

vManageがデバイスにセキュリティアプリケーションコンテナをインストールできない理由

内容

[概要](#)

[問題](#)

[解決方法](#)

[参考資料](#)

概要

このドキュメントでは、セキュリティポリシーがデバイステンプレートで使用される場合のセキュリティアプリケーションコンテナのインストールに関する問題とその解決方法について説明します。

問題

ユーザは、vManageで次のエラーを使用してセキュリティアプリケーションコンテナをインストールする必要があるセキュリティポリシーでデバイステンプレートを添付できません。

```
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
```

vManageコントローラの/var/log/nms/vmanage-server.logから、次のエラーが表示されます。

```
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)
[classess:]
at
com.viptela.vmanage.server.deviceaction.processor.config.AppHostingTemplateProcessor.checkAndEnableIox(AppHostingTemplateProcessor.java:358) [classes:]
at
com.viptela.vmanage.server.deviceaction.processor.config.AppHostingTemplateProcessor.preTemplatePushCheck(AppHostingTemplateProcessor.java:173) [classes:]
at
com.viptela.vmanage.server.deviceaction.processor.service.lxc.LxcInstallActionProcessor$LxcInstallActionWorker.startMaintenanceDeviceActions(LxcInstallActionProcessor.java:340) [classes:]
at
com.viptela.vmanage.server.deviceaction.DefaultActionWorker.startDeviceAction(DefaultActionWorker.java:82) [classes:]
at
com.viptela.vmanage.server.deviceaction.AbstractActionWorker.call(AbstractActionWorker.java:117) [classes:]
at
com.viptela.vmanage.server.deviceaction.AbstractActionWorker.call(AbstractActionWorker.java:35) [classes:]
at java.util.concurrent.FutureTask.run(FutureTask.java:266) [rt.jar:1.8.0_162]
at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1149) [rt.jar:1.8.0_162]
at java.util.concurrent.ThreadPoolExecutor$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
```

上に示すように、「Failed to enabled iox:null」は両方の出力に表示されます。これは、デバイスに接続された選択されたSecurity App Hostingプロファイルに対して、メモリの量が十分でないことを意味します。

解決方法

Security App Hostingプロファイルに起因するメモリの問題が疑われていたため、チェックが行われ、デフォルトプロファイルが使用されていることが検出されます。

SECURITY POLICY PARAMETERS

NAT

On Off

Resource Profile

デバイスのメモリが不足しているときに問題を引き起こすことが知られているハイプロファイルとは対照的です。

次のステップとして、デバイス自体のメモリ使用量が確認され、8 GbのRAMを搭載したC1111Xルータの空きメモリは約1 Gbであることがわかりました(空き容量に注意してください)。

```
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
```

同時に、**show version**の出力から、デバイスのRAMが8 Gbであることが確認されました(物理メモリに注意)。

```
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:.
```

Security Appコンテナをインストールできない理由はメモリ不足であるため、IOS-XE SD-WAN対応プラットフォームには最低限のROMmon要件があるため、ROMmonバージョンがチェックされます。このバージョンはデバイスで見つかります。

```
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)
```

16.10.2ソフトウェアを実行し、リリースノートに従って最低限必要なROMmonバージョンは16.9(1r)であるため、ROMmonはアップグレードされ、再び空きメモリがチェックされます。

```
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
```

上記の出力から、空きメモリと物理メモリ (5 Gb以上、8 Gb以上) に注意してください。

このSecurity Appコンテナのインストールが再びトリガーされた後、デバイステンプレートが取り外されて再度接続され、インストールが成功したことを示すメッセージが表示されます。

```
%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
```

次に、インストールがvManage側からどのように正常に行われたかを示します。

```
[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://10.10.10.100:8080/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

参考資料

- https://sdwan-docs.cisco.com/Product_Documentation/vManage_Help/Release_18.4/Security/Configuring_SD-WAN_Security/Configuring_the_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