Implementazione delle best practice SSDP sugli switch Catalyst serie 9000

Sommario

Introduzione

In questo documento vengono descritte le best practice per eliminare o limitare i pacchetti SSDP (Simple Service Discovery Protocol) sugli switch Catalyst serie 9000.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Operazione PIM (Protocol Independent Multicast)
- Modalità di utilizzo di SSDP specifico per l'ambiente

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Comprensione dei rischi SSDP negli ambienti aziendali

In generale, i dispositivi degli utenti finali, ad esempio i laptop e i telefoni cellulari, pubblicizzano automaticamente le funzionalità UPnP (Universal Plug-and-Play) che utilizzano il protocollo SSDP. I client inviano un pacchetto di annuncio multicast all'indirizzo IP 239.255.255.250. Questi annunci vengono spesso inviati con un valore TTL (Time to Live) pari a 1 e non vanno oltre la subnet locale degli host che hanno generato il pacchetto multicast. Per ricevere gli annunci di altri dispositivi nella rete, gli endpoint inviano inoltre un report sull'appartenenza IGMP all'indirizzo 239.255.255.250, che indica alla rete che anche il traffico multicast inviato a questo indirizzo IP da qualsiasi altra origine multicast deve essere inoltrato a questo client.

Negli ambienti aziendali che contengono centinaia o migliaia di endpoint che agiscono sia come origine sia come ricevitore interessato di questo gruppo, questa attività client può facilmente sovraccaricare i dispositivi di rete se non viene selezionata e può causare interruzioni una volta esaurite le risorse di rete.

Questa stanchezza si manifesta principalmente in due modi:

1. Esaurimento delle risorse hardware che causa errori del protocollo secondario
2. Esaurimento dell'interfaccia e della larghezza di banda della piattaforma da SSDP utilizzato come attacco DDoS (Distributed Denial of Service).

Anche se non discusse in dettaglio in questo documento, va notato che a causa della natura aperta di SSDP, è possibile per un utente malintenzionato inviare un pacchetto creato a un gruppo di client con questo servizio abilitato in modo da attivare l'invio di una risposta di grandi dimensioni a uno o a un gruppo di host di destinazione. La grande quantità di stato dell'interfaccia in uscita che viene creata significa anche che la capacità di prestazioni dello switch può essere significativamente aumentata da una piccola quantità di traffico multicast, in quanto lo switch deve fare una copia di ogni frame per ogni interfaccia in uscita all'interno del circuito integrato specifico dell'applicazione (ASIC, Application Specific Integrated Circuit). Nell'elenco delle interfacce in uscita, numero 20 o più, le interfacce presentano un rischio maggiore di problemi di capacità e di perdita di pacchetti.

Sintomi dell'esaurimento delle risorse hardware

Gli switch Catalyst serie 9000 eseguono la stampa dei syslog che indicano "fman_fp_image" o "FMFP" quando le risorse sono esaurite. Alcuni o tutti questi errori possono essere stampati quando lo switch ha esaurito le risorse e deve essere esaminato ulteriormente.

Si tratta di alcuni degli errori più comuni rilevati durante l'esaurimento delle risorse, ma non di un elenco completo.

Figura 1: esempio degli errori più comuni stampati che dimostrano l'esaurimento delle risorse su uno switch

```
%FMFP-3-OBJ_DWNLD_TO_DP_STUCK: R0/0: fman_fp_image: AOM download to Data Plane is stuck for more than 1
%FMFP-3-OBJ_DWNLD_TO_DP_RESUME: R0/0: fman_fp_image: AOM download of objects to Data Plane is back to n
%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 <add
%FED_L3_ERRMSG-3-RSRC_ERR: Chassis <num> R0/0: fed: Failed to allocate hardware resource for adj entry
```

Verifica dell'esaurimento delle risorse hardware causato da SSDP

Tutti gli switch Catalyst serie 9000 utilizzano ASIC speciali per eseguire la maggior parte del routing dei pacchetti a un throughput elevato. Questi ASIC utilizzano tabelle e risorse interne diverse che sono limitate nella loro capacità. Poiché i client SSDP agiscono sia come origini che come ricevitori per un gruppo multicast comune, l'hardware deve utilizzare queste risorse limitate per programmare un percorso nell'hardware per i pacchetti da seguire, anche se quei pacchetti non arrivano mai o vengono scartati per altri motivi (TTL 1). Quando le risorse hardware sono esaurite, non è possibile installare nuovi aggiornamenti o aggiunte per alcun gruppo, indipendentemente dalla relazione con SSDP. Un numero elevato di aggiornamenti SSDP non installati (stato churn) può anche essere inserito in coda nel software, causando l'interruzione o il mancato completamento degli aggiornamenti hardware per il traffico non multicast, con conseguente impatto sul traffico utente e interruzione della rete.

Questo documento è pertinente solo se la rete è configurata con PIM e dispone di uno stato multicast di livello 3 per l'indirizzo di gruppo SSDP noto. Per verificare questi criteri, eseguire il comando "**show ip mroute 239.255.255.250**" (se necessario, aggiungere istruzioni vrf). Il gruppo 239.255.255.250 è specifico del protocollo SSDP.

Se l'output del comando contiene un numero elevato di interfacce in uscita e/o ha un numero elevato di origini univoche per questo gruppo specifico, il sistema e la rete sono vulnerabili alle interruzioni causate da SSDP. Maggiore è il numero di interfacce in uscita e di origini univoche, maggiori sono le probabilità che ciò influisca sui servizi.

Figura 2: Output di esempio di "show ip mroute 239.255.255.250" con SSDP attivo sulla rete.

<#root>

```
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 meno che SSDP non venga utilizzato per uno scopo specifico, questo output dovrebbe essere vuoto o avere un numero ridotto di interfacce in uscita e/o un numero ridotto di origini univoche al fine di evitare l'esaurimento delle risorse e possibili impatti sul servizio.

Se viene rilevato un numero elevato di gruppi multicast, il comando "show platform software object-manager fp active statistics" o "show platform software object-manager fp switch active statistics" può essere utilizzato per verificare se una risorsa hardware è stata esaurita.

Nota: questo comando non è specifico dell'esaurimento delle risorse causato dal traffico

---

multicast. Altri problemi possono causare valori diversi da zero.

Figura 3: Output di "show platform software object-manager fp active statistics"in stato di problema

<#root>

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

L'output della figura 3 mostra i sintomi di uno switch con esaurimento delle risorse. Durante il normale funzionamento, alcune righe di output del comando non sono previste:

- In attesa di emissione: il valore previsto è zero o un valore vicino a tale valore. Se questo valore rimane grande e diverso da zero in più iterazioni del comando, significa che le risorse sono esaurite
- Riconoscimento in sospeso: previsto zero o un valore vicino a zero. Se questo valore rimane grande e diverso da zero in più iterazioni del comando, significa che le risorse sono esaurite
- Childless-delete-objects: Questo valore dovrebbe essere zero o vicino ad esso. Non sono previsti valori pari a 10+.
- Error-objects: il valore previsto è zero o un valore vicino a tale valore. Non sono previsti valori pari a 10+.

In uno stato in cui sono presenti numerosi contatori "in sospeso" o "in attesa di conferma", il rischio che l'hardware venga programmato in modo non corretto aumenta. L'hardware non correttamente programmato è una fonte comune di interruzioni del traffico unicast e multicast.

Il comando "**show platform hardware fed switch active fwd-asic resource utilization**" or in some models "**show platform hardware fed active fwd-asic resource utilization**" può essere utilizzato per esaminare alcune delle risorse limitate in

uso negli ASIC e determinare se una risorsa interna è stata esaurita:

Figura 4: Output di esempio di"show platform hardware fed active fwd-asic resource utilization"con una risorsa quasi esaurita.

<#root>

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
```

Nella figura 4 il valore per "RSC_RIL_INDEX" mostra che sono in uso 131065 voci, e solo 7 sono libere. Questa risorsa è utilizzata da un numero elevato di gruppi SSDP univoci. Anche se non riguarda solo il protocollo SSDP, le risorse con un numero basso di voci libere e un numero elevato di voci allocate indicano che lo switch ha quasi problemi di capacità e devono essere esaminate.

Il 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**" Può essere utilizzato per esaminare un'analisi stratificata dell'utilizzo per risorsa per ASIC. Un'altra possibile firma dell'esaurimento SSDP è la colonna "Valori utilizzati" per "Voci multicast L3" da chiudere o in corrispondenza di "Valori massimi".

Figura 5: Output di esempio di"show platform hardware fed active fwd-asic resource tcam utilization"in condizioni operative normali

<#root>

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

Impedisci esaurimento risorse causato da SSDP

Per interrompere l'esaurimento delle risorse, è necessario arrestare il traffico SSDP prima della creazione del primo hop L3 e dello stato multicast. La soluzione più rapida è usare un Access Control List (ACL) IPv4 applicato in entrata a tutte le interfacce L3 configurate con PIM che vede questo traffico. Verificare con il comando "show ip route 239.255.255.250" e controllare l'"interfaccia in arrivo" per ciascun gruppo. Indica l'interfaccia L3 da cui proviene il traffico e indica che possono esistere più interfacce di origine univoche. Questo esempio di configurazione consente a SSDP di funzionare al layer 2 e agli host L2 adiacenti di rilevare i servizi PNP, ma impedisce l'inoltro di annunci client oltre i limiti L3 e la creazione di stato multicast L3 su qualsiasi router o switch multicast.

Configurare un ACL esteso:

<#root>

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

Configurare sotto ciascuna interfaccia L3, applicare l'ACL nella direzione in entrata:

<#root>

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

Metodi alternativi per il blocco di SSDP

Esistono altri metodi per limitare o impedire completamente la creazione di uno stato dal traffico SSDP. Poiché ogni rete è diversa, non tutte sono ugualmente efficaci e possono presentare determinati vantaggi o svantaggi specifici per ogni ambiente. Al momento della stesura del presente documento, un ACL con routing che blocca il traffico sulla SVI rimane la modalità più consigliata, efficace e con la minore intensità di configurazione per raggiungere l'obiettivo di ridurre lo stato e il volume del traffico, consentendo comunque ai client finali di utilizzare questo protocollo per rilevare i servizi sulla VLAN locale.

Comprendere attentamente i vantaggi e gli svantaggi di ciascuno dei metodi per determinare se è possibile adattarlo meglio all'ambiente.

Metodo alternativo 1: configurare il filtro RP PIM per impedire la registrazione di SSDP con RP

Questo metodo è utile per gli ambienti con mapping statico di Rendezvous Point (RP) in cui la creazione di un ACL su un numero elevato di interfacce SVI o L3 può richiedere un'intensa configurazione.

- Il vantaggio di questo metodo è che consente di applicare una singola configurazione a più interfacce L3 contemporaneamente.
- Lo svantaggio di questo metodo è che il traffico viene ancora indirizzato alla CPU dello switch come parte della normale creazione di stato per un router del primo hop. In ambienti con grandi quantità di utenti connessi direttamente o indirettamente o grandi quantità di traffico SSDP, questo traffico puntato è ancora in concorrenza con altro traffico di rete legittimo per le risorse CPU. Volumi eccessivi di traffico SSDP possono causare un impatto del servizio sul traffico multicast legittimo se il volume di traffico rimane elevato.

Per implementare questo metodo, attenersi alla seguente procedura:

Configurare un ACL per impedire il traffico SSDP indesiderato:

```
Switch(config)#
ip access-list standard 10
Switch(config-std-nacl)#
deny 239.255.255.250 <-- Deny SSDP from registering
Switch(config-std-nacl)#
permit 224.0.0.0 15.255.255.255


<-- Permit any other group
```

Configurare l'ACL creato come parte del mapping statico RP

```
<#root>
Switch#
configure terminal
Switch(config)#
ip pim rp-address 192.168.1.1 10
Switch(config-if)#
end
```

Metodo alternativo 2: configurare le VACL (Vlan Access-Maps) in modo da negare tutto il traffico SSDP

Questo metodo è utile per gli ambienti in cui SSDP non è necessario a L2 o L3, o in cui il volume di traffico SSDP esaurirà lo snooping IGMP o altre risorse multicast L2 dello switch.

- Il vantaggio di questo metodo è la scalabilità a un numero elevato di vlan in una singola configurazione. Rappresenta inoltre la forma più efficace per eliminare tutto il traffico SSDP dalla rete.
- Lo svantaggio di questo metodo è che i client che utilizzano legittimamente SSDP per individuare servizi adiacenti L2 non funzioneranno correttamente. Tutto il traffico SSDP su entrambe le interfacce L2 e L3 verrà scartato e non verrà formato alcuno stato su L2 o L3. Questa configurazione non è in grado di bloccare la creazione dello stato dal traffico ricevuto sulle interfacce L3 native.

Configurare due ACL. Il primo deve corrispondere solo al traffico SSDP e il secondo deve essere un catch-all utilizzato per identificare tutto il normale traffico di rete.

```
<#root>
```

```
Switch(config)#
ip access-list extended match_ssdp
Switch(config-ext-nacl)#
permit ip any host 239.255.255.250
Switch(config-ext-nacl)#
exit
Switch(config)#ip access-list extended match_all
Switch(config-ext-nacl)#
permit ip any any
```

Configurare una mappa di accesso vlan con due numeri di sequenza. Uno nega SSDP, uno permette tutto il resto del traffico. Applicarlo alle vlan desiderate.

<#root>

```
Switch#
configure terminal
Switch(config)#
vlan access-map block_ssdp 10
Switch(config-access-map)#
match ip address match_ssdp
Switch(config-access-map)#
action drop
Switch(config-access-map)#
vlan access-map block_ssdp 20
Switch(config-access-map)#
match ip address match_all
Switch(config-access-map)#
action forward
Switch(config-access-map)#
exit
Switch(config)#
vlan filter block_ssdp vlan-list
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).