PROMISE®
TECHNOLOGY, INC.

VTRAK S3000

Storage Replication Adapter User Manual

Version 1.0

Copyright

Important data protection information

You should back up all data before installing any drive controller or storage peripheral. Promise Technology is not responsible for any loss of data resulting from the use, disuse or misuse of this or any other Promise Technology product.

Notice

Although Promise Technology has attempted to ensure the accuracy of the content of this manual, it is possible that this document may contain technical inaccuracies, typographical, or other errors. Promise Technology assumes no liability for any error in this publication, and for damages, whether direct, indirect, incidental, consequential or otherwise, that may result from such error, including, but not limited to loss of data or profits.

Promise Technology provides this publication “as is” without warranty of any kind, either express or implied, including, but not limited to implied warranties of merchantability or fitness for a particular purpose.

The published information in the manual is subject to change without notice. Promise Technology reserves the right to make changes in the product design, layout, and driver revisions without notification to its users.

This version of the *Product Manual* supersedes all previous versions.

Recommendations

In this *User Manual*, the appearance of products made by other companies, including but not limited to software, servers, and disk drives, is for the purpose of illustration and explanation only. Promise Technology does not recommend, endorse, prefer, or support any product made by another manufacturer.

Contents

Chapter 1: Installation and Configuration

The Promise Storage Replication Adapter (SRA) integrates with VMware vCenter Site Recovery Manager (SRM) to automate disaster recovery for systems using VMware Infrastructure with storage managed by VTrak S3000 technology.

In a typical environment, there will be two sites, the protected site or primary production site, and the recovery site. At each site, there is a VTrak S3000 server to manage storage for the host machines. In addition, the VTrak S3000 server replicates data from the protected site to the recovery site.

When a disaster occurs and the protected site is not available, the recovery plan can be run so that the system fails over to the server at the recovery site and the replicated data can be used.

For disaster recovery planning purposes, you can test your recovery plan through SRM. Testing can be done at any time without any impact to your production environment.

For more information about the Promise SRA solution, go to http://www.promise.com.

SRA Requirements

Promise Storage Replication Adapter (SRA) must be installed on each host where VMware vCenter Site Recovery Manager (SRM) is installed, at both the protected site and the recovery site.

Installing SRA

To install SRA:

1. Run the install program.

   If SRM is not detected, the installer stops.

2. Follow the onscreen instructions to complete the SRA installation wizard.

   If SRM is installed to its default location,

   C:\Program Files\VMware\VMware vCenter Site Recovery Manager

   SRA is installed under

   C:\Program Files\VMware\VMware vCenter Site Recovery Manager\scripts\SAN\VTrak

Because the Storage Replication Adapter (SRA) works within the framework of Site Recovery Manager (SRM), see your *VMware vCenter Site Recovery Manager User Guide* for instructions on how to set up and configure hosts for protection.

Configuring VTrak S3000 Servers to Protect Data

In addition to configuring hosts for protection, you must configure your VTrak S3000 servers to protect your data. This is done through the Promise Management Console. The following is an overview of the steps that must be performed. Refer to your *VTrak S3000 Server User Manual* for more information.

1. At the primary site, configure each host as a SAN Client and assign virtual devices to it.
2. Configure replication for each virtual device at the primary site that needs to be protected.

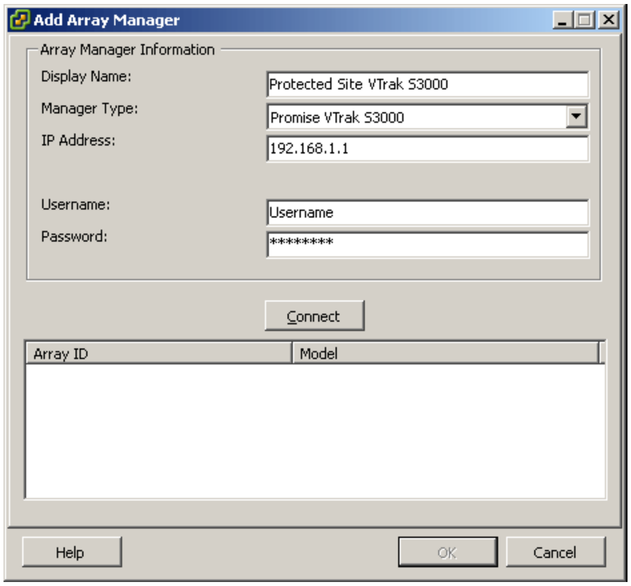
   The data is replicated to the VTrak S3000 server at the recovery site.

3. At the recovery site, configure each recovery host as a SAN Client.
4. Enable Snapshot for each of the replica devices at the recovery site.

Identifying VTrak S3000 Servers in the SRM Array Manager

During the configuration process, you must enter the IP address and the login credentials for the VTrak S3000 servers at both the primary site and the recovery site.

1. Launch the SRM Array Manager and select to configure the array manager.



Display Name: Protected Site VTrak S3000

Manager Type: Promise VTrak S3000

IP Address: 192.168.1.1

Username: Username

Password: ********

Note that *Promise VTrak S3000* appears as the Manager Type for SRA.

2. Enter the IP address and login information for each VTrak S3000 server.

   Refer to your *Site Recovery Manager User Guide* for detailed instructions about configuring and using SRM.

Chapter 2: Recovery and Failback

Recovery

When a disaster occurs and the protected site is not available, you run the recovery plan so that the system fails over to the server at the recovery site and you can access the replicated data.

Important

You must have:

- Configured SRM protection groups on the protected site
- A recovery plan at the recovery site

Following the instructions in the *Site Recovery Manager User Guide*.

Testing your Recovery Plan

Testing your recovery plan is an essential step. You can test your recovery plan through Site Recovery Manager (SRM), without affecting your production environment.

When you test your recovery plan, the VTrak S3000 server creates SnapshotViews from the latest point-in-time Snapshots of the relevant replicated devices on the recovery-side VTrak S3000 server and assigns the Snapshots to the recovery Host client. SRM finds these newly attached devices and imports any virtual machines on them.

When the test is finished, VTrak S3000 server unassigns the temporary SnapshotViews from the recovery Host client and deletes them.

To test your recovery plan:

1. Use the **Test Recovery Plan** option in SRM to execute the recovery plan in test mode.
2. When you are finished testing your recovery plan, use the **Stop** action in SRM to end the test.

If an error occurs, SnapshotViews remain assigned to the recovery Host. If this happens, an administrator must manually unassign and delete these SnapshotViews in the Management Console.

When a Disaster Occurs

A disaster occurs when the primary protected site is not available and replication has stopped. In that scenario, you run the recovery plan to fail-over the replicated devices on the recovery side and assign them to the recovery host.

The actions required to run the recovery plan differ depending upon whether the VTrak S3000 server at the protected site is *online* or *offline*.

Important

Failover leaves replicated devices in a *failed over* state. After the disaster has been resolved and the protected site is available again, you must manually perform a failback to return all systems to their original state.

VTrak S3000 Server at the Protected Site is Offline

If the VTrak S3000 server at the protected site is offline, use the **Run Recovery Plan** option in SRM.

VTrak S3000 Server at the Protected Site is Online

1. For each primary virtual device with replication enabled, manually unassign the device from its protected host and from all other SAN clients to which it may be assigned.
2. Use the **Synchronize** option under the Replication menu on the Management Console to synchronize replication for each virtual device.
3. Use the **Run Recovery Plan** option in SRM.

See the *VTrak S3000 Server User Manual* for instructions on unassigning virtual devices and synchronizing replication.

Fail-back

After a failover, replicated devices remain in a failed-over state. After the disaster has been resolved and the protected site is available again, you must perform a failback to return all hosts and storage to their original state.

In this example, before failover:

- Site A is the original *protected* site and its virtual devices are the *primary* devices.
- Site B is the original *recovery* site and its virtual devices are the *replica* devices.

After failover:

- The virtual devices at Site B are the *primary* devices and are assigned to the recovery Host.
- The virtual devices at Site A are the *replica* devices.

To failback both sites to their original state:

1. In the Management Console, connect to the VTrak S3000 server at Site B.

   The virtual devices that were failed-over are currently present as SAN Resources under the VTrak S3000 server at Site B.

   - If the VTrak S3000 server at Site A was *offline* when failover occurred, continue with step 2.
   - If the VTrak S3000 server at Site A was *online* when failover occurred, skip step 2 and continue with step 3.

2. For each failed-over virtual device at Site B, under the **Replication** menu choose the **Repair** option to repair the replication.

   See the *VTrak S3000 Server User Manual* for instructions on repairing replicated devices.

3. For each failed-over virtual device at Site B, under the **Replication** menu choose the **Synchronize** option to fully replicate the devices to Site A.

   Steps 2 and 3 re-establish replication with Site B now acting as the primary site and Site A as the recovery site.

4. Perform a fail-back to complete the rest of the process.

   For more information, see the *Site Recovery Manager User Guide*.

5. Unassign the virtual devices from the SAN client on the VTrak S3000 server at Site B.

   For more information, see “Recovery” on page 3.

6. Execute your recovery plan at Site A.
7. In the Management Console, connect to the VTrak S3000 server at Site A.
8. For each virtual device at Site A, under the **Replication** menu choose the **Repair** option to repair the replication.
9. For each virtual device at Site A, under the **Replication** menu choose the **Synchronize** option to fully replicate those devices to Site B.

Chapter 3: Troubleshooting

This Troubleshooting chapter contains information helpful in resolving common errors that might occur when configuring or using Storage Replication Adapter (SRA) with VMware vCenter Site Recovery Manager (SRM). The chapter also helps you to examine the SRA log files so you can diagnose other issues that are not explicitly covered by this document.

For issues related to using the Promise Failback Manager to perform a site failback, see the *Failback Manager Troubleshooting Guide*.

For general SRM-related issues that are outside the scope of this document, see the Troubleshooting chapter of the *SRM Administration Guide*.

Determining the SRA Version

To see which version of SRA is installed on a host:

In the Windows command line interface and under the SRA folder, run the **command.pl -v**.

Sample input,

```
> perl “C:\Program Files\VMware\VMware vCenter Site Recovery
Manager\scripts\SAN\IPStor\Common”
```

Important

If Perl is not in the path, enter the full path to the **Perl.exe** executable file.

Corresponding output,

```
Promise Storage Replication Adapter for VMware SRM
Version 4.0 (Build 400)
```

Generating Checksums of Installed Files

When you contact Technical Support, they might ask you to compute MD5 hash checksums of certain installed files under the SRA folder.

To compute MD5 hash checksums:

1. Go to http://support.microsoft.com/kb/841290, then download and install the *Microsoft File Checksum Integrity Verifier* utility.
2. At the Windows command-line, run the **fciv** utility with the full path to the file whose checksum you want to compute.

   You might be required to:

   - Enter the full path to the **fciv.exe** executable file.
   - Add the **fciv.exe** executable file to the PATH environment variable.

   For more information, see the documentation that comes with the utility.

   For example,

   ```
   > fciv “C:\Program Files\VMware\VMware vCenter Site Recovery
   Manager\scripts\SAN\IPStor\Common”
   ```

In most cases, you are asked to compute checksums of the following files under the SRA folder:

- command.pl
- discoverArrays.pl
- discoverLuns.pl
- failover.pl
- falcommon.pm
- handler.pl

Configuring Protection Errors

When you use the Configure Array Managers wizard while configuring protection, SRM invokes the SRA to collect information about the storage servers and their replicated devices. This section covers errors commonly encountered during this step.

Array script files not found

After installing the SRA, you attempt to configure array managers, but SRM cannot find any array script files.

Cause: SRM requires a restart before it can find a newly installed SRA.

Solution: Use the Windows Service Control Manager to stop and restart the Site Recovery Manager service.

Failed to connect to array management system

You enter the address and credentials for an array manager and click the **Connect** button, but SRM cannot connect to the storage array.

Cause: The storage server is not accessible.

Solution: Make sure the storage server is running. Ping the storage server IP address from the SRM server to verify the connection. If you entered the *hostname* of the storage server instead of its *IP address*, verify that the SRM server can resolve the hostname.

Failed to authenticate with array management system

You enter the address and credentials for an array manager and click the **Connect** button, SRM reports that authentication failed for the storage array.

Cause: You have the wrong credentials or entered the wrong credentials.

Solution: Make sure you entered the correct username and password in the Configure Array Managers wizard.

Make sure your user account exists on the storage server.

Unknown peer array for storage server

When you connect to a protected site storage server in the Configure Array Managers wizard, the hostname of the storage server is displayed under the Array ID column, but the Peer Array is listed as *Unknown*.

Cause: There are no devices configured with replication on the storage server.

Solution: Verify that

- You entered the correct storage server information wizard.
- Replication is correctly configured for the virtual devices containing the datastores you want to protect in SRM.

Cause: The credentials you entered do not belong to an administrative user.

Solution: Verify that the credentials you entered are for an account with administrative privileges.

No replicated datastores found

On the final screen of the Configure Array Managers wizard, SRM cannot find any replicated datastores.

Error Message:

```
Replicated devices could not be matched with datastores in the inventory.
```

Cause: The storage server did not assign any disks to the ESX host.

Solution: Verify that

- You entered the correct storage server information in the wizard.
- The storage server on the protected site serves virtual devices to the ESX hosts on the protected site.
- The storage server on the recovery site contains the replica disks of the original protected virtual disks.
- The SAN Clients corresponding to the ESX hosts are configured correctly.

Cause: There are no devices configured with replication on the storage server.

Solution: Verify that replication is correctly configured for the virtual devices containing the datastores you want to protect in SRM.

Cause: The credentials entered do not belong to an administrative user.

Solution: Verify that the credentials you enter are for an account with administrative privileges.

Note

If none of these situations apply, examine the SRM/SRA log files to further diagnose the issue. For more information, see “Examining Log Files” on page 7.

Testing or Running Recovery Plans

When you test or run a recovery plan, SRM invokes the SRA to one of the following actions:

- Create SnapshotViews of replica devices.
- Fail-over the replicated devices and assign them to the appropriate ESX hosts on the recovery site.

This section covers errors commonly encountered during this step.

Array with key <hostname> not found

When you test or run a recovery plan, SRM stops at the Prepare Storage step because the recovery side storage server was not found.

Cause: SRM cannot match the hostname of the recovery site storage server to the hostname returned by the protected site storage server.

Solution: Make sure the hostnames match, as described below.

When you first enter the protected site storage server, the wizard shows you:

- The hostname of the *storage server* under the **Array ID** column.
- The hostname of the *expected replica server* under the **Peer Array** column.

These names must match in your recovery plan.

Other failures during Prepare Storage step

There are several reasons why SRM fails during the Prepare Storage step of testing or running a recovery plan. Examine the SRM/SRA log files to pinpoint the error. See the sample error messages under “Examining Log Files,” below.

Examining Log Files

SRA outputs log messages that are captured by SRM. The SRA saves messages to an optional log file in its installation directory. Examine both of these logs to pinpoint errors in SRA operations. This section describes:

- How to access the log files.
- What to look for in the log files.
- Common error messages.

Examining SRA Logs

SRA saves log messages to a log file in its installation directory which is located in a sub-directory of the SRM installation path. By default, SRM is installed under the following location:

C:\Program Files\VMware\VMware vCenter Site Recovery Manager

The SRA log file is located at:

<SRM Installation Path>\scripts\SAN\IPStor\Common\sra-output.log

If you do not see a log file, the feature might be disabled. Enable logging in the SRA configuration file located at:

<SRM Installation Path>\scripts\SAN\IPStor\Common\config.ini

To edit the **config.ini** file:

1. Right-click the **config.ini** file and select **Properties** from the popup menu.
2. Make sure the Read Only box is NOT checked.
3. Open the file in a text editor.
4. Under the [Logfile] section, set the LogfileEnable value to **1**.
5. Set the LogfileLevel value to **trivia**.

After you have enabled the SRA log file, perform some SRA operations to generate fresh messages.

Examining SRM Logs

The SRM log file also lists SRA messages interspersed with SRM messages. And the SRM log contains messages about how SRM interacts with SRA. As a result, these logs could be more helpful.

The location of the SRM log files and the method of accessing them differs based on the version of Windows and the version of SRM. For more information, see the *SRM Administration Guide*.

SRA Log Format

Each message in the SRA log is prefixed by a string with the following format:

```
[<Timestamp> <Module> <Process ID> <Message Level>]
```

Use the *timestamp* to identify the messages logged at the approximate time the error occurred.

Modules that describe SRA operation at the time when the message is logged are:

- **discoverArrays** – Provides SRM with basic information about a storage server.
- **discoverLuns** – Provides SRM with a list of replicated devices on a server.
- **failover** – SRM invokes this module when you test or run a recovery plan.

Levels indicate the nature of the message:

- **Error** – SRA encountered a serious problem.
- **Warning** – SRA encountered a problem.
- **Trivia** – The most detailed message.
- **Verbose** – Some details in the message.
- **Info** – The least detailed message.

Resolving Common Error Messages

Message:

```
ISCLI Error: Failed to connect to server <address>
```

Cause: The storage server is not accessible.

Solution: Make sure the storage server is running. Ping the storage server IP address from the SRM server to verify the connection. If you entered the *hostname* of the storage server instead of its *IP address*, verify that the SRM server can resolve the hostname.

Message:

```
ISCLI Error: Authentication failed at server <address>
```

Cause: SRA fails to log into the storage server using the credentials supplied.

Solution: Verify that

- You entered the correct username and password in the Configure Array Managers wizard.
- The user has an account on the storage server.

Message:

```
Snapshot is disabled for the virtual device. Error: 0x09010049
```

Cause: SRA cannot create a SnapshotView of a device because Snapshot is not enabled.

Solution: In the Management Console, connect to the recovery side storage server and enable Snapshot on the replica device.

Message:

```
No Snapshots found, cannot perform failover test
```

Cause: SRA cannot create a SnapshotView of a device because the replica device has no Snapshots.

Solution: In the Management Console, connect to the recovery side storage server. Create at least one Snapshot for the replica device, either manually or by forcing a replication sync.

Message:

```
ISCLI Error: SnapshotView already exists
```

Cause: SRA cannot create a SnapshotView of the latest Snapshot of a replica device because a SnapshotView already exists. A SnapshotView exists because:

- You created a SnapshotView manually.
- An error during a previous test resulting in the SnapshotView remaining undeleted.

Solution: In the Management Console, connect to the recovery side storage server. Manually unassign the SnapshotView from any SAN clients and delete the SnapshotView.

Important

If the SnapshotView is assigned to one or more ESX servers, make sure the VMs on it are shut down and cleanly removed from inventory before unassigning the SnapshotView.

Message:

```
Cannot perform reversal while primary virtual device is still attached to a SAN client on the
primary SAN server
Unassign the primary virtual device from all SAN clients before running failover
```

Cause: SRA cannot failover a device because the original virtual device on the protected site is still assigned to one or more SAN Clients.

Solution: When running a recovery plan with the protected site still online, shut down all VMs, unassign virtual devices from all SAN Clients on the protected side storage server, and run a sync replication on these devices before you begin the failover process.

Message:

```
No SAN clients found with initiators specified for replica device <ID>
The device cannot be assigned
```

Cause: SRA cannot assign the device to the ESX host as requested by SRM because a SAN Client matching the initiators of the ESX host cannot be found.

Solution: Verify that

- A SAN Client exists under the recovery side storage server for each ESX host in the recovery site. Make sure
- The SAN Clients are correctly configured and map to the iSCSI or Fibre Channel initiators used by the ESX hosts.

Index