

ftScalable ストレージアレイ G2 ログ取得手順

内容: ftScalable ストレージアレイ G2 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 0.1 2011/04/27

ftScalable ストレージアレイ G2 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デバッグログと呼ばれています。

デバッグログの中は下記の内容が含まれます。

- ・ cfg ディレクトリ
- ・ mem ディレクトリ
- ・ var ディレクトリ
- ・ controller ファイル
- ・ mcinfo ファイル
- ・ store_log ファイル

🚞 store				
│ ファイル(E) 編集(E) 表示(V) ;	気に入り(A) ツール(T) ヘルプ(H)			
😋 戻る - 🕥 - 🏂 🔎 検索 խ フォノレダ 🏢・				
🤅 アドレス(D) 🗁 C.¥Documents and Settings¥maraï¥デスクトップ¥store 🛛 🕑 移動				
🔛 😂 このフォルダを共有する	🔷 名前 🔺 🔰 🔰 サイズ 種類	更新日時		
	Cfg ファイル フォルダ	2010/12/06 13:11		
Zolt	— 🛅 mem ファイル フォルダ	2010/12/06 13:11		
£0112 ×	📲 🧰 var 🦳 🧰 🤁 🧰 🦉 🦉 🧰 🦉	2010/12/06 13:11		
1723 デスカトップ	🦷 🖬 controller 1 KB 7ร/ม	2010/12/06 12:32		
	- 🖬 mcinfo 111 KB ファイル	2010/12/06 12:32		
	■ store_2010_12_06_12_31_11.lo 6,473 KB LOGS ファイル	2010/12/06 12:31		
🖉 🧕 マイ コンピュータ				
🧕 🧐 マイ ネットワーク		>		

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デバッグログを取 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、192.168.0.2 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。

デバッグログ取得方法

1. RAIDar からの取得

2192.168.0.2 [A] (Tazmo #1) - Windows Internet Explorer		1. RAIDar にログインします。
Esconder Activity 192.168.0.2/ Esconder Esconder	S * S Bing	
20633.68.70 [A] (Tazmo #1)	🏠 • 🔂 - 🖃 📾 • ページ(D) • セーフティ(S) • ツール(D) • 📦 •	
	Stratus Technologies Stratus [®] ftScalable ^{III} Storage G2 - RAIDar Utility	
	User name: "sanage Password Gener Language: user setting	
[] 192.168.0.2 [A] (Tazmo #1) - Windows Internet Explo	rerX	2 Table から Save Lare 右躍中
→		2. TOOIS から Save Logs を迭折
😪 Favorites 🛛 🍰 Ø Suggested Sites 🔹 🙋 Web Slice Galle	ry 👻	します。
192.168.0.2 [A] (Tazmo #1)	🏠 + 🗟 - 🖃 🚔 - Page + Safety + Tools + 🕢 -	
(stratus [®] ftScalable [™] Stor	age G2 - RAIDar Utility	
System Status		
System Time 2010-12-08 11:04:16	Tazmo #1 (AA-D95000)	
System Events 🔀 0 🔻 16 ႔ 18 🕦 66	View View Provisioning Configuration Tools Wizards Help Indate Firmware	
Configuration View	System Overview	
	Select an entry from the table to see the det. Reset Host Port	
Tazmo #1 (AA-D95000)	Rescan Disk Channels System Overview Clear Disk Metadata	
Vdisks	Health Component Count Car Shut Down or Restart Controller	
Hosts	C O K System 4.3	
Physical	C OK Dide 18 43TB	
Enclosure 0	C O DK Vdise 1 219.868	
	C Volumes 2 13.06B	
	C Snap Pools 0 0.0KB	
	C Snapshots 0	
Done	🔰 🕅 🎲 🗸 Trusted sites Protected Mode: Off	



	 デバッグログが zip 形式で 取得されるので Save で保存し ます。
System Status Tazmo #1 (AA-D95000) System Time 2010-12-08 13 13 26 System Versit 2010 Configuration View Do you want to open or save this file? Type: Compressed (2pped) Folder, 2.42MB From 192.168.0.2 Upen Save Physical While files from the Internet can be useful, some files can potentially ham you could be internet and but the source, do not open or save this file. What's the file? Source While files from the Internet can be useful, some files can potentially ham you councert. Hyou do not thut the source, do not open or save this file. What's the file? Save Loggs	

2. ftp での取得方法

ftpを実施して"get logs *filename.zip*"コマンドで取得する事が可能です。ftp が接続できない場合は 後述の ftp の有効化を参照して下さい。

例:

ftp 192.168.0.2

Connected to 192.168.0.2. 220-Welcome to Pure-FTPd. 220-You are user number 1 of 5 allowed. 220-Local time is now 14:18. Server port: 21. 220-This is a private system - No anonymous login 220 You will be disconnected after 15 minutes of inactivity. User (192.168.0.2:(none)): manage 331 User manage OK. Password required Password:***** 230-OK. Current restricted directory is / 230-Instructions for updating firmware in controller modules: 230 -1. Type 'put <filename> flash' where <filename> is the new firmware image to load. 230-2. It will take approximately 10 minutes for the new firmware to load and 230for the automatic restart to complete. Progress messages will be 230 displayed in this FTP interface during that time. Wait for the progress 230messages to indicate that the code load has completed. 230-3. If the partner firmware upgrade (PFU) feature is enabled, allow 230an additional 20 minutes for the partner controller to be updated. No messages will be displayed in the FTP interface during PFU. 230-230-If PFU is NOT enabled, log into the other controller and repeat steps 1-2. 230-4. WARNING! Do not power cycle or restart during the firmware update 230as this can result in loss of capabilities for this unit. 230-5. If you attempt to load an incompatible firmware version (such as code 230that is intended only for an iSCSI system on an FC system) the message 230-"*** Code Load Fail. Bad format image. ***" will be displayed and the FTP 230prompt will come back in just a few seconds. The code will not be loaded. 230 -230-Instructions for updating firmware in expansion modules: 230-1. Obtain the address of each enclosure management processor (EMP) in the form 230-<EMP-channel-ID>:<EMP-target-ID> (for example, 0:63 and 1:63) 230and obtain the firmware revision of each EMP. 230-Determine which EMPs need to be updated based on the revision. 230-Note: In the WBI, the EMP addresses are displayed by clicking on each 230enclosure in the Configuration View. The needed data is displayed in the fields labeled 'EMP A Bus ID', 'EMP B Bus ID', 'EMP A TargetID', 230-230-'EMP B Target ID', 'EMP A Revision', and 'EMP B Revision'. (The terms 230-'bus' and 'channel' are equivalent.) 230-Note: In the CLI, enter 'show enclosures'. The needed data is displayed in the columns labeled 'EMP A CH:ID Rev' and 'EMP B CH:ID Rev'. 230 -230-2. Log in via FTP with user name and password. 230-3. Type 'put <filename> encl:<EMP-channel-ID>:<EMP-target-ID>' 230where <filename> is the new firmware image to load. 230-4. It typically takes several minutes for the new firmware to load. Progress 230messages will be displayed in this FTP interface during that time. Wait

230- for the progress messages to indicate that the code load has completed.

230-WARNING! Do not power cycle or restart during the firmware update 230as this can result in loss of capabilities for this unit. 230-5. Repeat steps 3-4 for each EMP to update in each enclosure. 230-230-Instructions for updating disk firmware: 230-1. Obtain the address of each disk to be loaded in the form 230-<enclosure-ID>:<slot-number> (for example, 0:1 and 1:9) 230and obtain the firmware revision of each of these disks. 230-Determine which disks need to be updated based on the revision. 230-Note: In the WBI, the disk addresses are displayed by clicking on each 230enclosure in the Configuration View and then selecting the desired 230disk. The needed data is displayed in the fields labeled 'EnclosureID', 230-'Slot', and 'Revision'. 230-Note: In the CLI, enter 'show disks'. The needed data is displayed 230in the columns labeled 'Location' and 'Revision'. 230-2. Log in via FTP with user name and password. 230-3. Type 'put <filename> disk:<enclosure-ID>:<slot-number>' 230where <filename> is the new firmware image to load. 230-4. It typically takes several minutes for the new firmware to load. Progress 230messages will be displayed in this FTP interface during that time. Wait 230for the progress messages to indicate that the code load has completed. 230-WARNING! Do not power cycle or restart during the firmware update 230as this can result in loss of capabilities for this unit. 230-5. Repeat steps 3-4 for each disk to update in each enclosure. 230-230-Instructions for getting debug logs: 230-1. Log in with a user name and password. 2. Type 'get logs <filename.zip>' 230-230where <filename.zip> is the file to capture the system debug logs. 230-Note the debug logs are in a compressed archive format and will need to be uncompressed before viewing. 230-230 -230-Instructions for loading a license file: 230-1. Log in with a user name and password. 230-2. Type 'put <certificate.txt> license' 230where <certificate.txt> is the name of the license file generated 230for your specific system. 230 ftp> get logs store1223.zip 200 PORT command successful 119-Starting operation: STATUS: getting storage controller logs ... adding: store_2011_01_27__14_18_57.logsInitializing Obtaining Configuration Data from Storage Controller Obtaining Configuration Data from Storage Controller Obtaining Debug Logs from Storage Controller (deflated 90%)

Obtaining Debug Logs from Storage Controller Obtained Storage Controller Logs Success: Command completed successfully.

Exiting. done getting the storage controller logs STATUS: getting the management controller logs ... adding: controller (stored 0%) adding: mcinfo (deflated 89%) adding: cfg/log/appsv_019580_000002.log (deflated 93%) adding: cfg/log/appsv_019580_000003.log (deflated 93%) . adding: cfg/log/active/web_019579_000000.log (deflated 90%) adding: cfg/pfu/pfu.log (deflated 88%) adding: cfg/cpld.log (deflated 63%) adding: var/log/app.out (deflated 60%) adding: var/log/boot.out (deflated 62%) adding: var/log/messages (deflated 91%) adding: var/log/snmpd.log (deflated 39%) done getting the management controller logs RETURN_CODE: 12 119 Operation Complete. 150-Connecting to port 1756 150 1779.9 kbytes to download ftp: 1822638 bytes received in 0.23Seconds 7789.05Kbytes/sec. ftp>

<u>ftp の有効化</u>

下記のようにftpでエラーとなり接続できない場合は、telnetを実施してftpを有効化する必要があります。

C:¥Documents and Settings¥administrator>ftp 192.168.0.2 > ftp: connect :エラー番号が不明です

telnet を実施し"set protocols"コマンドで ftp を有効化します。

例:

telnet 192.168.0.2 192.168.0.2 login: manage Password:*******

Stratus ftScalable Storage AA-D95000 System Name: Tazmo #1 System Location:Uninitialized Location Version:L210R015

下記コマンドで現在の設定を確認 # 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 (SMI-S): Enabled **File Transfer Protocol (FTP): Disabled** Simple Network Management Protocol (SNMP): Enabled Service Debug (Debug): Enabled In-band SES Management (SES): Enabled

Success: Command completed successfully.

下記コマンドで ftp の有効化 # **set protocols ftp enabled** Success: Command completed successfully.

ftp が有効になったことを確認 # <mark>show protocols</mark> 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 (SMI-S): Enabled File Transfer Protocol (FTP): Enabled Simple Network Management Protocol (SNMP): Enabled Service Debug (Debug): Enabled In-band SES Management (SES): Enabled

Success: Command completed successfully.

以上