



STORAGE**FUSION**

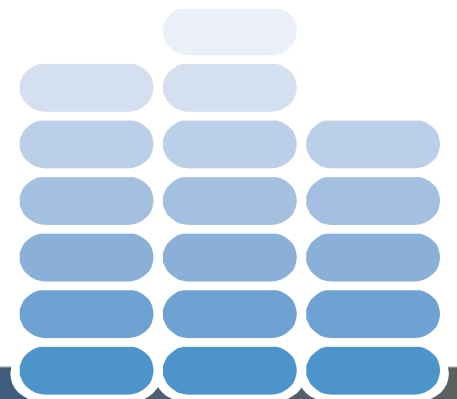
**Storage Resource Analysis
Enterprise Edition**

Data Collection Guide

July 2011

Tel: +44 (0)1707 387100
Email: info@StorageFusion.com
Web: www.StorageFusion.com

Storage Fusion Limited
Suite 104
29 Broadwater Road
Welwyn Garden City
Herts AL7 3BQ



NOTICE

Storage Fusion Limited provides this publication "as is" without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability or fitness for any particular purpose. Limited will not be liable (i) to you for any incidental, consequential, or indirect damages (including damages for loss of business profits, business interruption, loss of business information, and the like) arising out of the use of or inability to use this product even if Limited or any authorised Limited representative has been advised of the possibility of such damages, or (ii) for any claim by any other party. Further, Storage Fusion Limited reserves the right to make changes or improvements to the product described in this guide and to this publication without obligation of Storage Fusion Limited to notify any person of such revision or changes.

Trademarks

All trademarks or registered trademarks are the property of the respective manufacturers of the products associated with them.

Copyright

Copyright ©2008-2011 Storage Fusion Limited

All rights reserved. No part of this publication may be reproduced, translated or distributed without the prior written permission of Storage Fusion Limited.

Edition: July 2011

Contents

INTRODUCTION.....	4
OVERVIEW	4
SUPPORTED DEVICES	5
SUPPORTED FABRIC DEVICES.....	6
SUPPORTED VENDOR TOOLS	7
DATA COLLECTION	8
DISCOVERY	8
STORAGE ARRAY DATA COLLECTION.....	9
<i>EMC Symmetrix</i>	9
<i>Hitachi USP and AMS</i>	12
<i>HP EVA</i>	15
<i>HP XP</i>	17
<i>IBM Modular</i>	20
<i>IBM Enterprise</i>	22
<i>IBM XIV</i>	25
<i>IBM ESS</i>	27
<i>IBM SVC</i>	29
<i>EMC CLARiiON</i>	34
<i>RecoverPoint/SafeGuard</i>	38
<i>NetApp</i>	41
SAN FABRIC	46
<i>Brocade</i>	46
<i>Cisco</i>	50
VALIDATING THE DATA COLLECTION.....	54
ZIP FILES.....	54
ADDITIONAL DATA COLLECTED	55
WORLD WIDE NAME TO HOSTNAME MAPPING	55
DATA COLLECTION LOG FILES.....	56
UPLOADING DATA	56
AUTOMATING THE DATA COLLECTION PROCESS.....	56
WINDOWS	56
<i>Zip files</i>	57
<i>Uploading Data</i>	57
<i>Scheduling the script to automatically run</i>	58
UNIX	58
<i>Zip files</i>	58
<i>Uploading Data</i>	59
<i>Scheduling the script to automatically run</i>	60
SUPPORTED FEATURE LIST BY VENDOR	61

Introduction

Overview

This guide outlines the steps required to perform the configuration data gatherings, and also any prerequisites needed for the various data collections.

Refer to the table of contents to select the appropriate section for specific data collection steps required on your hardware devices.

Prior to using Storage Resource Analysis Enterprise Edition it is necessary for you to provide configuration data from each storage device or switch that you would like analysed.

To simplify the data collection process Storage Fusion can provide a script that will automatically execute the appropriate commands and create a number of data files. For some storage devices it isn't possible or practical to script the data collection and instead appropriate instructions are included within this guide.

Once you have collected the configuration data you can upload it to the web portal using a web browser.

Supported Devices

The following storage devices are supported by SRA Enterprise Edition.

Vendor	Family	Model	Supported	Collection Script Windows	Collection Script Unix
EMC	CLARiiON	AX-Series	Y	N	N
		CX-Series	Y	N	N
		CX-3 Series	Y	N	N
		CX-4 Series	Y	N	N
	Symmetrix	DMX Series	Y	Y	Y
		8000 Series	Y	Y	Y
		V-Max	Y	Y	Y
	RecoverPoint		Y	Y	N
HDS	Adaptable Modular Storage	AMS series	Y	Y	Y
	Thunder	9500 Series	Y	Y	Y
	Lightning	9900 Series	Y	Y	Y
	Universal Storage Platform	USP Series	Y	Y	Y
	Universal Storage Platform	USP V Series	Y	Y	Y
HP	XP	XP Series	Y	Y	Y
	EVA	EVA Series	Y	Y	N
IBM	Entry level and midrange	DS3000, 4000 and 5000	Y	Y	N
		XIV	Y	Y	N
	Enterprise disk storage	DS6000/8000	Y	Y	Y
	Enterprise Storage Server (ESS)	F10/F20/800	Y	Y	Y
	SAN Virtual Controller		Y	Y	Y
NetApp	FAS	200 Series	Y	Y	Y
		800 Series	Y	Y	Y
		900 Series	Y	Y	Y
		2000 Series	Y	Y	Y
		3000 Series	Y	Y	Y
		3100 Series	Y	Y	Y
		6000 Series	Y	Y	Y
R200	Y	Y	Y		

Table 1: Supported Devices

Supported Fabric Devices

SRA Enterprise Edition also supports the analysis of the SAN fabric for the following switches:

- Brocade SilkWorm series (switches and directors)
- Brocade DCX series
- Brocade DS220B, 200E, 300, 3250, 3850, 5100, 5300
- Brocade 5410, 5480
- Brocade Application Platform Model 7429
- Cisco MDS Series
- Cisco Fabric Switch for HP c-Class BladeSystem
- Cisco Fabric Switch for IBM BladeCenter

Supported Vendor Tools

Vendor	Family	Vendor Tool	Windows/Unix
EMC	CLARion	SP Collect	N/A
	Symmetrix/V-Max	Symmetrix Solutions Enabler SYMCLI	Windows/Unix
	RecoverPoint/Safeguard	Plink.exe and RecoverPoint CLI	Windows
HDS	AMS/Thunder	HiCommand Device Manager	Windows/Unix
	Lightening/USP	HiCommand Device Manager	Windows/Unix
HP	EVA	HP Storage Scripting Utility	Windows
	XP	Command View Advanced Edition	Windows/Unix
IBM	DS Modular	Storage Manager CLI(SMcli)	Windows
	DS Enterprise	Storage Manager CLI (DScli)	Windows/Unix
	ESS	esscli CLI	Windows/Unix
	SVC	svconfig	Windows/Unix
	XIV	XIV cli (xcli)	Windows
	V-Series	Plink.exe (Windows) / ssh (Unix)	Windows/Unix
NETAPP	FAS	Plink.exe (Windows) / ssh (Unix)	Windows/Unix

Table 3: Vendor Tools

Data Collection

Discovery

In most cases the SRA_Collect script will automatically discover the storages arrays controlled by the management station. Should you need to only collect data from specific arrays then you can create an include file.

Instructions:

1. Create a txt file with a list of array serial numbers or names* that you would like to collect configuration data from. Each serial number or name must be on a separate line.

Example Symmetrix file:

```
000292830183
000394740284
000384748203
000403824048
```

* Please review the below table to determine if you should specify a serial number or name.

2. Save the file in the same directory as the SRA_Collect script with the appropriate file name as shown in the below table. For example, symmetrix would be named symmetrix_include.txt.

Vendor	Filename	Serial Number or Name?
EMC Symmetrix	symmetrix_include.txt	Serial Number
Hitachi	hitachi_include.txt	Serial Number
HP XP	hpxp_include.txt	Serial Number
HP EVA	hpeva_include.txt	Name
IBM Mod	ibmmod_include.txt	Name

When the SRA_Collect script is executed configuration data will only be collected from the specified arrays.

Storage Array Data Collection.

EMC Symmetrix

Prerequisites

Management System requirements

Operating System: Windows 2000, Windows 2003, Windows 2008, Windows XP or Windows Vista, Solaris, AIX, HP-UX and Suse/RedHat Linux.

Vendor software: Symmetrix Solutions Enabler SYMCLI

User privileges

It is assumed that the user has an operational knowledge of the Operating System in use.

Access to the sra_collect file.

<i>sra_collect.cmd</i>	Script file for Windows that collects the configuration data.
<i>sra_collect</i>	Script file for Unix that collects the configuration data.

Set SYMCLI Environment Variables

The SYMCLI commands must be available via the PATH environment variable.

It is recommended that you perform a symcfg discover prior to running the sra_collect script. This will discover all Symmetrix arrays connected to the host and build or rebuild the Symmetrix configuration database file from information gathered.

IMPORTANT: The sra_collect script no longer executes the symcfg sync command. It is essential that this is run manually and allowed to complete prior to running the collection script.

If you are using replication (SRDF) then the collection script will need to be run locally on a management server connected to both arrays i.e. a management server that has a gatekeeper or LUN presented directly.

Please refer to the Solutions Enabler Symmetrix CLI Command Reference manual for further information.

If you wish to use an alternative database to the default set the variable SYMCLI_DB_FILE before running the sra_collect script e.g. SET SYMCLI_DB_FILE="C:\Path to alternative .bin file"

The SRA collection script will attempt to run all the collection commands against every local array discovered by the 'symcfg list' command. If you would like to exclude an array from the collection please create a file named ignore.txt in the

folder where you are running the script from. For example: c:\sra\ignore.txt. On each line include the serial number of the array that you would like to exclude and save the file. Further details on include files can be found in the Discovery section on page 7.

Collecting the configuration data

Windows

Create a new directory, for example C:\SRA.

Copy the *sra_collect.cmd* file into the directory.

Executing the Collection Script

Start a cmd shell.

Change directory into the directory where you saved the *sra_collect.cmd* file.

Enter the following command:

```
sra_collect symmetrix <directory> </s> </z> </u>
```

<directory>	Where you saved the <i>sra_collect.cmd</i> file.
</s>	Suppress any output messages appearing on screen.
</z>	the data files will be zipped using the 7zip command line utility.
</u>	the zipped file will be uploaded to the SRA Portal using the Windows WebClient Service.

Important: when using the upload switch you must also specify the zip switch as only zip files can be uploaded to the SRA Portal.

Example: `sra_collect symmetrix c:\sra`

Unix

Create a new directory, for example /opt/sra

Copy the *sra_collect* file into the /opt/sra directory.

Ensure that the execute attribute is set. For example, `chmod 755 sra_collect`.

Executing the Collection Script

Start a shell.

Change directory into the directory where you saved the *sra_collect* file.

Enter the following command:

```
sra_collect symmetrix <directory> </s> </z> </u>
```

<directory> Where you saved the sra_collect file.
</s> Suppress any output messages appearing on screen.
</z> the data files will be zipped using the zip command line utility.
</u> the zipped file will be uploaded to the SRA Portal using the cadaver command line utility.

Important: when using the upload switch you must also specify the zip switch as only zip files can be uploaded to the SRA Portal

Example: `sra_collect symmetrix /opt/sra`

Hitachi USP and AMS

Prerequisites

Management System requirements

Operating System: Windows 2000, Windows 2003, Windows 2008, Windows XP or Windows Vista, Solaris, AIX, HP-UX and Suse/RedHat Linux.

Vendor software: HiCommand Device Manager Software

User privileges

It is assumed that the user has an operational knowledge of the Operating System in use.

Access to the sra_collect file.

<i>sra_collect.cmd</i>	Script file that collects the configuration data.
<i>sra_collect</i>	Script file for Unix that collects the configuration data.

Set HiCommand Environment Variables

The HiCommandCLI.bat or HiCommandCLI.sh file must be available via the PATH environment variable.

To ensure successful CLI execution, the environment variable HDVM_CLI_MEM_SIZE must be set to an appropriate value.

Please refer the Hitachi Device Manager Software Command Line Interface (CLI) User's Guide for further information.

Verify your Hitachi Arrays Meet these Requirements

All storage subsystems must be configured for Device Manager operations.

Please refer to the Device Manager online Help for detailed information on storage subsystem requirements.

HiCommand Operations required before Data Collection

It is recommended that you perform a refresh of the configuration information of all storage subsystems that are managed by the Device Manager by performing a rediscovery operation on each storage subsystem that is managed by the Device Manager.

This can be achieved by using the HiCommandCLI RefreshStorageArray command. For storage subsystems that are managed by Device Manager, configuration information that was created or modified from the Remote Console, Storage Navigator or CCI is added to or updated in the Device Manager server database each time the RefreshStorageArrays command is executed.

Please refer to the Hitachi Device Manager Software Command Line Interface (CLI) User's Guide for detailed information.

It is also necessary to update all host and logical group information with their relevant world wide names. This can be achieved by running HiCommandCLI HostScan against the individual arrays or the complete storage estate. Again, refer to the Hitachi Device Manager Software Command Line Interface (CLI) User's Guide for detailed information.
Nb. HostScan is only available on Device manager V6 and later

Collecting the configuration data

Windows

Create a new directory, for example C:\SRA.

Copy the *sra_collect.cmd* file into the directory.

Executing the Collection Script

Note: If the script is run without specifying a username and password the HiCommandCLI will attempt to use the credentials stored in the HiCommand.properties file. If this file doesn't contain a valid username and password then they must be passed as arguments to the script. For example:
sra_collect hitachi c:\sra server-URL username password.

Start a cmd shell.

Change directory into the directory where you saved the *sra_collect.cmd* file.

Enter the following command:

```
sra_collect hitachi <directory> <serverport> <username> <password> </s> </z> </u>
```

<directory>	Where you saved the <i>sra_collect.cmd</i> file.
<serverport>	The IP address or hostname including the port of the Device Manager server. Note that if running locally you should specify http://localhost:2001/service
<username>	
<password>	
</s>	Suppress any output messages appearing on screen.
</z>	the data files will be zipped using the 7zip command line utility.
</u>	the zipped file will be uploaded to the SRA Portal using the Windows WebClient Service.

Important: when using the upload switch you must also specify the zip switch as only zip files can be uploaded to the SRA Portal.

Example:

```
sra_collect hitachi c:\SRA http://localhost:2001/service
username password
```

Unix

Create a new directory, for example /opt/sra.

Copy the sra_collect file into the /opt/sra directory.

Ensure that the execute attribute is set. For example, chmod 755 sra_collect.

Executing the Collection Script

Note: If the script is run without specifying a username and password, the HiCommandCLI will attempt to use the credentials stored in the HiCommand.properties file. If this file does not contain a valid username and password then they must be passed as arguments to the script. For example: sra_collect hitachi /opt/sra server-URL username password.

Start a cmd shell.

Change directory into the directory where you saved the *sra_collect.cmd* file.
Enter the following command:

```
sra_collect hitachi <directory> <serverport> <username> <password></s> </z> </u>
```

<directory>	Where you saved the sra_collect.cmd file.
<serverport>	The IP address or hostname including the port of the Device Manager server. Note that if running locally you should specify http://localhost:2001
<username>	
<password>	
</s>	Suppress any output messages appearing on screen.
</z>	the data files will be zipped using the zip command line utility.
</u>	the zipped file will be uploaded to the SRA Portal using the cadaver command line utility.

Important: when using the upload switch you must also specify the zip switch as only zip files can be uploaded to the SRA Portal.

Example:

```
sra_collect hitachi /opt/sra http://localhost:2001/service
```

HP EVA

Prerequisites

Management System requirements

System Operating System: Windows 2000, Windows 2003, Windows 2008, Windows XP or Windows Vista.

Vendor software: Storage Scripting Utility

User privileges

It is assumed that the user has an operational knowledge of the Operating System in use.

Access to the `sra_collect.cmd` file.

`sra_collect.cmd` Script file that collects the configuration data.

Set Environment Variables

The Storage System Scripting Utility (`ssu.exe`) must be available via the PATH environment variable.

Collecting the configuration data

Windows

Create a new directory, for example `C:\SRA`.

Copy the `sra_collect.cmd` file into the directory.

Executing the Collection Script

Start a cmd shell.

Change directory into the directory where you saved the `sra_collect.cmd` file.

Enter the following command:

```
sra_collect hpeva <directory> <username> <password> </s> </z> </u>
```

<directory>	Where you saved the <code>sra_collect.cmd</code> file.
<username>	ssu username
<password>	ssu password
</s>	Suppress any output messages appearing on screen.
</z>	the data files will be zipped using the 7zip command line utility.
</u>	the zipped file will be uploaded to the SRA Portal using the Windows WebClient Service.

Important: when using the upload switch you must also specify the zip switch as only zip files can be uploaded to the SRA Portal.

Example:

```
sra_collect hpeva c:\SRA username password
```

HP XP

Prerequisites

Management System requirements

Operating System: Windows 2000, Windows 2003, Windows 2008, Windows XP, Windows Vista, Solaris, AIX, HP-UX and Suse/RedHat Linux.

Vendor software: Command View Advanced Edition

User privileges

It is assumed that the user has an operational knowledge of the Operating System in use.

Access to the `sra_collect.cmd` file.

sra_collect.cmd Script file that collects the configuration data.

Set Command View AE Environment Variables

The `hdvmdi` command must be available via the `PATH` environment variable. To ensure successful CLI execution, the environment variable `HDVM_CLI_MEM_SIZE` must be set to an appropriate value.

Please refer the Command View AE Command Line Interface (CLI) User's Guide for further information.

Verify your HP XP Array Meets these Requirements

All storage subsystems must be configured for Command View operations.

Please refer to the Command View online Help for detailed information on storage subsystem requirements.

Command View operations required before data collection

It is recommended that you perform a refresh of the configuration information of all storage subsystems that are managed by Command View by performing a rediscovery operation on each storage subsystem that is managed by the Command View.

This can be achieved by using the `hdvmCLI RefreshStorageArray` command. For storage subsystems that are managed by Device Manager, configuration information that was created or modified from the Remote Console, Storage Navigator or CCI is added to or updated in the Device Manager server database each time the `RefreshStorageArrays` command is executed.

Please refer to the Command View Advanced edition Command Line Interface (CLI) User's Guide for detailed information.

It is also necessary to update all host and logical group information with their relevant world wide names. This can be achieved by running hdvmCLI HostScan against the individual arrays or the complete storage estate.

Again, refer to the Command View Advanced edition Command Line Interface (CLI) User's Guide for detailed information.

nb. HostScan is only available on Command View AE V6 and later

Collecting the configuration data

Windows

Create a new directory, for example C:\SRA.

Copy the *sra_collect.cmd* file into the directory.

Executing the Collection Script

Note: If the script is run without specifying a username and password hdvmCLI will attempt to use the credentials stored in the hdvmCLI.properties file. If this file doesn't contain a valid username and password then they must be passed as arguments to the script. For example: `sra_collect hpxp c:\sra server-URL username password`.

Start a cmd shell.

Change directory into the directory where you saved the *sra_collect.cmd* file.

Enter the following command:

```
sra_collect hpxp <directory> <serverport> <username> <password> </s> </z> </u>
```

<directory> Where you saved the *sra_collect.cmd* file

<serverport> The IP Address or hostname including the port of the Device Manager server.

Note that if running locally then you should specify as follows:
<http://localhost:2001/service>

<username>

<password>

</s> Suppress any output messages appearing on screen.

</z> the data files will be zipped using the 7zip command line utility.

</u> the zipped file will be uploaded to the SRA Portal using the Windows WebClient Service.

Important: when using the upload switch you must also specify the zip switch as only zip files can be uploaded to the SRA Portal.

Example:

```
sra_collect hpxp c:\SRA http://localhost:2001/service
username password
```

Unix

Create a new directory, for example /opt/sra

Copy the *sra_collect* file into the directory.

Executing the Collection Script

Note: If the script is run without specifying a username and password hdmCLI will attempt to use the credentials stored in the hdmCLI.properties file. If this file doesn't contain a valid username and password then they must be passed as arguments to the script. For example: *sra_collect hpxp /opt/sra server-URL username password*.

Start a shell.

Change directory into the directory where you saved the *sra_collect* file.

Enter the following command:

```
sra_collect hpxp <directory> <serverport> username password
```

<directory> Where you saved the *sra_collect* file.

<serverport> The IP Address or hostname including the port of the Device Manager server.

Note that if running locally then you should specify as follows:
<http://localhost:2001/service>

<username>

<password>

</s>

Suppress any output messages appearing on screen.

</z>

the data files will be zipped using the zip command line utility.

</u>

the zipped file will be uploaded to the SRA Portal using the cadaver command line utility.

Important: when using the upload switch you must also specify the zip switch as only zip files can be uploaded to the SRA Portal.

Example:

```
sra_collect hpxp /opt/sra http://localhost:2001/service
username password
```

IBM Modular

Prerequisites

Management System requirements

Operating System: Windows 2000, Windows 2003, Windows 2008, Windows XP or Windows Vista.

Vendor software: Storage Manager CLI(SMcli)

User privileges

It is assumed that the user has an operational knowledge of the Operating System in use.

Access to the `sra_collect.cmd` file.

`sra_collect.cmd` Script file that collects the configuration data.

Set Environment Variables

The Storage Manager CLI (SMcli) should be available via the PATH environment variable.

All storage subsystems must have been previously discovered by the Storage Manager software, this can be checked using the command: `SMcli -d`

If the above returns a list of storage subsystems then collection can proceed. If it doesn't then execute the following command to automatically discover any storage subsystems before proceeding with the collection: `SMcli -A`

The script will run a collection for every storage subsystem discovered. If for any reason you do not wish to collect for a particular array then remove it from the CLI with the following command: `SMcli -X -n ARRAY_NAME`.

Collecting the configuration data

Windows

Create a new directory, for example `C:\SRA`.

Copy the `sra_collect.cmd` file into the directory.

Executing the Collection Script

Start a cmd shell.

Change directory into the directory where you saved the `sra_collect.cmd` file.

Enter the following command: `sra_collect ibm_mod <directory> </s> </z> </u>`

<directory> Where you saved the sra_collect.cmd file.
</s> Suppress any output messages appearing on screen.
</z> the data files will be zipped using the 7zip command line utility.
</u> the zipped file will be uploaded to the SRA Portal using the Windows WebClient Service.

Important: when using the upload switch you must also specify the zip switch as only zip files can be uploaded to the SRA Portal.

Example:

```
sra_collect ibm_mod c:\sra
```

IMPORTANT: When collecting data from arrays that contain spaces in their names an include file must be used. The file must contain a list of all the arrays to be collected from, one array per line. Further details on include files can be found in the Discovery section on page 8.

IBM Enterprise

Prerequisites

Management System requirements

Operating System: Windows 2000, Windows 2003, Windows 2008, Windows XP or Windows Vista.

Vendor software: Storage Manager CLI (DScli)

User privileges

It is assumed that the user has an operational knowledge of the Operating System in use.

Access to the `sra_collect.cmd` file.

`sra_collect.cmd` Script file that collects the configuration data.

Set Environment Variables

For data collection from IBM DS6000 and DS8000 enterprise class storage arrays the `dscli` executable should be available via the `PATH` environment variable.

A valid profile file must be available for each storage image to be queried; each profile must have the 'devid' and 'hmc1' fields populated as the commands will be run using the contents of these files.

The script will attempt to run all necessary commands against every storage image, due to some features not being available on some versions of the hardware you may see errors while the script runs, this is normal and can be ignored.

Collecting the configuration data

Windows

Create a new directory, for example `C:\SRA`.

Copy the `sra_collect.cmd` file into the directory.

Executing the Collection Script

Start a cmd shell.

Change directory into the directory where you saved the `sra_collect.cmd` file.

Enter the following command:

```
sra_collect ibm_ent <directory> <username> <password> <profile_directory> </s> </z> </u>
```

<directory>	Where you saved the sra_collect.cmd file.
<username>	Username for logging into DScli.
<password>	Password for logging into DScli.
<profile_directory>	Path to folder containing DScli profile files.

n.b. Directory names containing spaces may cause problems on certain versions and configurations of Windows. We therefore recommend creating a folder named 'profiles' on the root of your filesystem e.g. c:\profiles

</s>	Suppress any output messages appearing on screen.
</z>	the data files will be zipped using the 7zip command line utility.
</u>	the zipped file will be uploaded to the SRA Portal using the Windows WebClient Service.

Important: when using the upload switch you must also specify the zip switch as only zip files can be uploaded to the SRA Portal.

Example:

```
sra_collect ibm_ent c:\sra admin letmein c:\profiles
```

Unix

Create a new directory, for example /opt/sra.

Copy the sra_collect file into the directory.

Executing the Collection Script

Start a shell.

Change directory into the directory where you saved the sra_collect file.

Enter the following command:

```
sra_collect ibm_ent <directory> <username> <password> <profile_directory> </s> </z> </u>
```

<directory>	Where you saved the sra_collect.cmd file.
<username>	Username for logging into DScli.
<password>	Password for logging into DScli.
<profile_directory>	Path to folder containing DScli profile files.

</s>	Suppress any output messages appearing on screen.
</z>	the data files will be zipped using the zip command line utility.
</u>	the zipped file will be uploaded to the SRA Portal using the cadaver command line utility.

Important: when using the upload switch you must also specify the zip switch as only zip files can be uploaded to the SRA Portal.

Example:

```
sra_collect ibm_ent /opt/sra admin letmein /profiles
```

IBM XIV

Prerequisites

Management System requirements

Operating System: Windows 2000, Windows 2003, Windows 2008, Windows XP or Windows Vista.

Vendor software: XIV cli (xcli)

User privileges

It is assumed that the user has an operational knowledge of the Operating System in use.

Access to the `sra_collect.cmd` file.

`sra_collect.cmd` Script file that collects the configuration data.

Set Environment Variables

IBM XIV data is collected by running various 'list' commands through the xcli. The output from each command is redirected to a local file on the computer where the script is executed from.

For the collection to work the xcli executable must be available in the PATH environment variable. You must also pass the script a valid set of user credentials in order for it to log onto the array.

The user specified needs only read-only access to the array unless you are using remote mirroring, in which case you will need full access.

The script relies on the existence of a file listing the IP addresses of the XIV arrays that data should be collected from, it must be called 'array_list.txt', it should be created in the directory that you're running the script from and each IP address should be on a new line within the file.

The script will attempt to run all necessary commands against every array, due to some features not being available on some versions of the hardware you may see errors while the script runs, this is normal and can be ignored.

Collecting the configuration data

Windows

Create a new directory, for example C:\SRA.

Copy the *sra_collect.cmd* file into the directory.

Executing the Collection Script

Start a cmd shell.

Change directory into the directory where you saved the *sra_collect.cmd* file.

Enter the following command:

```
sra_collect ibm_xiv <directory> username password </s> </z> </u>
```

<directory>	Where you saved the <i>sra_collect.cmd</i> file.
</s>	Suppress any output messages appearing on screen.
</z>	the data files will be zipped using the 7zip command line utility.
</u>	the zipped file will be uploaded to the SRA Portal using the Windows WebClient Service.

Important: when using the upload switch you must also specify the zip switch as only zip files can be uploaded to the SRA Portal.

Example:

```
sra_collect ibm_xiv c:\sra administrator password
```

IBM ESS

Prerequisites

Management System requirements

Operating System: Windows 2000, Windows 2003, Windows 2008, Windows XP or Windows Vista.

Vendor software: esscli CLI

User privileges

It is assumed that the user has an operational knowledge of the Operating System in use.

Access to the `sra_collect.cmd` file.

`sra_collect.cmd` Script file that collects the data for SRA.

Set Environment Variables

For data collection from IBM ESS F10, F20 and 800 enterprise class storage arrays the `esscli` executable should be available via the `PATH` environment variable.

A valid profile file must be available for each storage array to be queried, each profile must have the following structure

```
!Version 1.0            <--  MUST HAVE .  
-u username  
-p password  
-s 192.168.100.1
```

Collecting the configuration data

Windows

Create a new directory, for example `C:\SRA`.
Copy the `sra_collect.cmd` file into the directory.

Executing the Collection Script

The script will attempt to run all necessary commands against every storage array. However due to some features not being available on some versions of the hardware you may see errors while the script runs, this is normal and can be ignored.

```
sra_collect ibm_ess <directory> <path_to_profile_directory> </s> </z> </u>
```

<directory> Where you saved the `sra_collect.cmd` file.
<path_to_profile_directory> Path to directory containing the ESS array profiles.

n.b. Directory names containing spaces may cause problems on certain versions and configurations of Windows. We therefore recommend creating a folder named 'profiles' on the root of your filesystem e.g. c:\profiles

</s> Suppress any output messages appearing on screen.
</z> the data files will be zipped using the 7zip command line utility.
</u> the zipped file will be uploaded to the SRA Portal using the Windows WebClient Service.

Important: when using the upload switch you must also specify the zip switch as only zip files can be uploaded to the SRA Portal.

Example:

```
sra_collect ibm_ess c:\sra c:\profiles
```

Unix

Create a new directory, for example /opt/sra.

Copy the sra_collect file into the directory.

Executing the Collection Script

Start a shell.

Change directory into the directory where you saved the sra_collect file.

Enter the following command:

```
sra_collect ibm_ess <directory> <profile_directory> </s> </z> </u>
```

<directory> Where you saved the sra_collect.cmd file.
<profile_directory> Path to folder containing ESS array profiles.
</s> Suppress any output messages appearing on screen.
</z> the data files will be zipped using the zip command line utility.
</u> the zipped file will be uploaded to the SRA Portal using the cadaver command line utility.

Important: when using the upload switch you must also specify the zip switch as only zip files can be uploaded to the SRA Portal.

Example:

```
sra_collect ibm_ess /opt/sra /profiles
```

IBM SVC

The `svconfig` command line tool is used to back-up and restore the configuration of an SVC cluster. Storage Fusion utilises this feature to collect storage configuration data for the analysis.

Collection can be run manually by using the built in tool or if collection is to be carried out over a large estate or on a regular basis the process can be carried out by using the SRA EE collection script.

Manual Collection

The following files are created using the `svconfig backup` command. Please provide these files for each of the SVC systems you require analysing in a single zip file.

Filename	Description
<code>svc.config.backup.xml</code>	This file contains your cluster configuration data.
<code>svc.config.backup.sh</code>	This file contains the names of the commands that were issued to create the backup of the cluster.
<code>svc.config.backup.log</code>	This file contains details about the backup, including any error information that might have been reported.

Should you require further information on how to use the `svconfig` command then please refer to the IBM documentation at the following URL:

http://publib.boulder.ibm.com/infocenter/svc/ic/index.jsp?topic=/com.ibm.storage.svc.console.doc/svc_clustconfbackuptsk_1e4k69.html

Scripted Collection

Prerequisites

Management System requirements

Operating System: Windows 2000, Windows 2003, Windows 2008, Windows XP, Windows Vista, Solaris, AIX, HP-UX and Suse/RedHat Linux.

Vendor software: `Plink.exe`, `Pscp.exe` and `7zip` (Windows) / `ssh`, `scp` and `cadaver` (Unix) and an IBM SVC with `ssh` enabled.

User privileges

It is assumed that the user has an operational knowledge of the Operating System in use.

Access to the `sra_collect` file.

<code>sra_collect.cmd</code>	Script file for Windows that collects the data for SRA.
<code>sra_collect</code>	Script file for Unix that collects the data for SRA.

Windows:

Environment Setup for Collection

Prior to running the collection, it is necessary to create a text file that contains the hostname or IP address of each IBM SVC host including the associated login credentials.

You must create a file named srahosts.txt in c:\sra, add the IBM SVC hosts in the following format and save the file.

```
:: A line starting with a colon is ignored.  
:: IP Address, Username, Password, Type  
:: =====  
:: For a IBM SVC host append ibm_svc.
```

Example: (of srahosts.txt file contents)

```
Anibmsvc, root, A81TTW, ibm_svc  
192.168.100.87, root, M1Pa55W0rd, ibm_svc
```

Collecting the SRA Data

Create a new directory, for example C:\SRA.

Copy the Windows version of *sra_collect.cmd* file into the C:\SRA directory

Copy plink.exe into the C:\SRA directory

Copy the *srahosts.txt* file you created into the C:\SRA directory

IMPORTANT: To run a script automatically using an SSH connection you must first prevent SSH from requesting a password. You can do so by:

- Creating a public key on an IBM SVC. For further information please refer to the appropriate IBM SVC documentation.

- Run the plink command interactively at the command prompt, for example:

```
plink -ssh -l admin -pw Welc0me 192.168.100.29 svcinfo  
lsnode
```

The following message will be displayed.

```
The server's host key is not cached in the registry. You  
have no guarantee that the server is the computer you  
think it is.  
The server's rsa2 key fingerprint is:  
ssh-rsa 2048 16:bf:80:0a:ae:e4:12:9d:31:0f:42:a1:fc:8e:ad:90  
If you trust this host, enter "y" to add the key to  
PuTTY's cache and carry on connecting.  
If you want to carry on connecting just once, without  
adding the key to the cache, enter "n".  
If you do not trust this host, press Return to abandon the  
connection.  
Store key in cache? (y/n)
```

Answering y will prevent this message appearing the next time the plink command connects to host 192.168.100.29.

Repeat the above for each host that you are collecting data from.

Executing the Collection Script

Start a cmd shell.

Change directory into the directory where you saved the *sra_collect.cmd* file.

Enter the following command:

```
sra_collect ibm_svc <directory> </s> </z> </u>
```

<directory> Where you saved the sra_collect.cmd file.
</s> Suppress any output messages appearing on screen.
</z> the data files will be zipped using the 7zip command line utility.
</u> the zipped file will be uploaded to the SRA Portal using the Windows WebClient Service.

Important: when using the upload switch you must also specify the zip switch as only zip files can be uploaded to the SRA Portal.

Example: `sra_collect ibm_svc c:\sra`

Unix:

Environment Setup for Collection

Prior to running the collection it is necessary to create a text file that contains the hostname or IP address of each IBM SVC including the associated login credentials.

You must create a file named srahosts.txt in the same directory as the sra_collect script, add the IBM SVC hosts in the following format and save the file. Passwords are not stored in this file, instead you must setup authentication between the management console and the filers using SSH public keys.

```
:: A line starting with a colon is ignored.  
:: IP Address, Username, Type  
:: =====  
:: For a IBM host append ibm_svc.
```

Example: (of srahosts.txt file contents)

```
Anibmsvc,root,ibm_svc  
192.168.100.87,root,ibm_svc
```

Collecting the SRA Data

Create a new directory, for example `/opt/sra`.

Copy the Unix version of `sra_collect` file into the `/opt/sra` directory

Copy the `srahosts.txt` file you created into the `/opt/sra` directory

IMPORTANT: To run a script automatically using an SSH connection you must first prevent SSH from requesting a password. You can do so by:

- Creating a public key on the IBM SVC Storage Server.

For further information please refer to the appropriate IBM SVC Storage Server documentation.

Repeat the above for each host that you are collecting data from.

Executing the Collection Script

Change directory into the directory where you saved the `sra_collect` file.

Enter the following command:

```
sra_collect ibm_svc <directory> </s> </z> </u>
```

<directory>	Where you saved the <code>sra_collect</code> file.
</s>	Suppress any output messages appearing on screen.
</z>	the data files will be zipped using the zip command line utility.
</u>	the zipped file will be uploaded to the SRA Portal using the cadaver command line utility.

Important: when using the upload switch you must also specify the zip switch as only zip files can be uploaded to the SRA Portal.

Example: `sra_collect ibm_svc /opt/sra`

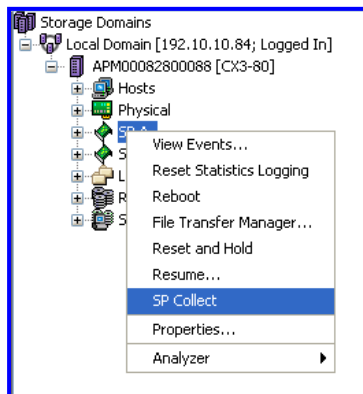
EMC CLARiION

SP Collect

SP collect is typically used to collect storage diagnostic information. Storage Fusion utilises this feature to collect storage configuration data for the analysis. SP collect is completed in two steps. The first step is to collect the information on the array in a single zip file.

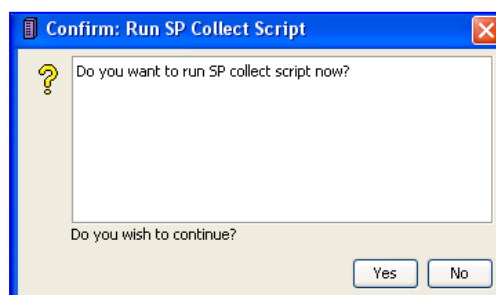
Once you have finished collecting the data please create a single zip file that contains all SP collects in to a single zip file. The zip file must not include any sub-directories.

The collection process must be completed on both storage processors of the array providing replicated LUNs.

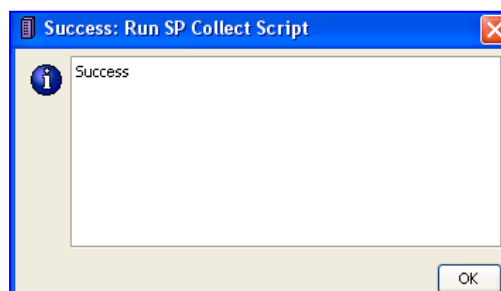


From Navisphere explorer:

- Right click on the required Storage Processor
- Select “SP Collect”

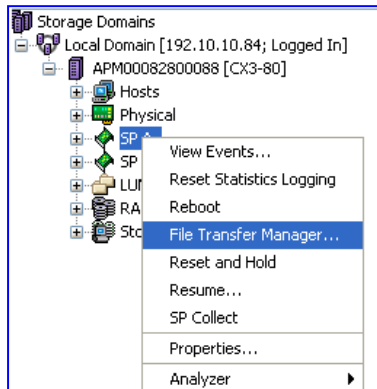


- Click “Yes”



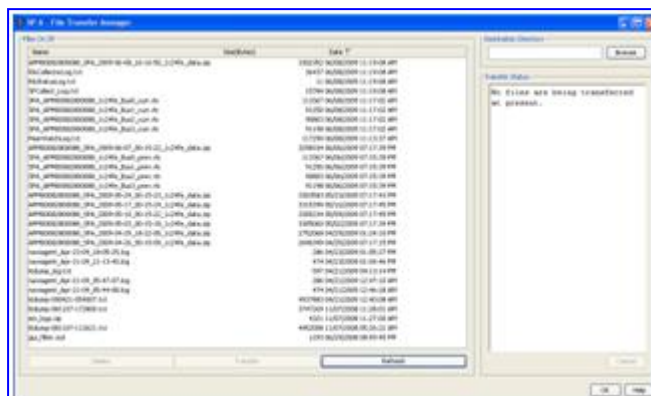
- Click “OK”

Once the collection is started start the file transfer manager to monitor the progress and to download the completed zip file.

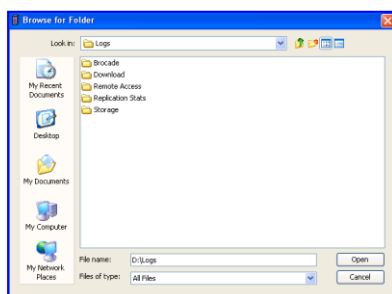


From Navisphere explorer:

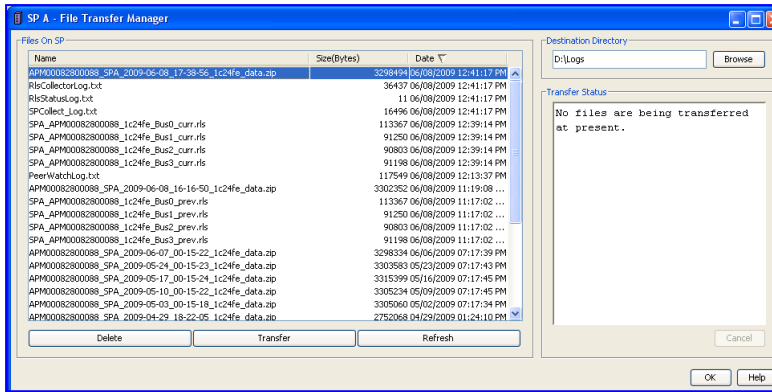
- Right click on the required Storage Processor
- Select “File Transfer Manager”



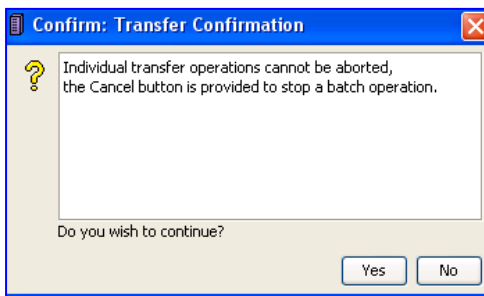
- Click on Date to order most current file on the top
- Click Refresh to update list
- Click “Browse” to select location to upload



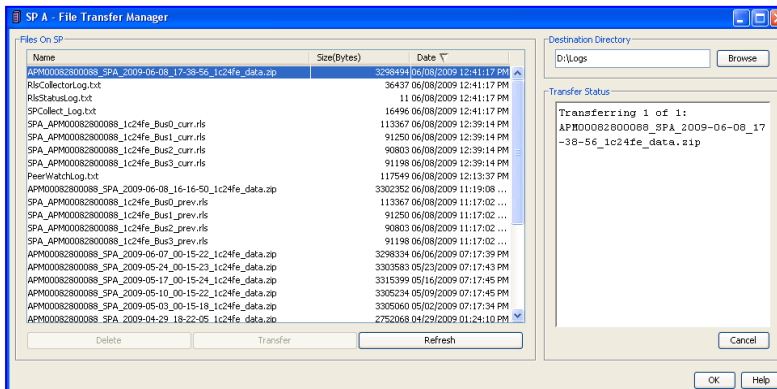
- Select directory to upload to
- Click “Open”



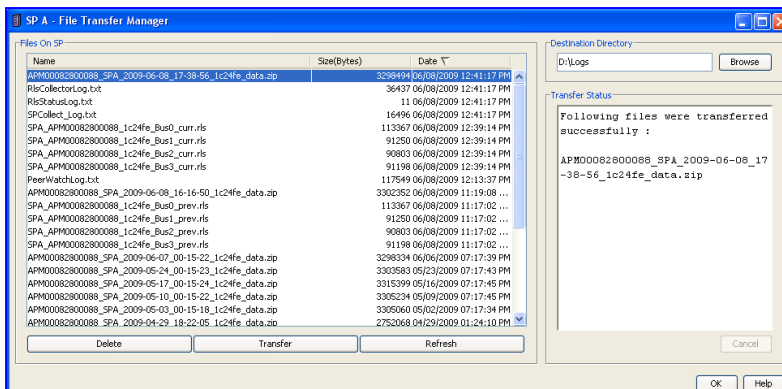
- Select the file to transfer
- Click “Transfer”

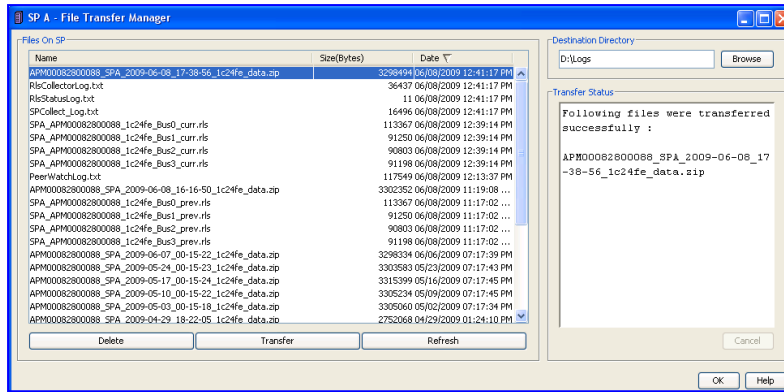


- Click “Yes”



- Wait for the transfer to complete





Once the transfer completes:

- Click "OK"

RecoverPoint/SafeGuard

Prerequisites

Management System requirements

Operating System: Windows 2000, Windows 2003, Windows 2008, Windows XP or Windows Vista.

Vendor software: Plink.exe and RecoverPoint CLI

User privileges

It is assumed that the user has an operational knowledge of the Operating System in use.

Environment Setup for Collection

Prior to running the collection it is necessary to create a text file that contains the hostname or IP address of each RecoverPoint Appliance including the associated login credentials.

You must create a file named srahosts.txt in c:\sra, add the RecoverPoint hosts in the following format and save the file.

```
:: A line starting with a colon is ignored.  
:: IP Address, Username, Password, Type  
:: =====  
:: For a RecoverPoint host append recpoint.
```

Example: (of srahosts.txt file contents)

```
192.168.100.60,admin,admin,recpoint  
192.168.100.25,admin,admin,recpoint  
RA1,admin,admin,recpoint
```

Collecting the configuration data

Windows

Create a new directory, for example C:\SRA.

Copy the *sra_collect.cmd* file into the C:\SRA directory

Copy plink.exe into the C:\SRA directory

Copy the *srahosts.txt* file you created into the C:\SRA directory

IMPORTANT: To run a script automatically using an SSH connection you must first prevent SSH from requesting a password. You can do so by:

- Creating a public key on the RecoverPoint Appliance (using the `add_ssh_key` command). For further information regarding the EMC RecoverPoint CLI please refer to the EMC RecoverPoint CLI Reference Guide.

- Run the plink command interactively at the command prompt, for example:

```
plink -ssh -l admin -pw Welc0me1291 192.168.100.29  
get_splitter_settings
```

The following message will be displayed.

The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.

The server's rsa2 key fingerprint is:

ssh-rsa 2048 16:bf:80:0a:ae:e4:12:9d:31:0f:42:a1:fc:8e:ad:90

If you trust this host, enter "y" to add the key to PuTTY's cache and carry on connecting.

If you want to carry on connecting just once, without adding the key to the cache, enter "n".

If you do not trust this host, press Return to abandon the connection.

Store key in cache? (y/n)

Answering y will prevent this message appearing the next time the plink command connects to host 192.168.100.29.

Repeat the above for each host that you are collecting data from.

Executing the Collection Script

Start a cmd shell.

Change directory into the directory where you saved the *sra_collect.cmd* file.

```
sra_collect recpoint <directory> </s> </z> </u>
```

<directory>	Where you saved the sra_collect.cmd file.
</s>	Suppress any output messages appearing on screen.
</z>	the data files will be zipped using the 7zip command line utility.
</u>	the zipped file will be uploaded to the SRA Portal using the Windows WebClient Service.

Important: when using the upload switch you must also specify the zip switch as only zip files can be uploaded to the SRA Portal.

Example:

```
sra_collect recpoint c:\sra
```

NetApp

Prerequisites

Management System requirements

Operating System: Windows 2000, Windows 2003, Windows 2008, Windows XP, Windows Vista, Solaris, AIX, HP-UX and Suse/RedHat Linux.

Vendor software: Plink.exe (Windows) / ssh (Unix) and NetApp filer with ssh enabled.

User privileges

It is assumed that the user has an operational knowledge of the Operating System in use.

Access to the sra_collect file.

sra_collect.cmd Script file for Windows that collects the data for SRA.
sra_collect Script file for Unix that collects the data for SRA.

Windows:

Environment Setup for Collection

Prior to running the collection it is necessary to create a text file that contains the hostname or IP address of each NetApp filer including the associated login credentials.

You must create a file named srahosts.txt in c:\sra, add the NetApp hosts in the following format and save the file.

```
:: A line starting with a colon is ignored.  
:: IP Address, Username, Password, Type  
:: =====  
:: For a RecoverPoint host append recpoint.  
:: For a NetApp host append netapp.
```

Example: (of srahosts.txt file contents)

```
filer1,root,A81TTW,netapp  
192.168.100.87,root,M1Pa55W0rd,netapp
```

Collecting the SRA Data

Create a new directory, for example C:\SRA.

Copy the Windows version of *sra_collect.cmd* file into the C:\SRA directory.

Copy plink.exe into the C:\SRA directory.

Copy the *srahosts.txt* file you created into the C:\SRA directory

IMPORTANT: To run a script automatically using an SSH connection you must first prevent SSH from requesting a password. You can do so by:

- Creating a public key on the RecoverPoint Appliance (using the `add_ssh_key` command). For further information regarding the EMC RecoverPoint CLI please refer to the EMC RecoverPoint CLI Reference Guide.
- Creating a public key on the NetApp filer. For further information please refer to the appropriate NetApp documentation.
- Run the plink command interactively at the command prompt, for example:

```
plink -ssh -l admin -pw Welc0me 192.168.100.29 sysconfig -a
```

The following message will be displayed.

```
The server's host key is not cached in the registry. You
have no guarantee that the server is the computer you
think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 2048 16:bf:80:0a:ae:e4:12:9d:31:0f:42:a1:fc:8e:ad:90
If you trust this host, enter "y" to add the key to
PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without
adding the key to the cache, enter "n".
If you do not trust this host, press Return to abandon the
connection.
Store key in cache? (y/n)
```

Answering y will prevent this message appearing the next time the plink command connects to host 192.168.100.29.

Repeat the above for each host that you are collecting data from.

Executing the Collection Script

Start a cmd shell.

Change directory into the directory where you saved the *sra_collect.cmd* file.

Enter the following command:

```
sra_collect netapp <directory> /s
```

<directory> Where you saved the sra_collect.cmd file.
</s> Suppress any output messages appearing on screen.
</z> the data files will be zipped using the 7zip command line utility.
</u> the zipped file will be uploaded to the SRA Portal using the Windows WebClient Service.

Important: when using the upload switch you must also specify the zip switch as only zip files can be uploaded to the SRA Portal.

Example: `sra_collect netapp c:\sra`

Unix:

Environment Setup for Collection

Prior to running the collection it is necessary to create a text file that contains the hostname or IP address of each NetApp filer including the associated login credentials.

You must create a file named srahosts.txt in the same directory as the sra_collect script, add the NetApp hosts in the following format and save the file. Passwords are not stored in this file, instead you must setup authentication between the management console and the filers using SSH public keys.

```
:: A line starting with a colon is ignored.  
:: IP Address, Username, Type  
:: =====  
:: For a NetApp host append netapp.
```

Example: (of srahosts.txt file contents)

```
filer1,root,netapp  
192.168.100.87,root,netapp
```

Collecting the SRA Data

Create a new directory, for example `/opt/sra`.

Copy the Unix version of `sra_collect` file into the `/opt/sra` directory

Copy the `srahosts.txt` file you created into the `/opt/sra` directory

IMPORTANT: To run a script automatically using an SSH connection you must first prevent SSH from requesting a password. You can do so by:

- Creating a public key on the NetApp filer.

For further information please refer to the appropriate NetApp documentation.

Repeat the above for each host that you are collecting data from.

Executing the Collection Script

Change directory into the directory where you saved the *sra_collect* file.

Enter the following command:

```
sra_collect netapp <directory> </s> </z> </u>
```

<directory> Where you saved the sra_collect file.

</s> Suppress any output messages appearing on screen.

</z> the data files will be zipped using the zip command line utility.

</u> the zipped file will be uploaded to the SRA Portal using the cadaver command line utility.

Important: when using the upload switch you must also specify the zip switch as only zip files can be uploaded to the SRA Portal.

Example: `sra_collect netapp /opt/sra`

SAN Fabric

Brocade

Prerequisites

Management System requirements

Operating System: Windows 2000, Windows 2003, Windows 2008, Windows XP, Windows Vista, Solaris, AIX, HP-UX and Suse/RedHat Linux.

Vendor software: Plink.exe (Windows) ssh (Unix) for data collection.
7zip/Unix zip and cadaver (Unix) for automating the upload of a collection.

User privileges

It is assumed that the user has an operational knowledge of the Operating System in use.

Access to the sra_collect file.

sra_collect.cmd Script file for Windows that collects the data for SRA.
sra_collect Script file for Unix that collects the data for SRA.

Windows:

Environment Setup for Collection

Prior to running the collection, it is necessary to create a text file that contains the hostname or IP address of each Brocade Fabric Switch including the associated login credentials.

You must create a file named srahosts.txt in c:\sra, add the Brocade Fabric Switch in the following format and save the file.

:: A line starting with a colon is ignored.
:: **IP Address, Username, Password, Type**
:: =====
:: For a Brocade Fabric Switch append brocade.

Example: (of srahosts.txt file contents)

BrocSwitch, root, A81TTW, brocade
192.168.100.87, root, M1Pa55W0rd, brocade

Collecting the SRA Data

Create a new directory, for example C:\SRA.

Copy the Windows version of *sra_collect.cmd* file into the C:\SRA directory

Copy plink.exe into the C:\SRA directory

Copy the *srahosts.txt* file you created into the C:\SRA directory

IMPORTANT: To run a script automatically using an SSH connection you must first prevent SSH from requesting a password. You can do so by:

- Creating a public key on a Brocade Fabric Switch.

For further information, please refer to the appropriate Brocade Fabric Switch documentation.

- Run the plink command interactively at the command prompt, for example:

```
plink -ssh -l admin -pw Welc0me 192.168.100.29 /bin/cat /proc/cpuinfo
```

The following message will be displayed.

```
The server's host key is not cached in the registry. You
have no guarantee that the server is the computer you
think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 2048 16:bf:80:0a:ae:e4:12:9d:31:0f:42:a1:fc:8e:ad:90
If you trust this host, enter "y" to add the key to
PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without
adding the key to the cache, enter "n".
If you do not trust this host, press Return to abandon the
connection.
Store key in cache? (y/n)
```

Answering y will prevent this message appearing the next time the plink command connects to host 192.168.100.29.

Repeat the above for each host that you are collecting data from.

Executing the Collection Script

Start a cmd shell.

Change directory into the directory where you saved the *sra_collect.cmd* file.

Enter the following command:

```
sra_collect brocade <directory> </s> </z> </u>
```

<directory> Where you saved the sra_collect.cmd file.
</s> Suppress any output messages appearing on screen.
</z> the data files will be zipped using the 7zip command line utility.
</u> the zipped file will be uploaded to the SRA Portal using the Windows WebClient Service.

Important: when using the upload switch you must also specify the zip switch as only zip files can be uploaded to the SRA Portal.

Example: `sra_collect brocade c:\sra`

Unix:

Environment Setup for Collection

Prior to running the collection it is necessary to create a text file that contains the hostname or IP address of each Brocade Fabric Switch including the associated login credentials.

You must create a file named srahosts.txt in the same directory as the sra_collect script, add the Brocade Fabric Switch in the following format and save the file. Passwords are not stored in this file, instead you must setup authentication between the management console and the filers using SSH public keys.

```
:: A line starting with a colon is ignored.  
:: IP Address, Username, Type  
:: =====  
:: For a Brocade Fabric Switch append brocade.
```

Example: (of srahosts.txt file contents)

```
BrocSwitch,root,brocade  
192.168.100.87,root,brocade
```

Collecting the SRA Data

Create a new directory, for example `/opt/sra`.

Copy the Unix version of `sra_collect` file into the `/opt/sra` directory

Copy the `srahosts.txt` file you created into the `/opt/sra` directory

IMPORTANT: To run a script automatically using an SSH connection you must first prevent SSH from requesting a password. You can do so by:

- Creating a public key on a Brocade Fabric Switch.

For further information, please refer to the appropriate Brocade Fabric Switch documentation

Repeat the above for each host that you are collecting data from.

Executing the Collection Script

Change directory into the directory where you saved the `sra_collect` file.

Enter the following command:

```
sra_collect brocade <directory> </s> </z> </u>
```

<directory>	Where you saved the <code>sra_collect</code> file.
</s>	Suppress any output messages appearing on screen.
</z>	the data files will be zipped using the zip command line utility.
</u>	the zipped file will be uploaded to the SRA Portal using the cadaver command line utility.

Important: when using the upload switch you must also specify the zip switch as only zip files can be uploaded to the SRA Portal.

Example: `sra_collect brocade /opt/sra`

Cisco

Prerequisites

Management System requirements

Operating System: Windows 2000, Windows 2003, Windows 2008, Windows XP, Windows Vista, Solaris, AIX, HP-UX and Suse/RedHat Linux.

Vendor software: Plink.exe (Windows) ssh (Unix) for data collection.

7zip/Unix zip and cadaver (Unix) for automating the upload of a collection.

User privileges

It is assumed that the user has an operational knowledge of the Operating System in use.

Access to the sra_collect file.

sra_collect.cmd	Script file for Windows that collects the data for SRA.
sra_collect	Script file for Unix that collects the data for SRA.

Windows:

Environment Setup for Collection

Prior to running the collection, it is necessary to create a text file that contains the hostname or IP address of each Cisco Fabric Switch including the associated login credentials.

You must create a file named srahosts.txt in c:\sra, add the Cisco Fabric Switch in the following format and save the file.

```
:: A line starting with a colon is ignored.  
:: IP Address, Username, Password, Type  
:: =====  
:: For a Cisco Fabric Switch append cisco.
```

Example: (of srahosts.txt file contents)

```
CiscoSwitch,root,A81TTW,cisco  
192.168.100.87,root,M1Pa55W0rd,cisco
```

Collecting the SRA Data

Create a new directory, for example C:\SRA.

Copy the Windows version of *sra_collect.cmd* file into the C:\SRA directory

Copy plink.exe into the C:\SRA directory

Copy the *srahosts.txt* file you created into the C:\SRA directory

IMPORTANT: To run a script automatically using an SSH connection you must first prevent SSH from requesting a password. You can do so by:

- Creating a public key on a Cisco Fabric Switch. For further information, please refer to the appropriate Cisco Fabric Switch documentation.

- Run the plink command interactively at the command prompt, for example:

```
plink -ssh -l admin -pw Welcome 192.168.100.29 /bin/cat /proc/cpuinfo
```

The following message will be displayed.

The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.

The server's rsa2 key fingerprint is:

ssh-rsa 2048 16:bf:80:0a:ae:e4:12:9d:31:0f:42:a1:fc:8e:ad:90

If you trust this host, enter "y" to add the key to

PuTTY's cache and carry on connecting.

If you want to carry on connecting just once, without adding the key to the cache, enter "n".

If you do not trust this host, press Return to abandon the connection.

Store key in cache? (y/n)

Answering y will prevent this message appearing the next time the plink command connects to host 192.168.100.29.

Repeat the above for each host that you are collecting data from.

Executing the Collection Script

Start a cmd shell.

Change directory into the directory where you saved the *sra_collect.cmd* file.

Enter the following command:

```
sra_collect cisco <directory> </s> </z> </u>
```

<directory> Where you saved the sra_collect.cmd file.
</s> Suppress any output messages appearing on screen.
</z> the data files will be zipped using the 7zip command line utility.
</u> the zipped file will be uploaded to the SRA Portal using the Windows WebClient Service.

Important: when using the upload switch you must also specify the zip switch as only zip files can be uploaded to the SRA Portal.

Example: `sra_collect cisco c:\sra`

Unix:

Environment Setup for Collection

Prior to running the collection it is necessary to create a text file that contains the hostname or IP address of each Cisco Fabric Switch including the associated login credentials.

You must create a file named srahosts.txt in the same directory as the sra_collect script, add the Cisco Fabric Switch in the following format and save the file. Passwords are not stored in this file, instead you must setup authentication between the management console and the filers using SSH public keys.

```
:: A line starting with a colon is ignored.  
:: IP Address, Username, Type  
:: =====  
:: For a Cisco Fabric Switch append cisco.
```

Example: (of srahosts.txt file contents)

```
CiscoSwitch,root,cisco  
192.168.100.87,root,cisco
```

Collecting the SRA Data

Create a new directory, for example `/opt/sra`.

Copy the Unix version of `sra_collect` file into the `/opt/sra` directory.

Copy the `srahosts.txt` file you created into the `/opt/sra` directory.

IMPORTANT: To run a script automatically using an SSH connection you must first prevent SSH from requesting a password. You can do so by:

- Creating a public key on a Cisco Fabric Switch.

For further information, please refer to the appropriate Cisco Fabric Switch documentation.

Repeat the above for each host that you are collecting data from.

Executing the Collection Script

Change directory into the directory where you saved the `sra_collect` file.

Enter the following command:

```
sra_collect cisco <directory> </s> </z> </u>
```

<directory>	Where you saved the <code>sra_collect</code> file.
</s>	Suppress any output messages appearing on screen.
</z>	the data files will be zipped using the zip command line utility.
</u>	the zipped file will be uploaded to the SRA Portal using the cadaver command line utility.

Important: when using the upload switch you must also specify the zip switch as only zip files can be uploaded to the SRA Portal.

Example: `sra_collect cisco /opt/sra`

Validating the data collection

Configuration data collected using the sra_collect script is written into a subdirectory of where the collection script is executed from. The below would be used if you have followed the examples in this guide:

Unix	/opt/sra
Windows	c:\sra

The file will be named ddmmymmhhmm where:

dd	Current day.	14
mm	Current month.	04
yyyy	Current year.	2010
hh	Current hour.	14
mm	Current minute.	08

A number of different files are created in this directory all of which are required for analysis. Under no circumstances should these files be renamed or their contents changed.

Zip files

To minimise the network bandwidth requirements and storage footprint it's mandatory that the configuration data is zipped prior to uploading it to the web portal.

Zip file requirements and recommendations are included below:

- You can have multiple zip files per vendor. For example, if you have two data centres and collected symmetrix data from both data centres then you can upload two zip files, one named symmetrix_dc1.zip and the other named symmetrix_dc2.zip.
- The zip file should have a meaningful name. We recommend using the following convention:

<model>_<COMPUTERNAME>_<ddmmyy>.zip Where:

model	See below list.*
COMPUTERNAME	The host name of the computer where sra_collect was executed.
ddmmyy	The day, month and year when the sra_collect was executed.

- All zip files must be created using zip (Unix), PKZIP, 7ZIP or Windows Compressed folders and must have a .zip extension. **Zip files from gzip or tar are not supported and will be rejected by the web portal.**

*SRA's discovery process is optimised to discover the following names at the start of the filename:

Filename	Description
emc_clar	EMC - CLARiiON
emc_rpoint	EMC – RecoverPoint
emc_symm	EMC - Symmetrix
hitachi	Hitachi Data Systems
hpxp	Hewlett Packard - HP XP
hpeva	Hewlett Packard - EVA
ibm_mod	IBM – Modular
ibm_ent	IBM – Enterprise
ibm_svc	IBM – SVC
ibm_xiv	IBM – XIV
ibm_ess	IBM – ESS
netapp	NetApp
brocade	Brocade
cisco	Cisco

Additional data collected

Data files that are collected without using the sra_collect script commands, from devices like NetApp, SafeGuard/RecoverPoint, CLARiiON, and your SAN switches, can be given descriptive names to identify the devices the data files were collected from. For each vendor create a separate zip file containing the configuration data. The zip file must not include any sub-directories. A NetApp example is included below:

```
NetApp_251110.zip
  filer1.txt
  filer2.txt
  prod_filer.txt
  dr_filer.txt
```

World Wide Name to Hostname Mapping

The default behaviour is to use the hostname that is configured within the array. For most vendors this is fine, however due to the flexibility of EMC Symmetrix and Hitachi arrays you may want to override the mapping using an external data source. Two options are available to perform the override, both requiring a CSV file.

Manually create a mapping file.

Using Excel create a mapping file in the following format.

```
server01,,,10000000c6729892,,,,  
server02,,,10000000c9259894,,,,
```

Switch created file.

Obtain the output from a switch in the following format.

```
Host,Port Name,Node WWN,PortWWN,Adapter Vendor,Adapter Model,Firmware  
Rev,Driver Rev
```

If you are using Excel to create the CSV file then it's recommended that row one contains the field descriptions. By including the field descriptions Excel will automatically append a comma to each record.

A single CSV file named `wwntohnmap.csv` should be provided in a zip file.

IMPORTANT: A mapping file needs to be provided for each Analysis Point.

Data collection log files

During the execution a detailed log file is created in the directory specified in the command line.

The log file is named `SRA_Collect_<DateTime>_<COMPUTERNAME>.log`.

This file can be viewed to check progress of the collection or to trouble-shoot problems.

Progress is displayed to screen detailing which task is being executed and the total number of tasks to process unless the `/s` parameter is used.

Uploading data

Once you have finished collecting the data you can upload it to the web portal using a web browser. Please review the web portal online documentation for further information.

Automating the data collection process

It is recommended that the data collection script is automated and scheduled to run at least once per week. However it's entirely your decision when you choose to analyse and publish the results to the Dashboard.

Windows

Zip files

The SRA_Collect script can automatically create a zip file using the 7-Zip command line interface and by specifying the /z command line parameter.

Instructions:

1. Download the 7-Zip CLI (7za.exe) from <http://www.7-zip.org/download.html>.
2. Ensure that the 7za.exe is available in the Windows path environment variable or that it's located in the same directory as the sra_collect script is run from.
3. Specify the /z parameter:

Example: `sra_collect c:\sra symmetrix /s /z`

Note: To suppress any output we also use the /s parameter.

Uploading Data

The SRA_Collect script can automatically upload the zip file to the portal by specifying the /u command line parameter.

The connection is established using Web-based Distributed Authoring and Versioning (WebDAV) methods which utilises the http protocol. You must therefore ensure that the Windows WebClient service is running and that your firewall allows outbound traffic on port 80 from the system where the script is run from.

Instructions:

1. Modify the following parameters in the sra_config.txt file:

Parameter	Example	Notes
SRA_URL*	http://upload.webportal.com/091	-
SRA_username*	USR091	-
SRA_password*	kd7Jy1Ap	-
SRA_drive	x:	The local drive to map to the web portal.

* These values will be provided to you by your technical support team.

2. Validate that you can manually establish a connection using the parameters from the sra_config.txt file:

NET USE <SRA_drive> <SRA_URL> <SRA_password> /user:<SRA_username>

Example: NET USE X: <http://upload.webportal.com/091> kd7Jy1Ap /user: USR091

3. Specify the /u parameter:

Example: `sra_collect c:\sra symmetrix /s /z /u`

IMPORTANT: You must specify the /z parameter when using /u.

Scheduling the script to automatically run

The `sra_collect` script can be executed using the Windows AT command or other scheduling tools. The following examples use the Windows AT command:

Instructions:

1. The vendor command line executable must be accessible from the system PATH environmental variable on the machine where the `sra_collect` command is executed from.
2. Start a cmd session as the administrator user.

- i) Schedule `sra_collect` to run once at 16:30 hours and upload the data to the portal.

```
at 16:30 cmd /c "c:\sra\sra_collect symmetrix c:\sra /s /z /u"
```

- ii) Schedule `sra_collect` to run silently at 06:00am every Monday and compress the data.

```
at 06:00 /every:M cmd /c "c:\sra\sra_collect symmetrix c:\sra /s /z"
```

- iii) Schedule `sra_collect` to run silently at 20:00 hours every day, compress the data and upload it to the portal.

```
at 20:00 /every:M,T,W,Th,F,Sa,Su cmd /c "c:\sra\sra_collect.  
symmetrix c:\sra /s /z /u"
```

Unix

Zip files

The `sra_collect` script can automatically create a zip file using the zip command line interface and by specifying the `/z` command line parameter.

Instructions:

1. Login to the system where the `sra_collect` script will be executed.
2. Enter the following command:

```
type zip
```

If the zip command is installed then output similar to the below will be displayed:

```
zip is /usr/bin/zip
```

Otherwise the following message will typically be displayed:

```
-bash: type: zip: not found
```

If the zip command isn't found please refer to your operating system on how to install the zip package.

3. Specify the /z parameter:

Example:

```
sra_collect symmetrix /home/sra /s /z
```

Note: To suppress any output we also use the /s parameter.

Uploading Data

The sra_collect script can automatically upload the zip file to the portal by specifying the /u command line parameter.

The connection is established using Web-based Distributed Authoring and Versioning (WebDAV) methods which utilises the http protocol.

You must therefore ensure that the cadaver WebDAV client for Unix is installed and that your firewall allows outbound traffic on port 80 from the system where the script is run from.

Instructions:

1. Modify the following parameters in the sra_config.txt file:

Parameter	Example	Notes
SRA_URL*	http://upload.webportal.com/091	-
SRA_username*	USR091	-
SRA_password*	kd7Jy1Ap	-
SRA_drive	n/a	Not required on Unix.

* These values will be provided to you by your technical support team.

2. Validate that you can manually establish a connection using the parameters from the sra_config.txt file:

```
cadaver <SRA_URL>
```

Example:

```
cadaver http://upload.webportal.com/091
```

```
Authentication required for WebDAV Server on server `192.168.100.101':
```

```
Username: USR091
```

```
Password: kd7Jy1Ap
```

```
Once logged in you will see:
```

```
dav:/091/>
```

```
Type exit to finish the test.
```

-
3. Specify the /u parameter:

Example: *sra_collect c:\sra symmetrix /s /z /u*

IMPORTANT: You must specify the /z parameter when using /u.

Scheduling the script to automatically run

The *sra_collect* script can be executed using the Unix Cron or at commands or other scheduling tools. The following examples use the Unix Cron command:

Instructions:

1. The vendor command line executable must be accessible from the system PATH environmental variable on the machine where the *sra_collect* command is executed from.
2. Start a shell session as a user who has the applicable permissions to schedule jobs.
3. The *crontab -e* command is typically used to manage cron jobs but please refer to your operating system for further information.

- i) Schedule *sra_collect* to collect symmetrix data, run silently at 06:00am every Monday and compress the data.

```
00 06 * * 1 /home/sra/sra_collect symmetrix /home/sra /s /z
```

- ii) Schedule *sra_collect* to collect symmetrix data, run silently at 20:00 hours every day, compress the data and upload it to the portal.

```
00 20 * * * /home/sra/sra_collect symmetrix /home/sra /s /z /u
```

- iii) Schedule *sra_collect* to collect hitachi data, run silently at 20:00 hours every day, compress the data and upload it to the portal.

```
00 20 * * * /home/sra/sra_collect hitachi /home/sra  
http://localhost:2001/service admin password /s /z /u
```



STORAGEFUSION

Storage Resource Analysis Enterprise Edition

Supported feature list by Vendor

	EMC CLARiiON	EMC Symmetrix	EMC V-Max	HDS	HP XP	HP EVA	IBM Modular	IBM Enterprise	IBM ESS	IBM SVC ¹	IBM XIV	NetApp FAS
Feature												
Local Snap	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	✓
Local Clone	✓	✓	✓	✓	✓	N/A	N/A	✓	✗	✓	N/A	N/A
Remote Clone	✓	✓	✓	✓	✓	✗	✗	✗	✗	✓	N/A	N/A
Remote Replication	✓	✓	✓	✓	✓	✓	✗	✓	✗	✓	✗	✓
Remote Snap	✓	✓	✓	✓	✓	✗	✗	✓	✗	✗	✗	✓
Thin Provisioning	✓	✓	✓	✓	✓	✗	N/A	✗	N/A	✗	✓	✗
Virtualisation	N/A	N/A	✗	✓	✓	✗	✗	✗	✗	✓	✗	✗
Mainframe	N/A	✓	✓	✓	✓	N/A	N/A	✓	✗	N/A	N/A	N/A
Storage Partitioning	✗	✗	✗	✗	✗	✗	✗	✗	✗	N/A	✗	✓

Key: ✓ Feature is supported; ✗ Feature isn't currently supported; Unknown – it's unknown whether the storage platform supports this feature; N/A – Not Applicable.

¹ Support is currently limited to IBM virtualised storage. IBM Mod, IBM Enterprise, Hitachi, HP XP (12000 and 24000) and IBM XIV. Please contact Storage Fusion if you are virtualising a different vendor.

General notes:

Capacity, Configuration, Tiering and Environmentals tabs and views are available for all supported platforms. The Virtualisation tab is only available when Virtualisation, Thin Provisioning or Snap is discovered.