Collect_OOB ログの取得方法

2024 年 10 月版

Nutanix ハードウェア(NX)にてハードウェア障害の発生やハイパーバイザのハングアップが生じた際に、ハードウェアの問題調査のため Nutanix のサポートから Collect_OOB[1]による診断情報の採取を依頼される場合があります。本ドキュメントではこの Collect_OOB ログの取得方法を紹介いたします。

前提条件

Collect_OOB による診断情報の収集は Nutanix から提供されるハードウェア(NX)に限られます。
DELL XC, HPE Proliant 等のサードパーティー製ハードウェアではご利用頂けないのでご注意ください[2]。

Nutanix 製ハードウェアの場合も、G7 までのハードウェアと G8 以降のハードウェアにて若干採取の方法が異なります。それぞれ以下の章をご確認ください。

- G8 以降での診断情報の採取
- G7 およびそれ以前での診断情報の採取

本件の採取はハングアップしているノードを前提としております。再起動してしまった場合はご利用頂けませんのでご注意ください。
また、Hyper-V および AHV ではハングアップすると自動的に再起動が行われてしまいます。こちらの防止については自動再起動の抑制方法についてをご確認ください。

IPMI を通じて情報採取を行うためあらかじめ該当のノードの IPMI の IP アドレス、ユーザ名、パスワードをご用意ください。
また Collect_OOB ログの採取では以下よりダウンロードされるスクリプトを使用いたします。

ファイル名: **2893_collect_oob_v3.3.tar.gz**

URL: http://download.nutanix.com/2893%2Fcollect_oob_v3.3.tar.gz

MD5: **843cec53751bbd605d1a37c3068f4e15**

あらかじめダウンロード、同じクラスタの問題を起こしたノード以外の CVM の/home/nutanix/tmp 以下に転送をお願いいたします

---

[1] "OOB"とは Out-Of-Band すなわち通常の経路とは異なる外部の経路を用いた情報収集を指します。
Collect_OOB の場合、障害を起こしたノードそのもののプロセッサを使用するのではなく、ノードのマザーボードに存在する管理用プロセッサ(BMC)を使用した診断情報の収集を行います。

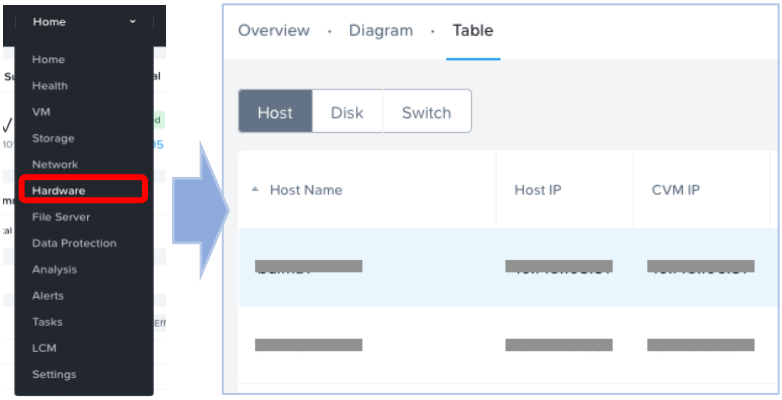
[2] サードパーティー製ハイパーバイザでのハードウェアによる障害の場合は、該当のベンダーのサポートにお問い合わせの上、調査およびパーツ交換などの対処の実施をお願いいたします。

BMC(IPMI)へのアクセスのための情報確認

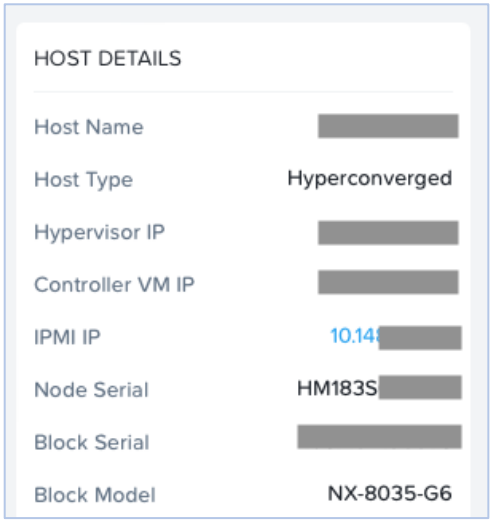
G8 以降の場合も G7 ないしそれ以前の場合も、情報の採取のために該当のノードの BMC へのアクセスが必要となります。なお、BMC についてはその通信のためのプロトコルから IPMI とも呼ばれております。

BMC(IPMI)へのアクセスへは ipmitool, ipmicfg などのコマンドの利用、あるいはウェブブラウザでのアクセス(IPMI WebUI)がございます。いずれの場合も IPMI のユーザ名とパスワード、および IP アドレスが必要になります。
採取の実施の前に対象のノードの IPMI の IP アドレス、ユーザ名、パスワードをご用意ください。

IPMI の IP アドレスは以下 Prism の Hardware(ハードウェア)の画面にてご確認頂けます。



1. Prism のメニューにて Hardware(ハードウェア)を選択
2. Hardware の画面の Table の一覧にて該当のノードをクリックして選択
3. Prism の画面を下にスクロール、左側の HOST DETAILS を確認



IPMI IP の項目が BMC(IPMI)の IP アドレスになる。この部分はリンクでありクリックすると IPMI Web UI へアクセスになる。また、ここで Node Serial や機器のモデルを確認できる。

IPMI のデフォルトのユーザ名は ADMIN(全て大文字)、
デフォルトのパスワードはそのノードのノードシリアルになります[3]。(ブロックシリアルではないのでご注意ください)

ハードウェアモデルの確認方法

なお、ご利用の機器のハードウェアのモデルについては、以下のコマンドでもご確認頂けます。

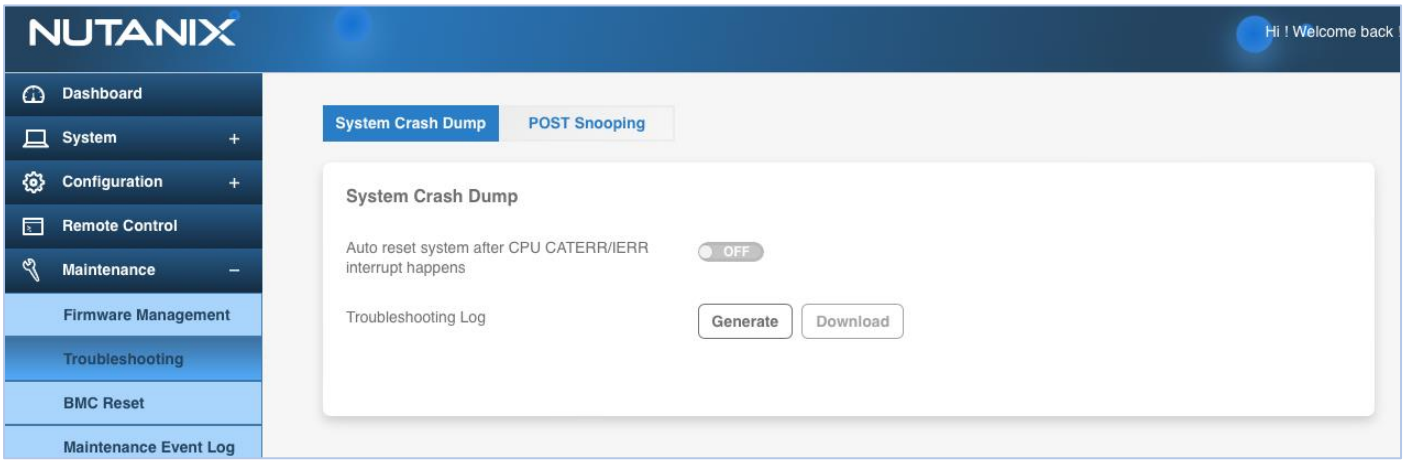
```
nutanix@cvm~$ ncli host ls | egrep 'Cont|Model'

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

[3] ノードシリアルはノードの背面のシールにも記載がございます。

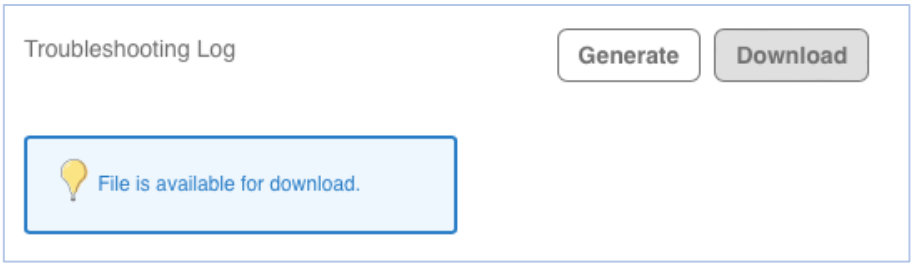
G8 以降での診断情報の採取

ウェブブラウザで **https://<IPMI IP>/** の URL でアクセスすると IPMI WebUI の画面が表示されます。

あらかじめ確認したユーザ名とパスワードでログイン、画面左側 Maintenance をクリック、表示された項目から Trouble Shooting を選択します。



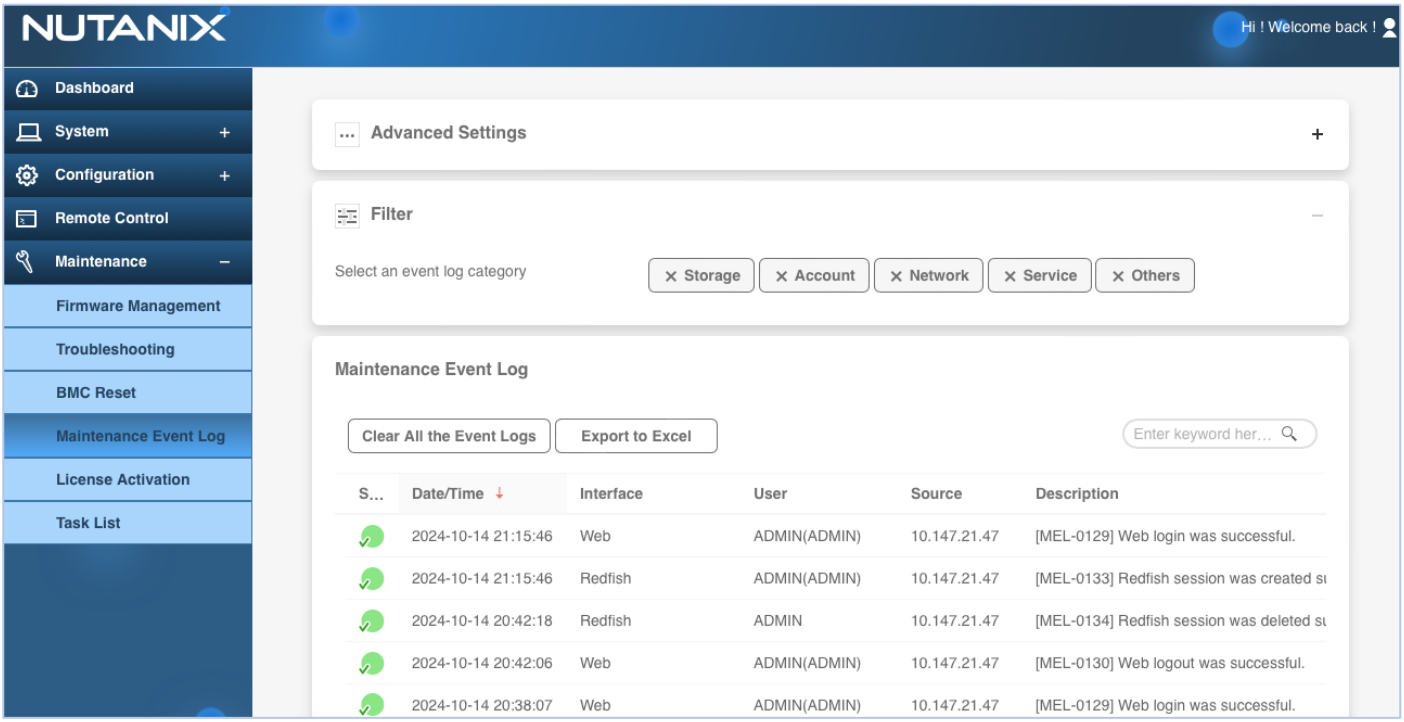
もし Download を押すことが可能な場合は、ここで Download をクリック、ログを保存します。
Download がまだ押せない場合は、その横の Dump ボタンをクリック、少し待つと以下の表示になるので Download ボタンが押してください。



IPMI WebUI へのアクセスについては次でも使用します。
ブラウザのウィンドウを閉じたり IPMI WebUI からログアウトせずそのまま次へ進めてください。

2. Event ログの採取

IPMI WebUI の画面左側 Maintenance をクリック、表示された項目から Maintenance Event Log を選択します。



この画面を表示しているブラウザのウィンドウ全体でスクリーンショットを採取します[4]。

また Export to Excel ボタンを押し、ダウンロードされてくる.xlsx ファイルを保存してください。

IPMI WebUI へのアクセスについては次でも使用します。
ブラウザのウィンドウを閉じたり IPMI WebUI からログアウトせずそのまま次へ進んでください。

[4] スクリーンショットは JPG,PNG など一般的な画像形式で保存してください。.xlsx などオフィス文書に保存されると意図せぬ圧縮が発生、確認に問題をきたす場合があるので避けてください。

3. Collect_OOB ログの採取

Collect_OOB ログの採取は以下の手順になります。手順が長いためお気を付けください。

a. あらかじめダウンロードをしておいた collect_oobs スクリプトを、現在問題が発生していないノードで実行されている CVM の/home/nutanix/tmp にコピーします。

b. コピーしたスクリプトを展開します。これはコピーした CVM に nutanix ユーザにて SSH でログイン、以下コマンドを実行することで行います。

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

最初のコマンドで /home/nutanix/tmp フォルダへ移動、次のコマンドで展開が実施されます。
このファイルを展開すると、/home/nutanix/tmp 以下に collect_oob フォルダが作成されます。

c. 続けて以下コマンドを実行し、collect_oob での情報の採取を行います。

```
nutanix@cvm:~/tmp$ cd collect_oob
nutanix@cvm:~/tmp/collect_oob$ ./collect_oob_logs.sh -i <IPMI IP> -u '<IPMI User>' -p '<IPMI Password>'
```

これから情報採取を行う、ハングアップしているノードの IP アドレスを<IPMI IP>に、<IPMI User>にはユーザ、<IPMI Password>はパスワードを指定します。
例えば障害を起こしているノードの IPMI の IP アドレスが 10.0.0.100, ユーザ名は ADMIN、パスワードが Oh my God!の場合、以下になります。

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

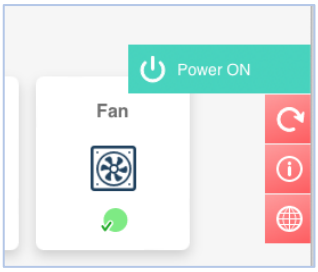
d. スクリプトが実行されるとしばらく出力があり、以下のメッセージが現れ、出力が一旦停止します。

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

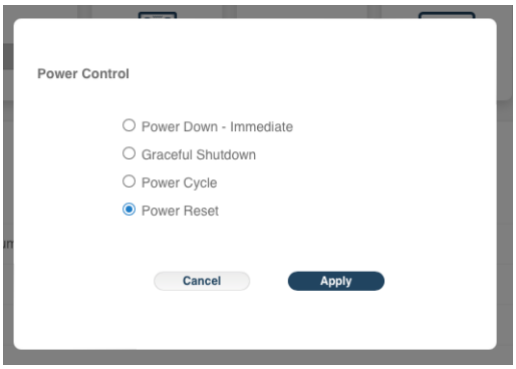
collect_oob スクリプトの実行は一旦そのまま置いておきハングアップしているノードを再起動します。

再起動については、先に使用した IPMI WebUI を使用します。

IPMI WebUI の画面右側、電源のマーク⏻の部分にマウスカーソルをあわせます。飛び出てきた Power ON と記載されている部分をクリックします。



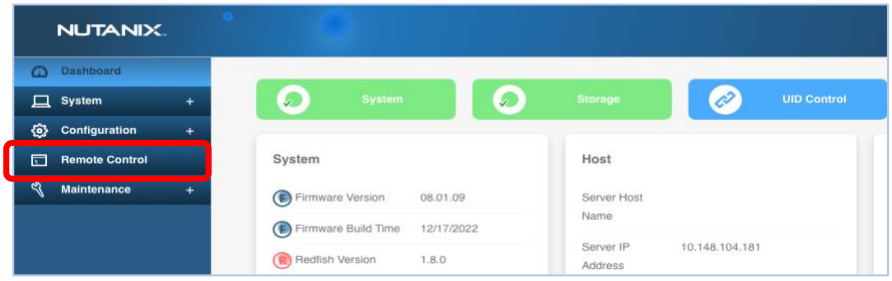
表示された Power Control パネルにて Power Reset[5]を選択、その下の Apply をクリックします。



ノードがリセットされ、再起動が行われます。

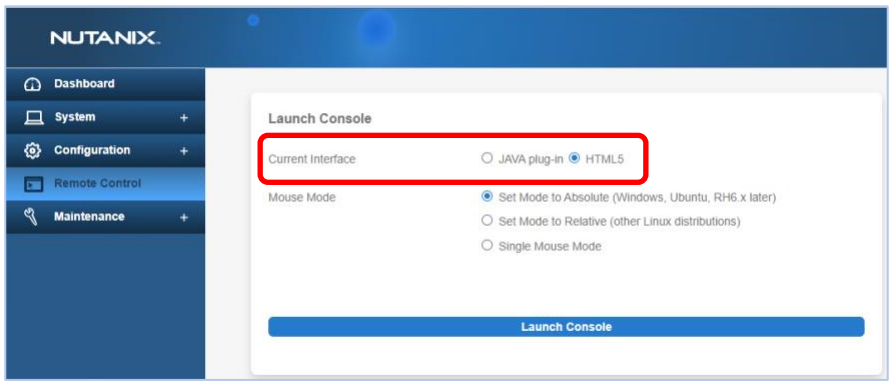
e. ノードの再起動の完了を待ちます。
ノードの起動状況を確認するため、IPMI WebUI からリモートコンソールを開いて様子を見ることが推奨となります。

画面左側の Remote Control を選択します。



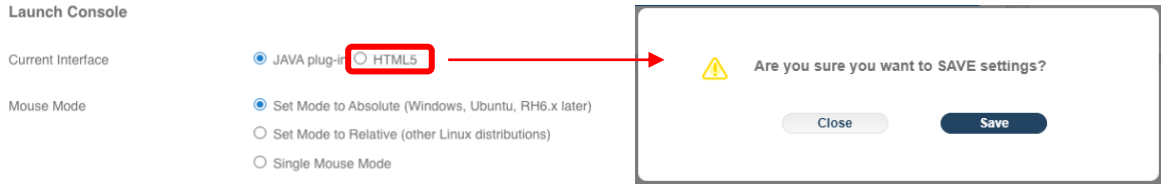
画面の Current Interface で HTML5 が選択されているのを確認します。

HTML5 が選択されている場合は画面下 Launch Console をクリック、リモートコンソールを起動します。



[5] Power Down - Immediate は即座に電源を落とす、Graceful Shutdown は ACPI の電源イベントを送付してハードウェアで動作しているハイパーバイザにシャットダウンを促す、Power Cycle は一旦電源をオフにしてから再度電源をオンにする、Power Reset は CPU に対してリセットを実施します。

Current Interface にて Java plug-in が選択されている場合は HTML5 をチェックします。
確認が表示されるので、Save を押して保存します。



リモートコンソールの画面を確認、ハイパーバイザの起動が起動している、あるいは起動に失敗している状態まで画面が進んでいるのを確認して、次へ進みます。

f. 以下の collect_oob のメッセージに Y を入力、リターンキーを押し処理を再開します。

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

しばらくすると collect_oob の処理が完了し、プロンプトが現れます。

g. collect_oob の実行フォルダ(/home/nutanix/tmp/collect_oob)にハングアップしたノードのノードシリアルを名称とするフォルダが作られております。

```
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
```

このフォルダを採取

collect_oob で採取したログはこのノードシリアルを名称としたフォルダの中に格納されます。
以下コマンドにてフォルダをアーカイブし、1 つのファイルにまとめます。

```
nutanix@cvm:~/tmp/collect_oob$ tar -zcvf <NODE_SERIAL>_oob_logs.tar.gz <NODE_SERIAL>/
```

<NODE_SERIAL>はフォルダ名になっているノードのシリアルを指します。上記例の ZM16BS034901 の場合、以下になります。

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

/home/nutanix/tmp/collect_oob 以下に上記で作成した **<NODE_SERIAL>_oob_logs.tar.gz** のアーカイブファイルが作成されております。これを CVM からコピー、採取してください

4.採取した情報の送付

以下について送付をお願いします。

- **Trouble Shooting ログ** : 1. Trouble Shooting ログの採取にて取得
- **Event Log スクリーンショット** : 2. Event ログの採取で取得
- **Event Log .xlsx ファイル** : 2. Event ログの採取で取得
- **<NODE_SERIAL>_oob_logs.tar.gz のアーカイブファイル** : 3. Collect_OOB ログの採取にて取得

また、できましたら 3. Collect_OOB ログの取得の際の CVM への SSH のログインで実行したコマンドとその出力のログについてもご送付を頂けますと幸いです。

Nutanix へのファイルの送につきましては、以下 URL のページにあります Nutanix サポートへファイルを送付するのドキュメントをご参照の上、サポートケースへの添付、あるいは SFTP サーバへのアップロードの実施をお願いいたします。

https://www.nutanix.com/jp/support-services/product-support/support-documentation

G7 およびそれ以前での診断情報の採取

1. Trouble Shooting ログの採取

ウェブブラウザで **`https://<IPMI IP>/`** の URL でアクセスすると IPMI WebUI の画面が表示されます。

あらかじめ確認したユーザ名とパスワードでログイン、画面右上 Miscellaneous の上にマウスカーソルを合わせ、表示されたメニューより Trouble Shooting を選択します。あるいは Miscellaneous をクリックして表示されたページの左端の一覧から Trouble Shooting をクリックします[6]。

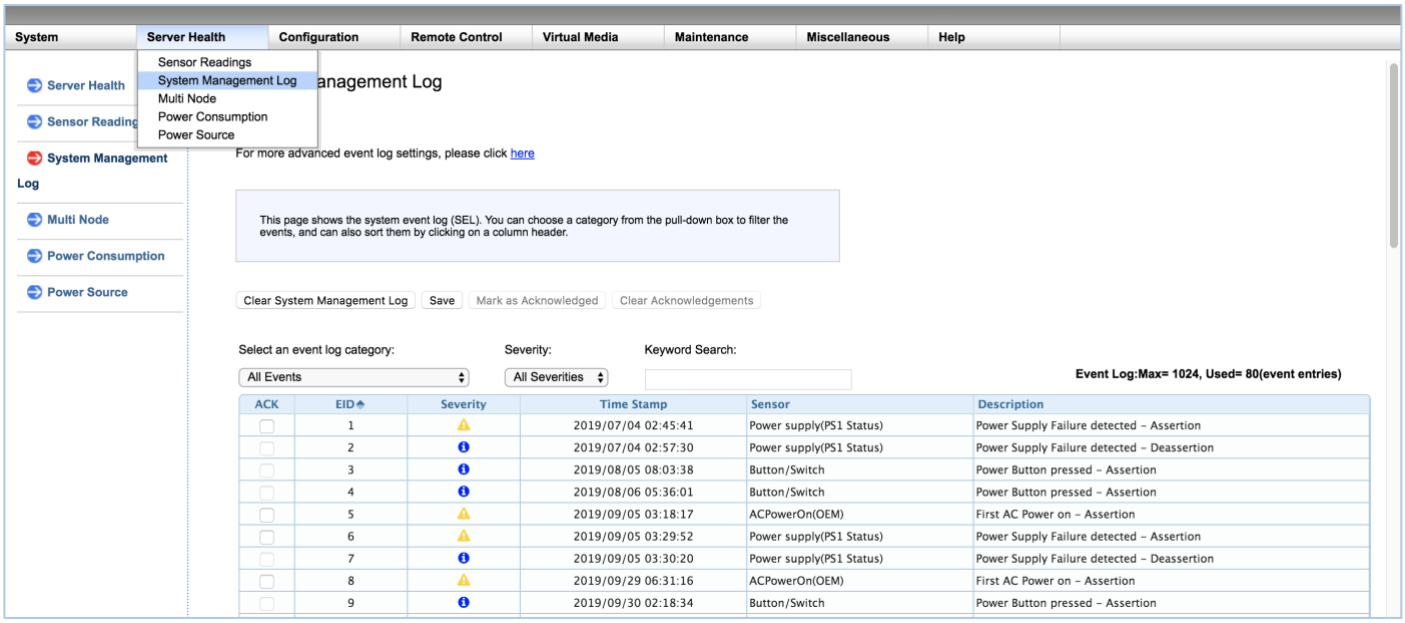
もし Download を押すことが可能な場合は、ここで Download をクリック、ログを保存します。
もし Download がまだ押せない場合は、その横の Dump ボタンをクリックして、数分待った後に Download ボタンが押せるか確認してください。

IPMI WebUI へのアクセスについては次でも使用します。
ブラウザのウィンドウを閉じたり IPMI WebUI からログアウトせずそのまま次へ進んでください。

[6] NX ハードウェア機器の種別および BMC のバージョンにより、Trouble Shooting のページが存在しない場合がございます。この場合は Trouble Shooting ログの採取は中断し、次の Event ログの採取に進めてください。

2. Event ログの採取

IPMI WebUI の画面左上 Server Health の上にマウスカーソルを合わせ、表示されたメニューより System Management Log(Event Log)[7]を選択します。あるいは Server Health をクリックして表示されたページの左端の一覧から System Management Log(Event Log)をクリックします



画面に表示されているイベントの一覧の表の Time Stamp の項目名の部分をクリックし、その後もう一度クリックします。すると、イベントの一覧の表が時系列降順(最も新しい日時が 1 行目)になります。それを確認後、IPMI WebUI を表示しているブラウザのウィンドウ全体でスクリーンショットを採取します[8]。

また、画面にある Save ボタンを押し、ダウンロードされてくる.csv ファイルを保存してください。

IPMI WebUI へのアクセスについては次でも使用します。
ブラウザのウィンドウを閉じたり IPMI WebUI からログアウトせずそのまま次へ進んでください。

[7] NX ハードウェア機器の種別および BMC のバージョンにより、System Management Log の場合、あるいは Event Log の場合がございます。どちらも同じ意味になります。
[8] スクリーンショットは JPG,PNG など一般的な画像形式で保存してください。.xlsx などオフィス文書に保存されると意図せぬ圧縮が発生、確認に問題をきたす場合があるので避けてください。

3. Collect_OOB ログの採取

Collect_OOB ログの採取は以下の手順になります。手順が長いためお気を付けください。

a. あらかじめダウンロードをしておいた collect_oobs スクリプトを、現在問題が発生していないノードで実行されている CVM の/home/nutanix/tmp にコピーします。

b. コピーしたスクリプトを展開します。これはコピーした CVM に nutanix ユーザにて SSH でログイン、以下コマンドを実行することで行います。

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

最初のコマンドで /home/nutanix/tmp フォルダへ移動、次のコマンドで展開が実施されます。
このファイルを展開すると、/home/nutanix/tmp 以下に collect_oob フォルダが作成されます。

c. 続けて以下コマンドを実行し、collect_oob での情報の採取を行います。

```
nutanix@cvm:~/tmp$ cd collect_oob
nutanix@cvm:~/tmp/collect_oob$ ./collect_oob_logs.sh -i <IPMI IP> -u '<IPMI User>' -p '<IPMI Password>'
```

これから情報採取を行う、ハングアップしているノードの IP アドレスを<IPMI IP>に、<IPMI User>にはユーザ、<IPMI Password>はパスワードを指定します。
例えば障害を起こしているノードの IPMI の IP アドレスが 10.0.0.100, ユーザ名は ADMIN、パスワードが Oh my God!の場合、以下になります。

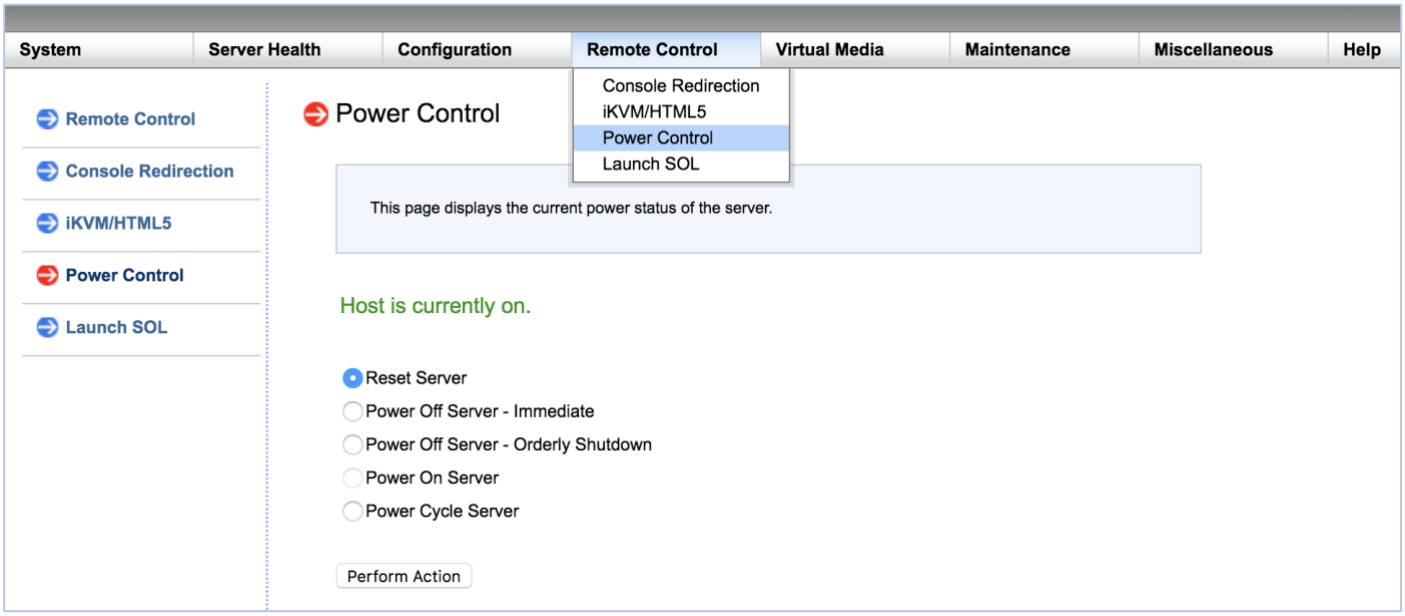
```
nutanix@cvm:~/tmp/collect_oob$ ./collect_oob_logs.sh -i 10.0.0.100 -u 'ADMIN' -p 'Oh my God!'
```

d. スクリプトが実行されるとしばらく出力があり、以下のメッセージが現れ、出力が一旦停止します。

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

collect_oob スクリプトの実行は一旦そのまま置いておきハングアップしているノードを再起動します。

再起動については、先に使用した IPMI WebUI を使用します。
画面上の Remote Control の上にマウスカーソルを合わせ、表示されたメニューより Power Control を選択します。あるいは Remote Control をクリックして表示されたページの左端の一覧から Power Control をクリックします。



表示された画面にて Reset Server を選択、その下の Perform Action をクリックします。
すると、ノードがリセットされ、再起動が行われます。

再起動の別の方法:
collect_oob を実行しているのとはもう一つ別の SSH でいずれかの CVM との接続をおこない、以下の ipmitool コマンドを実行する事でもノードのハードウェアの再起動を実施できます。

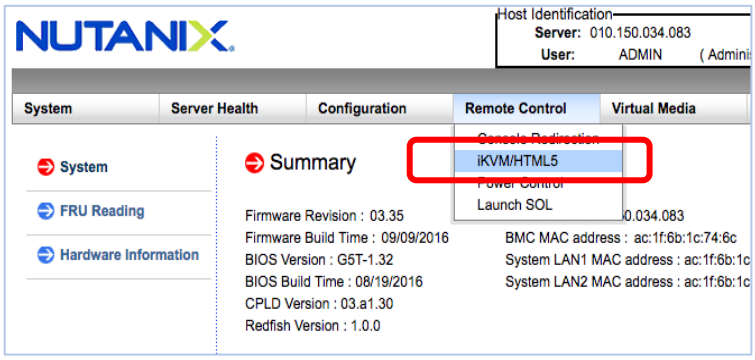
```
nutanix@cvm$ ipmitool -I lanplus -H <IPMI IP> -U <IPMI User> -P '<IPMI Password>' chassis power diag0
```

実施例:

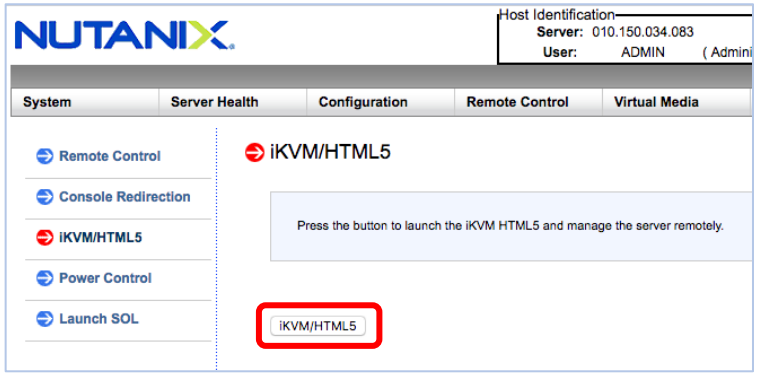
```
nutanix@cvm$ ./collect_oob_logs.sh -i 10.0.0.100 -u 'ADMIN' -p 'Oh my God!' chassis power diag0
```

e. ノードの再起動の完了を待ちます。
ノードの起動状況を確認するため、IPMI WebUI からリモートコンソールを開いて様子を見ることが推奨となります。

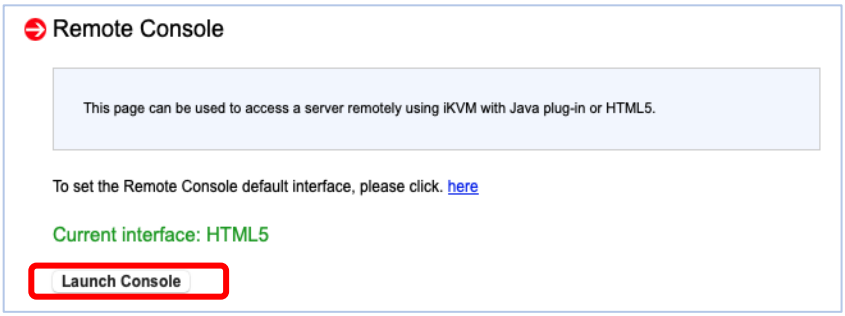
画面上の Remote Control の上にマウスカーソルを合わせ、表示されたメニューで iKVM/HTML5 を選択します。あるいは Remote Control をクリックして表示されたページの左端の一覧から iKVM/HTML5 をクリックします(右図)



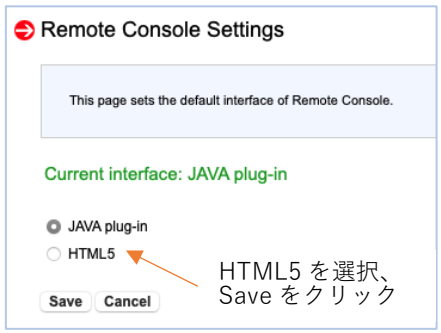
BMC のバージョンが 7.11 より前の場合は右のような画面が表示されるため、こちらの iKVM/HTML5 ボタンを押します。



BMC バージョンが 7.11 ないしそれ以降の場合は、右のような表示になります。
ここで、緑の文字で **Current Interface: HTML5** とあるのを確認します。



もし、こちらが **Java plug-in** とある場合はその上の文面の右端 here の部分のリンクをクリック、表示された画面で HTML5 を選択、Save を押して前の画面に戻り、**Current Interface: HTML5** とあるのを確認します。



その後、Launch Console をクリックします。

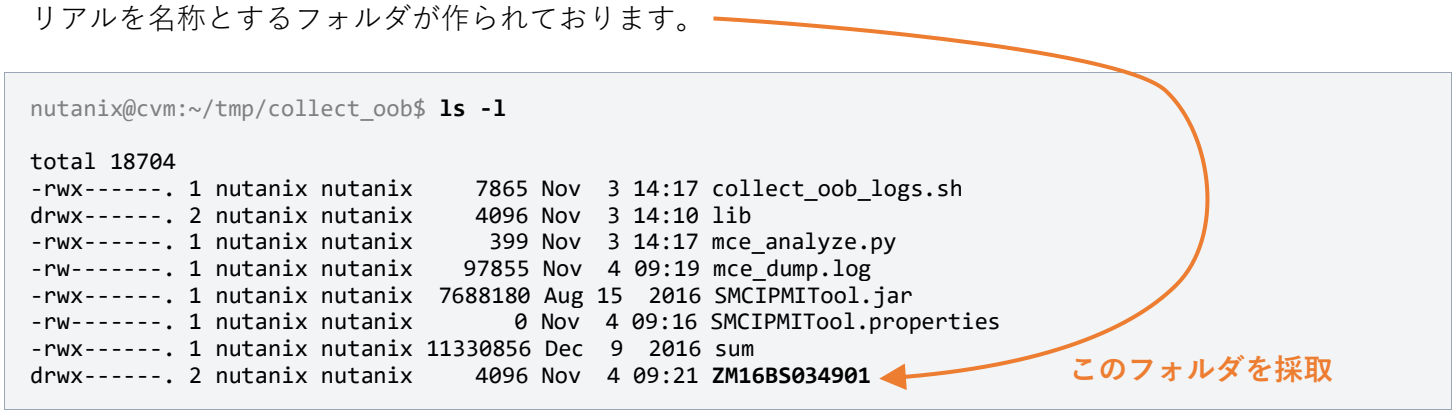
ハイパーバイザの起動が起動している、あるいは起動に失敗している状態まで画面が進んでいるのを確認して、次へ進みます。

f. 以下の collect_oob のメッセージに Y を入力、リターンキーを押し処理を再開します。

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

しばらくすると collect_oob の処理が完了し、プロンプトが現れます。

g. collect_oob の実行フォルダ(/home/nutanix/tmp/collect_oob)に、ハングアップしたノードのノードシリアルを名称とするフォルダが作られております。



collect_oob で採取したログはこのノードシリアルを名称としたフォルダの中に格納されます。
以下コマンドにてフォルダをアーカイブし、1 つのファイルにまとめます。

```
nutanix@cvm:~/tmp/collect_oob$ tar -zcvf <NODE_SERIAL>_oob_logs.tar.gz <NODE_SERIAL>/
```

<NODE_SERIAL>はフォルダ名になっているノードのシリアルを指します。上記例の ZM16BS034901 の場合、以下になります。

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

/home/nutanix/tmp/collect_oob 以下に上記で作成した **<NODE_SERIAL>_oob_logs.tar.gz** のアーカイブファイルが作成されております。これを CVM からコピー、採取してください。

4.採取した情報の送付

以下について送付をお願いします。

- **Trouble Shooting ログ** : 1. Trouble Shooting ログの採取にて取得
- **Event Log スクリーンショット** : 2. Event ログの採取で取得
- **Event Log CSV ファイル** : 2. Event ログの採取で取得
- **<NODE_SERIAL>_oob_logs.tar.gz のアーカイブファイル** : 3. Collect_OOB ログの採取にて取得

また、できましたら 3. Collect_OOB ログの取得の際の CVM への SSH のログインで実行したコマンドとその出力のログについてもご送付を頂けますと幸いです。

Nutanix へのファイルの送につきましては、以下 URL のページにあります Nutanix サポートへファイルを送付するのドキュメントをご参照の上、サポートケースへの添付、あるいは SFTP サーバへのアップロードの実施をお願いいたします。

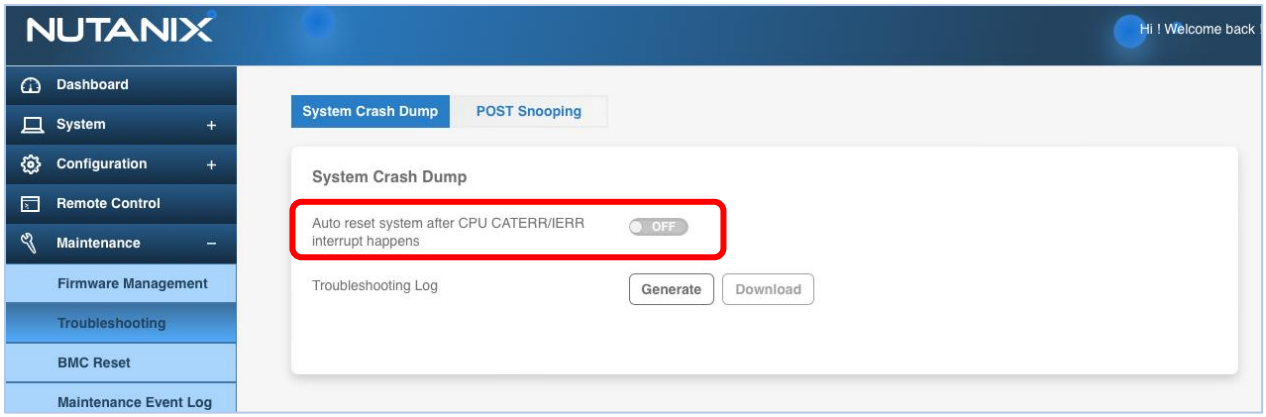
https://www.nutanix.com/jp/support-services/product-support/support-documentation

CATERR, IERR 発生時のノードの自動起動の抑制

CATERR, IERR は Intel 社製の CPU にて致命的なエラーが発生したことを示すイベントとなります。
BMC には CATERR, IERR を検出するとノードを自動的に再起動させる仕組みがございます。
自動的な再起動により速やかにハイパーバイザが再起動され、ノードを復帰することができます。
一方、Collect_OOB にて情報を採取、調査を行う場合には自動的に再起動されてしまうとその後の CPU の活動によりエラー時の状態が失われてしまい、調査ができなくなる恐れがございます。
ハードウェアの問題が疑われる場合には自動的な再起動を抑制することが必要となります。

G8 以降の場合:

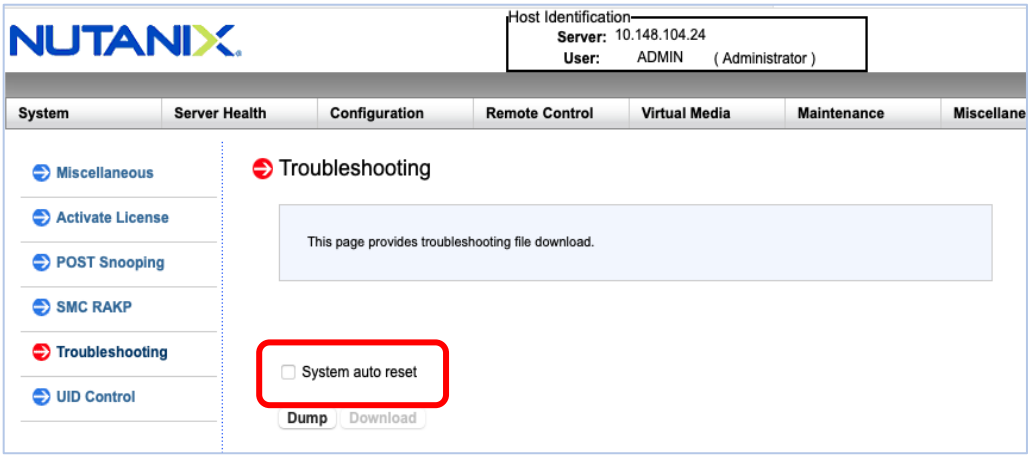
IPMI WebUI へアクセス、画面右側 Maintenance より Troubleshooting を選択、画面にある **`Auto reset system after CPU CATERR/IERR interrupt happens`** を **OFF** にします。



G7 とそれ以前の場合:

IPMI WebUI へアクセス、画面右上 Miscellaneous の上にマウスカーソルを合わせ、表示されたメニューより Trouble Shooting を選択します。あるいは Miscellaneous をクリックして表示されたページの左端の一覧から Trouble Shooting をクリックします

画面にある **`System auto reset`** のチェックを外します。



ハイパーバイザの自動再起動の抑制について

ハイパーバイザが AHV や Hyper-V の場合、ハイパーバイザのハングアップが生じますと自動的に再起動が行われ、ノードは再起動されます。
本ドキュメントの Collect_OOB での情報採取のためには一時的にこの自動的な再起動を抑制する必要がございます。
以下は抑制方法についての説明となります。

AHV ハイパーバイザ

AHV ホストにログイン、以下コマンドの実行します[9]。

```
[root@ahv]# echo 0 > /proc/sys/kernel/panic
[root@ahv]# echo "kernel.panic = 0" >> /etc/sysctl.conf
[root@ahv]# systemctl stop kdump.service
[root@ahv]# systemctl disable kdump.service
```

自動的な再起動を再度有効にする場合は、**AHV ホストにログイン**して以下のコマンドを実行します。

```
[root@ahv]# echo 60 > /proc/sys/kernel/panic
[root@ahv]# systemctl enable kdump.service
[root@ahv]# systemctl start kdump.service
[root@ahv]# sed -i /'kernel.panic = 0'/d /etc/sysctl.conf
```

[9] もしご利用の AOS が 5.15.3 ないしそれ以前、AHV ハイパーバイザが AHV-20170830.453 ないしそれ以前の場合、自動的な再起動の抑制は以下になります。

```
[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
```

また再度の有効化は以下になります。

```
[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

Hyper-V ホストの PowerShell にて以下を実行します。

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

自動的な再起動を再度有効にする場合は、Hyper-V ホストの PowerShell にて以下を実行します。

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

Hyper-V ホストにて PowerShell のコマンドを実行するにはいくつか方法がございますが、もっとも用意なのは RDP にて Hyper-V ホストに Administrator アカウントでサインイン、表示されるコマンドプロンプトウィンドウを確認します。
Windows Sever 2012 などで cmd.exe が実行されている(コマンドプロンプトが **C:>**など)の場合は、powershell と入力し実行、PowerShell を起動してから上のコマンドを実行します。

デフォルトのコマンドプロンプトが PowerShell(コマンドプロンプトが **PS C:>**など)の場合は、そのまま上記のコマンドを実行します。