Dépannage de la défaillance du connecteur Linux Secure Endpoint 18

Table des matières

Introduction

Ce document décrit l'erreur 18 sur le connecteur Secure Endpoint Linux.

Erreur 18 : surveillance des événements du connecteur surchargée

Le moteur de protection comportementale améliore la visibilité des connecteurs sur l'activité du système. Avec cette visibilité accrue, il est possible que la surveillance de l'activité du système du connecteur soit saturée par la quantité d'activité du système. Dans ce cas, le connecteur déclenche le défaut 18 et passe en mode dégradé. Référez-vous à l'article Défaillances du connecteur Linux du point d'extrémité sécurisé Cisco pour plus de détails sur la défaillance 18. Sur le connecteur Linux, le status peut être utilisée dans l'interface de ligne de commande Secure Endpoint Linux pour vérifier si le connecteur fonctionne en mode dégradé et si des défaillances sont survenues. Si le défaut 18 est déclenché, exécutez la commande status dans l'interface de ligne de commande Secure Endpoint Linux affiche la panne avec l'une des deux gravités possibles :

1. Erreur 18 avec gravité majeure

```
ampcli> status
Status:                 Connected
Mode:                   Degraded
Scan:                   Ready for scan
Last Scan:              2023-06-19 02:02:03 PM
Policy:                 Audit Policy for FireAMP Linux (#1)
Command-line:           Enabled
Orbital:                Disabled
```

```
Behavioural Protection: Protect
Faults:                 1 Major
Fault IDs:      18
                ID 18 - Major: Connector event monitoring is overloaded. Investigate the most acti
```

2. Erreur 18 avec gravité critique

```
ampcli> status
Status:                 Connected
Mode:                   Degraded
Scan:                   Ready for scan
Last Scan:              2023-06-19 02:02:03 PM
Policy:                 Audit Policy for FireAMP Linux (#1)
Command-line:           Enabled
Orbital:                Disabled
Behavioural Protection: Protect
Faults:                 1 Critical
Fault IDs:      18
                ID 18 - Critical: Connector event monitoring is overloaded. Investigate the most a
```

Surcharge de la surveillance des événements du connecteur : gravité majeure

Lorsque le défaut 18 est déclenché avec une gravité majeure, cela signifie que la surveillance des événements du connecteur est surchargée, mais qu'elle peut toujours surveiller un plus petit ensemble d'événements système. Le connecteur bascule en niveau de gravité majeur et surveille moins d'événements équivalents à la surveillance disponible dans les connecteurs antérieurs à 1.22.0. Si le flot d'événements système est court et que la charge de surveillance des événements redescend dans une plage acceptable, le défaut 18 est effacé et le connecteur reprend la surveillance de tous les événements système. Si le flot d'événements système s'aggrave et que la charge de surveillance des événements augmente jusqu'à un niveau critique, la panne 18 est augmentée avec un niveau de gravité critique et le connecteur passe à un niveau de gravité critique.

Surcharge de la surveillance des événements du connecteur : gravité critique

Lorsque la défaillance 18 est élevée avec une gravité critique, cela signifie que le connecteur subit un nombre excessif d'événements système qui le mettent en danger. Le connecteur passe à une gravité critique plus restrictive. Dans cet état, le connecteur surveille uniquement les événements critiques pour permettre au connecteur de se nettoyer et de se concentrer sur la récupération. Si le flot d'événements finit par retomber dans une plage plus acceptable, la panne est entièrement résolue et le connecteur reprend la surveillance de tous les événements du système.

Guide D'Action En Cas De Défaillance

Si le connecteur soulève un problème 18 d'une gravité majeure ou critique, certaines étapes doivent être prises pour examiner et résoudre le problème. Les étapes de résolution de la défaillance 18 varient en fonction du moment et de la raison du déclenchement de la défaillance :

1. La panne 18 a été soulevée lors d'une nouvelle installation du connecteur Linux
2. La panne 18 a été déclenchée après des modifications récentes du système d'exploitation
3. La faille 18 a été soulevée spontanément

4. Le problème 18 a été soulevé lors du réapprovisionnement d'une machine avec le connecteur Linux déjà installé ou lors de la mise à jour du connecteur vers la version 1.22.0+

Cas 1 : nouvelle installation

Si le défaut 18 et le mode dégradé sont observés lors d'une nouvelle installation du connecteur Linux, vous devez d'abord vous assurer que votre système répond à la configuration système requise. Après avoir vérifié que la configuration requise est conforme ou supérieure à la configuration minimale requise, si le problème persiste, vous devez rechercher les processus les plus actifs sur le système. Vous pouvez afficher les processus actifs actuels sur un système Linux à l'aide de `top` (ou similaire) dans le terminal. Si les processus consommant la plus grande quantité de CPU sont reconnus comme étant bénins, vous pouvez créer de nouvelles exclusions de processus pour exclure ces processus de la surveillance.

Exemple de scénario :

Supposons qu'après une nouvelle installation, la panne 18 et le mode dégradé s'affichent via l'interface de ligne de commande Secure Endpoint Linux. Rexécution du `top` dans une machine Ubuntu a affiché ces processus actifs :

```
Tasks: 223 total,   5 running, 218 sleeping,   0 stopped,   0 zombie
%Cpu(s): 29.4 us, 34.3 sy,  0.0 ni, 36.2 id,  0.0 wa,  0.0 hi,  0.1 si,  0.0 st
MiB Mem :   7943.0 total,   3273.9 free,   2357.6 used,   2311.5 buff/cache
MiB Swap:   2048.0 total,   2048.0 free,      0.0 used.   5141.2 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
  34896 user1     20   0   18136   3292   3044 R  96.7   0.0   0:04.89 trusted_process
   4296 user1     20   0  823768  52020  38900 R  48.0   0.6   0:10.90 gnome-terminal-
    117 root      20   0       0      0      0 I  12.3   0.0   0:01.86 kworker/u64:6-events_unbound
  34827 root      20   0       0      0      0 I  10.3   0.0   0:00.47 kworker/u64:2-events_unbound
   1880 user1     20   0  353080 101600  70164 S   6.3   1.2   0:30.37 Xorg
  34576 root      20   0       0      0      0 R   6.3   0.0   0:01.46 kworker/u64:1-events_unbound
   2089 user1     20   0 3939120 251332 104008 S   3.0   3.1   0:23.25 gnome-shell
    132 root      20   0       0      0      0 I   1.3   0.0   0:02.67 kworker/2:2-events
   6951 root      20   0 1681560 213536  74588 S   1.3   2.6   0:41.30 ampdaemon
    741 root      20   0  253648  13352   9280 S   0.3   0.2   0:01.54 polkitd
    969 root      20   0  153600   3788   3512 S   0.3   0.0   0:00.36 prlshprint
   2291 user1     20   0  453636  29388  20060 S   0.3   0.4   0:03.75 prlcc
      1 root      20   0  169608  13116   8524 S   0.0   0.2   0:01.95 systemd
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.01 kthreadd
      3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_gp
      4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_par_gp
      5 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 slub_flushwq
      6 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 netns
      8 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/0:0H-events_highpri
     10 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 mm_percpu_wq
```

Nous voyons qu'il y a un processus très actif, appelé `trusted_process` dans cet exemple. Dans ce cas, je suis familier avec ce processus et il est de confiance, il n'y a aucune raison pour moi d'être soupçonneux de ce processus. Pour effacer la panne 18, le processus approuvé peut être ajouté à une exclusion de processus dans le portail. Reportez-vous à l'article Configurer et identifier les exclusions de point de terminaison sécurisé Cisco pour en savoir plus sur les meilleures pratiques lors de la création d'exclusions.

Cas 2 : Modifications récentes

Si vous avez apporté des modifications récentes à votre système d'exploitation, telles que l'installation d'un nouveau programme, alors la panne 18 et le mode dégradé peuvent être observés si ces nouvelles modifications augmentent l'activité du système. Utilisez la même stratégie de correction que celle décrite dans la nouvelle installation, recherchez toutefois les processus liés aux modifications récentes, tels qu'un nouveau processus exécuté par un programme récemment installé.

Cas 3 : Activité malveillante

Le moteur de protection comportementale augmente les types d'activité du système qui sont surveillés. Le connecteur dispose ainsi d'une perspective plus large sur le système et peut détecter des attaques comportementales plus complexes. Cependant, la surveillance d'une plus grande quantité d'activité du système expose également le connecteur à un risque plus élevé d'attaques par déni de service (DoS). Si le connecteur est saturé par l'activité du système et passe en mode dégradé avec la panne 18, il continue à surveiller les événements critiques du système jusqu'à ce que l'activité globale du système soit réduite. Cette perte de visibilité sur les événements système réduit la capacité du connecteur à protéger votre machine. Il est essentiel que vous recherchiez immédiatement les processus malveillants sur le système. Utilisez `top` (ou similaire) sur votre système Linux pour afficher les processus actifs actuels et prendre les mesures appropriées pour remédier à la situation si des processus potentiellement malveillants sont identifiés.

Cas 4 : Connecteurs requis

Le moteur de protection comportementale améliore la capacité du connecteur à protéger l'activité de votre machine, mais pour ce faire, il doit consommer plus de ressources que dans les versions précédentes. Si la panne 18 est fréquemment déclenchée, qu'aucun processus bénin n'entraîne une charge importante et qu'aucun processus malveillant ne semble agir sur la machine, vous devez vous assurer que votre système répond à la configuration minimale requise.

Voir également

- Utiliser l'interface de ligne de commande Secure Endpoint Mac/Linux
- Défaillances des connecteurs Linux Cisco Secure Endpoint
- Configuration et identification des exclusions de terminaux sécurisés Cisco
- Guide de l'utilisateur Secure Endpoint (PDF)

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.