Implementación de prácticas recomendadas de SSDP en switches Catalyst serie 9000

Contenido

Introducción

Este documento describe las configuraciones de prácticas recomendadas diseñadas para descartar o limitar los paquetes del protocolo simple de detección de servicios (SSDP) en los switches Catalyst serie 9000.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Operación de multidifusión independiente de protocolo (PIM)
- Cómo se utiliza SSDP específico para su entorno

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Catalyst 9200
- Cisco Catalyst 9300
- Cisco Catalyst 9400
- Cisco Catalyst 9500
- Cisco Catalyst 9600

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Comprender los riesgos de SSDP en entornos empresariales

En general, los dispositivos de los usuarios finales, como los portátiles y los teléfonos móviles, anuncian automáticamente sus funciones Universal Plug-and-Play (UPnP) que utilizan el protocolo SSDP. Los clientes envían un paquete de anuncio multicast a la dirección IP 239.255.255.250. Estos anuncios suelen enviarse con un tiempo de vida (TTL) de 1 y no van más allá de la subred local de los hosts que generaron el paquete de multidifusión. Para recibir los anuncios de otros dispositivos en la red, los terminales también envían un informe de afiliación IGMP a la dirección 239.255.255.250, que indica a la red que el tráfico multicast enviado a esta dirección IP desde cualquier otra fuente multicast también debe ser reenviado a este cliente.

En entornos empresariales que contienen cientos o miles de terminales que actúan como origen y como receptor interesado de este grupo, esta actividad del cliente puede saturar fácilmente los dispositivos de red si no se controla y puede provocar interrupciones una vez que se hayan agotado los recursos de red.

Este agotamiento ocurre principalmente de una de dos maneras:

1. Agotamiento de recursos de hardware que provoca fallos de protocolo secundarios
2. Agotamiento del ancho de banda de la interfaz y la plataforma desde el SSDP utilizado como ataque de denegación de servicio (DDoS) distribuido.

Si bien no se trata en detalle en este documento, se debe tener en cuenta que debido a la naturaleza abierta de SSDP, es posible que un atacante envíe un paquete diseñado a un grupo de clientes con este servicio habilitado para activar una respuesta grande que se envíe a uno o a un grupo de hosts de destino. La gran cantidad de estado de la interfaz saliente que se crea también significa que la capacidad de rendimiento del switch se puede destacar significativamente a partir de una pequeña cantidad de tráfico de multidifusión, ya que el switch es necesario para hacer una copia de cada trama para cada interfaz saliente dentro del circuito integrado específico de la aplicación (ASIC). Las listas de interfaces salientes que suman 20 o más interfaces corren un mayor riesgo de problemas de capacidad y pérdida de paquetes.

Síntomas del agotamiento de los recursos de hardware

Los switches Catalyst de la serie 9000 imprimen los syslogs que mencionan "fman_fp_image" o "FMFP" cuando se han agotado los recursos. Algunos o todos estos errores pueden imprimirse cuando el switch ha experimentado un agotamiento de recursos y es necesario investigarlos más a fondo.

Estos son algunos de los errores más comunes observados durante el agotamiento de los recursos, pero no son una lista completa.

Figura 1: Ejemplo de los errores más comunes impresos que son evidencia del agotamiento de recursos en un switch

```
%FMFP-3-OBJ_DWNLD_TO_DP_STUCK: R0/0: fman_fp_image: AOM download to Data Plane is stuck for more
than 1800 seconds for <object details>
%FMFP-3-OBJ_DWNLD_TO_DP_RESUME: R0/0: fman_fp_image: AOM download of objects to Data Plane is
back to normal
%FMFP_QOS-6-QOS_STATS_STALLED: R0/0: fman_fp_image: statistics stalled
%FMFP-3-OBJ_DWNLD_TO_DP_FAILED: R0/0: fman_fp_image: adj <hex>, Flags None download to DP failed
%FMFP-3-OBJ_DWNLD_TO_DP_FAILED: R0/0: fman_fp_image: adj <hex>, Flags Midchain download to DP
failed
%FED_L3M_ERRMSG-3-RSRC_ERR: Switch <num> R0/0: fed: Failed to allocate hardware resource for
```

```
group <address> - rc:<number or error>
%FED_L3_ERRMSG-3-RSRC_ERR: Chassis <num> R0/0: fed: Failed to allocate hardware resource for adj
entry due to hardware resource exhaustion - rc:<number or error>
```

Verificación del Agotamiento de Recursos de Hardware Causado por SSDP

Todos los switches Catalyst de la serie 9000 utilizan ASIC especiales para realizar la mayoría del routing de paquetes con un alto rendimiento. Estos ASIC aprovechan diferentes tablas y recursos internos que son finitos en su capacidad. Debido a que los clientes SSDP actúan como fuentes y receptores para un grupo de multidifusión común, el hardware debe utilizar estos recursos limitados para programar una trayectoria en el hardware para que los paquetes sigan, incluso si esos paquetes nunca llegan o se descartan por otras razones (TTL 1). Una vez agotados los recursos de hardware, no se pueden instalar nuevas actualizaciones o adiciones para ningún grupo, independientemente de su relación con SSDP. Un gran número de actualizaciones de SSDP no instaladas (conmutación por estado) también puede colocarse en cola en el software, lo que también puede provocar que se interrumpan o fallen las actualizaciones de hardware para el tráfico no multidifusión, lo que afecta al tráfico de los usuarios y provoca interrupciones en la red.

Este documento sólo es relevante si su red está configurada con PIM y tiene el estado multicast de capa 3 para la dirección de grupo SSDP conocida. Para verificar este criterio, ejecute el comando "**show ip mroute 239.255.255.250**" (agregue instrucciones vrf si es necesario). El grupo 239.255.255.250 es específico del protocolo SSDP.

Si el resultado del comando contiene un gran número de interfaces salientes y/o tiene un gran número de fuentes únicas para este grupo específico, esto indica que el sistema y la red son vulnerables a las interrupciones causadas por SSDP. Cuanto mayor sea el número de interfaces salientes y de fuentes únicas, mayores serán las probabilidades de que esto pueda afectar al servicio.

Figura 2: Ejemplo de salida de "show ip mroute 239.255.255.250" con SSDP activo en la red.

```
Switch#show ip mroute 239.255.255.250
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       G - Received BGP C-Mroute, g - Sent BGP C-Mroute,
       N - Received BGP Shared-Tree Prune, n - BGP C-Mroute suppressed,
       Q - Received BGP S-A Route, q - Sent BGP S-A Route,
       V - RD & Vector, v - Vector, p - PIM Joins on route,
       x - VxLAN group
Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 239.255.255.250), 00:08:35/stopped, RP 10.0.0.1, flags: SJC
  Incoming interface: GigabitEthernet0/0/1.40, RPF nbr 10.0.0.1
  Outgoing interface list:
    GigabitEthernet0/0/1.101, Forward/Sparse, 00:08:35/00:02:40
    GigabitEthernet0/0/1.102, Forward/Sparse, 00:08:35/00:02:38
```

```
    GigabitEthernet0/0/1.100, Forward/Sparse, 00:08:35/00:02:39

(10.1.1.2, 239.255.255.250), 00:01:40/00:01:19, flags: T
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    GigabitEthernet0/0/1.40, Forward/Sparse, 00:01:40/00:01:40, A
    GigabitEthernet0/0/1.100, Forward/Sparse, 00:01:40/00:02:39
    GigabitEthernet0/0/1.102, Forward/Sparse, 00:01:40/00:02:38
    GigabitEthernet0/0/1.101, Forward/Sparse, 00:01:40/00:02:40

(10.1.1.3, 239.255.255.250), 00:02:03/00:00:56, flags: JT
  Incoming interface: GigabitEthernet0/0/1.40, RPF nbr 10.1.1.1
  Outgoing interface list:
    GigabitEthernet0/0/1.100, Forward/Sparse, 00:02:03/00:02:39
    GigabitEthernet0/0/1.102, Forward/Sparse, 00:02:03/00:02:38
    GigabitEthernet0/0/1.101, Forward/Sparse, 00:02:03/00:02:40

(10.1.1.4, 239.255.255.250), 00:08:35/00:02:32, flags: T
  Incoming interface: GigabitEthernet0/0/1.40, RPF nbr 10.1.1.1
  Outgoing interface list:
    GigabitEthernet0/0/1.100, Forward/Sparse, 00:08:35/00:02:39
    GigabitEthernet0/0/1.102, Forward/Sparse, 00:08:35/00:02:38
    GigabitEthernet0/0/1.101, Forward/Sparse, 00:08:35/00:02:40, A
```

A menos que SSDP se utilice para un propósito específico, se espera que este resultado esté vacío, o tenga un número bajo de interfaces salientes y/o tenga un número bajo de fuentes únicas para evitar el agotamiento de los recursos y posibles impactos en el servicio.

Si se observa un gran número de grupos multicast, el comando **show platform software object-manager fp active statistics** o **show platform software object-manager fp switch active statistics** se puede utilizar para determinar si se ha agotado un recurso de hardware.

> **Nota:** Este comando no es específico del agotamiento de recursos desencadenado por el tráfico multicast, otros problemas pueden hacer que estos valores no sean cero.

Figura 3: Salida de **"show platform software object-manager fp active statistics"**en estado de problema

```
Switch#show platform software object-manager fp active statistics
Forwarding Manager Asynchronous Object Manager Statistics
Object update: Pending-issue: 109058, Pending-acknowledgement: 76928   <-- Pending-issue is very
high, this
Batch begin:   Pending-issue: 0, Pending-acknowledgement: 0                  is not expected.
Batch end:     Pending-issue: 0, Pending-acknowledgement: 0
Command:       Pending-acknowledgement: 0
Total-objects: 304085
Stale-objects: 0
Resolve-objects: 0
Childless-delete-objects: 530
Error-objects: 1098

Paused-types: 127
```

El resultado de la figura 3 muestra los síntomas de un switch con agotamiento de recursos. Hay varias líneas de salida de comandos que no se esperan durante el funcionamiento normal:

- Problema pendiente: Se espera que esto sea cero o cercano. Si este sigue siendo un valor grande, distinto de cero en varias iteraciones del comando, es un signo del agotamiento de

los recursos
- Confirmación pendiente: Se espera que esto sea cero o cercano. Si este sigue siendo un valor grande, distinto de cero en varias iteraciones del comando, es un signo del agotamiento de los recursos
- Childless-delete-Objects: Se espera que esto sea cero o cercano. No se esperan valores de más de 10.
- Objetos de error: Se espera que esto sea cero o cercano. No se esperan valores de más de 10.

De forma uniforme, en un estado en el que hay un gran número de contadores de "problemas pendientes" o de "reconocimiento pendiente" aumenta el riesgo de que el hardware se vuelva mal programado. El hardware programado incorrectamente es una fuente común de interrupciones del tráfico de unidifusión y multidifusión.

El comando "**show platform hardware fed switch active fwd-asic resource utilization**" or in some models "**show platform hardware fed active fwd-asic resource utilization**" se puede utilizar para observar algunos de los recursos finitos en uso en los ASIC y determinar si se ha agotado un recurso interno:

Figura 4: Ejemplo de salida de"show platform hardware fed active fwd-asic resource utilization"con un recurso casi agotado.

```
Switch#show platform hardware fed active fwd-asic resource utilization
Resource Info for ASIC Instance: 0
Resource Name           Allocated Free
-----------------------------------------
RSC_DI                     3822       38076
RSC_FAST_DI                   0         192
RSC_RIET_0                    1        1024
RSC_RIET_1                    0         512
RSC_RIET_2                    0         512
RSC_RIET_3                    0         512
RSC_RIET_4                    0         512
RSC_RIET_5                    0         512
RSC_RIET_6                    0         256
RSC_RIET_7                    0         255
RSC_VLAN_LE                 116        3976
RSC_L3IF_LE                 116        3907
RIM_RSC_DGT                   1         255
RSC_VPN_PREFIX_ID             1       32768
RSC_LABEL_STACK_ID            1       65536
RSC_RI                     7358       82730
RSC_LI_RI                     0         129
RSC_PORT_LE_RI                0        2048
RSC_PORT_LE                   0        1827
RSC_RI_REP                10635      120437
RSC_SI                    11842      119072
RSC_SI_IND                    1         255
RSC_SI_STATS               3550       45602
RSC_RCP1_FID                  1        1023
RSC_RCP2_FID                  1        1023
RSC_RCP3_FID                  1        1023
RSC_RCP4_FID                  1        1023
RSC_LV1_ECR                   1          63
RSC_LV2_ECR                   3         253
RSC_ENH_ECR                   1           0
RSC_RPF_MATCH                12        1012
RSC_PLC                       1        2047
```

```
RSC_PLC_PF                    1         255
RSC_MTU_INDEX                 6         250
RSC_EGR_REDIRECT_INDEX        2        2046
RSC_RIL_INDEX 131065 7 <-- Free entries extremely low, this is not expected.
RSC_SIF                       1        1023
RSC_GROUP_LE                  1        1023
RSC_RI_REP_LOCAL              1           0
RSC_EXT_SI                  512       65024
```

En la figura 4, el valor de "RSC_RIL_INDEX" muestra que hay 131065 entradas en uso y sólo 7 son libres. Este recurso lo consumen grandes cantidades de grupos SSDP únicos. Aunque no es específico de SSDP, los recursos que tienen un número bajo de entradas libres y un número alto de entradas asignadas son señales de que el switch se encuentra cerca de un problema de capacidad, y deben investigarse.

El comando "**show platform hardware fed switch active fwd-asic resource tcam utilization**" or on some models "**show platform hardware fed active fwd-asic resource tcam utilization**" se puede utilizar para ver un desglose por ASIC de la utilización por recurso. Otra posible firma del agotamiento de SSDP es la columna "Valores usados" para las "Entradas de multidifusión de L3" que se acercan a o en los "Valores máximos".

Figura 5: Ejemplo de salida de"show platform hardware fed active fwd-asic resource tcam utilization"en funcionamiento normal

```
Switch#show platform hardware fed active fwd-asic resource tcam utilization
CAM Utilization for ASIC  [0]
 Table                                              Max Values        Used Values
 ------------------------------------------------------------------------------
 Unicast MAC addresses                               32768/768       6160/21
 L3 Multicast entries                                32768/768       3544/8      <-- Normal
Utilization, not near Max Values
 L2 Multicast entries                                 2304            181        <-- Normal
Utilization, not near Max Values
 Directly or indirectly connected routes            212992/1536     11903/39
 Input Ipv4 QoS Access Control Entries                5632             17
 Input Non Ipv4 QoS Access Control Entries            2560             36
 Output Ipv4 QoS Access Control Entries               6144             13
 Output Non Ipv4 QoS Access Control Entries           2048             27
 Input Ipv4 Security Access Control Entries           7168             12
 Input Non Ipv4 Security Access Control Entries       5120             76
 Output Ipv4 Security Access Control Entries          7168             11
 Output Non Ipv4 Security Access Control Entries      8192             27
 Ingress Netflow ACEs                                 1024              8
 Policy Based Routing ACEs                            3072             20
 Egress Netflow ACEs                                  1024              8
 Flow SPAN ACEs                                        512              5
 Flow Egress SPAN ACEs                                 512              8
 Control Plane Entries                                1024            235
 Tunnels                                              2816             26
 Lisp Instance Mapping Entries                         512              3
 Input Security Associations                           512              4
 SGT_DGT                                             32768/768          0/1
 CLIENT_LE                                            8192/512          0/0
```

```
INPUT_GROUP_LE                                  1024             0
OUTPUT_GROUP_LE                                 1024             0
Macsec SPD                                       256             2
```

Evitar el agotamiento de recursos causado por SSDP

Para detener el agotamiento de los recursos, el tráfico SSDP debe detenerse antes de la primera creación de estado de salto de capa 3 y multidifusión. La solución más rápida es utilizar una lista de control de acceso (ACL) IPv4 aplicada al ingreso a todas las interfaces L3 configuradas con PIM que ven este tráfico. Verifique con el comando "**show ip mroute 239.255.255.250**" y observe la "Interfaz Entrante" para cada grupo. Esto indica a qué interfaz L3 se origina el origen del tráfico y debe tener en cuenta que puede haber más de una interfaz de origen única. Este ejemplo de configuración permite que SSDP funcione en la capa 2 y permite que los hosts adyacentes a L2 detecten los servicios PNP, pero evita que los anuncios de cliente se reenvíen a través de los límites de L3, y evita la creación de estado multicast de L3 en cualquier router o switch multicast.

Configure una ACL extendida:

ip access-list extended BLOCK_SSDP remark Block SSDP **deny ip any host 239.255.255.250 <-- Deny SSDP**
permit ip any any **<-- Permit any other group**

Configure en cada interfaz L3, aplique la ACL en la dirección de ingreso:

```
Switch#configure terminal
Switch(config)#interface vlan100
Switch(config-if)#ip access-group BLOCK_SSDP in
Switch(config-if)#end
```