Voer SSDP Best Practices op Catalyst 9000 Series Switches in

Inhoud

Inleiding

Dit document beschrijft de optimale werkmethoden die zijn ontworpen om de pakketten Simple Service Discovery Protocol (SSDP) op Catalyst 9000 Series switches te laten vallen of beperken.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Protocol Independent Multicast (PIM)-exploitatie
- Hoe SSDP specifiek voor uw omgeving wordt gebruikt

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

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

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Ga uit van SSDP-risico's in ondernemingsomgevingen

In het algemeen maken eindgebruikers-apparaten zoals laptops en mobiele telefoons automatisch reclame voor hun Universal Plug-and-Play (UPnP)-functies die gebruik maken van het SSDP-protocol. Clients verzenden een multicast advertentiepakket naar het IP-adres van 239.255.255.250. Deze advertenties worden vaak verzonden met een tijd om (TTL) van 1 te leven, en gaan niet verder dan het lokale net van de hosts die het multicast-pakket gegenereerd hebben. Om de advertenties van andere apparaten op het netwerk te ontvangen, verzenden endpoints ook een IGMP Membership Report naar het adres 239.255.255.250, dat het netwerk vertelt dat multicast verkeer dat vanuit een andere multicast bron naar dit IP-adres wordt gestuurd ook naar deze client moet worden doorgestuurd.

In bedrijfsomgevingen die honderden of duizenden eindpunten bevatten die allemaal als bron, en een geïnteresseerde ontvanger van deze groep optreden, kan deze clientactiviteit gemakkelijk netwerkapparaten overweldigen als ze niet wordt gecontroleerd en kan ze uitvallen als de netwerkbronnen zijn uitgeput.

Deze uitputting vindt voornamelijk op twee manieren plaats:

1. Uitputting van hardware-bronnen die secundaire protocolfouten veroorzaakt
2. Uitputting van interface- en platformbandbreedte van SSDP die als gedistribueerde Denial of Service (DDoS) wordt gebruikt.

Hoewel dit document niet in detail is besproken, moet worden opgemerkt dat vanwege de open aard van het GVDB het voor een aanvaller mogelijk is om een samengesteld pakket naar een groep klanten te sturen met deze service die is ingeschakeld om een grote respons op te wekken naar een of een groep doelhosts wordt verstuurd. De grote hoeveelheid uitgaande interfacestatus die wordt gecreëerd, betekent ook dat de capaciteit voor de prestaties van de switch aanzienlijk kan worden benadrukt vanaf een kleine hoeveelheid multicast verkeer omdat de switch verplicht is één exemplaar van elk kader te maken voor elke uitgaande interface in het Application Specific Integrated Circuit (ASIC). Uitgaande interfacelijsten die nummer 20 of meer interfaces hebben een hoger risico op capaciteitsproblemen en pakketverlies.

Symptomen van uitputting van hardwarebronnen

Catalyst 9000 Series switches afdrukken syslogs die "fman_fp_image" of "FMFP" vermelden wanneer de middelen zijn uitgeput. Een deel van deze fouten of een deel daarvan kan worden afgedrukt wanneer de switch een uitputting van de middelen heeft ondervonden en verder moet worden onderzocht.

Dit zijn enkele van de meest voorkomende fouten die tijdens de uitputting van middelen worden gezien, maar het is geen volledige lijst.

Afbeelding 1: Steekproef van de meest voorkomende gedrukte fouten die het bewijs zijn van uitputting van middelen op een 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>
```

Controleer de hardware-bron-uitputting veroorzaakt door SSDP

Alle Catalyst 9000 Series switches gebruiken speciale ASICs om de meerderheid van pakket uit te voeren routing bij hoge doorvoersnelheid. Deze ASIC's maken gebruik van verschillende tabellen en interne middelen die eindig zijn in hun hoedanigheid. Omdat SSDP-clients zowel als bronnen als ontvangers voor een gemeenschappelijke multicast-groep fungeren, moet de hardware deze beperkte middelen gebruiken om een pad in hardware-pakketten te programmeren die moeten worden gevolgd, zelfs als die pakketten nooit om andere redenen komen of worden gedropt (TTL 1). Zodra de hardwarebronnen zijn uitgeput, kunnen geen nieuwe updates of toevoegingen voor een groep worden geïnstalleerd, ongeacht de relatie met het SSDP. Grote aantallen niet-geïnstalleerde SSDP-updates (state churn) kunnen ook in de wachtrij voor software staan, dit kan er ook toe leiden dat hardwareupdates voor niet-multicast verkeer worden onderbroken of mislukt, wat invloed heeft op het gebruikersverkeer en netwerkstoringen veroorzaakt.

Dit document is alleen relevant als uw netwerk is geconfigureerd met PIM en Layer 3 multicast status heeft voor het bekende SSDP-groepsadres. Om deze criteria te controleren, voert u de opdracht uit "**show ip mroute 239.255.255.250**" (indien nodig vrf - verklaringen toevoegen). De groep 239.255.255.250 is specifiek voor het SSDP-protocol.

Als de opdrachtoutput een groot aantal uitgaande interfaces bevat en/of een groot aantal unieke bronnen voor deze specifieke groep heeft, betekent dit dat het systeem en het netwerk kwetsbaar zijn voor storingen die door het SSDP worden veroorzaakt. Hoe hoger het aantal uitgaande interfaces en unieke bronnen, hoe groter de kans dat dit van invloed kan worden op de service.

Afbeelding 2: Monsteruitvoer van "show ip mroute 239.255.255.250" opdracht met SSDP actief op het netwerk.

```
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
```

Tenzij het SSDP voor een specifiek doel wordt gebruikt, wordt verwacht dat deze output leeg is of een laag aantal uitgaande interfaces heeft en/of een laag aantal unieke bronnen heeft om uitputting van de hulpbron en mogelijke diensteneffecten te voorkomen.

Als een groot aantal multicast groepen wordt gezien, kan de opdracht "**show platform software object-manager fp actieve statistics**" of "**show platform software object-manager fp switch" worden gebruikt om te vertellen of een hardwarebron is uitgeput.**

> **Opmerking:** Deze opdracht is niet specifiek voor resource uitputting die door multicast verkeer wordt veroorzaakt, andere problemen kunnen deze waarden niet-nul veroorzaken.

Afbeelding 3: Uitvoer van **"show platform software object-manager fp active statistics"**in probleemtoestand

```
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
```

De output van figuur 3 toont symptomen van een switch met uitputting van de middelen. Er zijn meerdere opdrachtoutput lijnen die niet verwacht worden tijdens normaal gebruik:

- In afwachting van afgifte: Verwacht wordt dat dit nul is, of dicht bij hem. Als dit een grote, niet-nulwaarde over verscheidene iteraties van het bevel blijft, is dat een teken van uitputting van

middelen
- In afwachting van erkenning: Verwacht wordt dat dit nul is, of dicht bij hem. Als dit een grote, niet-nulwaarde over verscheidene iteraties van het bevel blijft, is dat een teken van uitputting van middelen
- Kinderloze verwijderaars-objecten: Naar verwachting is dit nul of dichtbij het niveau. Waarden van meer dan 10 worden niet verwacht.
- Fout-objecten: Naar verwachting is dit nul of dichtbij het niveau. Waarden van meer dan 10 worden niet verwacht.

In een staat waar er grote aantallen tellers ‘hangende-kwestie' of ‘hangende-erkenningsvraag' zijn verhoogt consistent het risico dat de hardware verkeerd geprogrammeerd wordt. Onjuist geprogrammeerde hardware is een veel voorkomende bron van uitval naar unicast en multicast verkeer.

De opdracht "**show platform hardware fed switch active fwd-asic resource utilization**" or in some models "**show platform hardware fed active fwd-asic resource utilization**" kan worden gebruikt om een aantal van de eindige middelen die op de ASIC's worden gebruikt te bekijken en om te bepalen of een interne bron is uitgeput:

Afbeelding 4: Monsteruitvoer van"show platform hardware fed active fwd-asic resource utilization"met één hulpbron nabij uitputting.

```
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
```

In figuur 4 toont de waarde voor "RSC_RIL_INDEX" 131065 waarden in gebruik en slechts 7 zijn gratis. Deze hulpbron wordt gebruikt door grote aantallen unieke SSDP-groepen. Hoewel het GVDB niet specifiek is, zijn middelen die een laag aantal gratis inzendingen en een hoog aantal toegewezen inzendingen bevatten tekens die de switch in de buurt van een capaciteitskwestie is, en moeten ze worden onderzocht.

De opdracht "**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**" kan worden gebruikt om te kijken naar een per-ASIC uitsplitsing van gebruik naar bron. Een andere mogelijke handtekening van de SSDP-uitputting is de kolom "Gebruikte waarden" voor "L3 Multicast items" om deze te sluiten op of bij de "Max Values".

Afbeelding 5: Monsteruitvoer van"show platform hardware fed active fwd-asic resource tcam utilization"bij normaal gebruik

```
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
```

Voorkomen dat door SSDP wordt uitgescheiden

Om uitputting van middelen tegen te gaan, moet het SSDP verkeer vóór de eerste L3 hoop en multicast state creatie worden gestopt. De snelste oplossing is om een IPv4 Access Control List (ACL) te gebruiken die is toegepast op alle L3-interfaces die zijn geconfigureerd met PIM in dit verkeer. Controleer met de opdracht "toon ip route 239.255.255.250" en kijk naar de "inkomende interface" voor elke groep. Dit geeft aan welke L3-interface de bron van het verkeer is afgeleid en wees erop dat er meer dan één unieke broninterface kan zijn. Dit configuratievoorbeeld maakt SSDP in staat om bij Layer 2 te werken en laat L2-aangrenzende hosts toegang bieden om PNP-services te ontdekken, maar voorkomt dat clientadvertenties over L3-grenzen worden doorgestuurd, en voorkomt de creatie van L3 multicast op elke multicast router of switch.

Configureer een uitgebreide ACL:

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**

Configureer onder elke L3-interface de ACL in de invoerrichting:

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