Mise en oeuvre des meilleures pratiques SSDP sur les commutateurs de la gamme Catalyst 9000

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Components Used](#)
[Comprendre les risques liés au SSDP dans les environnements d'entreprise](#)
[Symptômes de l'épuisement des ressources matérielles](#)
[Vérifier l'épuisement des ressources matérielles causé par le protocole SSDP](#)
[Empêcher l'épuisement des ressources causé par le protocole SSDP](#)

Introduction

Ce document décrit les meilleures pratiques de configuration conçues pour supprimer ou limiter les paquets SSDP (Simple Service Discovery Protocol) sur les commutateurs de la gamme Catalyst 9000.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Fonctionnement du protocole PIM (Protocol Independent Multicast)
- Utilisation du protocole SSDP spécifique à votre environnement

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- 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 votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Comprendre les risques liés au SSDP dans les environnements d'entreprise

En général, les périphériques des utilisateurs finaux tels que les ordinateurs portables et les téléphones mobiles annoncent automatiquement leurs fonctionnalités UPnP (Universal Plug-and-Play) qui utilisent le protocole SSDP. Les clients envoient un paquet d'annonce de multidiffusion à l'adresse IP 239.255.255.250. Ces annonces sont souvent envoyées avec une durée de vie de 1 et ne dépassent pas le sous-réseau local des hôtes qui ont généré le paquet de multidiffusion. Pour recevoir les annonces d'autres périphériques sur le réseau, les points de terminaison envoient également un rapport d'appartenance IGMP à l'adresse 239.255.255.250, qui indique au réseau que le trafic de multidiffusion envoyé à cette adresse IP à partir de toute autre source de multidiffusion doit également être transféré à ce client.

Dans les environnements d'entreprise qui contiennent des centaines ou des milliers de terminaux agissant tous à la fois comme source et comme destinataire intéressé de ce groupe, cette activité client peut facilement submerger les périphériques réseau si elle n'est pas contrôlée et peut provoquer des pannes une fois les ressources réseau épuisées.

Cette épuisement se produit principalement de deux façons :

1. Épuisement des ressources matérielles qui déclenche des échecs de protocole secondaires
2. Épuisement de la bande passante de l'interface et de la plate-forme à partir du protocole SSDP utilisé comme attaque par déni de service distribué (DDoS).

Bien que ce document ne traite pas en détail, il convient de noter qu'en raison de la nature ouverte du protocole SSDP, un pirate peut envoyer un paquet élaboré à un groupe de clients avec ce service activé afin de déclencher une réponse importante à un ou plusieurs hôtes de destination. La grande quantité d'état d'interface sortante créée signifie également que la capacité de performance du commutateur peut être considérablement mise en évidence à partir d'un petit volume de trafic multidiffusion, car le commutateur est tenu de faire une copie de chaque trame pour chaque interface sortante dans le circuit intégré spécifique à l'application (ASIC). L'interface sortante indique que le nombre d'interfaces 20 ou plus présente un risque plus élevé de problèmes de capacité et de perte de paquets.

Symptômes de l'épuisement des ressources matérielles

Les commutateurs de la gamme Catalyst 9000 impriment des syslogs qui mentionnent « fman_fp_image » ou « FMFP » lorsque les ressources sont épuisées. Certaines, ou la totalité, de ces erreurs peuvent être imprimées lorsque le commutateur a connu une épuisement des ressources et doit être étudié plus avant.

Il s'agit de quelques-unes des erreurs les plus courantes observées lors de l'épuisement des ressources, mais il ne s'agit pas d'une liste exhaustive.

Figure 1 : Exemple des erreurs les plus courantes imprimées qui sont la preuve de l'épuisement des ressources sur un commutateur

```
%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>
```

Vérifier l'épuisement des ressources matérielles causé par le protocole SSDP

Tous les commutateurs de la gamme Catalyst 9000 utilisent des circuits ASIC spéciaux pour effectuer la majorité du routage de paquets à haut débit. Ces ASIC exploitent différentes tables et ressources internes qui sont limitées dans leur capacité. Comme les clients SSDP agissent à la fois comme sources et récepteurs pour un groupe de multidiffusion commun, le matériel doit utiliser ces ressources limitées pour programmer un chemin dans le matériel que les paquets doivent suivre, même si ces paquets ne viennent jamais ou ne sont jamais abandonnés pour d'autres raisons (TTL 1). Une fois les ressources matérielles épuisées, aucune nouvelle mise à jour ou ajout pour un groupe, quelle que soit sa relation avec SSDP, ne peut être installé. Un grand nombre de mises à jour SSDP non installées (désactivation d'état) peuvent également être mises en file d'attente dans le logiciel, ce qui peut également entraîner l'interruption ou l'échec des mises à jour matérielles pour le trafic non multicast, ce qui affecte le trafic utilisateur et provoque des pannes de réseau.

Ce document n'est pertinent que si votre réseau est configuré avec PIM et a un état de multidiffusion de couche 3 pour l'adresse de groupe SSDP connue. Pour vérifier ces critères, exécutez la commande "**show ip mroute 239.255.255.250**" (ajoutez des instructions vrf si nécessaire). Le groupe 239.255.255.250 est spécifique au protocole SSDP.

Si le résultat de la commande contient un grand nombre d'interfaces sortantes et/ou un grand nombre de sources uniques pour ce groupe spécifique, cela indique que le système et le réseau sont vulnérables aux pannes causées par le protocole SSDP. Plus le nombre d'interfaces sortantes et de sources uniques est élevé, plus les chances que cela puisse avoir un impact sur le service sont grandes.

Figure 2 : Exemple de sortie de "show ip mroute 239.255.255.250" avec SSDP actif sur le réseau.

```
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
```

Àmoins que le protocole SSDP ne soit utilisé à des fins spécifiques, ce résultat devrait être vide, ou avoir un faible nombre d'interfaces sortantes et/ou avoir un faible nombre de sources uniques afin d'éviter l'épuisement des ressources et les répercussions possibles sur le service.

Si un grand nombre de groupes de multidiffusion est visible, la commande "**show platform software object-manager fp active statistics**" ou "**show platform software object-manager fp switch active statistics**" peut être utilisée pour déterminer si une ressource matérielle a été épuisée.

> **Note**: Cette commande n'est pas spécifique à l'épuisement des ressources déclenché par le trafic de multidiffusion, d'autres problèmes peuvent faire que ces valeurs soient différentes de zéro.

Figure 3 : Résultats de **"show platform software object-manager fp active statistics"**dans l'état du problème

```
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

Le résultat de la figure 3 montre les symptômes d'un commutateur avec épuisement des ressources. Plusieurs lignes de sortie de commande ne sont pas attendues en fonctionnement normal :

- En attente : On s'attend à ce que ce chiffre soit égal à zéro, ou proche de celui-ci. Si cette valeur reste importante et non nulle sur plusieurs itérations de la commande, c'est un signe d'épuisement des ressources
- Accusé de réception en attente : On s'attend à ce que ce chiffre soit égal à zéro, ou proche de celui-ci. Si cette valeur reste importante et non nulle sur plusieurs itérations de la commande, c'est un signe d'épuisement des ressources
- Objets de suppression sans enfant : Cela devrait être zéro ou proche. Les valeurs de 10+ ne sont pas attendues.
- Objets d'erreur : Cela devrait être zéro ou proche. Les valeurs de 10+ ne sont pas attendues.

Dans un état où il y a un grand nombre de compteurs « en attente » ou « en attente d'accusé de réception » augmente le risque que le matériel ne soit pas programmé correctement. Le matériel mal programmé est une source commune de pannes pour le trafic de monodiffusion et de multidiffusion.

La commande "**show platform hardware fed switch active fwd-asic resource utilization**" or in some models "**show platform hardware fed active fwd-asic resource utilization**" peut être utilisé pour examiner certaines des ressources finies utilisées sur les ASIC et déterminer si une ressource interne a été épuisée :

Figure 4 : Exemple de sortie de"show platform hardware fed active fwd-asic resource utilization"avec une ressource presque épuisée.

```
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
```

Dans la figure 4, la valeur de « RSC_RIL_INDEX » indique qu'il y a 131065 entrées en cours d'utilisation, et seulement 7 sont gratuites. Cette ressource est consommée par un grand nombre de groupes SSDP uniques. Bien qu'il ne soit pas spécifique au protocole SSDP, les ressources dont le nombre d'entrées libres est faible et le nombre élevé d'entrées allouées indiquent que le commutateur est proche d'un problème de capacité et doivent être examinées.

La commande "**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**" peut être utilisé pour examiner une ventilation par ASIC de l'utilisation par ressource. Une autre signature possible de l'épuisement du protocole SSDP est la colonne « Valeurs utilisées » pour les entrées de multidiffusion de couche 3 à proximité ou au niveau des « Valeurs max. ».

Figure 5 : Exemple de sortie de"show platform hardware fed active fwd-asic resource tcam utilization"en fonctionnement 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
```

Empêcher l'épuisement des ressources causé par le protocole SSDP

Pour arrêter l'épuisement des ressources, le trafic SSDP doit être arrêté avant la création du premier saut de couche 3 et de l'état de multidiffusion. La solution la plus rapide consiste à utiliser une liste de contrôle d'accès IPv4 appliquée en entrée à toutes les interfaces de couche 3 configurées avec PIM qui voient ce trafic. Vérifiez avec la commande **show ip mroute 239.255.255.250** et regardez l'interface entrante de chaque groupe. Ceci indique l'interface de couche 3 à partir de laquelle provient la source du trafic et être conscient qu'il peut y avoir plus d'une interface source unique. Cet exemple de configuration permet au protocole SSDP de fonctionner au niveau de la couche 2 et permet aux hôtes contigus de couche 2 de découvrir des services PNP, mais empêche le transfert des annonces client au-delà des limites de couche 3 et empêche la création de l'état de multidiffusion de couche 3 sur tout routeur ou commutateur de multidiffusion.

Configurer une liste de contrôle d’accès étendue :

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**

Configurez sous chaque interface L3, appliquez la liste de contrôle d’accès dans la direction d’entrée :

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