Collect_OOB ログの取得方法

Nutanix サーバがハングアップやハードウェア障害時に、Nutanix サポートより Collect_OOB ログの取得が依頼される場合があります。本ドキュメントで Collect_OOB ログの取得方法を紹介します。

前提条件

1. サーバモデルが NX であること。（Dell XC、Lenovo サーバで実行してはいけません）
   ※CVM で”ncli host ls”というコマンドで確認できます。

```
nutanix@cvm~$ ncli host ls | egrep 'Cont|Model'

Controller VM Address       : 10.148.106.41
Block Serial (Model)        : 18SM6H020151 (NX-3060-G6)
```

2. IPMI の UDP ポート 623（Virtual Media/IPMI command port）が有効になっていること。
   ※IPMI WebUI → Configuration → Port から確認できます。

3. サーバがハングアップした状態で取得する必要があります。

取得方法

本手順では以下のログが取得されます。順番に取得して、Nutanix サポートへご送付お願いします。

1）IPMI Trouble Shooting ログ
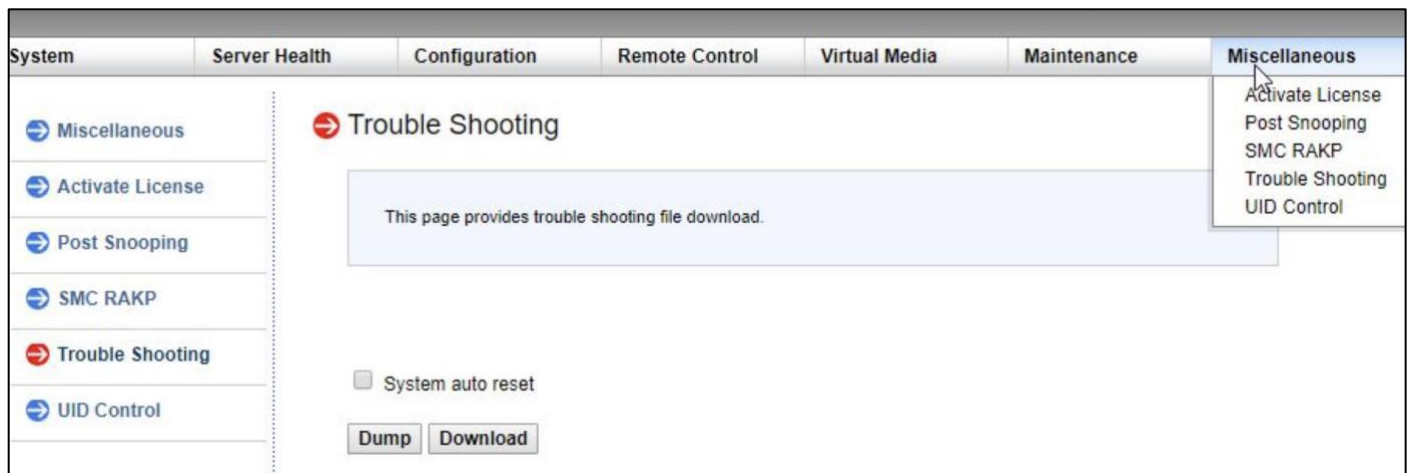2）IPMI Event ログ
3）Collect_OOB ログ

以下、詳細手順を説明します。

1）IPMI Trouble Shooting ログ

IPMI WebUI → Miscellaneous → Trouble Shooting ページで、Download をクリックして、ファイルを保存します。Download がグレーの場合、Dump を先にクリックし、Download が数分後クリックできるようになりましたら、Download をクリックして保存します。

※System auto reset のチェックを外してから実行します。
※機種や BMC バージョンによって Trouble Shooting オプションが無い場合もあります。
※Trouble Shooting オプションが無い場合は次のステップに進みます。

2）IPMI Event ログ

IPMI WebUI → Server Health → Event Log(もしくは System Management Log)ページで直近の
イベントの画面ショットを取ります。

3）Collect_OOB ログ

a. 以下のツールをダウンロードします。
   Download location: http://download.nutanix.com/2893%2Fcollect_oob_v3.3.tar.gz
   MD5SUM: 843cec53751bbd605d1a37c3068f4e15

b. **問題が発生していない** CVM の /home/nutanix/tmp に SCP などで転送します。

c. ファイルを解凍します。

```
nutanix@cvm:~/tmp$ tar zxvf 2893_collect_oob_v3.3.tar.gz
```

d. 以下コマンドを実行してログを収集します。

```
nutanix@cvm:~/tmp$ cd collect_oob

nutanix@cvm:~/tmp/collect_oob$ ./collect_oob_logs.sh -i <ハングアップしたホストの IPMI アドレス> -u
ADMIN -p '<IPMI ADMIN ユーザのパスワード>'
```

　２つめのコマンドの実行例：

```
nutanix@cvm:~/tmp/collect_oob$ ./collect_oob_logs.sh -i 10.0.0.100 -u ADMIN -p 'ADMIN'
```

　※IPMI のユーザ名 ADMIN, パスワード ADMIN、IPMI の IP アドレスが 10.0.0.100 の場合

e. 以下のメッセージが表示されましたら**ハングアップしたホスト**をリブートします。

```
Please press "Y" after doing warm reboot to the system 10.0.0.100
```

方法 1）もう一つ Putty/Teraterm を起動し、任意一台の CVM から以下コマンドで**ハングアップしたホス
ト**をリブートします。リブートが失敗した場合のみ、方法 2 でリブートします。

```
nutanix@cvm$ ipmitool -I lanplus -H <ハングしたホストの IPMI アドレス> -U ADMIN -P '<IPMI ADMIN ユーザ
のパスワード>' chassis power diag
```

方法 2）**ハングアップしたホスト**の IPMI にログインして、Reset Server でリブートします。
IPMI WebUI　→Remote Control　→Power Control　→Reset Server

f. **ハングアップしたホスト**が起動しましたら、以下のメッセージが表示された CVM に戻って、
   Y を入力して、Enter キーを押します。

```
Please press "Y" after doing warm reboot to the system 10.0.0.100: Y
```

g. collecty_oob の実行フォルダ(/home/nutanix/tmp/collect_oob)に、ハングアップしたホストの
   シリアル番号でフォルダが作られます。ログはそのフォルダの中に格納されます。

```
nutanix@cvm:~/tmp/collect_oob$ ls -l

total 18704

-rwx------. 1 nutanix nutanix      7865 Nov   3 14:17 collect_oob_logs.sh

drwx------. 2 nutanix nutanix      4096 Nov   3 14:10 lib

-rwx------. 1 nutanix nutanix       399 Nov   3 14:17 mce_analyze.py

-rw-------. 1 nutanix nutanix     97855 Nov   4 09:19 mce_dump.log

-rwx------. 1 nutanix nutanix   7688180 Aug 15   2016 SMCIPMITool.jar

-rw-------. 1 nutanix nutanix         0 Nov   4 09:16 SMCIPMITool.properties

-rwx------. 1 nutanix nutanix  11330856 Dec   9   2016 sum

drwx------. 2 nutanix nutanix      4096 Nov   4 09:21 ZM16BS034901 <<<  このフォルダを取得
```

h. 以下コマンドで作成されたフォルダをアーカイブし、一つのファイルにまとめます。
    例：作られたフォルダの名前が **ZM16BS034901** の場合

```
nutanix@cvm:~/tmp/collect_oob$ tar -zcvf ZM16BS034901_oob_logs.tar.gz ZM16BS034901/
```

上記コマンドを実行すると、ZM16BS034901_oob_logs.tar.gz と言うファイルが、collecty_oob の
実行フォルダ(/home/nutanix/tmp/collect_oob) に作成されます。作成された圧縮ファイル(上記の
例の場合 ZM16BS034901_oob_logs.tar.gz)を SCP などで取得して、弊社までお送りください。

弊社へのファイルの送付につきましては、「日本語のサポート資料」にある「Nutanix サポートへ
ファイルを送付する」をご参照ください。

補足

・CVM/Hypervisor が IPMI と異なるネットワークに存在する場合の取得方法：
 1. IPMI と同じネットワークで Linux 仮想マシンを構築します。
 2. 以下コマンドで IPMI ツールをインストールします。（CentOS の場合）
     yum install ipmitools
 3. ダウンロードした Collect OOB スクリプトを該当マシンに転送して、仮想マシンで実行します。

・Supermicro Update Manager バージョンの確認方法：

```
nutanix@cvm:~$ /home/nutanix/foundation/lib/bin/smcsumtool/sum | head -2

Supermicro Update Manager (for UEFI BIOS) 2.0.0 (2017/11/08) (x86_64)

Copyright©2017 Super Micro Computer, Inc. All rights reserved
```

注意事項

Hypervisor が AHV や Hyper-V の場合、ハングアップが発生したとき自動的にホストが再起動されます。問題を調査するためにはホストで一時的にこの「ハングアップによる再起動」を無効にして、次回ハングアップ時に collect_oob ログを取得する必要があります。
以下の方法でハングアップによる再起動を無効、有効にすることができます。

・再起動を無効にする方法：
 AHV の場合、以下コマンドを **AHV ホスト**にログインしてから順番に実行します。

```
[root@ahv]# echo 0 > /proc/sys/kernel/panic

[root@ahv]# echo "kernel.panic = 0" >> /etc/sysctl.conf

[root@ahv]# chkconfig kdump off

[root@ahv]# service kdump stop
```

 Hyper-V の場合、以下のコマンドを **Hyper-V ホスト**に RDP 等でログオンしてから順番に実行します。

```
>powershell

PS> Set-Property HKLM:¥SYSTEM¥ControlSet001¥Control¥CrashControl -Name AutoReboot -Value 0
```

・再起動を有効にする方法：

AHV の場合、以下コマンドを **AHV ホスト**にログインしてから順番に実行します。

```
[root@ahv]# echo 60 > /proc/sys/kernel/panic

[root@ahv]# service kdump start

[root@ahv]# chkconfig kdump on

[root@ahv]# sed -i /'kernel.panic = 0'/d /etc/sysctl.conf
```

Hyper-V の場合、以下のコマンドを **Hyper-V ホスト**に RDP 等でログオンしてから順番に実行します。

```
>powershell

PS> Set-Property HKLM:¥SYSTEM¥ControlSet001¥Control¥CrashControl -Name AutoReboot -Value 1
```