Implementierung von SSDP Best Practices auf Catalyst Switches der Serie 9000

Inhalt

Einleitung

In diesem Dokument werden Best Practice-Konfigurationen beschrieben, mit denen die SSDP-Pakete (Simple Service Discovery Protocol) auf Catalyst Switches der Serie 900 verworfen oder eingeschränkt werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Protocol Independent Multicast (PIM)-Betrieb
- Verwendung von SSDP speziell für Ihre Umgebung

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Verständnis der SSDP-Risiken in Unternehmensumgebungen

Im Allgemeinen geben Endbenutzergeräte wie Laptops und Mobiltelefone automatisch ihre UPnP-Funktionen (Universal Plug-and-Play) an, die das SSDP-Protokoll verwenden. Clients senden ein Multicast-Werbepaket an die IP-Adresse 239.255.255.250. Diese Anzeigen werden häufig mit einer TTL (Time to Live) von 1 gesendet und gehen nicht über das lokale Subnetz der Hosts hinaus, die das Multicast-Paket generiert haben. Um Werbung für andere Geräte im Netzwerk zu erhalten, senden Endpunkte außerdem einen IGMP-Mitgliedschaftsbericht an die Adresse 239.255.255.250, die dem Netzwerk mitteilt, dass Multicast-Datenverkehr, der von einer anderen Multicast-Quelle an diese IP-Adresse gesendet wird, auch an diesen Client weitergeleitet werden muss.

In Unternehmensumgebungen, die Hunderte oder Tausende von Endpunkten enthalten, die alle als Quelle und als interessierter Empfänger dieser Gruppe fungieren, kann diese Clientaktivität Netzwerkgeräte leicht überlasten, wenn sie nicht kontrolliert werden, und Ausfälle verursachen, sobald die Netzwerkressourcen erschöpft sind.

Diese Erschöpfung geschieht hauptsächlich auf zwei Arten:

1. Erschöpfung der Hardwareressourcen, die sekundäre Protokollfehler auslöst
2. Die Bandbreitenbelegung von Schnittstellen und Plattformen durch SSDP wird als DDoS-Angriff (Distributed Denial of Service) verwendet.

Obwohl in diesem Dokument nicht ausführlich erläutert wird, ist zu beachten, dass ein Angreifer aufgrund des offenen Charakters von SSDP ein erstelltes Paket an eine Gruppe von Clients mit aktiviertem Dienst senden kann, um eine große Antwort an einen oder mehrere Zielhosts zu senden. Der hohe Anteil des ausgehenden Schnittstellenstatus, der erstellt wird, bedeutet auch, dass die Switch-Performance-Kapazität bei einem geringen Anteil an Multicast-Datenverkehr stark beansprucht werden kann, da der Switch eine Kopie jedes Frames für jede ausgehende Schnittstelle innerhalb des Application Specific Integrated Circuit (ASIC) erstellen muss. In der Liste der ausgehenden Schnittstellen ist angegeben, dass mindestens 20 Schnittstellen ein höheres Risiko für Kapazitätsprobleme und Paketverluste aufweisen.

Symptome eines erschöpfenden Hardwareressourcen

Catalyst Switches der Serie 9000 drucken Syslogs, die "fman_fp_image" oder "FMFP" angeben, wenn die Ressourcen ausgeschöpft wurden. Einige oder alle dieser Fehler können ausgegeben werden, wenn der Switch eine Ressourcenauslastung festgestellt hat und weiter untersucht werden muss.

Dies sind einige der häufigeren Fehler, die während der Ressourcenauslastung beobachtet wurden, jedoch keine umfassende Liste.

Abbildung 1: Beispiel für die häufigsten Fehlermeldungen, die den Nachweis eines erschöpften Zugriffs auf einen Switch erbringen

```
%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>
```

Überprüfung des durch SSDP verursachten Hardwareressourcenverlusts

Alle Catalyst Switches der Serie 9000 verwenden spezielle ASICs, um die Mehrzahl der Paketweiterleitungen bei hohem Durchsatz durchzuführen. Diese ASICs nutzen verschiedene Tabellen und interne Ressourcen, die in ihrer Kapazität begrenzt sind. Da SSDP-Clients sowohl als Quellen als auch als Empfänger für eine gemeinsame Multicast-Gruppe fungieren, muss die Hardware diese begrenzten Ressourcen verwenden, um einen Pfad in der Hardware zu programmieren, damit Pakete folgen, auch wenn diese Pakete aus anderen Gründen (TTL 1) nie kommen oder verworfen werden. Sobald die Hardwareressourcen erschöpft sind, können unabhängig von der Beziehung zu SSDP keine neuen Updates oder Ergänzungen für eine Gruppe installiert werden. Eine große Anzahl nicht installierter SSDP-Updates (Zustandsabwanderung) kann auch in der Software in Warteschlangen gesetzt werden. Dies kann auch dazu führen, dass Hardware-Updates für Nicht-Multicast-Datenverkehr unterbrochen oder fehlschlagen, was sich auf den Benutzerdatenverkehr auswirkt und Netzwerkausfälle verursacht.

Dieses Dokument ist nur relevant, wenn Ihr Netzwerk mit PIM konfiguriert ist und über Layer-3-Multicast-Status für die bekannte SSDP-Gruppenadresse verfügt. Um diese Kriterien zu überprüfen, führen Sie den Befehl "**show ip mroute 239.255.255.250**" (Fügen Sie ggf. VRF-Anweisungen hinzu.) Die Gruppe 239.255.255.250 ist spezifisch für das SSDP-Protokoll.

Wenn die Befehlsausgabe eine große Anzahl ausgehender Schnittstellen enthält und/oder eine große Anzahl eindeutiger Quellen für diese spezielle Gruppe enthält, bedeutet dies, dass das System und das Netzwerk anfällig für Ausfälle sind, die durch SSDP verursacht werden. Je mehr ausgehende Schnittstellen und eindeutige Quellen vorhanden sind, desto höher sind die Chancen, dass sich dies negativ auf den Service auswirken kann.

Abbildung 2: Beispielausgabe für "show ip mroute 239.255.255.250" mit im Netzwerk aktiver SSDP.

```
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
```

Wenn SSDP nicht für einen bestimmten Zweck verwendet wird, ist davon auszugehen, dass diese Ausgabe leer ist oder nur über eine geringe Anzahl ausgehender Schnittstellen verfügt und/oder nur über eine geringe Anzahl eindeutiger Quellen verfügt, um eine Ressourcenerschöpfung und mögliche Auswirkungen auf die Dienste zu verhindern.

Wenn eine große Anzahl von Multicast-Gruppen erkannt wird, **kann** der Befehl "**show platform software object-manager fp active statistics**" oder "**show platform software object-manager fp switch active statistics**" verwendet werden, um festzustellen, ob eine Hardwareressource erschöpft ist.

> **Anmerkung:** Dieser Befehl ist nicht spezifisch für die durch Multicast-Datenverkehr ausgelöste Ressourcenauslastung. Andere Probleme können dazu führen, dass diese Werte nicht null sind.

Abbildung 3: Ausgabe von **"show platform software object-manager fp active statistics"**im Problemzustand

```
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

Die Ausgabe von Abbildung 3 zeigt Symptome eines Switches mit Ressourcenauslastung. Es gibt mehrere Befehlsausgabelinien, die im Normalbetrieb nicht zu erwarten sind:

- Ausstehende Ausgabe: Es wird erwartet, dass dieser Wert gleich Null oder nahe daran liegt. Wenn dieser Wert über mehrere Iterationen des Befehls hinweg ein großer Wert ohne null bleibt, ist dies ein Zeichen für eine Ressourcenerschöpfung.
- Bestätigung ausstehend: Es wird erwartet, dass dieser Wert gleich Null oder nahe daran liegt. Wenn dieser Wert über mehrere Iterationen des Befehls hinweg ein großer Wert ohne null bleibt, ist dies ein Zeichen für eine Ressourcenerschöpfung.
- Kindlose Löschobjekte: Es wird erwartet, dass dieser Wert gleich Null oder nahe daran liegt. Werte von 10+ sind nicht zu erwarten.
- Fehlerobjekte: Es wird erwartet, dass dieser Wert gleich Null oder nahe daran liegt. Werte von 10+ sind nicht zu erwarten.

In einem Zustand, in dem eine große Anzahl von Zählern für ausstehende oder ausstehende Bestätigungen vorhanden ist, erhöht sich das Risiko, dass die Hardware falsch programmiert wird. Falsch programmierte Hardware ist eine häufige Ursache für Ausfälle des Unicast- und Multicast-Datenverkehrs.

Der Befehl "**show platform hardware fed switch active fwd-asic resource utilization**" or in some models "**show platform hardware fed active fwd-asic resource utilization**" kann verwendet werden, um einige der in den ASICs verwendeten endlichen Ressourcen zu überprüfen und festzustellen, ob eine interne Ressource ausgeschöpft wurde:

Abbildung 4: Beispielausgabe für"show platform hardware fed active fwd-asic resource utilization"mit einer Ressource beinahe erschöpft.

```
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 Abbildung 4 zeigt der Wert für "RSC_RIL_INDEX", dass 131065 Einträge verwendet werden und nur 7 kostenlos sind. Diese Ressource wird von einer großen Anzahl eindeutiger SSDP-Gruppen genutzt. Obwohl nicht nur SSDP-spezifisch, weisen Ressourcen mit einer geringen Anzahl freier Einträge und einer hohen Anzahl zugewiesener Einträge darauf hin, dass sich der Switch in der Nähe eines Kapazitätsproblems befindet, und müssen untersucht werden.

Der Befehl "**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**" kann verwendet werden, um eine ASIC-basierte Aufschlüsselung der Nutzung nach Ressourcen zu untersuchen. Eine weitere mögliche Signatur von SSDP-Erschöpfung ist die Spalte "Used Values" (Verwendete Werte) für "L3-Multicast-Einträge", die nahe oder an der Spalte "Max Values" (Maximale Werte) angeordnet ist.

Abbildung 5: Beispielausgabe für"show platform hardware fed active fwd-asic resource tcam utilization"im Normalbetrieb

```
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
```

Verhinderung des Ressourcenausfalls durch SSDP

Um die Ressourcenerschöpfung zu stoppen, muss der SSDP-Datenverkehr vor der Erstellung des ersten L3-Hop- und Multicast-Zustands gestoppt werden. Die schnellste Lösung ist die Verwendung einer IPv4-Zugriffskontrollliste (ACL) für den Eingang an allen L3-Schnittstellen, die mit PIM konfiguriert sind, das diesen Datenverkehr empfängt. Überprüfen Sie mit dem Befehl **"show ip mroute 239.255.255.250"**, und sehen Sie sich die "Incoming Interface" (Eingehende Schnittstelle) für jede Gruppe an. Dies zeigt an, von welcher L3-Schnittstelle die Quelle des Datenverkehrs stammt, und es kann mehr als eine eindeutige Quellschnittstelle geben. Dieses Konfigurationsbeispiel ermöglicht die Arbeit von SSDP auf Layer 2 und ermöglicht es L2-benachbarten Hosts, PNP-Dienste zu erkennen. Client-Meldungen können jedoch über L3-Grenzen hinweg weitergeleitet werden, und es wird verhindert, dass L3-Multicast-Zustände auf einem beliebigen Multicast-Router oder -Switch erstellt werden.

Konfigurieren einer erweiterten Zugriffskontrollliste:

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**

Konfigurieren Sie unter jeder L3-Schnittstelle die ACL in Eingangsrichtung:

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