ftServer におけるログ取得手順
(Linux 編)

Rev 0.5: 2017/06/08

はじめに

このドキュメントではftServerに関する障害調査を行う際に、必要となるログ･データの取得方法を説明しています。ログ・データの取得には、初期解析用のデータの取得方法と、詳細な調査を行うときのデータ取得方法があります。特別な理由でOS側のログが必要となった場合には「RHELログの取得について」をご参照下さい。尚、状況に応じてこれらのログの取得の他に追加のログや情報の取得を別途依頼させていただく場合がございます。

■初期解析用データ取得方法について

ftServerハードウェア障害の初期調査段階で必要なデータやログファイルを収集し、1つのアーカイブファイルにまとめるという方法です。一般的なハードウェア故障の判断などに有効です。

次の方法でログを取得します。
尚、この作業を実施する際にはrootアカウントでログインして下さい。
(通常の設定では、一般ユーザアカウントにはログファイルへのアクセス権がありません)

① 次のコマンドで作成される /tmp/sralog.tgz を取得します。

```
# cd /
# rpm -qa > /tmp/rpm-qa.txt
# /opt/ft/bin/ftsmaint ls > /tmp/ftsmaint.txt
# /opt/ft/bin/ftsmaint lslong > /tmp/ftsmaintlong.txt
# cat /proc/mdstat > /tmp/mdstat.txt
# mdadm -D /dev/md* > /tmp/mdadm.txt
# tar czf /tmp/sralog.tgz ./var/log/messages* ./var/opt/ft/log/ring_buffer*
  ./var/opt/ft/log/osm.log* ./tmp/rpm-qa.txt ./tmp/ftsmaint.txt
  ./tmp/ftsmaintlong.txt ./tmp/mdstat.txt ./tmp/mdadm.txt
```

注意:上記の tar コマンドの記述はファイル名が分かりやすいように改行を入れて記載していますが、実際に取得する際には、ファイル名の後はスペースを入れて改行せずに続けて入力してください。

② ログの取得が終わったら、1.で/tmpディレクトリ上に作成したファイル削除します。

```
# rm -f /tmp/sralog.tgz /tmp/rpm-qa.txt /tmp/ftsmaint.txt /tmp/ftsmaintlong.txt
  /tmp/mdstat.txt /tmp/mdadm.txt
```

■詳細データ取得方法について

Stratusサポートセンターより、必要に応じて詳細データの取得を依頼することがあります。詳細データは buggrabber ツールがログファイルを一箇所に集めて1つのファイルに圧縮したファイルを生成します。収集するログファイルの量によりますが、ファイルサイズは100MBから数ギガバイトになる事があります。

次の方法でログを取得します。
尚、この作業を実施する際にはrootアカウントでログインして下さい。
(通常の設定では、一般ユーザアカウントにはログファイルへのアクセス権がありません)

<< RHEL 7 を使用している場合 (AUL 11.0) >>

① 次のスクリプトでログを採取します。

```
# /opt/ft/sbin/buggrabber
```

Buggrabber を実行するとディレクトリ /home/BugPool/BugYYYYMMDD.tar(たとえば Bug20170101.tar)にログファイルがまとめられます。このファイルを取得します。

② ログの取得後、作成したファイルを削除します。

```
# rm -rf /home/BugPool/BugYYYYMMDD.tar
```

<< RHEL 6 を使用している場合 (AUL 8.0 または AUL 9.0) >>
<< RHEL 5 を使用している場合 (ftSSS 7.X または ftSSS 6.0.5.1以降) >>

① 次のスクリプトでログを採取します。

```
# /opt/ft/sbin/buggrabber.pl
```

buggrabber.pl を実行するとディレクトリ /home/BugPool/BugYYYYMMDD.tar(たとえば Bug20170101.tar)にログファイルがまとめられます。このファイルを取得します。

② ログの取得後、作成したファイルを削除します。

```
# rm -rf /home/BugPool/BugYYYYMMDD.tar
```

<< RHEL 5 を使用している場合 (ftSSS 6.0.5.0以前) >>

① 次のスクリプトでログを採取します。

```
# /opt/ft/sbin/buggrabber.pl
```

ディレクトリ /home/BugPool/Bug_YYYYMMDD(たとえばBug_20100531)にログファイルが集められます。

② 次のコマンドでログファイルをまとめます。(Bug_YYYYMMDD の部分は今作成されたディレクトリ名を入れてください。)ここで作成された/home/BugPool/Bug_YYYYMMDD.tgz を取得します。

```
# cd /home/BugPool
# tar czf ./Bug_YYYYMMDD.tgz ./Bug_YYYYMMDD
```

③ ログの取得後、作成したファイルを削除します。

```
# rm -rf ./Bug_YYYYMMDD ./Bug_YYYYMMDD.tgz
```

■RHELログの取得について

Red Hat Enterprise Linuxオペレーティング・システムの調査を行う場合には、次のコマンドでログを取得します。RHELログの取得はストラタスのサポートセンターより依頼があった場合に実施して下さい。
尚、この作業を実施する際にはrootアカウントでログインして下さい。

実行前に、システムにインストールされている sos パッケージのバージョンを確認します。

```
# rpm -q sos
```

<< RHEL 7 を使用している場合 (sos version 3) >>

sosreport コマンドを実行可能です。

```
# sosreport
```

作成されるファイルは次の通りです。

/var/tmp/sosreport-<ホスト名>.<入力したID>-<日時>.tar.xz
/var/tmp/sosreport-<ホスト名>.<入力したID>-<日時>.tar.xz.md5

<< RHEL 6 を使用している場合 (sos version 3) >>

sosreport コマンドを実行する前に、次のように /etc/sos.conf ファイルを編集して
“disable”オプションの行に “pci”を追加してください。
この変更を行わずに sosreport を実行したときには、ftServerのCPUエンクロージャの片系が一旦切り離され、その後自動的に二重化に復旧する動作が発生します。

修正するファイル:
/etc/sos.conf

修正内容:

(修正前)
disable = memory, hardware

(修正後)
disable = memory, hardware, pci

変更後、sosreport コマンドを実行可能です。
sosreport

作成されるファイルは次の通りです。
/tmp/sosreport-<ホスト名>.<入力したID>-<日時>.tar.xz
/tmp/sosreport-<ホスト名>.<入力したID>-<日時>.tar.xz.md5

<< RHEL 6 を使用している場合 (sos version 2) >>

Sosreport コマンドを実行可能です。
sosreport

作成されるファイルは次の通りです。
/tmp/sosreport-<ホスト名>.<入力したID>-<日時>.tar.xz
/tmp/sosreport-<ホスト名>.<入力したID>-<日時>.tar.xz.md5

<< RHEL 5 を使用している場合 (sos version 1) >>

sosreport コマンドを実行する前に、次のようにファイルを編集して “/proc/bus” の行をコメント行にしてください。
この変更を行わずに sosreport を実行したときには、ftServerのCPUエンクロージャの片系が一旦切り離され、その後自動的に二重化に復旧する動作が発生します。

修正するファイル:
/usr/lib/python2.4/site-packages/sos/plugins/hardware.py

修正内容:

（修正前）
self.addCopySpec("/proc/bus")

（修正後）
self.addCopySpec("/proc/bus")

変更後、sosreport コマンドを実行可能です。
sosreport

作成されるファイルは次の通りです。
/tmp/sosreport-<ホスト名>.<入力したID>-XXXXXX-XXXXXX.tar.bz2
/tmp/sosreport-<ホスト名>.<入力したID>-XXXXXX-XXXXXX.tar.bz2.md5

(sos version 3の実行例)

```
# sosreport

sosreport (version 3.2)

This command will collect diagnostic and configuration information from
this Red Hat Enterprise Linux system and installed applications.

An archive containing the collected information will be generated in
/var/tmp and may be provided to a Red Hat support representative.
```

```
Any information provided to Red Hat will be treated in accordance with
the published support policies at:

  https://access.redhat.com/support/

The generated archive may contain data considered sensitive and its
content should be reviewed by the originating organization before being
passed to any third party.

No changes will be made to system configuration.

Press ENTER to continue, or CTRL-C to quit.
← Enter を入力します
Please enter your first initial and last name [localhost.localdomain]:
← Enter を入力します
Please enter the case id that you are generating this report for:
1234← 適当な数字を入力します
 Setting up archive ...
 Setting up plugins ...
 Running plugins. Please wait ...
...
Your sosreport has been generated and saved in:
  /var/tmp/sosreport-localhost.localdomain.1234-20160304104725.tar.xz

The checksum is: 929aac341d2ae3f0d14ba54c48104cf5

Please send this file to your support representative.
------------------------------------------------------------------
```