Comprendre les incidents dus aux logiciels

Contenu

Introduction

Ce document explique les causes les plus fréquentes des incidents logiciels, et décrit les informations que vous devez collecter afin d'effectuer le dépannage.Si vous ouvrez une demande de services TAC d'un incident logiciel, les informations que vous serez invité à collecter seront essentielles pour résoudre le problème.

Conditions préalables

Conditions requises

Les lecteurs de ce document devraient avoir connaissance des sujets suivants :

- Comment dépanner les pannes de routeur.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Une panne logicielle se produit lorsque le routeur détecte une erreur grave et irrécupérable et se recharge de manière à ne pas transmettre de données endommagées. La grande majorité des

plantages logiciels sont causés par des bogues logiciels Cisco IOS®, bien que certaines plates-formes (telles que l'ancien Cisco 4000) puissent signaler un problème matériel comme une panne logicielle.

Si vous n'avez pas effectué de mise sous tension ou rechargé manuellement le routeur, le résultat de la commande **show version** affiche ceci :

```
Router uptime is 2 days, 21 hours, 30 minutes
System restarted by error - Software-forced crash, PC 0x316EF90 at 20:22:37 edt
System image file is "flash:c2500-is-l.112-15a.bin", booted via flash
```

Si vous disposez de la sortie d'une commande **show version** de votre périphérique Cisco, vous pouvez utiliser Cisco CLI Analyzer (clients enregistrés uniquement) pour afficher les problèmes potentiels et les correctifs.

Causes possibles

Ce tableau explique les raisons possibles des pannes forcées par logiciel :

Motif	Explication

Délais de surveillance	Le processeur utilise des compteurs pour éviter les boucles infinies et fait cesser la réponse routeur. En fonctionnement normal, le processeur réinitialise ces compteurs à intervalles réguliers. Si vous ne le faites pas, le système se recharge. Les dépassements de délai de surveillance signalés comme des pannes forcées par logiciel sont liés au logiciel. Référez-vo Dépannage des délais d'attente de chien de garde pour plus d'informations sur d'autres type délais d'attente de chien de garde. Le système était coincé dans une boucle avant le rechargement. Par conséquent, la trace de pile n'est pas nécessairement pertinente. Vous pouvez reconnaître ce type de panne logicielle dans les lignes suivantes des journaux de console :
	`%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = Exec`
	
	`and`
	
	`*** System received a Software forced crash ***`
	`signal = 0x17, code = 0x24, context= 0x60ceca60`

Mémoire faible	Lorsqu'un routeur ne dispose pas de suffisamment de mémoire, il peut se recharger lui-mêm le signaler comme une panne logicielle. Dans ce cas, les messages d'erreur d'allocation de mémoire apparaissent dans les journaux de console :
	`%SYS-2-MALLOCFAIL: Memory allocation of 734 bytes failed from 0x6015EC84,`
	`pool Processor, alignment 0`

Image logicielle corrompue	Au moment du démarrage, un routeur peut détecter qu'une image du logiciel Cisco IOS est endommagée, renvoyer le message `de somme de contrôle de l'image compressée est incorrec` tenter de recharger. Dans ce cas, l'événement est signalé comme une panne logicielle.
	`Error : compressed image checksum is incorrect 0x54B2C70A`
	`Expected a checksum of 0x04B2C70A`
	
	`*** System received a Software forced crash ***`
	`signal= 0x17, code= 0x5, context= 0x0`
	`PC = 0x800080d4, Cause = 0x20, Status Reg = 0x3041f003`
	
	Cela peut être dû à une image du logiciel Cisco IOS qui a été corrompue lors du transfert ver routeur. Dans ce cas, vous pouvez charger une nouvelle image sur le routeur pour résoudre problème. [Pour obtenir une méthode de récupération ROMMON pour votre plate-forme, reportez-vous à Procédure de récupération ROMmon pour les routeurs Cisco 7200, 7300, 74

Autres défauts	7500, RSP7000, Catalyst 5500 RSM, uBR7107 Routeurs des gammes 200, uBR10000 et 12000.] Cela peut également être dû à un matériel de mémoire défectueux ou à un bogue logiciel. Les erreurs qui provoquent des plantages sont souvent détectées par le matériel du process qui appelle automatiquement le code spécial de gestion des erreurs dans le moniteur ROM.L moniteur de ROM identifie l'erreur, imprime un message, enregistre les informations sur la pa et relance le système. Il y a des plantages dans lesquels rien de tout cela ne peut se produire (voir Délais d'attente de chien de garde), et il y a des plantages dans lesquels le logiciel déte le problème et appelle la fonction crashdump. Il s'agit d'un vrai crash « logiciel forcé ». Sur le plates-formes Power PC, « crash forcé par logiciel » n'est pas la raison de redémarrage imprimée lorsque la fonction crashdump est appelée - au moins jusqu'à très récemment. Sur plates-formes (avant la version 12.2(12.7) du logiciel Cisco IOS), elles sont appelées excepti SIGTRAP. Par tous les autres moyens, les SIGTRAP et les SFC sont identiques.

Dépannage

Les pannes forcées par logiciel sont généralement causées par des bogues du logiciel Cisco IOS. Si des messages d'erreur d'allocation de mémoire sont présents dans les journaux, consultez Résolution des problèmes de mémoire.

Si les messages d'erreur d'allocation de mémoire ne s'affichent pas et que vous n'avez pas rechargé ou mis le routeur sous tension après l'arrêt forcé du logiciel, le meilleur outil que vous pouvez utiliser est l'analyseur CLI de Cisco (clients enregistrés uniquement) pour rechercher un ID de bogue correspondant connu. Cet outil intègre les fonctionnalités de l'ancien outil Stack Decoder.

Exemple :

1. Collectez le résultat de **show stack** à partir du routeur.
2. Accédez à l'outil Cisco CLI Analyzer (clients enregistrés uniquement).
3. Sélectionnez **show stack** dans le menu déroulant.
4. Collez dans la sortie que vous avez collectée.
5. Cliquez sur **Soumettre**.Si la sortie décodée de la commande **show stack** correspond à un bogue logiciel connu, vous recevrez les ID de bogue des bogues logiciels les plus probables qui auraient pu provoquer un plantage forcé par le logiciel.
6. Cliquez sur les liens hypertexte de l'ID de bogue pour afficher d'autres détails de bogue à partir de la boîte à outils des bogues Cisco (clients enregistrés uniquement) qui peut vous aider à déterminer la correspondance correcte de l'ID de bogue.

Lorsque vous avez identifié un ID de bogue qui correspond à votre erreur, reportez-vous au champ « corrigé » pour déterminer la première version du logiciel Cisco IOS qui contient la correction du bogue.

Si vous n'êtes pas certain de l'ID de bogue ou de la version du logiciel Cisco IOS qui contient la correction du problème, mettez à niveau votre logiciel Cisco IOS vers la dernière version de votre série de versions. Ceci est utile car la dernière version contient des correctifs pour un grand nombre de bogues. Même si cela ne résout pas le problème, le rapport de bogues et le processus de résolution sont plus simples et plus rapides quand vous avez la dernière version du logiciel.

Si, après avoir utilisé l'analyseur CLI de Cisco, vous suspectez ou avez identifié un bogue qui reste non résolu, nous vous recommandons d'ouvrir une demande de service TAC pour fournir des informations supplémentaires pour aider à résoudre le bogue, et pour une notification plus

rapide lorsque le bogue est finalement résolu.

Procédures de configuration

Si le problème est identifié comme un nouveau bogue logiciel, un ingénieur du centre d'assistance technique Cisco peut demander que vous configuriez le routeur pour collecter un *vidage principal*. Il est parfois nécessaire d'effectuer un vidage de coeur pour identifier les actions possibles pour corriger le bogue logiciel.

Pour collecter des informations plus utiles dans le vidage principal, nous vous recommandons d'utiliser la commande **debug sanity** masquée. Cela entraîne la vérification de l'intégrité de chaque tampon utilisé dans le système lorsqu'il est alloué et lorsqu'il est libéré. La commande **debug sanity** doit être exécutée en mode d'exécution privilégié (mode enable) et implique un certain CPU, mais n'affecte pas significativement la fonctionnalité du routeur. Si vous souhaitez désactiver la vérification de la santé mentale, utilisez la commande EXEC privilégiée **undebug sanity**.

Pour les routeurs dont la mémoire principale est inférieure ou égale à 16 Mo, vous pouvez utiliser le protocole TFTP (Trivial File Transfer Protocol) pour collecter le vidage principal. Il est recommandé d'utiliser le protocole FTP (File Transfer Protocol) si le routeur dispose de plus de 16 Mo de mémoire principale. Utilisez les procédures de configuration de cette section. Vous pouvez également vous reporter à Création de dumps principaux.

Exécutez les étapes suivantes pour configurer votre routeur :

1. Configurez le routeur à l'aide de la commande **configure terminal**.
2. Tapez **exception dump n.n.n.n**, où n.n.n.n est l'adresse IP de l'hôte serveur TFTP (Trivial File Transfer Protocol) distant.
3. Quittez le mode de configuration.

Procédure de configuration d'hôte du serveur TFTP

Exécutez les étapes suivantes pour configurer un hôte de serveur TFTP :

1. Créez un fichier sous le répertoire /tftpboot sur l'hôte distant à l'aide d'un éditeur de votre choix. Le nom de fichier est le nom d'hôte-coeur du routeur Cisco.
2. Sur les systèmes UNIX, modifiez le mode d'autorisation du fichier « hostname-core » pour qu'il soit globalement compatible (666). Vous pouvez vérifier la configuration TFTP via la commande **copy running-config tftp** sur ce fichier.
3. Vérifiez que vous disposez de plus de 16 Mo d'espace disque disponible sous /tftpboot.Si le système tombe en panne, la commande **exception dump** crée sa sortie dans le fichier ci-dessus. Si le routeur dispose de plus de 16 Mo de mémoire principale, utilisez FTP (File Transfer Protocol) ou RCP (Remote Copy Protocol) pour obtenir le vidage principal. Sur le routeur, configurez ceci :

   ```
   exception protocol ftp
   exception dump n.n.n.n
   ip ftp username ip ftp password ip ftp source-interface exception core-file
   ```

   Lorsque vous avez collecté un vidage de noyau, téléchargez-le sur ftp://ftp-sj.cisco.com/incoming (sous UNIX, tapez **pftp ftp ftp-sj.cisco.com**, puis **cd entrant**), puis

informez le propriétaire de votre dossier et indiquez le nom du fichier.

Informations à collecter si vous ouvrez une demande de service TAC

Si vous avez toujours besoin d'assistance après avoir suivi les étapes de dépannage ci-dessus et que vo souhaitez créer une demande de service auprès du TAC Cisco, veillez à inclure les informations suivante

- **show technical-support** output - Le résultat de la commande **show technical-support** fournit des informations sur l'état actuel du routeur, ainsi que des informations clés stockées par le routeur avant panne.
- Journaux de console : les journaux de console, souvent enregistrés sur un serveur Syslog, peuvent f des informations précieuses sur les événements qui se produisent sur le routeur avant un plantage. C indices sont souvent les renseignements les plus importants que vous pouvez recueillir.
- crashinfo file (si présent) - Cisco vous recommande d'utiliser une version du logiciel Cisco IOS qui pr en charge la fonctionnalité crashinfo afin de résoudre les problèmes avec succès. Pour cela, la versio doit répondre aux autres besoins de votre réseau. Reportez-vous à Récupération d'informations à pa fichier Crashinfo ou utilisez l'outil Software Advisor (clients enregistrés uniquement) pour localiser un version du logiciel Cisco IOS prenant en charge la fonctionnalité crashinfo. Un avantage potentiel est si vous avez une version plus ancienne du logiciel Cisco IOS, les versions plus récentes du logiciel IO qui prennent en charge cette fonctionnalité pourraient déjà avoir votre bogue corrigé.

Pour joindre des informations à votre demande de service, téléchargez-les via l'outil de demande de serv TAC (clients enregistrés uniquement). Si vous ne pouvez pas accéder à l'outil de demande de service du centre d'assistance technique, vous pouvez envoyer les informations dans une pièce jointe à un e-mail à attach@cisco.com avec votre numéro de dossier dans la ligne d'objet de votre message.

Attention : Ne redémarrez pas manuellement le routeur ou ne le mettez pas hors tension avant de collecte informations ci-dessus, si possible, car cela peut entraîner la perte d'informations importantes nécessaire pour déterminer la cause première du problème.

Informations connexes

- Résolution des problèmes de blocage de routeurs
- Récupération d'informations depuis le fichier Crashinfo
- Création de core dumps (images de mémoire)
- Dépannage des problèmes de mémoire
- Support technique - Cisco Systems