONA recopila los datos de la sesión de ISE y los carga en S3 cada 10 minutos
    1. estos datos contienen información de usuario<->IP, y a veces también incluye el nombre de host
2. IseSessionsMiner analiza los datos cargados y asocia las IP a los dispositivos cuando es posible. NO crea un dispositivo si aún no existe uno. Al mismo tiempo, recopila los mapeos IP de los nombres de host disponibles<->cada vez que tenemos un dispositivo.
3. A continuación, crea un archivo en s3 con esas asignaciones en el mismo formato en que ONA cargaría uno desde sus búsquedas de DNS inversas
4. Luego le dice al sistema que cargue esos hostnames tal como cargaría los hostnames ONA.

Preguntas frecuentes

¿Por qué veo IP en un dispositivo XDRA que ya no están asociadas a ese dispositivo lógico en mi red?

Desafortunadamente, no hay nada que podamos hacer al respecto.

El sistema no puede saber si la asociación anterior no es válida o es el resultado de, por ejemplo, una interfaz de red física adicional.

No se ha enviado ninguna información de nombre de host a XDRA, ¿por qué mi dispositivo que utiliza direcciones IPv4 e IPv6 se muestra como 2 dispositivos distintos?

Sin la información del nombre de host, no podemos saber que hay IP diferentes asociadas con el mismo dispositivo lógico en su red.

¿Por qué aparecen varios dispositivos lógicos de diferentes subredes en el mismo dispositivo XDCAM?

XDRA actualmente no tiene forma de distinguir de qué subred proviene la telemetría, por lo que la misma IP siempre se agrupa en un dispositivo.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).