

Pourquoi vManage ne parvient pas à installer le conteneur d'applications de sécurité sur un périphérique ?

Contenu

[Introduction](#)

[Problème](#)

[Solution](#)

[Références](#)

Introduction

Ce document décrit un problème avec l'installation du conteneur d'applications de sécurité lorsque la stratégie de sécurité est utilisée dans un modèle de périphérique et comment le résoudre.

Problème

L'utilisateur ne peut pas joindre le modèle de périphérique avec une stratégie de sécurité qui a requis l'installation du conteneur d'applications de sécurité avec cette erreur sur un vManage :

```
Failed to install 1/1 Security App container (app-hosting-UTD-Snort-Feature-aarch64_be-1.0.8_SV2.9.11.1_XE16.10). Failed to enabled iox: null
05 Apr 2019 11:46:09 AM IST
[5-Apr-2019 6:16:09 UTC] Total number of Security App containers to be installed: 1. Security App containers to be installed are following: [app-hosting-UTD-Snort-Feature-aarch64_be-1.0.8_SV2.9.11.1_XE16.10]
[5-Apr-2019 6:16:09 UTC] Started 1/1 Security app container (app-hosting-UTD-Snort-Feature-aarch64_be-1.0.8_SV2.9.11.1_XE16.10) installation
[5-Apr-2019 6:16:10 UTC] Checking if iox is enabled on device
[5-Apr-2019 6:16:18 UTC] Failed to install 1/1 Security App container (app-hosting-UTD-Snort-Feature-aarch64_be-1.0.8_SV2.9.11.1_XE16.10).
Failed to enabled iox: null
```

À partir de l'adresse `/var/log/nms/vmanage-server.log` sur un contrôleur vManage, cette erreur peut être vue :

```
05-Apr-2019 08:41:54,488 UTC ERROR [vManage] [AppHostingTemplateProcessor] (device-action-lxc_install-10) |default| Error while enabling iox on device-C1111X-8P-FGL230513Y0-1.1.1.1: rpc-reply error: <rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="5">
  <rpc-error>
    <error-type>application</error-type>
    <error-tag>invalid-value</error-tag>
    <error-severity>error</error-severity>
    <error-message unknown:lang="en">inconsistent value: Device refused one or more
commands</error-message>
  </error-info>
```

```

<severity xmlns=" http://cisco.com/yang/cisco-ia">error_cli</severity>;
<detail xmlns=" http://cisco.com/yang/cisco-ia">;
  <bad-cli>
    <bad-command>iox</bad-command>
    <error-location>1</error-location>
    <parser-response/>          </bad-cli>
  </detail>
</error-info>
</rpc-error>
</rpc-reply>

```

```

at com.tailf.jnc.NetconfSession.recv_rpc_reply_ok(Unknown Source) [JNC-1.2.jar:]
at com.tailf.jnc.NetconfSession.recv_rpc_reply_ok(Unknown Source) [JNC-1.2.jar:]
at com.tailf.jnc.NetconfSession.commit(Unknown Source) [JNC-1.2.jar:]
at
com.viptela.vmanage.server.device.common.NetConfClient.commitAndUnlock(NetConfClient.java:458)
[classes:]
at
com.viptela.vmanage.server.deviceaction.processor.config.AppHostingTemplateProcessor.checkAndEna
bleIox(AppHostingTemplateProcessor.java:358) [classes:]
at
com.viptela.vmanage.server.deviceaction.processor.config.AppHostingTemplateProcessor.preTemplate
PushCheck(AppHostingTemplateProcessor.java:173) [classes:]
at
com.viptela.vmanage.server.deviceaction.processor.service.lxc.LxcInstallActionProcessor$LxcInsta
llActionWorker.startMaintenanceDeviceActions(LxcInstallActionProcessor.java:340) [classes:]
at
com.viptela.vmanage.server.deviceaction.DefaultActionWorker.startDeviceAction(DefaultActionWorke
r.java:82) [classes:]
at
com.viptela.vmanage.server.deviceaction.AbstractActionWorker.call(AbstractActionWorker.java:117)
[classes:]
at
com.viptela.vmanage.server.deviceaction.AbstractActionWorker.call(AbstractActionWorker.java:35)
[classes:]
at java.util.concurrent.FutureTask.run(FutureTask.java:266) [rt.jar:1.8.0_162]
at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1149)
[rt.jar:1.8.0_162]
at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:624)
[rt.jar:1.8.0_162]
at java.lang.Thread.run(Thread.java:748) [rt.jar:1.8.0_162]

```

```

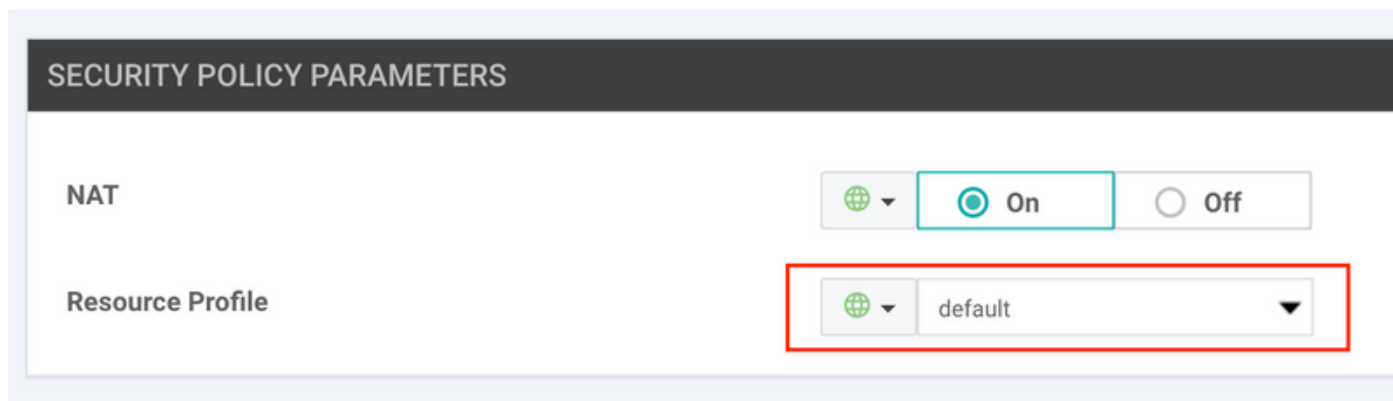
05-Apr-2019 08:41:54,496 UTC ERROR [vManage] [LxcInstallActionProcessor] (device-action-
lxc_install-10) |default| On device C1111X-8P-FGL230513Y0-1.1.1.1, Failed to install 1/1
Security App container (app-hosting-UTD-Snort-Feature-aarch64_be-1.0.8_SV2.9.11.1_XE16.10).
Failed to enabled iox: null
05-Apr-2019 08:41:54,524 UTC INFO [vManage] [DeviceActionStatusDAO] (device-action-lxc_install-
10) |default| End task lxc_install
05-Apr-2019 08:41:54,533 UTC INFO [vManage] [DeviceActionStatusDAO] (device-action-lxc_install-
10) |default| Publish client event: ACTIVITY
05-Apr-2019 08:41:54,533 UTC INFO [vManage] [DeviceActionStatusDAO] (device-action-lxc_install-
10) |default| Publish client event: DEVICE_ACTION

```

Comme on peut le voir ci-dessus, certains messages peu informatifs « Échec de l'activation de l'iox : null » est visible dans les deux sorties, ce qui signifie parfois que la quantité de mémoire n'est pas suffisante pour le profil d'hébergement d'application de sécurité sélectionné qui était connecté au périphérique.

Solution

Étant donné que des problèmes de mémoire dus au profil d'hébergement d'applications de sécurité ont été suspectés, il est vérifié, puis il est découvert que le profil par défaut est utilisé.



Contrairement au profil **élevé** connu pour causer des problèmes lorsque le périphérique n'a pas assez de mémoire.

Ensuite, la consommation de mémoire a été vérifiée sur le périphérique lui-même et il a été découvert que le routeur C1111X avec 8 Go de RAM ne dispose que d'environ 1 Go de mémoire libre (veuillez noter **Free**) :

```
cEdge10#show memory platform
Virtual memory : 11512180736
Pages resident : 730200
Major page faults: 2501
Minor page faults: 114581800

Architecture : aarch64_be
Memory (kB)
  Physical : 3758804
  Total : 3758804
  Used : 2620884
  Free : 1137920
  Active : 2191472
  Inactive : 807536
  Inact-dirty : 0
  Inact-clean : 0
  Dirty : 0
  AnonPages : 1473636
  Bounce : 0
  Cached : 1212660
  Commit Limit : 1813864
  Committed As : 3224504
  High Total : 0
  High Free : 0
  Low Total : 3758804
  Low Free : 1137920
  Mapped : 416524
  NFS Unstable : 0
  Page Tables : 17160
  Slab : 170624
  Writeback : 0

Swap (kB)
  Total : 0
  Used : 0
  Free : 0
  Cached : 0
```

```
Buffers (kB)      : 312844
```

```
Load Average
```

```
1-Min           : 0.60  
5-Min           : 0.66  
15-Min          : 0.86
```

En même temps, à partir de la sortie **show version**, il a été confirmé que le périphérique a 8 Go de RAM (note **mémoire physique**) :

```
cisco C1111X-8P (1RU) processor with 1453914K/6147K bytes of memory.  
Processor board ID FGL230513Y0  
1 Virtual Ethernet interface  
10 Gigabit Ethernet interfaces  
32768K bytes of non-volatile configuration memory.  
8388608K bytes of physical memory.  
6336511K bytes of flash memory at bootflash:.
```

Le manque de mémoire est la raison pour laquelle le conteneur d'applications de sécurité ne peut pas être installé. La version ROMmon est donc vérifiée car la configuration minimale de ROMmon est requise pour les plates-formes prises en charge par IOS-XE SD-WAN. Cette version se trouve sur le périphérique :

```
cEdge10#show platform | b Firmware  
Slot      CPLD Version      Firmware Version  
-----  
0         17100501           16.8(1r)  
R0        17100501           16.8(1r)  
F0        17100501           16.8(1r)
```

Lorsque vous exécutez le logiciel 16.10.2 et selon les notes de publication, la version minimale requise de ROMmon est 16.9(1r), donc ROMmon a été mis à niveau et la mémoire libre est de nouveau vérifiée :

```
cEdge10#sh memory platform  
Virtual memory : 11516805120  
Pages resident : 708276  
Major page faults: 2303  
Minor page faults: 1705306  
  
Architecture : aarch64_be  
Memory (kB)  
Physical      : 8143440  
Total         : 8143440  
Used          : 2571908  
Free          : 5571532  
Active        : 2213868  
Inactive      : 1128140  
Inact-dirty   : 0  
Inact-clean   : 0  
Dirty         : 8  
AnonPages     : 1410328  
Bounce        : 0  
Cached        : 1619664  
Commit Limit  : 4006184  
Committed As  : 3136948  
High Total    : 0  
High Free     : 0
```

```
Low Total      : 8143440
Low Free      : 5571532
Mapped        : 397692
NFS Unstable  : 0
Page Tables   : 17216
Slab          : 158776
Writeback     : 0
```

À partir de la sortie ci-dessus, notez la mémoire libre et physique (plus de 5 Go et 8 Go en conséquence).

Une fois que l'installation du conteneur d'applications de sécurité a été déclenchée à nouveau lorsque le modèle de périphérique est détaché et attaché de nouveau et que les messages relatifs à l'installation réussie sont affichés :

```
%IOSXE-5-PLATFORM: R0/0: VCONFD_NOTIFIER: Install status: cc761b3b-cb3b-4070-81de-9b842fd68b27
download-start. Message Downloading http://10.10.10.100:8080/software/package/lxc/app-
hosting_UTD-Snort-Feature-x86_64_1.0.8_SV2.9.11.1_XE16.10_secapp-
ucmk9.16.10.2.1.0.8_SV2.9.11.1_XE16.10.x86_64.tar?deviceId=10.10.10.10
%Cisco-SDWAN-cEdge10-action_notifier-6-INFO-1400002: R0/0: VCONFD_NOTIFIER: Notification:
4/5/2019 09:54:4 system-software-install-status severity-level:minor host-name:cEdge10 system-
ip:10.10.10.10 status:download-start install-id:cc761b3b-cb3b-4070-81de-9b842fd68b27
message:Downloading http://10.10.10.100:8080/software/package/lxc/app-hosting_UTD-Snort-Feature-
x86_64_1.0.8_SV2.9.11.1_XE16.10_secapp-
ucmk9.16.10.2.1.0.8_SV2.9.11.1_XE16.10.x86_64.tar?deviceId=10.10.10.10
%IOSXE-5-PLATFORM: R0/0: VCONFD_NOTIFIER: Install status: cc761b3b-cb3b-4070-81de-9b842fd68b27
download-complete. Message Downloaded app image to /bootflash/.UTD_IMAGES/app-hosting_UTD-Snort-
Feature-x86_64_1.0.8_SV2.9.11.1_XE16.10_secapp-ucmk9.16.10.2.1.0.8_SV2.9.11.1_XE16.10.x86_64.tar
%Cisco-SDWAN-cEdge10-action_notifier-6-INFO-1400002: R0/0: VCONFD_NOTIFIER: Notification:
4/5/2019 09:54:5 system-software-install-status severity-level:minor host-name:cEdge10 system-
ip:10.10.10.10 status:download-complete install-id:cc761b3b-cb3b-4070-81de-9b842fd68b27
message:Downloaded app image to /bootflash/.UTD_IMAGES/app-hosting_UTD-Snort-Feature-
x86_64_1.0.8_SV2.9.11.1_XE16.10_secapp-ucmk9.16.10.2.1.0.8_SV2.9.11.1_XE16.10.x86_64.tar
%IOSXE-5-PLATFORM: R0/0: VCONFD_NOTIFIER: Install status: 9fd36cd6-f601-4fac-a5b0-1a36f06ba18a
verification-complete. Message NOOP
%Cisco-SDWAN-cEdge10-action_notifier-6-INFO-1400002: R0/0: VCONFD_NOTIFIER: Notification:
4/5/2019 9:54:5 system-software-install-status severity-level:minor host-name:cEdge10 system-
ip:10.10.10.10 status:verification-complete install-id:cc761b3b-cb3b-4070-81de-9b842fd68b27
message:NOOP
%VMAN-5-PACKAGE_SIGNING_LEVEL_ON_INSTALL: R0/0: vman: Package 'iox-
utd_1.0.8_SV2.9.11.1_XE16.10.tar' for service container 'utd' is 'Cisco signed', signing level
cached on original install is 'Cisco signed'
%VIRT_SERVICE-5-INSTALL_STATE: Successfully installed virtual service utd
%IOSXE-5-PLATFORM: R0/0: VCONFD_NOTIFIER: Install status: cc761b3b-cb3b-4070-81de-9b842fd68b27
install-start. Message Success, App state: DEPLOYED
%Cisco-SDWAN-cEdge10-action_notifier-6-INFO-1400002: R0/0: VCONFD_NOTIFIER: Notification:
4/5/2019 09:54:5 system-software-install-status severity-level:minor host-name:ISR-4331 system-
ip:10.10.10.10 status:install-start install-id:cc761b3b-cb3b-4070-81de-9b842fd68b27
message:Success, App state: DEPLOYED
```

Et voici comment l'installation a réussi du côté de vManage :

```
[6-Apr-2019 12:38:13 CEST] Total number of Security App containers to be installed: 1. Security
App containers to be installed are following: [app-hosting-UTD-Snort-Feature-x86_64-
1.0.8_SV2.9.11.1_XE16.10]
[6-Apr-2019 12:38:13 CEST] Started 1/1 Security app container (app-hosting-UTD-Snort-Feature-
x86_64-1.0.8_SV2.9.11.1_XE16.10) installation
[6-Apr-2019 12:38:14 CEST] Checking if iox is enabled on device
[6-Apr-2019 12:38:17 CEST] Waiting for iox to be enabled on device
[6-Apr-2019 12:40:05 CEST] iox enable
[6-Apr-2019 12:40:05 CEST] Iox enabled on device
```

[6-Apr-2019 12:40:11 CEST] Security App container image: app-hosting_UTD-Snort-Feature-x86_64_1.0.8_SV2.9.11.1_XE16.10_secapp-ucmk9.16.10.2.1.0.8_SV2.9.11.1_XE16.10.x86_64.tar

[6-Apr-2019 12:40:19 CEST] Connection Instance: 0, Color: biz-internet

[6-Apr-2019 12:40:19 CEST] Downloading http://10.10.100:8080/software/package/lxc/app-hosting_UTD-Snort-Feature-x86_64_1.0.8_SV2.9.11.1_XE16.10_secapp-ucmk9.16.10.2.1.0.8_SV2.9.11.1_XE16.10.x86_64.tar?deviceId=10.10.10.10

[6-Apr-2019 12:56:45 CEST] Downloaded app image to /bootflash/.UTD_IMAGES/app-hosting_UTD-Snort-Feature-x86_64_1.0.8_SV2.9.11.1_XE16.10_secapp-ucmk9.16.10.2.1.0.8_SV2.9.11.1_XE16.10.x86_64.tar

[6-Apr-2019 12:56:48 CEST]

[6-Apr-2019 12:57:19 CEST] Success, App state: DEPLOYED

[6-Apr-2019 12:57:27 CEST] utd installed successfully

Current state is deployed

[6-Apr-2019 12:57:27 CEST] app-hosting-UTD-Snort-Feature-x86_64 installed in DEPLOYED state

[6-Apr-2019 12:57:27 CEST] Finished 1/1 Security app container (app-hosting-UTD-Snort-Feature-x86_64-1.0.8_SV2.9.11.1_XE16.10) installation

Références

- https://sdwan-docs.cisco.com/Product_Documentation/vManage_Help/Release_18.4/Security/Configuring_Security_Virtual_Image_for_IPS%2F%2FIDS_and_URL_Filtering
- https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.4/Release_Notes/Release_Notes_for_IOS_XE_SD-WAN_Release_16.10_and_SD-WAN_Release_18.4#ROMmon_Requirements_Matrix