Comprenez les incidents 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 des crash de routeur.

Composants utilisés

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. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Un incident logiciel se produit quand le routeur détecte une erreur grave et irrémédiable, et se

recharge de sorte qu'il ne transmette pas des données corrompues. Une immense majorité d'incidents logiciels sont provoqué par par des erreurs de programmation de Cisco IOS®, bien que quelques Plateformes (telles que vieux Cisco 4000) puissent signaler un problème matériel comme incident logiciel.

Si vous alimentation-n'avez pas fait un cycle ou avez manuellement rechargé le routeur, la sortie de la commande de **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 avez la sortie d'une commande de **show version de** votre périphérique de Cisco, vous pouvez employer l'analyseur de Cisco CLI (clients enregistrés seulement) pour afficher des éventuels problèmes et des difficultés.

Causes possibles

Cette table explique les possibles raison pour des incidents logiciels :

Raison	Explication

Dépassements du délai de surveillance	Le processeur utilise des temporisateurs pour éviter les boucles infinies, et fait cesser le routeur de répondre. En fonctionnement le fonctionnement normal, la CPU remet à l'état initial ces temporisateurs à intervalles réguliers. Manque de faire ainsi des résultats dans rechargement du système. Dépassements du délai de surveillance qui sont signalés car l incidents logiciels sont liés au logiciel. Référez-vous aux dépassements du délai de surveillance de dépannage pour des informations sur d'autres types de dépassements du délai de surveillance. Le système a été coincé dans une boucle avant la recharge. Par conséquent, le suivi de pile n'est pas nécessairement approprié. Vous pouvez identifier ce type d'incident logiciel dans ces lignes des logs 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 basse	Quand un routeur exécute si bas sur la mémoire, elle peut par la suite se recharger et le signaler comme incident logiciel. Dans ce cas, les messages d'erreur de défaillance d'allocation de mémoire apparaissent dans les logs 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 le détecter qu'une image de logiciel Cisco IOS est corrompue, renvoient la `somme de contrôle comprimée d'image est` message `incorrect`, e tentative de recharger. Dans ce cas, l'événement est signalé comme incident logiciel. `Erro 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`
	Ceci peut sont provoqué par par une image de logiciel Cisco IOS qui a été corrompue réellement pendant le transfert au routeur. Dans ce cas, vous pouvez charger une nouvel image sur le routeur pour résoudre le problème. [Pour une méthode de récupération ROMmon pour votre plate-forme, référez-vous à la procédure de récupération ROMmon pour le Cisco 7200, les 7300, les 7400, les 7500, le RSP7000, le Catalyst 5500 RSM,

D'autres défauts	l'uBR7100, l'uBR7200, l'uBR10000, et les Routeurs de gamme 12000.] il peut sont provoc par également par le matériel défectueux de mémoire ou par une erreur de programmatio Les erreurs qui entraînent des crash sont souvent détectées par le processeur matériel, q appelle automatiquement le code spécial de traitement des erreurs dans le moniteur ROM Le moniteur de ROM identifie l'erreur, imprime un message, enregistre les informations su la pann, et relance le système. Il y a des crash dans lesquels aucune de ceci ne peut se produire (voir les dépassements du délai de surveillance), et il y a des crash dans lesquel logiciel détecte le problème et appelle la fonction de crashdump. C'est un crash « logiciel- forcé » vrai. Sur des Plateformes de Power PC, le « incident logiciel » n'est pas la raison reprise imprimée quand la fonction de crashdump obtient appelé - au moins jusque très à récemment. Sur ces Plateformes (avant version du logiciel Cisco IOS 12.2(12.7)), ceux-ci désigné sous le nom des exceptions « SIGTRAP ». De toutes autres manières, SIGTRAP et SFCs sont identique.

Dépannez

Des incidents logiciels sont typiquement provoqués par des bogues de logiciel Cisco IOS. Si les messages d'erreur de défaillance d'allocation de mémoire sont présents dans les logs, voir les problèmes de mémoire de dépannage.

Si vous ne voyez pas des messages d'erreur de défaillance d'allocation de mémoire, et vous n'avez pas manuellement rechargé ou alimentation-avez fait un cycle le routeur après l'incident logiciel, le meilleur outil que vous pouvez utiliser est l'analyseur de Cisco CLI (clients enregistrés seulement) pour rechercher un ID connu de bogue correspondante. Cet outil incorpore la fonctionnalité du vieil outil de décodage de pile.

Exemple :

1. Collectez la sortie de la **pile d'exposition du** routeur.
2. Allez à l'outil d'analyseur de Cisco CLI (clients enregistrés seulement).
3. **Pile** choisie d'**exposition du** menu déroulant.
4. Pâte dans la sortie que vous avez collectée.
5. Le clic **soumettent**.Si la sortie décodée de la commande de **pile d'exposition** apparie une erreur de programmation connue, vous recevrez les id de bogue des erreurs de programmation le plus susceptibles qui pourraient avoir entraîné l'incident logiciel.
6. Cliquez sur en fonction les hyperliens d'ID de bogue pour visualiser les détail du bogue supplémentaires de la boîte à outils de bogue Cisco (clients enregistrés seulement) qui peut vous aider à déterminer la correspondance correcte d'ID de bogue.

Quand vous avez identifié un ID de bogue qui apparie votre erreur, référez-vous au « réparé dans » le domaine pour déterminer la première version de logiciel de Cisco IOS qui contient la difficulté pour la bogue.

Si vous êtes incertain au sujet de l'ID de bogue, ou de la version de logiciel de Cisco IOS qui contient la difficulté pour le problème, améliorez votre logiciel de Cisco IOS à la dernière version dans votre série de versions. Ceci aide parce que, la dernière version contient des difficultés pour un grand nombre de bogues. Même si ceci ne résout pas le problème, introduisez des erreurs pour tests l'enregistrement et le processus de résolution est plus simple et plus rapide quand vous avez la dernière version du logiciel.

Si, après que vous utilisiez l'analyseur de Cisco CLI, vous suspectez ou avez franchement identifié une bogue qui demeure non résolue, nous recommandons que vous ouvriez une

demande de services TAC de fournir les informations complémentaires pour aider à résoudre la bogue, et pour une notification plus rapide quand la bogue est finalement résolue.

Procédures de configuration

Si le problème est identifié comme nouvelle erreur de programmation, un ingénieur TAC Cisco peut demander que vous configurez le routeur pour collecter un *vidage de mémoire*. Un vidage de mémoire est parfois exigé pour identifier ce qui peut être fait pour réparer l'erreur de programmation.

Pour collecter plus de vidage mémoire des informations utiles au centre, nous recommandons que vous utilisiez la commande masquée de **debug sanity**. Ceci entraîne chaque mémoire tampon qui est utilisée dans le système validité-à vérifier quand il est alloué et quand il est libéré. La commande de **debug sanity** doit être émise dans le mode d'exécution privilégié (mode enable) et implique une certaine CPU, mais n'affecte pas de manière significative la fonctionnalité du routeur. Si vous voulez désactiver la validité vérifiant, utilisez la commande de privileged exec de **validité d'undebug**.

Pour les Routeurs qui ont 16 Mo ou moins de mémoire centrale, vous pouvez employer le Protocole TFTP (Trivial File Transfer Protocol) pour collecter le vidage de mémoire. Il est recommandé que vous utilisez le Protocole FTP (File Transfer Protocol) si le routeur a plus que 16MB de mémoire centrale. Utilisez les procédures de configuration dans cette section. Alternativement, référez-vous à créer des vidages de mémoire.

Terminez-vous ces étapes pour configurer votre routeur :

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

Procédure de configuration d'hôte de serveur TFTP

Terminez-vous ces étapes pour configurer un hôte de serveur TFTP :

1. Créez un fichier sous le répertoire de /tftpboot sur le serveur distant avec l'aide d'un éditeur de votre choix. Le nom du fichier est l'adresse Internet-noyau de routeur de Cisco.
2. Sur des systèmes Unix, Changez le mode d'autorisation du fichier de « adresse Internet-noyau » pour être globalement compatible (666). Vous pouvez vérifier le TFTP installé par la commande de **tftp de copy running-config** sur ce fichier.
3. Veillez-vous pour avoir plus de 16 Mo d'espace disque libre sous /tftpboot.Si les blocages système, la commande d'**exception dump** crée sa sortie au fichier ci-dessus. Si le routeur a plus de 16 Mo de mémoire centrale, employez le Protocole FTP (File Transfer Protocol) ou le protocole de copie à distance (RCP) pour obtenir le vidage de mémoire. Sur le routeur, configurez ceci :**exception protocol ftp exception dump n.n.n.n ip ftp username** *<string>* **ip ftp password** *<string>* **ip ftp source-interface** *<slot/port/interface>* **exception core-file** *<core-filename>* Quand vous avez collecté un vidage de mémoire, téléchargez-le à ftp://ftp-sj.cisco.com/incoming (dans l'UNIX, tapez le **pftp ftp-sj.cisco.com** et puis le **cd entrant**), et informez le propriétaire de votre cas et incluez le nom du fichier.

Informations à collecter si vous ouvrez une demande de service TAC

Si vous avez besoin d'assistance après avoir suivi les étapes de dépannage ci-dessus et voulez toujours une demande de service avec Cisco TAC, soyez sûr d'inclure les informations suivantes :

- **affichez le Soutien technique** sorti – La sortie de la commande de **Soutien technique d'exposition** fou des informations sur l'état actuel du routeur, et également l'information principale stockée par le route avant un crash.
- Messages de console – La console se connecte, souvent enregistré à un serveur de Syslog, peut fou des données de valeur au sujet des événements qui se produisent sur le routeur avant un crash. Ces indices sont souvent la plupart d'informations importantes que vous pouvez collecter.
- fichier crashinfo (si présent) – Cisco recommande que vous utilisiez une version logicielle de Cisco IO prend en charge la caractéristique de crashinfo afin de dépanner avec succès. Pour ceci, la version d répondre aux autres besoins de votre réseau. Voyez récupérer les informations à partir du fichier cra ou utilisez l'outil de conseiller de logiciel (clients enregistrés seulement) pour localiser une version de logiciel de Cisco IOS qui prend en charge la caractéristique de crashinfo. Une bonification potentielle que si vous avez une version plus ancienne de logiciel de Cisco IOS, les versions logicielles plus nouvelles IOS qui prennent en charge cette caractéristique pourraient déjà avoir votre bogue réparée

Afin de relier les informations à votre demande de service, téléchargez-la par l'outil de demande de servic TAC (clients enregistrés seulement). Si vous ne pouvez pas accéder à l'outil de demande de service TAC vous pouvez envoyer les informations dans une pièce jointe à un courriel à attach@cisco.com avec votre numéro de dossier dans le champ objet de votre message.

Attention : S'il vous plaît ne rechargez pas manuellement ou arrêt et redémarrage le routeur avant que vo collectiez les informations ci-dessus, si possible, car ceci peut causer les informations importantes d'être perdue qui sont nécessaires pour déterminer l'origine 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