



ftScalable ストレージにおけるログ取得方法の解説

内容: ftScalable ストレージに関する障害調査を行う際に、必要となるログ・データの取得方法になります。

Rev 0.2: 2011/04/27

ftScalable ストレージログ取得内容

ftScalable ストレージにはロギング機能が備わっており、ログには下記内容が含まれています。

ftScalable ストレージのログは store log と呼ばれています。

- ・ デバイスのステータスと構成情報が含まれる Device Status Summary
- ・ 両コントローラ(Active-Active 状態の場合)からのイベントログ
- ・ 両コントローラ(Active-Active 状態の場合)からのデバッグログ
- ・ 各コントローラの起動時の Boot ログ
- ・ 最大 4 つまでのダンプファイル
- ・ Management Controller のトレースログ (ログインしているコントローラから取得)

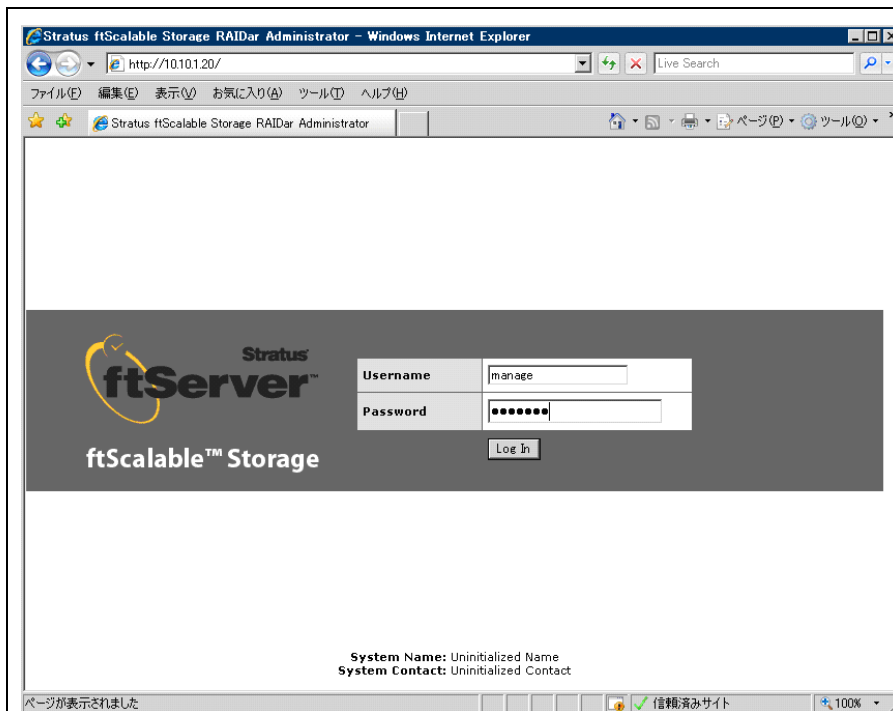
ftScalable ストレージの障害発生時は下記 2 つの方法の内何れからの手順で store_log を取得する必要があります。

- ① RAIDar を使用したログの取得
- ② FTP を使用したログの取得

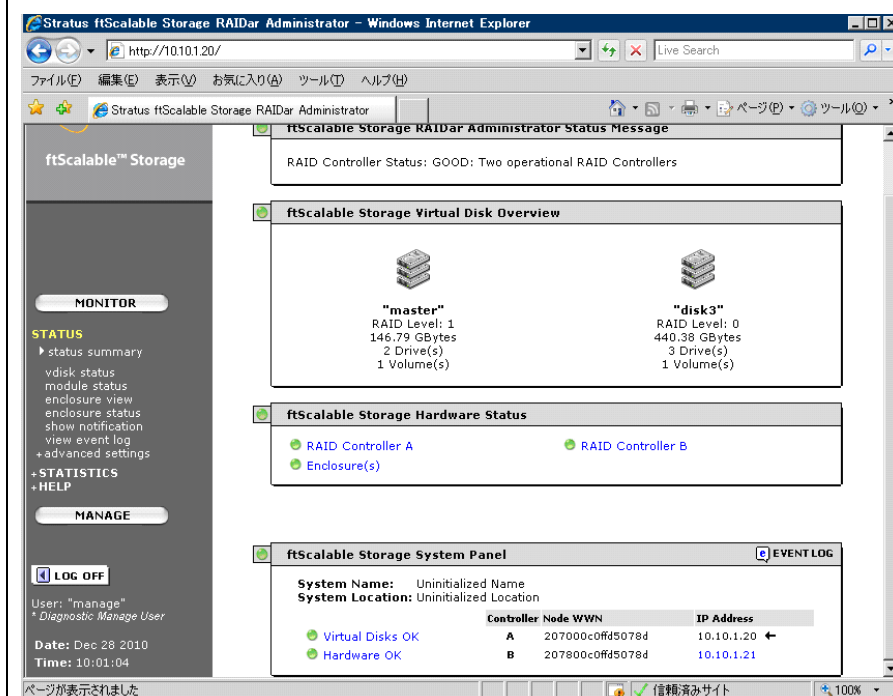
※本資料においては、ftScalable ストレージに設定されている IP アドレスは、10.10.1.20 を使用しています。

※本資料で使用する manage ユーザのパスワードについては、別途お知らせします。

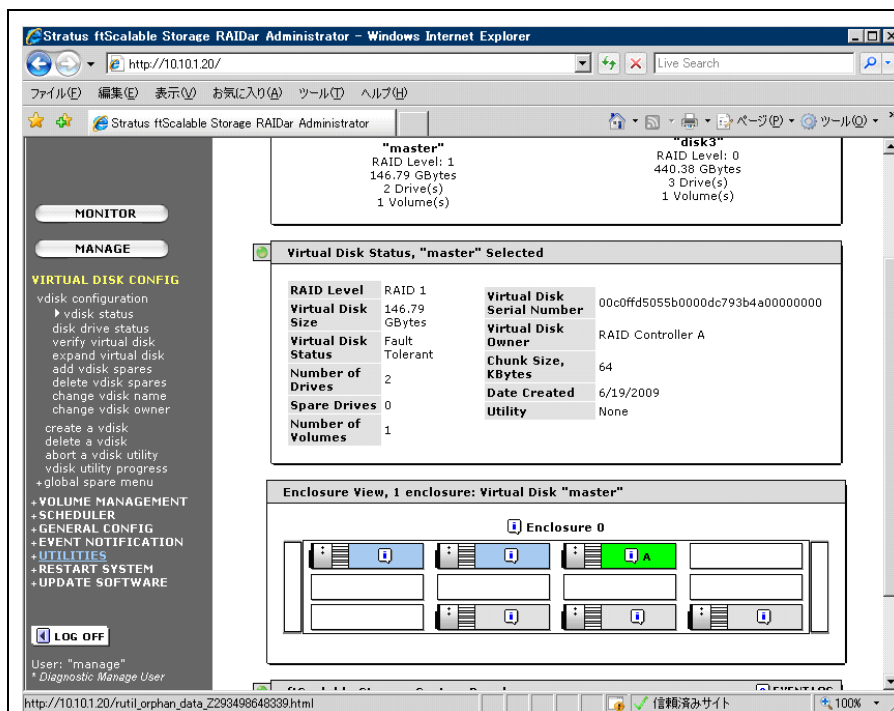
1. RAIDar を使用したログの取得方法



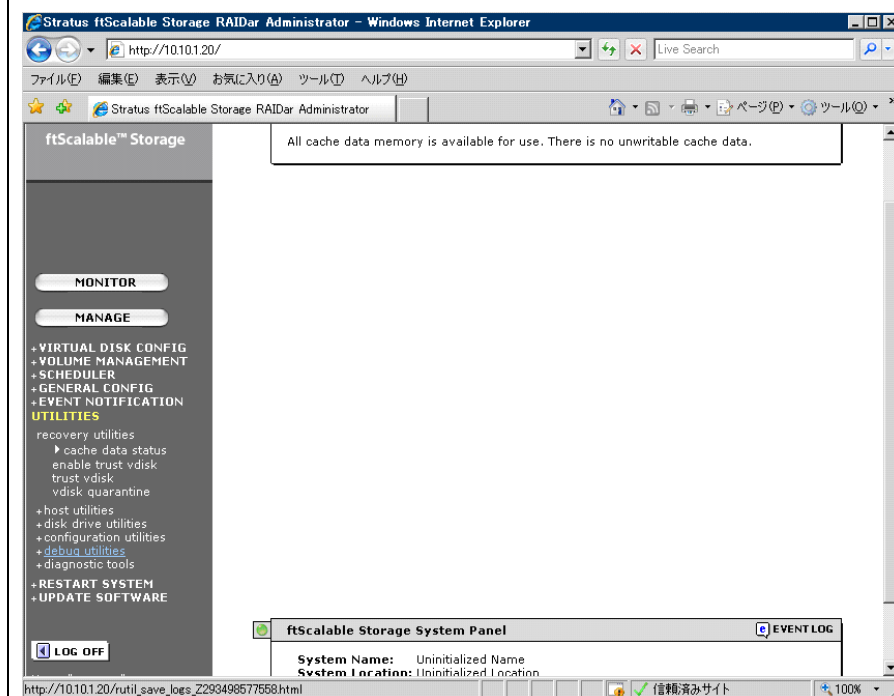
1. RAIDar にログイン
します。



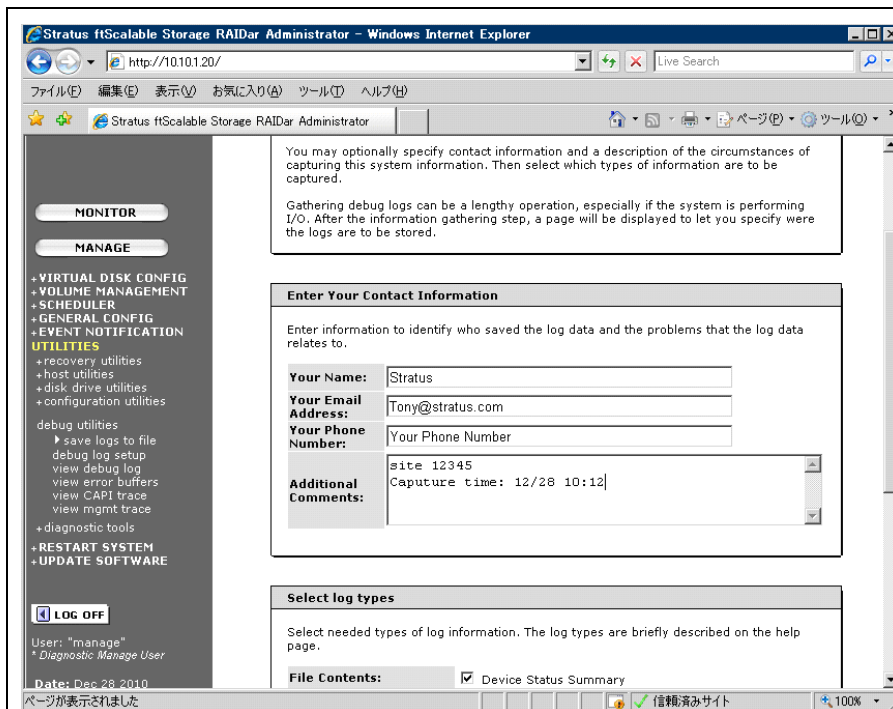
2. MANAGE メニュー
をクリックします。



3. UTILITIES メニューをクリックします。

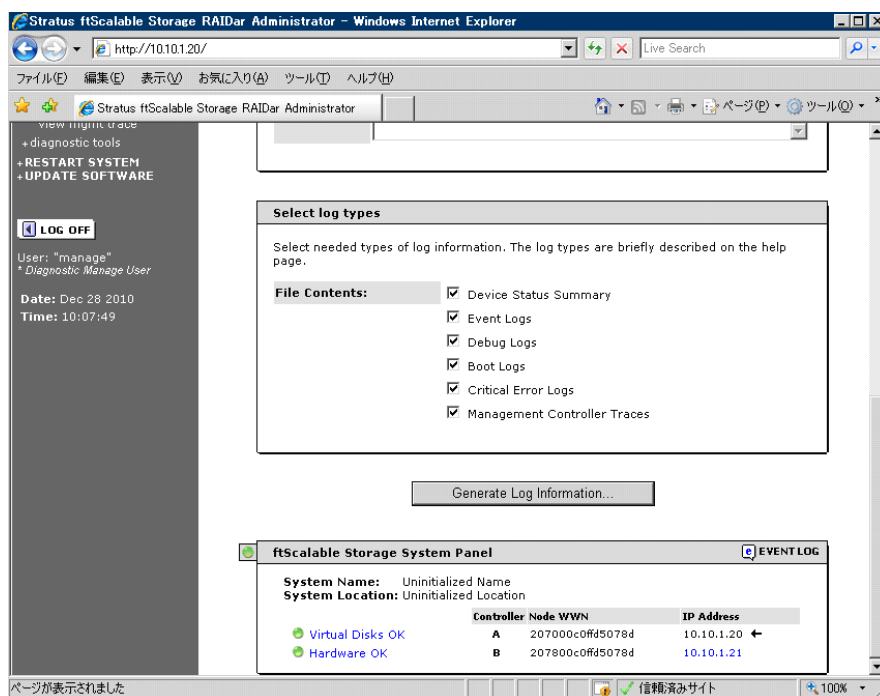


4. debug utilities メニューをクリックします。

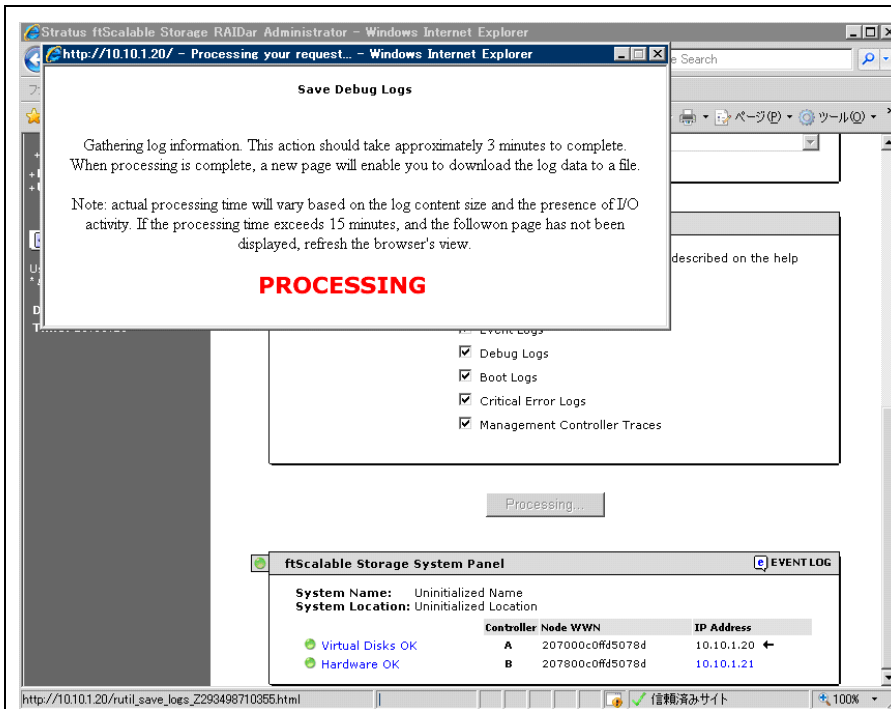


5. Enter Your Contact Informationに情報を入力します(必須ではありません)。

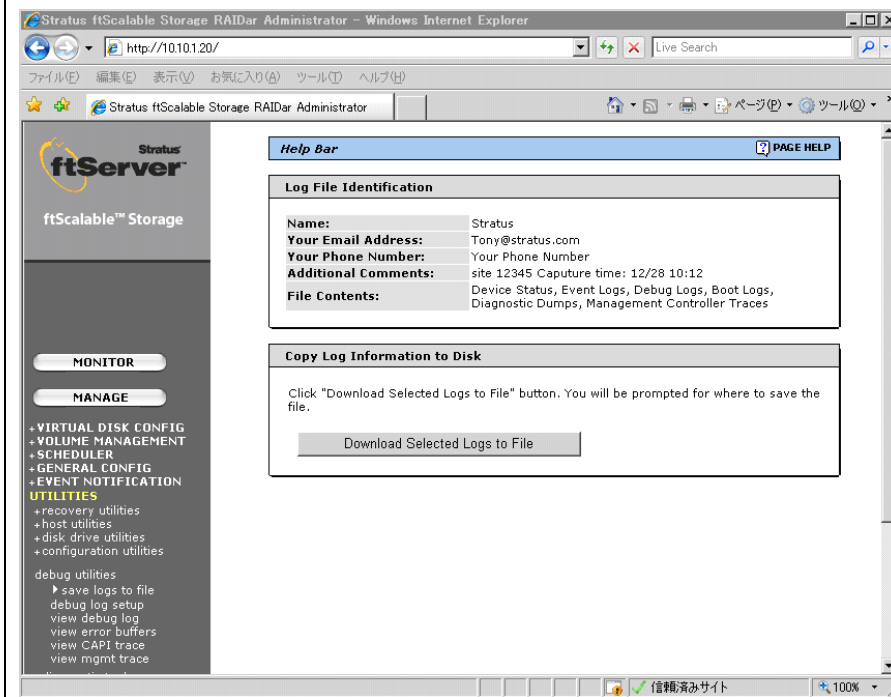
※ ftScalable Storageの時刻がServerとずれている場合があるので取得時間をAdditional Commentsに入力して下さい。



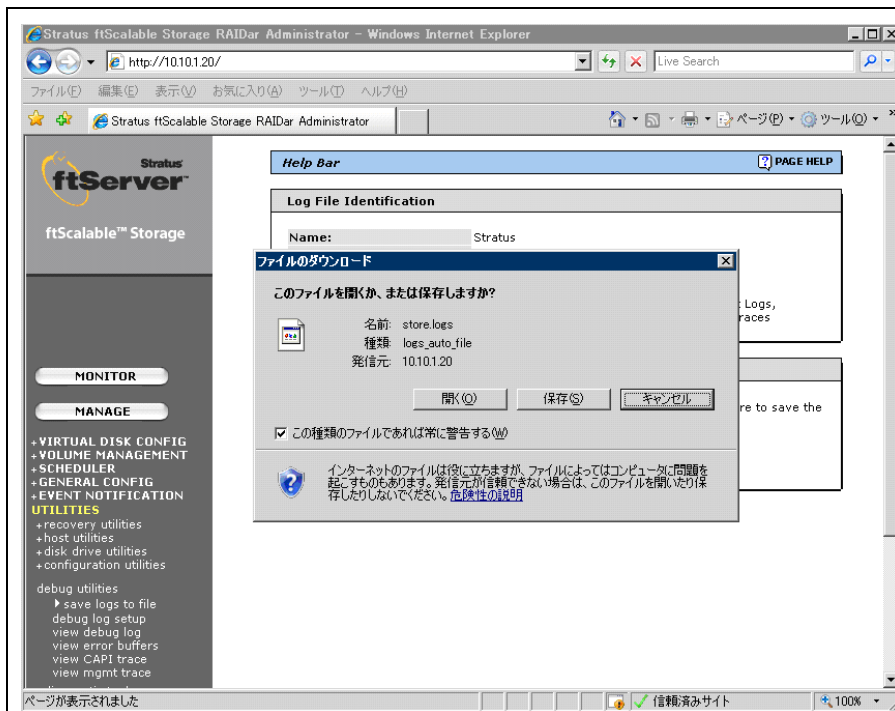
6. Select logs typesで全てのチェックボックスにチェックが入っていることを確認してGenerate Log Informationをクリックします。



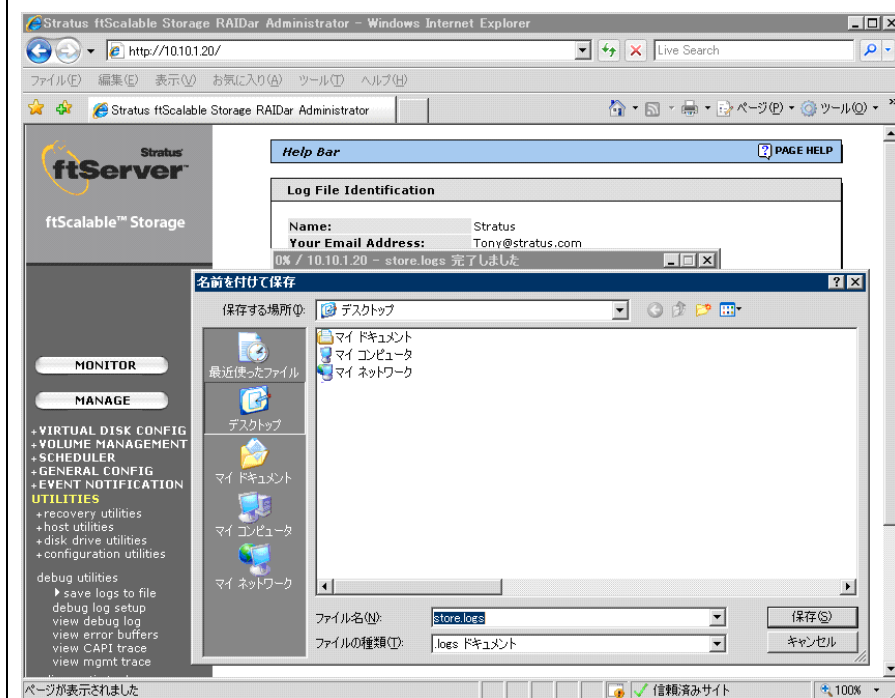
7. store log の取得が開始されます。



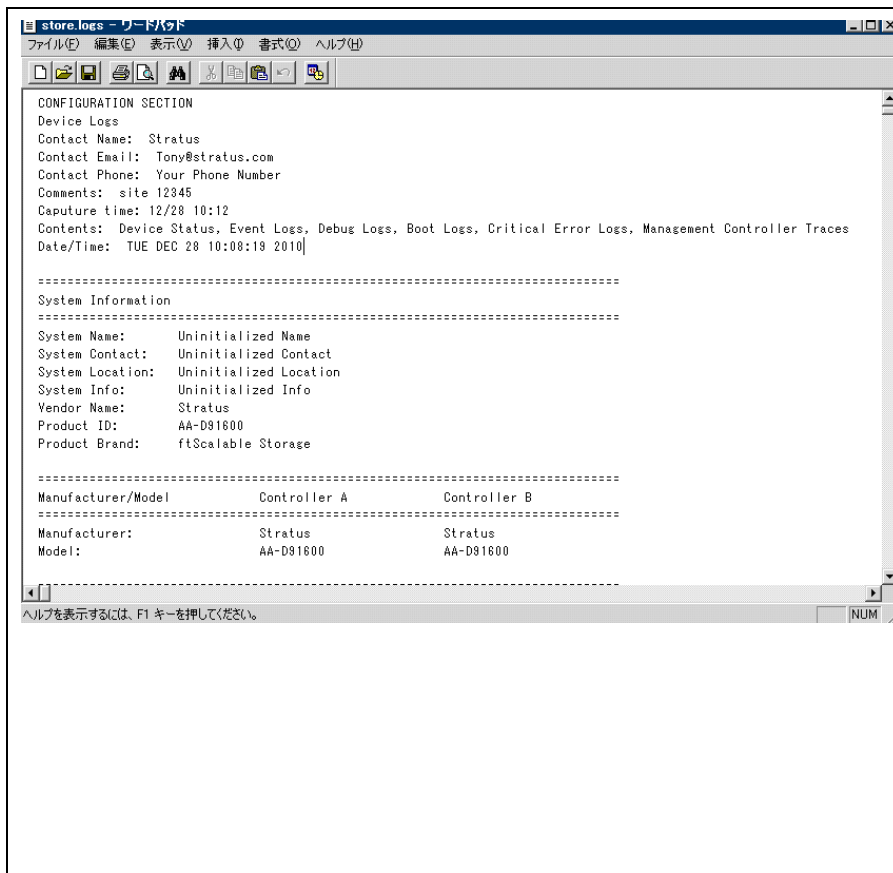
8. Download Selected Logs to File をクリックします。



9. 保存をクリックします。



10. 保存先を選択し保存をクリックします。



11. 保存したログが開けることを確認します。

2. FTP を使用したログの取得

コマンドプロンプト (Windows) もしくはターミナルソフトウェア (Unix/Linux) を開き ftScalable Storage へ ftp でログインし、"get logs *filename*" コマンドで store_log を取得します。

例) **ftp 10.10.1.20**

Connected to 10.10.1.20

214-FTP server ready

AA-D91900 RAID Controller A

System Name: Japan wombat

Location: Rokubancho

Instructions for updating firmware:

1. Log in with user name and password.
2. Type 'put <filename> flash'
where <filename> is the new firmware image to load.
3. It will take approximately 10 minutes for the new firmware to load and for the automatic restart to complete. Progress messages will be displayed in this FTP interface during that time. Wait for the progress messages to indicate that the code load has completed.

If the partner firmware upgrade (PFU) feature is enabled, allow an additional 20 minutes for the partner controller to be updated.

No messages will be displayed in the FTP interface during PFU.

WARNING! Do not power cycle or restart during the firmware update as this can result in loss of capabilities for this unit.

Note: If you attempt to load an incompatible firmware version (such as code that is intended only for an iSCSI system on an FC system) the message "*** Code Load Fail. Bad format image. ***" will be displayed and the FTP prompt will come back in just a few seconds. The code will not be loaded.

Instructions for updating JBOD EMP firmware:

1. Obtain all the IOM addresses to be loaded in the form
<channel-ID>:<EMP-number> (for example, 0:15 or 1:31).

Note: In the WBI, the IOM addresses are displayed on the

Manage > Update Software > Enclosure Firmware > Show Enclosures page.

There are 2 EMPs per enclosure.

2. Log in with user name and password.
3. Type 'put <filename> encl:<channel-ID>:<EMP-number>'
where <filename> is the new firmware image to load.
4. It typically takes several minutes for the new firmware to load. Progress messages will be displayed in this FTP interface during that time. Wait for the progress messages to indicate that the code load has completed.
WARNING! Do not power cycle or restart during the firmware update as this can result in loss of capabilities for this unit.
5. Repeat steps 3-4 for each EMP in each enclosure to be loaded.

Instructions for updating Drive firmware:

1. Obtain all the drive addresses to be loaded in the form
<channel-ID>:<DRIVE-number> (for example, 0:1 or 1:128).
Note: In the WBI, the drive addresses are displayed on the
Manage > Update Software > Disk Drive Firmware.
2. Log in with user name and password.
3. Type 'put <filename> disk:<channel-ID>:<DRIVE-number>'
where <filename> is the new firmware image to load.
4. It typically takes several minutes for the new firmware to load. Progress messages will be displayed in this FTP interface during that time. Wait for the progress messages to indicate that the code load has completed.
WARNING! Do not power cycle or restart during the firmware update as this can result in loss of capabilities for this unit.
5. Repeat steps 3-4 for each drive to update in each enclosure.

Instructions for getting debug logs:

1. Log in with user name and password.
2. Type 'get logs <filename>'
where <filename> is the file to capture the system debug logs.

Current Management Controller Firmware: W420P63 Jul 30 2010

214 Login

```
User (10.10.1.20:(none)): manage
331 Password required
Password:*****
230 User logged in
ftp>
230 User logged in
ftp> type binary
200 Type set to I, binary mode
ftp> get logs store_log
200 Port set okay
150 Opening BINARY mode data connection
226 Transfer complete
4440064 bytes received in 2.71 seconds (1598.85 Kbytes/sec)
ftp>bye
```

* ftp のポートが開いていない場合、コントローラに telnet して下記コマンドを実施しポートを開きます。

telnet 10.10.1.20

```
Login: manage
Password: *****
```

```
Stratus AA-D91900
System Name: Japan wombat
System Location: Rokubancho
Version: W420P63
```

* show protocols で ftp が有効になっているか確認します。

show protocols

```
Service and Security Protocols
```

```
-----
Web Browser Interface           (HTTP)   : Enabled
Secure Web Browser Interface   (HTTPS)  : Enabled
Command Line Interface         (Telnet) : Enabled
Secure Command Line Interface  (SSH)    : Enabled
Storage Management Initiative Specification(SMIS) : Disabled
```

File Transfer Protocol	(FTP) : Disabled
Simple Network Management Protocol	(SNMP) : Enabled
Service Interface	(Service): Enabled
Service Debug	(Debug) : Disabled
Inband SES Management	(SES) : Enabled
Inband CAPI Management	(CAPI) : Enabled

* set protocols で ftp を有効にします。

set protocols ftp enabled

Info: Setting FTP to enabled

Success: Committed Out-Of-Band protocol changes.

* show protocols で ftp が有効になっていることを確認します。

show protocols

Service and Security Protocols

```
-----
Web Browser Interface          (HTTP) : Enabled
Secure Web Browser Interface   (HTTPS) : Enabled
Command Line Interface         (Telnet) : Enabled
Secure Command Line Interface  (SSH) : Enabled
Storage Management Initiative Specification(SMIS) : Disabled
```

File Transfer Protocol	(FTP) : Enabled
Simple Network Management Protocol	(SNMP) : Enabled
Service Interface	(Service): Enabled
Service Debug	(Debug) : Disabled
Inband SES Management	(SES) : Enabled
Inband CAPI Management	(CAPI) : Enabled