UNH-IOL iSCSI CONSORTIUM

iSNS Interoperability Test Suite
Version 1.0

Technical Document

Last Updated: July 21, 2008

iSCSI Consortium
InterOperability Laboratory
University of New Hampshire

Digitally signed by UNH-IOL
Date: 2008.07.21
11:05:25 -04'00'

121 Technology Drive, Suite 2
Durham, NH 03824
Phone: (603) 862-1908
Fax: (603) 862-4181
http://www.iol.unh.edu/iscsi

TABLE OF CONTENTS

The University of New Hampshire
InterOperability Laboratory

MODIFICATION RECORD

[1]August 22, 2006 (Version 0.1) DRAFT RELEASE
Atsushi Fukayama: Initial Release

[2]August 29, 2006 (Version 0.2) DRAFT RELEASE
David Woolf: Formatted as UNH-IOL Test Suite

[3]September 15, 2006 (Version 0.3) DRAFT RELEASE
David Woolf: Completed Groups 3 and 4

[4]November 1, 2006 (Version 0.4) DRAFT RELEASE
David Woolf: Completed Group 5 and Appendices.

[5]December 5, 2006 (Version 0.5) DRAFT RELEASE
David Woolf: Various updates.

[6]July 10, 2008 (Version 1.0) RELEASE
Peter Scruton: Performed modifications including: rewording the introduction, and an attempt to reorganize the wording and organization of certain procedures and observable results for clarity. Substantive changes were made to test 5.3.

ACKNOWLEDGMENTS

The University of New Hampshire would like to acknowledge the efforts of the following individuals in the development of this test suite.

Atsushi Fukayama	Nippon Telephone and Telegraph (NTT)
Peter Scruton	UNH InterOperability Laboratory (UNH-IOL)
David Woolf	UNH InterOperability Laboratory (UNH-IOL)

INTRODUCTION

The University of New Hampshire's InterOperability Laboratory (IOL) is an institution designed to improve the interoperability of standards based products by providing an environment where a product can be tested against other implementations of a standard.

These tests are designed to determine if an iSCSI product supporting iSNS can Interoperate with other devices that are also designed to support iSNS. iSNS is specified in RFC 4171 *"Internet Storage Name Service"* published by the IETF (hereafter referred to as the "iSNS Standard"). Successful completion of all tests contained in this suite does not guarantee that the tested device will successfully operate with all other iSNS products.

The tests contained in this document are organized in order to simplify the identification of information related to a test, and to facilitate in the actual testing process. Tests are separated into groups, primarily in order to reduce setup time in the lab environment, however the different groups typically also tend to focus on specific aspects of device functionality. A two-number, dot-notated naming system is used to catalog the tests, where the first number indicates the general group of tests. The second number indicates the test number within that group. This format allows for the addition of future tests in the appropriate groups without requiring the renumbering of the subsequent tests.

The test definitions themselves are intended to provide a high-level description of the motivation, resources, procedures, and methodologies specific to each test. Formally, each test description contains the following sections:

Purpose

The purpose is a brief statement outlining what the test attempts to achieve. The test is written at the functional level.

References

This section specifies all reference material *external* to the test suite, including the specific sub clause references for the test in question, and any other references that might be helpful in understanding the test methodology and/or test results. External sources are always referenced by a bracketed number (e.g., [1]) when mentioned in the test description. Any other references in the test description that are not indicated in this manner refer to elements within the test suite document itself (e.g., "Appendix 5.A", or "Table 5.1.1-1")

Resource Requirements

The requirements section specifies the test hardware and/or software needed to perform the test. This is generally expressed in terms of minimum requirements, however in some cases specific equipment manufacturer/model information may be provided.

Last Modification

This specifies the date of the last modification to this test.

Discussion

The discussion covers the assumptions made in the design or implementation of the test, as well as known limitations. Other items specific to the test are covered here as well.

Test Setup

The setup section describes the initial configuration of the test environment. Small changes in the configuration should not be included here, and are generally covered in the test procedure section (next).

Test Procedure

The procedure section of the test description contains the systematic instructions for carrying out the test. It provides a cookbook approach to testing, and may be interspersed with observable results.

Observable Results

This section lists the specific observables that can be examined by the tester in order to verify that the devices are operating properly. When multiple values for an observable are possible, this section provides a short discussion on how to interpret them. The determination of a pass or fail outcome for a particular test is generally based on the successful (or unsuccessful) detection of a specific observable.

Possible Problems

This section contains a description of known issues with the test procedure, which may affect test results in certain situations. It may also refer the reader to test suite appendices and/or other external sources that may provide more detail regarding these issues.

REFERENCES

The following documents are referenced in this text:

[1] IETF RFC 4171

GROUP 1: REGISTRATION AND DISCOVERY TEST

Overview: This group of tests verifies that iSNS clients can register and discover Storage Nodes properly.

Test #1.1: Start and Stop Target Device

Purpose: To verify iSNS target client can properly register target Storage Nodes and initiator client can discover them.

Reference: iSNS standard

Resource Requirements:

- An iSNS server.
- Local management interface of the server that is capable of monitoring registered Storage Nodes.
- An iSCSI initiator device that is capable of iSNS client.
- Local management interface of the initiator device that is capable of monitoring discovered target Storage Nodes.
- An iSCSI target device that is capable of iSNS client.
- Monitoring facilities capable of capturing and decoding iSNS PDUs.

Last Modification: May 22, 2008

Discussion: After starting up iSCSI target device, the iSNS target client should register all target Storage Nodes in the device to iSNS server, so that iSNS initiator clients can discover the target Storage Nodes. When the target device stops the service, the iSNS target client should deregister all the target Storage Nodes and initiator clients should be notified of it.

In this test, the target device should have several target Storage Nodes, if possible. This is because interoperability problems can occur while the client is registering the second and later nodes, which results in “Source Unknown” or “Source Unauthorized” error.

There are mainly two methods for initiators to automatically detect the target’s start / stop: State Change Notification and query repetition. For more details, see Appendices. This test does not depend which method is supported.

Test setup:

- The iSNS server, iSCSI initiator device, iSCSI target device are connected and out of service.
- The iSCSI initiator and target device should be configured with iSNS client functionality turned on.
- The iSNS initiator and target client should be manually configured with the server address.
- All Storage Nodes are in the same Discovery Domain that is enabled.

Procedure:

- Start the monitoring facility to capture iSNS PDUs.
- Startup the iSNS server.
- Startup the iSCSI initiator.
- C1: Check list of registered Storage Nodes by the server’s management interface.
- C2: Check information of the registered Storage Nodes in the list obtained in C1.
- Startup the iSCSI target.
- C3: Check list of registered Storage Nodes by the server’s management interface.
- C4: Check information of the registered Storage Nodes in the list obtained in C3.
- C5: Check list of discovered target Storage Nodes by the initiator’s management interface.
- C6: Check information of the discovered Storage Nodes in the list obtained in C5.
- Stop the iSCSI target.
- C7: Check list of registered Storage Nodes by the server’s management interface.
- C8: Check list of discovered target Storage Nodes by the initiator’s management interface.
- Stop the iSCSI initiator.
- C9: Check list of registered Storage Nodes by the server’s management interface.

Observable Results:

- C1: Verify that the initiator Storage Node is in the list.
- C2: Verify that the initiator Storage Node's information the interface provides is correct. The information includes *iSCSI Name*, *iSCSI Node Type*, *iSCSI Node Alias*, *ESI Port*, *SCN Port*, and *Portal IP Address*.
- C3: Verify that all target Storage Nodes are in the list.
- C4: Verify that, for each target Storage Node, information is correct, including *iSCSI Name*, *iSCSI Node Type*, *iSCSI Node Alias*, *Portal IP Address*, *Portal TCP/UDP Port*, and association between *Portal Group Tag* and Portal.
- C5: Verify that all target Storage Nodes are in the list.
- C6: Verify that, for each target Storage Node, information is correct, including *iSCSI Name*, *iSCSI Node Type*, *iSCSI Node Alias*, *Portal IP Address*, *Portal TCP/UDP Port*, and association between *Portal Group Tag* and Portal.
- C7: Verify that any target Storage Nodes are NOT in the list.
- C8: Verify that any target Storage Nodes are NOT in the list.
- C9: Verify that the initiator Storage Node is NOT in the list.

Possible Problems:

- Some management interfaces, especially GUI-based ones, are implemented in a reactive manner, which do not reflect the latest information until the tester explicitly commands to update the information.
- Some ways of updating the information invoke iSNS DevAttrQry command. This prevents the tester from verifying the initiator can automatically detect the target.
- If the initiator device has firewall functionality, SCN message sent by server should be dropped. This results in the initiator being unable to detect the target's startup and stop.
- Dependent on whether the Discovery Domain the Storage Nodes belong to is Default DD or others, some server implementations change its behavior in SCN propagation, which affects results of some verification.

Test #1.2: Start and Stop Initiator Device

Purpose: To verify iSNS initiator client can properly register initiator Storage Node and discover target Storage Nodes registered before.

Reference: iSNS standard

Resource Requirements:

- An iSNS server.
- Local management interface of the server that is capable of monitoring registered Storage Nodes.
- An iSCSI initiator device that is capable of iSNS client.
- Local management interface of the initiator device that is capable of monitoring discovered target Storage Nodes.
- An iSCSI target device that is capable of iSNS client.
- Monitoring facilities capable of capturing and decoding iSNS PDUs.

Last Modification: May 22, 2008

Discussion: After starting up iSCSI initiator device, the iSNS initiator client should register Storage Node within the device to the iSNS server. The initiator should discover target Storage Nodes already registered after the registration. When the initiator device stops the service, the iSNS initiator client should deregister the initiator Storage Node.

In this test, the target device should have several target Storage Nodes, if possible. This is because interoperability problems can occur while the client is registering the second and later nodes, which results in “Source Unknown” or “Source Unauthorized” error.

There are mainly two methods for initiators to automatically detect the target’s start / stop: State Change Notification and query repetition. For more details, see Appendices. This test does not depend which method is supported.

Test setup:

- The iSNS server, iSCSI initiator device, iSCSI target device are connected and out of service.
- The iSCSI initiator and target device should be configured with iSNS client functionality turned on.
- The iSNS initiator and target client should be manually configured with the server address.
- All Storage Nodes are in the same Discovery Domain that is enabled.

Procedure:

- Start the monitoring facility to capture iSNS PDUs.
- Startup the iSNS server.
- Startup the iSCSI target.
- C1: Check list of registered Storage Nodes by the server’s management interface.
- C2: Check information of the registered Storage Nodes in the list obtained in C1.
- Startup the iSCSI initiator.
- C3: Check list of registered Storage Nodes by the server’s management interface.
- C4: Check information of the registered Storage Nodes in the list obtained in C3.
- C5: Check list of discovered target Storage Nodes by the initiator’s management interface.
- C6: Check information of the discovered Storage Nodes in the list obtained in C5.
- Stop the iSCSI initiator.
- C7: Check list of registered Storage Nodes by the server’s management interface.
- Stop the iSCSI target.
- C8: Check list of registered Storage Nodes by the server’s management interface.

If the same set of devices, i.e., the server, initiator, and target, passed the test #1.1, procedures C2 and C4 can be omitted.

Observable Results:

- C1: Verify that all target Storage Nodes are in the list.
- C2: Verify that, for each target Storage Node, information is correct, including *iSCSI Name*, *iSCSI Node Type*, *iSCSI Node Alias*, *Portal IP Address*, *Portal TCP/UDP Port*, and association between *Portal Group Tag* and Portal.
- C3: Verify that the initiator Storage Node is in the list.
- C4: Verify that the initiator Storage Node's information the interface provides is correct. The information includes *iSCSI Name*, *iSCSI Node Type*, *iSCSI Node Alias*, and *Portal IP Address*.
- C5: Verify that all target Storage Nodes are in the list.
- C6: Verify that, for each target Storage Node, information is correct, including *iSCSI Name*, *iSCSI Node Type*, *iSCSI Node Alias*, *ESI Port*, *SCN Port*, *Portal IP Address*, *Portal TCP/UDP Port*, and association between *Portal Group Tag* and Portal.
- C7: Verify that the initiator Storage Node is NOT in the list.
- C8: Verify that any target Storage Nodes are NOT in the list.

Possible Problems:

- Some management interfaces, especially GUI-based ones, are implemented in a reactive manner, which do not reflect the latest information until the tester explicitly commands to update the information.
- Some ways of updating the information invoke iSNS DevAttrQry command. This prevents the tester from verifying the initiator can automatically detect the target.
- If the initiator device has firewall functionality, SCN message sent by server should be dropped. This results in the initiator being unable to detect the targets startup and stop.
- Dependent on whether the Discovery Domain the Storage Nodes belong to is Default DD or others, some server implementations change its behavior in SCN propagation, which affects results of some verification.

Test #1.3: Add and Remove Discovery Domain Membership of Target

Purpose: To verify the a change of Discovery Domain configuration regarding target Storage Nodes can be detected by initiator in the same Discovery Domain.

Reference: iSNS standard

Resource Requirements:

- An iSNS server.
- Local management interface of the server that is capable of monitoring registered Storage Nodes.
- An iSCSI initiator device that is capable of iSNS client.
- Local management interface of the initiator device that is capable of monitoring discovered target Storage Nodes.
- An iSCSI target device that is capable of iSNS client.
- Monitoring facilities capable of capturing and decoding iSNS PDUs.

Last Modification: August 8, 2006

Discussion: When new target Storage Nodes are added to Discovery Domain, initiators in the DD should discover them automatically. Likewise, when target Storage Nodes are removed, initiators should detect the removal. These functionalities allow operator of storage systems to provision new storage resource to the initiators online and without going to the initiator sites. And they can notify the initiators of unavailability of the target Storage Nodes from remote site.

Test setup:

- The iSNS server, iSCSI initiator device, iSCSI target device are connected and out of service.
- The iSCSI initiator and target device should be configured with iSNS client functionality turned on.
- The iSNS initiator and target client should be manually configured with the server address.
- The iSCSI target device should be configured with two Storage Nodes. They are designated as “Target0” and “Target1” in this test.
- The iSCSI initiator device has one Storage Node designated as “Initiator0” in this test.
- Discovery Domain of the three Storage Nodes are configured as the table shown below:

Initial DD configuration.

Discovery Domain Set	DDS Status	Discovery Domain	Storage Node
DDS0	Disabled	DD0	Target0, Target1
DDS1	Enabled	DD1	Initiator0

Procedure:

- Start the monitoring facility to capture iSNS PDUs.
- Startup the iSNS server.
- Startup the iSCSI initiator.
- C1: Check list of registered Storage Nodes within DD1 by the server’s management interface.
- Startup the iSCSI target.
- C2: Check list of registered Storage Nodes within DD0 by the server’s management interface.
- C3: Check list of registered Storage Nodes within DD1 by the server’s management interface.
- C4: Check list of discovered target Storage Nodes by the initiator’s management interface.
- Add all target Storage Nodes into *DD1* by the server’s management interface.
- C5: Check list of registered Storage Nodes within DD1 by the server’s management interface.
- C6: Check list of discovered target Storage Nodes by the initiator’s management interface.
- Remove the target Storage Nodes from *DD1*.
- C7: Check list of registered Storage Nodes within DD1 by the server’s management interface.
- C8: Check list of discovered target Storage Nodes by the initiator’s management interface.

Observable Results:

- C1: Verify that the initiator Storage Node is in the list.
- C2: Verify that all target Storage Nodes are in the list.
- C3: Verify that any target Storage Nodes are NOT in the list.
- C4: Verify that any target Storage Nodes are NOT in the list.
- C5: Verify that all target Storage Nodes are in the list.
- C6: Verify that all target Storage Nodes are in the list.
- C7: Verify that any target Storage Nodes are NOT in the list.
- C8: Verify that any target Storage Nodes are NOT in the list.

Possible Problems:

- Some management interfaces, especially GUI-based ones, are implemented in a reactive manner, which do not reflect the latest information until the tester explicitly commands to update the information.
- Some ways of updating the information invoke iSNS DevAttrQry command. This prevents the tester from verifying the initiator can automatically detect the target.
- If the initiator device has firewall functionality, SCN message sent by server should be dropped. This results in the initiator being unable to detect the targets startup and stop.
- Dependent on whether the Discovery Domain the Storage Nodes belong to is Default DD or others, some server implementations change its behavior in SCN propagation, which affects results of some verification.

Test #1.4: Add and Remove Discovery Domain Membership of Initiator

Purpose: To verify that a change of Discovery Domain regarding an initiator Storage Node can be detected by the initiator so that it can find target Storage Nodes in new DD and no longer access ones in an old DD.

Reference: iSNS standard

Resource Requirements:

- An iSNS server.
- Local management interface of the server that is capable of monitoring registered Storage Nodes.
- An iSCSI initiator device that is capable of iSNS client.
- Local management interface of the initiator device that is capable of monitoring discovered target Storage Nodes.
- An iSCSI target device that is capable of iSNS client.
- Monitoring facilities capable of capturing and decoding iSNS PDUs.

Last Modification: May 22, 2008

Discussion: When initiator Storage Node is added to a Discovery Domain, the initiator should discover target Storage Nodes in the DD automatically. Likewise, when the initiator is removed, it should detect disappearance of the target Storage Nodes. These functionalities allow operator of storage systems to provision new storage resource to the initiators online and without going to the initiator sites. And they can notify the initiators of unavailability of the target Storage Nodes from remote site.

Test setup:

- The iSNS server, iSCSI initiator device, iSCSI target device are connected and out of service.
- The iSCSI initiator and target device should be configured with iSNS client functionality turned on.
- The iSNS initiator and target client should be manually configured with the server address.
- The iSCSI target device should be configured with two Storage Nodes. They are designated as “Target0” and “Target1” in this test.
- The iSCSI initiator device has one Storage Node designated as “Initiator0” in this test.
- Discovery Domain of the three Storage Nodes are configured as the table shown below:

Initial DD configuration.

Discovery Domain Set	DDS Status	Discovery Domain	Storage Node
DDS0	Disabled	DD0	Initiator0
DDS1	Enabled	DD1	Target0, Target1

Procedure:

- Start the monitoring facility to capture iSNS PDUs.
- Startup the iSNS server.
- Startup the iSCSI target.
- C1: Check list of registered Storage Nodes within DD1 by the server’s management interface.
- C2: Check list of registered Storage Nodes within DD0 by the server’s management interface.
- Startup the iSCSI initiator.
- C3: Check list of registered Storage Nodes within DD0 by the server’s management interface.
- C4: Check list of registered Storage Nodes within DD1 by the server’s management interface.
- C5: Check list of discovered target Storage Nodes by the initiator’s management interface.
- Add the initiator Storage Node into *DD1* by the server’s management interface.
- C6: Check list of registered Storage Nodes within DD1 by the server’s management interface.
- C7: Check list of discovered target Storage Nodes by the initiator’s management interface.
- Remove the initiator Storage Node from *DD1*.
- C8: Check list of registered Storage Nodes within DD1 by the server’s management interface.
- C9: Check list of discovered target Storage Nodes by the initiator’s management interface.

Observable Results:

- C1: Verify that all target Storage Nodes are in the list.
- C2: Verify that no Storage Nodes are in the list.
- C3: Verify that the initiator Storage Node is in the list.
- C4: Verify that the initiator Storage Node is NOT in the list.
- C5: Verify that no target Storage Nodes are in the list.
- C6: Verify that the initiator Storage Node is in the list.
- C7: Verify that all target Storage Nodes are in the list.
- C8: Verify that the initiator Storage Node is NOT in the list.
- C9: Verify that no target Storage Nodes are in the list.

Possible Problems:

- Some management interfaces, especially GUI-based ones, are implemented in a reactive manner, which do not reflect the latest information until the tester explicitly commands to update the information.
- Some ways of updating the information invoke iSNS DevAttrQry command. This prevents the tester from verifying the initiator can automatically detect the target.
- If the initiator device has firewall functionality, SCN message sent by server should be dropped. This results in the initiator being unable to detect the targets startup and stop.
- Dependent on whether the Discovery Domain the Storage Nodes belong to is Default DD or others, some server implementations change its behavior in SCN propagation, which affects results of some verification.

Test #1.5: Enable / Disable Discovery Domain

Purpose: To verify initiator clients in disabled Discovery Domain do not detect target clients while ones in enabled Discovery Domain do.

Reference: iSNS standard

Resource Requirements:

- An iSNS server.
- Local management interface of the server that is capable of monitoring registered Storage Nodes.
- An iSCSI initiator device that is capable of iSNS client.
- Local management interface of the initiator device that is capable of monitoring discovered target Storage Nodes.
- An iSCSI target device that is capable of iSNS client.
- Monitoring facilities capable of capturing and decoding iSNS PDUs.

Last Modification: December 5, 2006

Discussion: Within disabled Discovery Domains, i.e., ones not belonging to any enabled Discovery Domain Set, any information about their members must not be exchanged. This allows SAN administrators to temporarily prevent initiators from discovering and connecting to targets for maintenance reasons without permanently deleting the Discovery Domain.

At the timing when a Discovery Domain is enabled or disabled, SCN should be triggered so that the initiator can query for target discovery.

If a target Storage Node and an initiator Storage Node are both in two different Discovery Domains and only one DD is disabled, the initiator should not lose the target.

Test setup:

- An iSNS server, iSCSI initiator device, iSCSI target device are connected and out of service.
- The iSCSI initiator and target device should be configured with iSNS client functionality turned on.
- The iSNS initiator and target client should be manually configured with the server address.
- The iSCSI target device should be configured with two Storage Nodes. They are designated as “Target0” and “Target1” in this test.
- The iSCSI initiator device has one Storage Node designated as “Initiator0” in this test.
- Discovery Domain of the three Storage Nodes are configured as the table “DD configuration (i)” shown below:

DD configuration (i)

Discovery Domain Set	DDS Status	Discovery Domain	Storage Node
DDS0	Disabled	DD0	Initiator0, Target0, Target1
DDS1	Enabled	DD1	Initiator0, Target1

DD configuration (ii)

Discovery Domain Set	DDS Status	Discovery Domain	Storage Node
DDS0	Disabled	DD0	Initiator0, Target0, Target1
DDS1	Enabled	DD0	Initiator0, Target0, Target1
		DD1	Initiator0, Target1

Procedure:

- Startup the iSNS server.
- Startup the iSCSI initiator.
- Startup the iSCSI target.
- C1: Check list of registered Storage Nodes within DD0 by the server’s management interface.
- C2: Check list of registered Storage Nodes within DD1 by the server’s management interface.
- C3: Check list of discovered target Storage Nodes by the initiator’s management interface.
- Apply the DD configuration (ii) by the server’s management interface.

- C4: Check list of discovered target Storage Nodes by the initiator’s management interface.
- Apply the DD configuration (i) by the server’s management interface.
- C5: Check list of discovered target Storage Nodes by the initiator’s management interface.
- Stop the iSCSI target.
- C6: Check list of discovered target Storage Nodes by the initiator’s management interface.

Observable Results:

- C1: Verify that Initiator0, Target0 and Target1 are all in the node list.
- C2: Verify that Initiator0 and Target1 are both in the node list and Target0 is not.
- C3: Verify that Target1 is in the target list and Target0 is not.
- C4: Verify that Target0 and Target1 are both in the target list.
- C5: Verify that Target1 is in the target list and Target0 is not.
- C6: Verify that neither Target0 nor Target1 is not in the target list.

Possible Problems:

- Some management interfaces, especially GUI-based ones, are implemented in a reactive manner, which do not reflect the latest information until the tester explicitly commands to update the information.
- Some ways of updating the information invoke iSNS DevAttrQry command. This prevents the tester from verifying the initiator can automatically detect the target.
- If the initiator device has firewall functionality, SCN message sent by server should be dropped. This results in the initiator being unable to detect the targets startup and stop.
- Dependent on whether the Discovery Domain the Storage Nodes belong to is Default DD or others, some server implementations change its behavior in SCN propagation, which affects results of some verification.

Test #1.6: Start and Stop Target Storage Nodes On-The-Fly

Purpose: To verify dynamically added target Storage Nodes can be properly registered / deregistered and detected by initiator.

Reference: iSNS standard

Resource Requirements:

- An iSNS server, initiator client, and target client.
- Local management resource capable of monitoring registered initiator and target nodes.
- Monitoring facilities capable of capturing and decoding iSCSI PDUs.

Last Modification: May 22, 2008

Discussion: Some iSCSI target devices allow users to add / delete Storage Nodes while the device is operating. Those target devices should be able to register / deregister the newly added / deleted Storage Nodes. Furthermore, initiators should detect those changes.

Test setup: The iSNS server, iSCSI initiator device, iSCSI target device are connected and out of service. The target device should be configured with two Storage Nodes. All Storage Nodes of target and initiator are in the same Discovery Domain that is enabled.

Procedure:

- Start the monitoring facility to capture iSNS PDUs.
- Startup the iSNS server.
- Startup the iSCSI initiator.
- Make the initiator discover the server by manually specifying the server address.
- C1: Check list of registered Storage Nodes within DD by the server's management interface.
- C2: Observe the information provided by the server about the initiator.
- After the initiator Storage Node becomes visible on the server console startup the iSCSI target.
- Make the target discover the server by manually specifying the server address.
- C3: Check list of registered Storage Nodes within DD by the server's management interface.
- C4: Observe the information provided by the server about the target Storage Nodes.
- C5: Check list of discovered target Storage Nodes by the initiator's management interface.
- C6: Observe the information provided by the initiator about the target Storage Nodes.
- After all target Storage Nodes become visible on the server and initiator console, add two new Storage Nodes within the target device.
- C7: Check list of registered Storage Nodes within DD by the server's management interface.
- C8: Observe the information provided by the server about the target Storage Nodes.
- C9: Check list of discovered target Storage Nodes by the initiator's management interface.
- C10: Observe the information provided by the initiator about the target Storage Nodes.
- After the new Storage Nodes become visible on the server and initiator console, delete the two target Storage Nodes that were registered at the startup.
- C11: Check list of registered Storage Nodes within DD by the server's management interface.
- C12: Check list of discovered target Storage Nodes by the initiator's management interface.
- After the deleted Storage Nodes become invisible on the server and initiator console, add two new Storage Nodes within the target device.
- C13: Check list of registered Storage Nodes within DD by the server's management interface.
- C14: Check list of discovered target Storage Nodes by the initiator's management interface.
- Wait until the new Storage Nodes become visible on the server and initiator console.
- Stop the iSCSI target.
- C15: Check list of registered Storage Nodes within DD by the server's management interface.
- C16: Check list of discovered target Storage Nodes by the initiator's management interface.

Observable Results:

- C1: Verify that the initiator Storage Node becomes visible from the server after the initiator started.
- C2: Verify that the initiator Storage Node information the server provides is correct.
- C3: Verify that the target Storage Nodes, which were registered at startup all become visible from the server.
- C4: Verify that the target Storage Nodes information the server provides is correct.
- C5: Verify that the target Storage Nodes, which were registered at startup all become visible from the initiator.
- C6: Verify that the target Storage Nodes information the initiator provides is correct.
- C7: Verify that the target Storage Nodes, which were registered at startup and on the fly, all become visible from the server after the target started.
- C8: Verify that the target Storage Nodes information the server provides is correct.
- C9: Verify that the target Storage Nodes, which were registered at startup and on the fly, all become visible from the initiator after the target started.
- C10: Verify that the target Storage Nodes information the initiator provides is correct.
- C11: Verify that the target Storage Nodes, which were registered at startup become no longer visible from the server after the target started while the Storage Nodes that were added on the fly remain visible to the server.
- C12: Verify that the target Storage Nodes, which were registered at startup become no longer visible from the initiator after the target started while the Storage Nodes that were added on the fly remain visible to the initiator.
- C13: Verify that only the four target Storage Nodes that were added on the fly remain visible to the server.
- C14: Verify that only the four target Storage Nodes that were added on the fly remain visible to the initiator.
- C15: Verify that the target Storage Nodes, which were deregistered at device stop and on the fly, all become invisible from the initiator.
- C16: Verify that the target Storage Nodes, which were deregistered at device stop and on the fly, all become invisible from the server.

Possible Problems:

- Some target devices do not support on-the-fly addition and deletion of Storage Nodes. In that case, this test item does not apply.
- The management consoles can be implemented in a reactive manner, which do not reflect the latest information until the tester refreshes the console.
- Some ways of refreshing the console can invoke queries to acquire the latest information. This prevents the tester from verifying the initiator can automatically detect the target. See Appendix D.
- There can be no management console provided. In such cases, using other interface like command-line interface and system log file should be considered. Those options can be considered also for getting the latest information if the console does not display the latest information.

Test #1.7: Start and Stop Target Devices within Two Isolated Discovery Domains

Purpose: To verify information of target Storage Nodes addition / removal is limited within Discovery Domains.

Reference: iSNS standard

Resource Requirements:

- An iSNS server.
- One or two initiator devices dependent on whether the device permits two initiator Storage Nodes within the device. Name the nodes as "Initiator0" and "Initiator1"
- One or two target devices dependent on whether the device permits two target Storage Nodes within the device. Name the nodes as "Target0" and "Target1".
- Local management resource capable of monitoring registered initiator and target nodes.
- Monitoring facilities capable of capturing and decoding iSCSI PDUs.

Last Modification: May 22, 2008

Discussion: For initiators, information of targets belonging to the same Discovery Domain must be available, while those in different Discovery Domains must not.

Test setup: The iSNS server, iSCSI initiator device, iSCSI target device are connected and out of service. Discovery Domain configuration is listed below.

Initial DD configuration.

Discovery Domain Set	DDS Status	Discovery Domain	Storage Node
DDS0	Enabled	DD0	Initiator0, Target0
DDS1	Enabled	DD1	Initiator1, Target1

Procedure:

- Startup the iSNS server.
- Startup the iSCSI initiators.
- C1: Check list of registered Storage Nodes within DD by the server's management interface.
- C2: Observe the information provided by the server about the initiator Storage Nodes.
- Startup the iSCSI targets.
- C3: Check list of discovered target Storage Nodes by the server's management interface.
- C4: Observe the information provided by the server about the target Storage Nodes.
- Wait until Target1 becomes visible on Initiator1's console.
- C5 and C6: Check to see what Target Storage Nodes are visible from each of the Initiator Storage Nodes.
- C7: Observe the information provided by the server about the target Storage Nodes.
- Stop Target0 and Target1.
- Wait until Target1 becomes invisible from Initiator1.
- Wait until Target0 and Target1 becomes invisible from the server.
- C8: Check to see if any Target Storage Nodes are visible from each of the Initiator Storage Nodes.

Observable Results:

- C1: Verify that the initiator Storage Nodes become visible from the server.
- C2: Verify that the initiator Storage Nodes information the server provides is correct.
- C3: Verify that the target Storage Nodes become all visible from the server after the target started.
- C4: Verify that the target Storage Nodes information the server provides is correct.
- C5: Verify that Target0 and Target1 are visible from Initiator0 and Initiator1, respectively.
- C6: Verify that Target0 and Target1 are invisible from each other and from Initiator1 and Initiator0, respectively.
- C7: Verify that the target Storage Nodes information the server provides is correct.

- C8: Verify that Target0 and Target1 become no longer visible from Initiator0 and Initiator1, respectively, after the targets are stopped.

Possible Problems:

- The management consoles can be implemented in a reactive manner, which do not reflect the latest information until the tester refreshes the console.
- Some ways of refreshing the console can invoke queries to acquire the latest information. This prevents the tester from verifying the initiator can automatically detect the target. See Appendix D.
- There can be no management console provided. In such cases, using other interface like command-line interface and system log file should be considered. Those options can be considered also for getting the latest information if the console does not display the latest information.

Test #1.8: Start and Stop Target Device Belonging to Two Discovery Domains

Purpose: To verify initiator clients in different Discovery Domains can detect addition / removal of target belonging to all of those Discovery Domains.

Reference: iSNS standard

Resource Requirements:

- An iSNS server.
- One or two initiator devices dependent on whether the device permits two initiator Storage Nodes within the device. Name the nodes as “Initiator0” and “Initiator1”
- One or two target devices dependent on whether the device permits two target Storage Nodes within the device. Name the nodes as “Target0” and “Target1”.
- Local management resource capable of monitoring registered initiator and target nodes.
- Monitoring facilities capable of capturing and decoding iSCSI PDUs.

Last Modification: May 22, 2008

Discussion: If an iSNS client triggering an SCN belongs to more than one Discovery Domains, the SCN should be delivered to clients within all the Discovery Domains.

Test setup: The iSNS server, iSCSI initiator device, iSCSI target device are connected and out of service. Discovery Domain configuration is listed below.

DD configuration

Discovery Domain Set	DDS Status	Discovery Domain	Storage Node
Default DDS	Enabled	DD0	Initiator0, Target0
		DD1	Initiator1, Target0, Target1

Procedure:

- Startup the iSNS server.
- Startup the iSCSI initiators.
- Wait until the initiator Storage Nodes, i.e., Initiator0 and Initiator1, become visible on the server console.
- C1 and C2: Observe the Storage Nodes that are visible to the server.
- Startup the iSCSI targets.
- Wait until the target Storage Nodes, i.e., Target0 and Target1, become visible on the server console.
- C3 and C4: Observe the Storage Nodes that are visible to the server
- Wait until Target0 becomes visible on Initiator0.
- Wait until Target1 becomes visible on Initiator0’s console.
- C5 and C6: Check to see what Target Storage Nodes are visible from each of the Initiator Storage Nodes.
- C7: Observe the information the initiator Storage Nodes report about the target Storage Nodes.
- Stop Target0 and Target1.
- Wait until Target0 becomes invisible from Initiator0.
- Wait until Target1 becomes invisible from Initiator0 and Initiator1.
- C8: Check to see what Target Storage Nodes are visible from each of the Initiator Storage Nodes.

Observable Results:

- C1: Verify that the initiator Storage Nodes become visible from the server after the initiator started.
- C2: Verify that the initiator Storage Nodes information the server provides is correct.
- C3: Verify that the target Storage Nodes become all visible from the server after the target started.
- C4: Verify that the target Storage Nodes information the server provides is correct.
- C5: Verify that Target0 is visible from Initiator0 and Initiator1.
- C6: Verify that Target1 is visible from Initiator1 and invisible from Initiator0.

- C7: Verify that the target Storage Nodes information the initiators provide is correct.
- C8: Verify that Target0 and Target1 become invisible from Initiator0 and Initiator1.

Possible Problems:

- The management consoles can be implemented in a reactive manner, which do not reflect the latest information until the tester refreshes the console.
- Some ways of refreshing the console can invoke queries to acquire the latest information. This prevents the tester from verifying the initiator can automatically detect the target. See Appendix D.
- There can be no management console provided. In such cases, using other interface like command-line interface and system log file should be considered. Those options can be considered also for getting the latest information if the console does not display the latest information.

Test #1.9: Start and Stop Target Devices within Different Discovery Domains Sharing One Initiator

Purpose: To verify target clients in different Discovery Domains can detect addition / removal of target belonging to all of those Discovery Domains.

Reference: iSNS standard

Resource Requirements:

- An iSNS server.
- One or two initiator devices dependent on whether the device permits two initiator Storage Nodes within the device. Name the nodes as “Initiator0” and “Initiator1”
- One or two target devices dependent on whether the device permits two target Storage Nodes within the device. Name the nodes as “Target0” and “Target1”.
- Local management resource capable of monitoring registered initiator and target nodes.
- Monitoring facilities capable of capturing and decoding iSCSI PDUs.

Last Modification: May 23, 2008

Discussion: If an iSNS client triggering an SCN belongs to more than one Discovery Domains, the SCN should be delivered to clients within all the Discovery Domains.

Test setup: The iSNS server, iSCSI initiator device, iSCSI target device are connected and out of service. Discovery Domain configuration is listed below.

DD configuration

Discovery Domain Set	DDS Status	Discovery Domain	Storage Node
Default DDS	Enabled	DD0	Initiator0, Target0
		DD1	Initiator0, Initiator1, Target1

Procedure:

- Startup the iSNS server.
- Startup the iSCSI targets. If the targets have management console, make it visible.
- Wait until the target Storage Nodes, i.e., Target0 and Target1, become visible on the server console.
- C1 and C2: Observe the Storage Nodes that are visible to the server.
- Startup the iSCSI initiators. If the initiators have management console, make it visible.
- Wait until the initiator Storage Nodes, i.e., Initiator0 and Initiator1, become visible on the server console.
- C3 and C4: Observe the Storage Nodes that are visible to the server.
- Wait until Initiator0 becomes visible on Target0 and Target1.
- C5: Observe the Storage Nodes that are visible to the Target Storage Nodes.
- Wait until Initiator1 becomes visible on Target1’s console.
- C6 and C7: Observe the Storage Nodes that are visible to the Target Storage Nodes.
- Stop Target0 and Target1.
- Wait until Initiator0 becomes invisible from Target0 and Target1.
- Wait until Initiator1 becomes invisible from Target1.
- C8: Observe the Storage Nodes that are visible to the Initiator Storage Nodes.

Observable Results:

- C1: Verify that the target Storage Nodes become visible from the server.
- C2: Verify that the target Storage Nodes information the server provides is correct.
- C3: Verify that the initiator Storage Nodes become all visible from the server after the initiator started.
- C4: Verify that the initiator Storage Nodes information the server provides is correct.
- C5: Verify that Initiator0 is visible from Target0 and Target1.
- C6: Verify that Initiator1 is visible from Target1 and invisible from Target0.

- C7: Verify that the initiator Storage Nodes information as observed from the Target Storage Nodes is correct.
- C8: Verify that Target0 and Target1 become invisible from Initiator0 and Initiator1, after the initiators are stopped.

Possible Problems:

- The management consoles can be implemented in a reactive manner, which do not reflect the latest information until the tester refreshes the console.
- Some ways of refreshing the console can invoke queries to acquire the latest information. This prevents the tester from verifying the initiator can automatically detect the target. See Appendix D.
- There can be no management console provided. In such cases, using other interface like command-line interface and system log file should be considered. Those options can be considered also for getting the latest information if the console does not display the latest information.

GROUP 2: ANOMALY TEST

Overview: This group of tests verifies that iSNS server and clients can properly handle anomaly conditions in consistent ways and continue to work together after recovery.

Test #2.1: Sudden Disconnection and Reconnection with Target Device

Purpose: To verify that, when communication between target device and server is lost, server deregisters the target and that, after recovery from the communication failure, the target is re-registered.

Reference: iSNS standard

Resource Requirements:

- iSNS server, target, and initiator devices.
- Local management resource capable of monitoring registered initiator and target nodes.
- Monitoring facilities capable of capturing and decoding iSCSI PDUs.

Last Modification: July 2, 2008

Discussion: When server lost reachability with client, it must deregister the client entry after a certain implementation-dependent interval elapsed (*either twice the ESI Interval or the Registration Period*). After communication recovery, the client should notice the deregistration and try to re-register itself. Other clients which are interested in the disconnected client's event should notice the deregistration and re-registration.

Test setup: The iSNS server, iSCSI initiator device, iSCSI target device are connected and out of service. The target device should have at least two target Storage Nodes, if possible. All Storage Nodes are in one enabled Discovery Domain.

Procedure:

- Start the monitoring facility to capture iSNS PDUs.
- Startup the iSNS server.
- Startup the iSCSI initiator.
- C1: Wait until the initiator Storage Node becomes visible on the server console.
- Startup the iSCSI target. If the target has management console, make it visible.
- C2: Wait until the target Storage Nodes become visible on the server console.
- C3: Wait until the target Storage Nodes become visible on the initiator console.
- Unplug network cable of the target device that is used for communication with the server.
- C4: Check every 1 minute if the target Storage Node entries disappear from the server console. Report the latency from the unplugging, if disappeared. Continue to check if the Storage Nodes have disappeared until after the expiration of *ESI Interval* x2 or *Registration Period*.
- If the Storage Nodes did not disappear from the server console then restart the server and ensure that the Storage Nodes are not present on the server console before continuing.
- C5: Check if the target Storage Nodes disappeared from the initiator console.
- Plug the network cable back in.
- C6 and C7: Check every 1 minute if the target Storage Node entries appear on the server console. Report the latency from the plugging, if appeared. Continue to check if the Storage Nodes have disappeared until after the expiration of *ESI Interval* or *Registration Period* x 5 seconds.
- If the target Storage Node does not appear on the server console then restart the target and ensure that the Target Storage Nodes are present on the server console before continuing.
- C8 and C9: Wait until the target Storage Nodes appear on the initiator console.

Observable Results:

- C1: Verify that the initiator Storage Node becomes visible from the server after the initiator started.
- C2: Verify that the target Storage Nodes become all visible from the server after the target started.
- C3: Verify that the target Storage Nodes become all visible from the initiator.
- C4: Verify that the target Storage Nodes become all invisible from the server after unplugging.
- C5: Verify that the target Storage Nodes become all invisible from the initiator.
- C6: Verify that the target Storage Nodes become all visible from the server after plugging.
- C7: Verify that the target Storage Nodes information the server provides is correct.

- C8: Verify that the target Storage Nodes become all visible from the initiator after plugging.
- C9: Verify that the target Storage Nodes information the initiator provides is correct.

Possible Problems:

- Some management interfaces, especially GUI-based ones, are implemented in a reactive manner, which do not reflect the latest information until the tester explicitly commands to update the information.
- Some ways of updating the information invoke iSNS DevAttrQry command. This prevents the tester from verifying the initiator can automatically detect the target.
- If the initiator device has firewall functionality, SCN message sent by server should be dropped. This results in the initiator being unable to detect the targets startup and stop.
- Dependent on whether the Discovery Domain the Storage Nodes belong to is Default DD or others, some server implementations change its behavior in SCN propagation, which affects results of some verification.

Test #2.2: Sudden Disconnection and Reconnection with Initiator Device

Purpose: To verify that, when communication between initiator device and server is lost, server deregisters the initiator and that, after recovery from the communication failure, the initiator is re-registered.

Reference: iSNS standard

Resource Requirements:

- iSNS server, target, and initiator devices.
- Local management resource capable of monitoring registered initiator and target nodes.
- Monitoring facilities capable of capturing and decoding iSCSI PDUs.

Last Modification: July 3, 2008

Discussion: When server lost reachability with client, it must deregister the client entry after a certain implementation-dependent interval elapsed. After communication recovery, the client should notice the deregistration and try to re-register itself. Other clients which are interested in the disconnected client's event should notice the deregistration and re-registration.

Test setup: The iSNS server, iSCSI initiator device, iSCSI target device are connected and out of service. The target device should have at least two target Storage Nodes, if possible. All Storage Nodes are in one enabled Discovery Domain.

Procedure:

- Start the monitoring facility to capture iSNS PDUs.
- Startup the iSNS server.
- Startup the iSCSI target.
- C1: Wait until the target Storage Nodes become visible on the server console.
- Startup the iSCSI initiator. If the initiator has management console, make it visible.
- C2: Wait until the initiator Storage Node becomes visible on the server console.
- C3: Wait until the target Storage Nodes become visible on the initiator console.
- Unplug network cable of the initiator device that is used for communication with the server.
- C4: Check every 1 minute if the Initiator Storage Node entries disappear from the server console. Report the latency from the unplugging, if disappeared. Continue to check if the Initiator Storage Nodes have disappeared until after the expiration of *ESI Interval* x2 or *Registration Period*.
- C5: Check to see if the target Storage Nodes are visible from the Initiator.
- Plug the network cable.
- C6 and C7: Check every 1 minute if the initiator Storage Node entries appear on the server console. Report the latency from the plugging, if appeared. Continue to check if the Initiator Storage Nodes have disappeared until after the expiration of *ESI Interval* or *Registration Period* x 5 seconds.
- If the initiator Storage Nodes are not visible on the server console then restart the initiator and ensure that the Target Storage Nodes are present on the server console before continuing.
- C8 and C9: Wait until the target Storage Nodes become visible on the initiator console.

Observable Results:

- C1: Verify that the target Storage Nodes become all visible from the server after the target started.
- C2: Verify that the initiator Storage Node becomes visible from the server after the initiator started.
- C3: Verify that the target Storage Nodes become visible from the initiator.
- C4: Verify that the initiator Storage Node becomes invisible from the server after unplugging.
- C5: Verify that the target Storage Nodes become invisible from the initiator.
- C6: Verify that the initiator Storage Node becomes visible from the server after plugging.
- C7: Verify that the initiator Storage Node information the server provides is correct.
- C8: Verify that the target Storage Nodes become visible from the initiator after plugging.
- C9: Verify that the target Storage Node information the initiator provides is correct.

Possible Problems:

- Some management interfaces, especially GUI-based ones, are implemented in a reactive manner, which do not reflect the latest information until the tester explicitly commands to update the information.
- Some ways of updating the information invoke iSNS DevAttrQry command. This prevents the tester from verifying the initiator can automatically detect the target.
- If the initiator device has firewall functionality, SCN message sent by server should be dropped. This results in the initiator being unable to detect the targets startup and stop.
- Dependent on whether the Discovery Domain the Storage Nodes belong to is Default DD or others, some server implementations change its behavior in SCN propagation, which affects results of some verification.

Test #2.3: Sudden Termination of Server and Recovery

Purpose: To verify that, when server is inappropriately terminated without deregistering clients, clients survived and the server recovered can communicate properly.

Reference: iSNS standard

Resource Requirements:

- iSNS server, target, and initiator devices.
- Local management resource capable of monitoring registered initiator and target nodes.
- Monitoring facilities capable of capturing and decoding iSCSI PDUs.

Last Modification: July 3, 2008

Discussion: Abnormal termination of server can make the server lose part of iSNS database content, which results in internal state inconsistency between the server and clients. In other words, server could have no registration entry of a client while the client recognizes it is registered at the server.

After the server recovered, the server and clients should continue to work properly. Elements of this test are outside the scope of the iSNS standard and are therefore implementation specific. This is an informative test.

Test setup: The iSNS server, iSCSI initiator device, iSCSI target device are connected and out of service. The target device should have at least two target Storage Nodes, if possible. All Storage Nodes are in one enabled Discovery Domain.

Procedure:

- Startup the iSNS server.
- Startup the iSCSI initiator and target. If they have management console, make it visible.
- C1: Wait until all Storage Nodes become visible on the server console.
- Unplug all network cables of the server that are used for communication with the clients.
- Stop and restart the server.
- Plug the network cables after the server is restarted.
- **If the Initiator or Target Storage Node is still visible in the server console (i.e. the Storage Nodes were not deleted from the Server Console after the server restart):**
    - Use a Traffic Analyzer to monitor traffic between the Initiator or Target and the Server for Registration or Query from the Initiator or Target to the Server.
    - Wait for either ESI Interval x 3 or Registration Period to elapse. If no Registration of Query is seen, stop then restart the Initiator or Target. Verify that after the device restart a Registration occurred.
- **If the Initiator or Target Storage Node is not visible in the server console (i.e. the Storage Nodes were deleted from the Server Console after the server restart):**
    - Wait until the initiator and target Storage Nodes become visible on the server console. Report the latency from the plugging.
    - Wait for either ESI Interval x 3 or Registration Period to elapse. If the initiator or Target does not become visible in the server console in this time, stop then restart the Initiator or Target. Verify that after the device restart a Registration occurred.
- C2 and C3: Observe the Storage Nodes that are present on the server console.
- C4 and C5: Wait until all target Storage Nodes become visible on the initiator console.

Observable Results:

- C1: Verify that the initiator and target Storage Nodes become visible from the server console after the initiator and target are started.
- C2: After unplugging and plugging the server, verify that the initiator and target Storage Nodes are visible from the server after performing the above procedure.
- C3: Verify that the initiator and target Storage Node information the server provides is correct.

- C4: Verify that the target Storage Node become visible from the initiator after performing the above procedure.
- C5: Verify that the target Storage Node information the initiator provides is correct.

Possible Problems:

- The management consoles can be implemented in a reactive manner, which do not reflect the latest information until the tester refreshes the console.
- Some ways of refreshing the console can invoke queries to acquire the latest information. This prevents the tester from verifying the initiator can automatically detect the target. See Appendix D.
- There can be no management console provided. In such cases, using other interface like command-line interface and system log file should be considered. Those options can be considered also for getting the latest information if the console does not display the latest information.

Test #2.4: Sudden Termination of Target Device

Purpose: To verify that, after target recovered from abnormal termination without deregistration, the server and the target can communicate properly.

Reference: iSNS standard

Resource Requirements:

- iSNS server, target, and initiator devices.
- Local management resource capable of monitoring registered initiator and target nodes.
- Monitoring facilities capable of capturing and decoding iSCSI PDUs.

Last Modification: July 3, 2008

Discussion: Abnormal termination of target can result in internal state inconsistency between server and the target. In other words, server could have registration entry of the target while the client recognizes it is not registered yet.

After the target recovered, the server and target should continue to work properly. Elements of this test are outside the scope of the iSNS standard and are therefore implementation specific. This is an informative test.

Test setup: The iSNS server, iSCSI initiator device, iSCSI target device are connected and out of service. The target device should have at least two target Storage Nodes, if possible. All Storage Nodes are in one enabled Discovery Domain.

Procedure:

- Startup the iSNS server.
- Startup the iSCSI initiator and target. If they have management console, make it visible.
- C1: Wait until all Storage Nodes become visible on the server console.
- Unplug network cable of the target that is used for communication with the server.
- Stop and restart the target.
- Plug the network cables after the target is restarted.
- Use a Traffic Analyzer to monitor traffic between the Target and the Server for Registration from the Target to the Server.
- C2 and C3: Wait for either ESI Interval x 3 or Registration Period to elapse. If no Registration of Query is seen, stop then restart Target. Verify that after the device restart a Registration occurred. Report the latency from the plugging to when the Registration occurred.
- C4 and C5: Wait until all target Storage Nodes become visible on the initiator console.

Observable Results:

- C1: Verify that the initiator and target Storage Nodes become visible from the server console after the initiator and target are started.
- C2: After unplugging, restarting and plugging the target, verify that the initiator and target Storage Nodes are visible from the server after performing the above procedure.
- C3: Verify that the initiator and target Storage Node information the server provides is correct.
- C4: Verify that the target Storage Node become visible from the initiator after performing the above procedure.
- C5: Verify that the target Storage Node information the initiator provides is correct.

Possible Problems:

- The management consoles can be implemented in a reactive manner, which do not reflect the latest information until the tester refreshes the console.
- Some ways of refreshing the console can invoke queries to acquire the latest information. This prevents the tester from verifying the initiator can automatically detect the target. See Appendix D.

- There can be no management console provided. In such cases, using other interface like command-line interface and system log file should be considered. Those options can be considered also for getting the latest information if the console does not display the latest information.

Test #2.5: Sudden Termination of Initiator Device

Purpose: To verify that, after initiator recovered from abnormal termination without deregistration, the server and the initiator can communicate properly.

Reference: iSNS standard

Resource Requirements:

- iSNS server, target, and initiator devices.
- Local management resource capable of monitoring registered initiator and target nodes.
- Monitoring facilities capable of capturing and decoding iSCSI PDUs.

Last Modification: July 7, 2008

Discussion: Abnormal termination of initiator can result in internal state inconsistency between server and the initiator. In other words, server could have registration entry of the initiator while the initiator recognizes it is not registered yet.

After the initiator recovered, the server and initiator should continue to work properly. Elements of this test are outside the scope of the iSNS standard and are therefore implementation specific. This is an informative test.

Test setup: The iSNS server, iSCSI initiator device, iSCSI target device are connected and out of service. The target device should have at least two target Storage Nodes, if possible. All Storage Nodes are in one enabled Discovery Domain.

Procedure:

- C1: Startup the iSNS server, iSCSI initiator and iSCSI target. If they have management console, make it visible. Wait until all Storage Nodes become visible on the server console.
- Unplug network cable of the initiator that is used for communication with the server.
- Stop and restart the initiator.
- Plug the network cables after the initiator is restarted.
- Use a Traffic Analyzer to monitor traffic between the Initiator and the Server for Registration from the Initiator to the Server.
- C2 and C3: Wait for either ESI Interval x 3 or Registration Period to elapse. If no Registration of Query is seen, stop then restart Initiator. Verify that after the device restart a Registration occurred. Report the latency from the plugging to when the Registration occurred.
- C4 and C5: Wait until all target Storage Nodes become visible on the initiator console.

Observable Results:

- C1: Verify that the initiator and target Storage Nodes become visible from the server console after the initiator and target are started.
- C2: After unplugging, restarting and plugging the initiator, verify that the initiator and target Storage Nodes are visible from the server after performing the above procedure.
- C3: Verify that the initiator and target Storage Node information the server provides is correct.
- C4: Verify that the target Storage Node become visible from the initiator after performing the above procedure.
- C5: Verify that the target Storage Node information the initiator provides is correct.

Possible Problems:

- The management consoles can be implemented in a reactive manner, which do not reflect the latest information until the tester refreshes the console.
- Some ways of refreshing the console can invoke queries to acquire the latest information. This prevents the tester from verifying the initiator can automatically detect the target. See Appendix D.

- There can be no management console provided. In such cases, using other interface like command-line interface and system log file should be considered. Those options can be considered also for getting the latest information if the console does not display the latest information.

GROUP 3: AUTOMATIC LOGIN / LOGOUT TEST

Overview: This group of tests verifies that iSNS server client system can properly work with iSCSI target initiator system so as to define iSCSI initiator-target nexus and stimulate iSCSI login/logout.

Test #3.1: Login/Logout Trigger by Target Registration/Deregistration

Purpose: Verify that, when target Storage Node is registered / deregistered, initiator in the same DD can automatically login to / logout from the target Storage Node.

Reference: iSNS standard

Resource Requirements:

- iSNS server, target, and initiator devices.
- Local management resource capable of monitoring registered initiator and target nodes.
- Monitoring facilities capable of capturing and decoding iSCSI PDUs.

Last Modification: July 10, 2008

Discussion: When a server loses reachability with client, it must deregister the client entry after a certain implementation-dependent interval elapsed. After communication recovery, the client (target) should notice the deregistration and try to re-register itself. Other clients which are interested in the disconnected client's event should notice the deregistration and re-registration.

Test setup: The iSNS server, iSCSI initiator device, iSCSI target device are connected and out of service. The target device should have at least two target Storage Nodes, if possible. All Storage Nodes are in one enabled Discovery Domain.

Procedure:

- Start the monitoring facility to capture iSNS PDUs.
- Startup the iSNS server. Configure the servers DD to already include the iSCSI target before the target performs registration.
- Startup the iSCSI target.
- C1: Wait until the target Storage Nodes becomes visible on the server console.
- Startup the iSCSI initiator. If the initiator has management console, make it visible.
- C2: Wait until the initiator Storage Node becomes visible on the server console.
- C3: Wait until the target Storage Nodes becomes visible on the initiator console.
- Deregister the target client from the server.
- C4: Check every 1 minute if the Storage Node entries disappear from the server console. Report the latency from the deregistration. Otherwise, expire after *ESI Interval* or *Registration Period* x 5 seconds.
- C5: Wait until the target Storage Nodes become no longer visible on the initiator console.
- Register the target client with the server.
- C6 and C7: Check every 1 minute if the initiator Storage Node entries appear on the server console. Report the latency from the registration, if appeared. Otherwise, expire after *ESI Interval x 2* or *Registration Period*.
- C8 and C9: Wait until the target Storage Nodes become visible on the initiator console.

Observable Results:

- C1: Verify that the target Storage Nodes become all visible from the server after the target started.
- C2: Verify that the initiator Storage Node becomes visible from the server after the initiator started.
- C3: Verify that the target Storage Nodes become visible from the initiator.
- C4: Verify that the target Storage Node becomes no longer visible from the server after deregistration.
- C5: Verify that the target Storage Nodes become no longer visible from the initiator.
- C6: Verify that the target Storage Node becomes visible from the server after registration.
- C7: Verify that the target Storage Node information the server provides is correct.
- C8: Verify that the target Storage Nodes become visible from the initiator after registration.
- C9: Verify that the target Storage Node information the initiator provides is correct.

Possible Problems:

- Some management interfaces, especially GUI-based ones, are implemented in a reactive manner, which do not reflect the latest information until the tester explicitly commands to update the information.
- Some ways of updating the information invoke iSNS DevAttrQry command. This prevents the tester from verifying the initiator can automatically detect the target.
- If the initiator device has firewall functionality, SCN message sent by server should be dropped. This results in the initiator being unable to detect the targets startup and stop.
- Dependent on whether the Discovery Domain the Storage Nodes belong to is Default DD or others, some server implementations change its behavior in SCN propagation, which affects results of some verification.

Test #3.2: Login/Logout Trigger by Adding/Removing Target in Discovery Domain

Purpose: Verify that, when a target Storage Node is added to or removed from a DD, an initiator in the same DD can automatically login to / logout from the target Storage Node.

Reference: iSNS standard

Resource Requirements:

- iSNS server, target, and initiator devices..
- Local management resource capable of monitoring registered initiator and target nodes.
- Monitoring facilities capable of capturing and decoding iSCSI PDUs.

Last Modification: July 10, 2008

Discussion: When a server adds an initiator client to a DD, it is expected that the initiator client performs Login with the target client in the DD.

Test setup: The iSNS server, iSCSI initiator device, iSCSI target device are connected and out of service. The target device should have at least two target Storage Nodes, if possible. All Storage Nodes are in one enabled Discovery Domain.

Procedure:

- Start the monitoring facility to capture iSNS PDUs.
- Startup the iSNS server. Configure the server such that the initiator and target clients will not be added to a DD upon registration.
- Startup the iSCSI target. Allow the target to register with the server.
- C1: Wait until the target Storage Nodes become visible on the server console.
- Startup the iSCSI initiator. If the initiator has management console, make it visible. Allow the initiator to register with the server.
- C2: Wait until the initiator Storage Node becomes visible on the server console.
- Add the initiator and target clients to the same DD.
- C3: Wait until the target Storage Nodes become visible on the initiator console.
- Remove the target from the DD.
- C4: Check every 1 minute if the Target Storage Node entries disappear from the initiator. Report the latency from the DD removal, if disappeared. Otherwise, expire after *ESI Interval* or *Registration Period* x 5 seconds.
- Add the target to the DD.
- C5: Observe the information about the target Storage Nodes as reported by the server.
- Check every 1 minute if the target Storage Node entries appear on the server console. Report the latency from the addition, if appeared. Otherwise, expire after *ESI Interval* or *Registration Period* x 5 seconds.
- C6 and C7: Wait until the target Storage Nodes become visible on the initiator console.

Observable Results:

- C1: Verify that the target Storage Nodes become all visible from the server after the target started.
- C2: Verify that the initiator Storage Node become visible from the server after the initiator started.
- C3: Verify that the target Storage Nodes become visible from the initiator once it is added to the same DD.
- C4: Verify that the target Storage Node becomes no longer visible from the initiator after being removed from the DD.
- C5: Verify that the initiator Storage Node information the server provides is correct.
- C6: Verify that the target Storage Nodes become visible from the initiator after being added to the DD.
- C7: Verify that the target Storage Node information the initiator provides is correct.

Possible Problems:

- Some management interfaces, especially GUI-based ones, are implemented in a reactive manner, which do not reflect the latest information until the tester explicitly commands to update the information.
- Some ways of updating the information invoke iSNS DevAttrQry command. This prevents the tester from verifying the initiator can automatically detect the target.
- If the initiator device has firewall functionality, SCN message sent by server should be dropped. This results in the initiator being unable to detect the targets startup and stop.
- Dependent on whether the Discovery Domain the Storage Nodes belong to is Default DD or others, some server implementations change its behavior in SCN propagation, which affects results of some verification.

Test #3.3: Login/Logout Trigger by Adding/Removing Initiator in Discovery Domain

Purpose: Verify that, when an initiator Storage Node is added to or removed from a DD, an initiator in the same DD can automatically login to / logout from the target Storage Node.

Reference: iSNS standard

Resource Requirements:

- iSNS server, target, and initiator devices.
- Local management resource capable of monitoring registered initiator and target nodes.
- Monitoring facilities capable of capturing and decoding iSCSI PDUs.

Last Modification: July 10, 2008

Discussion: When a server notifies an initiator client that a new target client has been added to the local discovery domain, the initiator client is expected to Login with the added target client.

Test setup: The iSNS server, iSCSI initiator device, iSCSI target device are connected and out of service. The target device should have at least two target Storage Nodes, if possible. All Storage Nodes are in one enabled Discovery Domain.

Procedure:

- Start the monitoring facility to capture iSNS PDUs.
- Startup the iSNS server. Configure the server such that the initiator and target clients will not be added to a DD upon registration.
- Startup the iSCSI target. Allow the target to register with the server.
- C1: Wait until the target Storage Nodes become visible on the server console.
- Startup the iSCSI initiator. If the initiator has management console, make it visible. Allow the initiator to register with the server.
- C2: Wait until the initiator Storage Node becomes visible on the server console.
- Add the initiator and target clients to the same DD.
- C3: Wait until the target Storage Nodes become visible on the initiator console.
- Remove the initiator from the DD.
- C4: Check every 1 minute if the target Storage Node entries disappear from the initiator console. Report the latency from the DD removal, if disappeared. Otherwise, expire after *ESI Interval* or *Registration Period* x 5 seconds.
- Add the initiator to the DD.
- C5: Observe the information about the target Storage Nodes as reported by the server.
- Check every 1 minute if the target Storage Node entries appear on the initiator console. Report the latency from the addition, if appeared. Otherwise, expire after *ESI Interval* or *Registration Period* x 5 seconds.
- C6 and C7: Wait until the target Storage Nodes become visible on the initiator console.

Observable Results:

- C1: Verify that the target Storage Nodes become all visible from the server after the target started.
- C2: Verify that the initiator Storage Node becomes visible from the server after the initiator started.
- C3: Verify that the target Storage Nodes become visible from the initiator once they are added to the same DD.
- C4: Verify that the target Storage Node becomes no longer visible from the initiator after being removed from the DD.
- C5: Observe the information about the initiator Storage Node as reported by the server.
- C6: Verify that the target Storage Nodes become visible from the initiator after plugging.
- C7: Verify that the target Storage Node information the initiator provides is correct.

Possible Problems:

- Some management interfaces, especially GUI-based ones, are implemented in a reactive manner, which do not reflect the latest information until the tester explicitly commands to update the information.
- Some ways of updating the information invoke iSNS DevAttrQry command. This prevents the tester from verifying the initiator can automatically detect the target.
- If the initiator device has firewall functionality, SCN message sent by server should be dropped. This results in the initiator being unable to detect the targets startup and stop.
- Dependent on whether the Discovery Domain the Storage Nodes belong to is Default DD or others, some server implementations change its behavior in SCN propagation, which affects results of some verification.

Test #3.4: Login/Logout Trigger by Enabling/Disabling Discovery Domain

Purpose: Verify that, when a Discovery Domain is enabled or disabled, an initiator will automatically login to / logout from a target Storage Node in the same Discovery Domain.

Reference: iSNS standard

Resource Requirements:

- iSNS server, target, and initiator devices.
- Local management resource capable of monitoring registered initiator and target nodes.
- Monitoring facilities capable of capturing and decoding iSCSI PDUs.

Last Modification: July 7, 2008

Discussion: When a server enables a Discovery Domain, an initiator client is expected to Login with any target clients within the new Discovery Domain.

Test setup: The iSNS server, iSCSI initiator device, iSCSI target device are connected and out of service. The target device should have at least two target Storage Nodes, if possible.

Procedure:

- Start the monitoring facility to capture iSNS PDUs.
- Startup the iSNS server. Configure the server such that the initiator and target clients will not be added to a DD upon registration.
- Startup the iSCSI target. Allow the target to register with the server.
- C1: Wait until the target Storage Nodes become visible on the server console.
- Startup the iSCSI initiator. If the initiator has management console, make it visible. Allow the initiator to register with the server.
- C2: Wait until the initiator Storage Node becomes visible on the server console.
- Add the initiator and target clients to the same DD, then enable the DD.
- C3: Wait until the target Storage Nodes become visible on the initiator console.
- Disable the DD.
- C4: Check every 1 minute if the Storage Node entries disappear from the server console. Report the latency from the DD disablement, if disappeared. Otherwise, expire after *ESI Interval* or *Registration Period* x 5 seconds.
- Enable the DD.
- C5 and C6: Check every 1 minute if the initiator Storage Node entries appear on the server console. Report the latency from the DD enablement, if appeared. Wait at least after *ESI Interval* or *Registration Period* x 5 seconds.
- C7 and C8: Wait until the target Storage Nodes become visible on the initiator console.

Observable Results:

- C1: Verify that the target Storage Nodes become all visible from the server after the target started.
- C2: Verify that the initiator Storage Node becomes visible from the server after the initiator started.
- C3: Verify that the target Storage Nodes become visible from the initiator once they are added to the same DD.
- C4: Verify that the initiator Storage Node becomes no longer visible from the server after the DD is disabled.
- C5: Verify that the initiator Storage Node becomes visible from the server after the DD is enabled.
- C6: Verify that the initiator Storage Node information the server provides is correct.
- C7: Verify that the target Storage Nodes become visible from the initiator.
- C8: Verify that the target Storage Node information the initiator provides is correct.

Possible Problems:

- Some management interfaces, especially GUI-based ones, are implemented in a reactive manner, which do not reflect the latest information until the tester explicitly commands to update the information.
- Some ways of updating the information invoke iSNS DevAttrQry command. This prevents the tester from verifying the initiator can automatically detect the target.
- If the initiator device has firewall functionality, SCN message sent by server should be dropped. This results in the initiator being unable to detect the targets startup and stop.
- Dependent on whether the Discovery Domain the Storage Nodes belong to is Default DD or others, some server implementations change its behavior in SCN propagation, which affects results of some verification.

GROUP 4: TARGET ACCESS CONTROL TEST

Overview: This group of tests verifies that iSCSI target can delegate access control of initiator to iSNS server.

Test #4.1: iSCSI Login Request by Initiator within Discovery Domain

Purpose: Verify that target Storage Node allows iSCSI login request from initiator within the DD the target Storage Node belongs to.

Reference: iSNS standard

Resource Requirements:

- iSNS server, target, and initiator devices.
- Local management resource capable of monitoring registered initiator and target nodes.
- Monitoring facilities capable of capturing and decoding iSCSI PDUs.

Last Modification: July 7, 2008

Discussion: A Login Request PDU to an iSCSI Target from an iSCSI Initiator should be answered with a Login Response PDU with status Accept, if the parameters are conformant to the iSCSI standard and the Login Request originates from within the Discovery Domain of the iSCSI Target.

Test setup: The iSNS server, iSCSI initiator device, iSCSI target device are connected and out of service. The target device should have at least two target Storage Nodes, if possible.

Procedure:

- Start the monitoring facility to capture iSNS and iSCSI PDUs.
- Startup the iSNS server. Configure the server such that the initiator and target clients will be added to a DD upon registration.
- Startup the iSCSI target. Allow the target to register with the server.
- C1: Wait until the target Storage Nodes become visible on the server console.
- Startup the iSCSI initiator. If the initiator has management console, make it visible. Allow the initiator to register with the server.
- C2: Wait until the initiator Storage Node becomes visible on the server console.
- Add the initiator and target clients to the same DD, then enable the DD.
- C3 and C4: Wait until the target Storage Nodes become visible on the initiator console.

Observable Results:

- C1: Verify that the target Storage Nodes become all visible from the server after the target started.
- C2: Verify that the initiator Storage Node becomes visible from the server after the initiator started.
- C3: Verify that the target Storage Nodes become visible from the initiator once they are added to the same DD.
- C4: Verify that the first Login Request from the iSCSI Initiator is accepted by the iSCSI target.

Possible Problems:

- Some management interfaces, especially GUI-based ones, are implemented in a reactive manner, which do not reflect the latest information until the tester explicitly commands to update the information.
- Some ways of updating the information invoke iSNS DevAttrQry command. This prevents the tester from verifying the initiator can automatically detect the target.
- If the initiator device has firewall functionality, SCN message sent by server should be dropped. This results in the initiator being unable to detect the targets startup and stop.
- Dependent on whether the Discovery Domain the Storage Nodes belong to is Default DD or others, some server implementations change its behavior in SCN propagation, which affects results of some verification.

Test #4.2: iSCSI Login Request by Newly Added Initiator within Discovery Domain

Purpose: Verify that target Storage Node allows iSCSI login request from initiator within the DD the target Storage Node belongs to, when the iSCSI initiator was not in the DD when the target node was first added to the DD.

Reference: iSNS standard

Resource Requirements:

- iSNS server, target, and initiator devices.
- Local management resource capable of monitoring registered initiator and target nodes.
- Monitoring facilities capable of capturing and decoding iSCSI PDUs.

Last Modification: July 8, 2008

Discussion: A Login Request PDU to an iSCSI Target from an iSCSI Initiator should be answered with a Login Response PDU with status Accept, if the parameters are conformant to the iSCSI standard and the Login Request originates from within the Discovery Domain of the iSCSI Target.

Test setup: The iSNS server, iSCSI initiator device, iSCSI target device are connected and out of service. The target device should have at least two target Storage Nodes, if possible.

Procedure:

- Start the monitoring facility to capture iSNS and iSCSI PDUs.
- Startup the iSNS server. Configure the server such that the initiator and target clients will not be added to a DD upon registration.
- Startup the iSCSI target. Allow the target to register with the server. Add the target to a DD.
- C1: Wait until the target Storage Nodes become visible on the server console.
- Startup the iSCSI initiator. If the initiator has management console, make it visible. Allow the initiator to register with the server.
- C2: Wait until the initiator Storage Node becomes visible on the server console.
- Add the initiator client to the same DD as the target, then enable the DD.
- C3 and C4: Wait until the target Storage Nodes become visible on the initiator console.

Observable Results:

- C1: Verify that the target Storage Nodes become all visible from the server after the target started.
- C2: Verify that the initiator Storage Node becomes visible from the server after the initiator started.
- C3: Verify that the target Storage Nodes become visible from the initiator once they are added to the same DD.
- C4: Verify that the first Login Request from the iSCSI Initiator is accepted by the iSCSI target.

Possible Problems:

- Some management interfaces, especially GUI-based ones, are implemented in a reactive manner, which do not reflect the latest information until the tester explicitly commands to update the information.
- Some ways of updating the information invoke iSNS DevAttrQry command. This prevents the tester from verifying the initiator can automatically detect the target.
- If the initiator device has firewall functionality, SCN message sent by server should be dropped. This results in the initiator being unable to detect the targets startup and stop.
- Dependent on whether the Discovery Domain the Storage Nodes belong to is Default DD or others, some server implementations change its behavior in SCN propagation, which affects results of some verification.

Test #4.3: iSCSI Login Request by Initiator outside of Discovery Domain

Purpose: Verify that target Storage Node denies iSCSI login request from initiator out of the DD the target Storage Node belongs to.

Reference: iSNS standard

Resource Requirements:

- iSNS server, target, and initiator devices.
- Local management resource capable of monitoring registered initiator and target nodes.
- Monitoring facilities capable of capturing and decoding iSCSI PDUs.

Last Modification: July 8, 2008

Discussion: A Login Request PDU to an iSCSI Target from an iSCSI Initiator outside the Discovery Domain should be answered with a Login Response PDU with status reject, even if the parameters are conformant to the iSCSI standard.

Test setup: The iSNS server, iSCSI initiator device, iSCSI target device are connected and out of service. The target device should have at least two target Storage Nodes, if possible.

Procedure:

- Start the monitoring facility to capture iSNS and iSCSI PDUs.
- Startup the iSNS server. Configure the server such that the initiator and target clients will be added to separate DD's upon registration.
- Startup the iSCSI target. Allow the target to register with the server.
- C1: Wait until the target Storage Nodes become visible on the server console.
- Startup the iSCSI initiator. If the initiator has management console, make it visible. Allow the initiator to register with the server.
- C2: Wait until the initiator Storage Node becomes visible on the server console.
- Provide the IP address of the target to the initiator to begin a Login sequence manually.
- C3: The initiator should transmit a Login Request PDU to the iSCSI client.

Observable Results:

- C1: Verify that the target Storage Nodes become all visible from the server after the target started.
- C2: Verify that the initiator Storage Node becomes visible from the server after the initiator started.
- C3: Verify that the first Login Request from the iSCSI Initiator is rejected by the iSCSI target.

Possible Problems:

- Some management interfaces, especially GUI-based ones, are implemented in a reactive manner, which do not reflect the latest information until the tester explicitly commands to update the information.
- Some ways of updating the information invoke iSNS DevAttrQry command. This prevents the tester from verifying the initiator can automatically detect the target.
- If the initiator device has firewall functionality, SCN message sent by server should be dropped. This results in the initiator being unable to detect the targets startup and stop.
- Dependent on whether the Discovery Domain the Storage Nodes belong to is Default DD or others, some server implementations change its behavior in SCN propagation, which affects results of some verification.

Test #4.4: iSCSI Login Request by Initiator Removed from Discovery Domain

Purpose: Verify that target Storage Node denies iSCSI login request from initiator which has been removed from the DD the target Storage Node belongs to.

Reference: iSNS standard

Resource Requirements:

- iSNS server, target, and initiator devices.
- Local management resource capable of monitoring registered initiator and target nodes.
- Monitoring facilities capable of capturing and decoding iSCSI PDUs.

Last Modification: July 8, 2008

Discussion: A Login Request PDU to an iSCSI Target from an iSCSI Initiator recently removed from the Discovery Domain should be answered with a Login Response PDU with status reject, even if the parameters are conformant to the iSCSI standard.

Test setup: The iSNS server, iSCSI initiator device, iSCSI target device are connected and out of service. The target device should have at least two target Storage Nodes, if possible.

Procedure:

- Start the monitoring facility to capture iSNS and iSCSI PDUs.
- Startup the iSNS server. Configure the server such that the initiator and target clients will be added to the same DD upon registration.
- Startup the iSCSI target. Allow the target to register with the server.
- C1: Wait until the target Storage Nodes become visible on the server console.
- Startup the iSCSI initiator. If the initiator has management console, make it visible. Allow the initiator to register with the server.
- C2: Wait until the initiator Storage Node becomes visible on the server console.
- C3: Wait until the target Storage Nodes becomes visible on the initiator console.
- Remove the initiator from the DD.
- Provide the IP address of the target to the initiator to begin a Login sequence manually.
- C4: The initiator should transmit a Login Request PDU to the iSCSI client.

Observable Results:

- C1: Verify that the target Storage Nodes become all visible from the server after the target started.
- C2: Verify that the initiator Storage Node becomes visible from the server after the initiator started.
- C3: Verify that the target Storage Nodes become visible from the initiator.
- C4: Verify that the first Login Request from the iSCSI Initiator is rejected by the iSCSI target.

Possible Problems:

- Some management interfaces, especially GUI-based ones, are implemented in a reactive manner, which do not reflect the latest information until the tester explicitly commands to update the information.
- Some ways of updating the information invoke iSNS DevAttrQry command. This prevents the tester from verifying the initiator can automatically detect the target.
- If the initiator device has firewall functionality, SCN message sent by server should be dropped. This results in the initiator being unable to detect the targets startup and stop.
- Dependent on whether the Discovery Domain the Storage Nodes belong to is Default DD or others, some server implementations change its behavior in SCN propagation, which affects results of some verification.

Test #4.5: iSCSI Login Request to Wrong Storage Node

Purpose: Verify that target Storage Node denies iSCSI login request from initiator in a different DD than the Storage Node but in a same DD as a different Storage Node in the same device.

Reference: iSNS standard

Resource Requirements:

- iSNS server, target, and initiator devices.
- Local management resource capable of monitoring registered initiator and target nodes.
- Monitoring facilities capable of capturing and decoding iSCSI PDUs.

Last Modification: July 8, 2008

Discussion: A Login Request PDU to an iSCSI Target from an iSCSI Initiator in a different DD than the Storage Node but in the same DD as a different Storage Node in the same device should be answered with a Login Response PDU with status reject, even if the parameters are conformant to the iSCSI standard.

Test setup: The iSNS server, iSCSI initiator device, iSCSI target device are connected and out of service. The target device should have at least two target Storage Nodes, if possible.

Procedure:

- Start the monitoring facility to capture iSNS and iSCSI PDUs.
- Startup the iSNS server. Configure the server such that different nodes on the target clients will be added to separate DD’s upon registration. For convenience we will refer to the first two of these nodes as Target 1 and Target 2.
- Startup the iSCSI target. Allow the target to register with the server. Target 1 and Target 2 should now be in separate DD’s.
- C1: Wait until the target Storage Nodes become visible on the server console.
- Startup the iSCSI initiator. If the initiator has management console, make it visible. Allow the initiator to register with the server. Ensure that the initiator is in the same DD as Target 1, but is not in any DD with Target 2.
- C2: Wait until the initiator Storage Node becomes visible on the server console.
- C3: Wait until Target 1 becomes visible on the initiator console.
- Provide the IP address (and any other necessary information) of Target 2, which is in the other DD, to the initiator to begin a Login sequence manually.
- C4: The initiator should transmit a Login Request PDU to the iSCSI client attempting to Login to Target 2.

Observable Results:

- C1: Verify that the target Storage Nodes become all visible from the server after the target started.
- C2: Verify that the initiator Storage Node becomes visible from the server after the initiator started.
- C3: Verify that the target Storage Nodes become visible from the initiator.
- C4: Verify that the first Login Request from the iSCSI Initiator is rejected by the iSCSI target.

Possible Problems:

- Some management interfaces, especially GUI-based ones, are implemented in a reactive manner, which do not reflect the latest information until the tester explicitly commands to update the information.
- Some ways of updating the information invoke iSNS DevAttrQry command. This prevents the tester from verifying the initiator can automatically detect the target.
- If the initiator device has firewall functionality, SCN message sent by server should be dropped. This results in the initiator being unable to detect the targets startup and stop.

- Dependent on whether the Discovery Domain the Storage Nodes belong to is Default DD or others, some server implementations change its behavior in SCN propagation, which affects results of some verification.

Test #4.6: iSCSI Session Termination Triggered by Initiator Removal

Purpose: Verify that target Storage Node closes an existing iSCSI session with initiator that is removed from DD.

Reference: iSNS standard

Resource Requirements:

- iSNS server, target, and initiator devices.
- Local management resource capable of monitoring registered initiator and target nodes.
- Monitoring facilities capable of capturing and decoding iSCSI PDUs.

Last Modification: July 8, 2008

Discussion: An iSCSI session between an iSCSI Target and Initiatior should be closed by the target if an Initiator is removed from the DD that the target is in.

Test setup: The iSNS server, iSCSI initiator device, iSCSI target device are connected and out of service. The target device should have at least two target Storage Nodes, if possible.

Procedure:

- Start the monitoring facility to capture iSNS and iSCSI PDUs.
- Startup the iSNS server. Configure the server such that the target clients will be added to the same DD upon registration.
- Startup the iSCSI target. Allow the target to register with the server.
- C1: Wait until the target Storage Nodes become visible on the server console.
- Startup the iSCSI initiator. If the initiator has a management console, make it visible. Allow the initiator to register with the server. Add the initiator to the same DD as one of the target nodes.
- C2: Wait until the initiator Storage Node becomes visible on the server console.
- C3: Wait until the target Storage Nodes becomes visible on the initiator console.
- The initiator should transmit a Login Request PDU to the iSCSI client.
- C4: Allow the initiator to open an iSCSI session to the target for transmitting Data.
- C5: Remove the initiator from the DD while a session between the initiator and target is active.

Observable Results:

- C1: Verify that the target Storage Nodes become all visible from the server after the target started.
- C2: Verify that the initiator Storage Node becomes visible from the server after the initiator started.
- C3: Verify that the target Storage Nodes become visible from the initiator.
- C4: Verify that the first Login Request from the iSCSI Initiator is accepted by the iSCSI target.
- C5: Verify that the iSCSI session is closed once the initiator is removed from the DD.

Possible Problems:

- Some management interfaces, especially GUI-based ones, are implemented in a reactive manner, which do not reflect the latest information until the tester explicitly commands to update the information.
- Some ways of updating the information invoke iSNS DevAttrQry command. This prevents the tester from verifying the initiator can automatically detect the target.
- If the initiator device has firewall functionality, SCN message sent by server should be dropped. This results in the initiator being unable to detect the targets startup and stop.
- Dependent on whether the Discovery Domain the Storage Nodes belong to is Default DD or others, some server implementations change its behavior in SCN propagation, which affects results of some verification.
- It may be difficult to get an iSCSI session to stay open long enough for the initiator to be removed from the DD while the session is active. Care must be taken to ensure that the Session is active when the initiator is removed from the DD.

GROUP 5: NETWORK COMPATIBILITY TEST

Overview: This group of tests verifies that set of devices under test works under special network environment.

Test #5.1: iSCSI Access Behind NAT

Purpose: Verify that clients in one private IPv4 address space behind NAT can properly register to a server in a different IPv4 address space, that initiator can discover target, and that initiator can login to the target.

Reference: iSNS standard

Resource Requirements:

- iSNS server, target, and initiator devices.
- Local management resource capable of monitoring registered initiator and target nodes.
- Monitoring facilities capable of capturing and decoding iSCSI PDUs.

Last Modification: July 8, 2008

Discussion: If in the same discovery domain, an iSCSI initiator client should be able to register with a server and begin a Login session with an iSCSI target client, even if the target client is in a different IPv4 address space and behind NAT.

Test setup: The iSNS server, iSCSI initiator device, iSCSI target device are connected but in different IPv4 address spaces. The target device should be behind NAT.

Procedure:

- Start the monitoring facility to capture iSNS and iSCSI PDUs.
- Startup the iSNS server. Configure the server such that the target clients will be added to a DD upon registration.
- Startup the iSCSI target. Allow the target to register with the server.
- C1: Wait until the target Storage Nodes become visible on the server console.
- Startup the iSCSI initiator. If the initiator has management console, make it visible. Allow the initiator to register with the server. Add the initiator to the same DD as one of the target nodes.
- C2: Wait until the initiator Storage Node becomes visible on the server console.
- C3: Wait until the target Storage Nodes becomes visible on the initiator console.
- The initiator should transmit a Login Request PDU to the iSCSI client.
- C4: Allow the initiator to open an iSCSI session to the target for transmitting Data.

Observable Results:

- C1: Verify that the target Storage Nodes become all visible from the server after the target started.
- C2: Verify that the initiator Storage Node becomes visible from the server after the initiator started.
- C3: Verify that the target Storage Nodes become visible from the initiator.
- C4: Verify that the first Login Request from the iSCSI Initiator is accepted by the iSCSI target.

Possible Problems:

- Some management interfaces, especially GUI-based ones, are implemented in a reactive manner, which do not reflect the latest information until the tester explicitly commands to update the information.
- Some ways of updating the information invoke iSNS DevAttrQry command. This prevents the tester from verifying the initiator can automatically detect the target.
- If the initiator device has firewall functionality, SCN message sent by server should be dropped. This results in the initiator being unable to detect the targets startup and stop.
- Dependent on whether the Discovery Domain the Storage Nodes belong to is Default DD or others, some server implementations change its behavior in SCN propagation, which affects results of some verification.
- It may be difficult to get an iSCSI session to stay open long enough for the initiator to be removed from the DD while the session is active. Care must be taken to ensure that the Session is active when the initiator is removed from the DD.

Test #5.2: Multi Port Node

Purpose: Verify that server and clients having two or more NICs for iSCSI and iSNS can properly register at a server, the initiator can discover the target, and that the initiator can login to the target.

Reference: iSNS standard

Resource Requirements:

- iSNS server, target, and initiator devices, at least one of which has multiple ports.
- Local management resource capable of monitoring registered initiator and target nodes.
- Monitoring facilities capable of capturing and decoding iSCSI PDUs.

Last Modification: July 10, 2008

Discussion: If in the same discovery domain, clients with multiple ports, should be able to register with a server which has multiple ports, and begin a Login session with an iSCSI target client which has multiple ports.

Test setup: The iSNS server, iSCSI initiator device, iSCSI target device are connected. At least one of the devices has multiple physical ports.

Procedure:

- Start the monitoring facility to capture iSNS and iSCSI PDUs.
- Startup the iSNS server. Configure the server such that the target clients will be added to a DD upon registration.
- Startup the iSCSI target. Allow the target to register with the server.
- C1: Wait until the target Storage Nodes become visible on the server console.
- Startup the iSCSI initiator. If the initiator has management console, make it visible. Allow the initiator to register with the server. Add the initiator to the same DD as one of the target nodes.
- C2: Wait until the initiator Storage Node becomes visible on the server console.
- C3: Wait until the target Storage Nodes become visible on the initiator console.
- The initiator should transmit a Login Request PDU to the iSCSI client.
- C4: Allow the initiator to open an iSCSI session to the target for transmitting Data.

Observable Results:

- C1: Verify that the target Storage Nodes become all visible from the server after the target started.
- C2: Verify that the initiator Storage Node becomes visible from the server after the initiator started.
- C3: Verify that the target Storage Nodes become visible from the initiator.
- C4: Verify that the first Login Request from the iSCSI Initiator is accepted by the iSCSI target.

Possible Problems:

- Some management interfaces, especially GUI-based ones, are implemented in a reactive manner, which do not reflect the latest information until the tester explicitly commands to update the information.
- Some ways of updating the information invoke iSNS DevAttrQry command. This prevents the tester from verifying the initiator can automatically detect the target.
- If the initiator device has firewall functionality, SCN message sent by server should be dropped. This results in the initiator being unable to detect the targets startup and stop.
- Dependent on whether the Discovery Domain the Storage Nodes belong to is Default DD or others, some server implementations change its behavior in SCN propagation, which affects results of some verification.

Test #5.3: iSCSI Access thru VLAN

Purpose: Verify that, under the condition that two pairs of initiator and targets are in the same DD and different VLANs that clients can properly register at the server and iSCSI sessions can be opened within the same VLAN.

Reference: iSNS standard

Resource Requirements:

- iSNS server, target, and initiator devices.
- Local management resource capable of monitoring registered initiator and target nodes.
- Monitoring facilities capable of capturing and decoding iSCSI PDUs.

Last Modification: July 18, 2008

Discussion: VLANs are used to partition the network so traffic can be segmented. A given port can be a member of multiple VLANs. If an iSNS server is a member of two different VLANs and one of those VLANs contain an Initiator and a Target and the other VLAN contains a different Initiator and Target then all of the Storage Nodes should be able to register with the iSNS server. Even if all of the Storage Nodes are in the same DD neither Initiator should be able to log into a Target Storage Node on the other VLAN. In addition, the failure to log into one Target advertised by the Server should not cause the Initiator to no longer be able to access another Target advertised by the Server.

Test setup: The iSNS server, one iSCSI initiator device, and one iSCSI target device are in one DD in one VLAN. Another initiator device and target device are in the same DD but different VLAN. The IP address of the initiator and target is the same as the IP address of the other initiator and target in the other VLAN.

Procedure:

- Start the monitoring facility to capture iSNS and iSCSI PDUs.
- Configure a VLAN capable switch such that two ports (connected to Initiator 1 and Target 1) are in a single VLAN and two other ports (connected to Initiator 2 and Target 2) are in a separate VLAN. Also a fifth port should be configured (connected to the iSNS Server) such that it is in both VLANs. Ensure that all 5 ports are not members of any other VLANs.
- Startup the iSNS server. Configure the server such that all of the ports in the target and initiator clients will be added to a single DD upon registration. Startup the iSCSI targets. Allow the target to register with the server.
- C1: Wait until the target Storage Nodes become visible on the server console.
- Startup the iSCSI initiator. If the initiator has management console, make it visible. Allow the initiator to register with the server.
- C2: Wait until the two initiator Storage Nodes becomes visible on the server console.
- C3: Wait until the target Storage Nodes becomes visible on the initiator consoles.
- Have Initiator 1 attempt to log into Target 2.
- Have Initiator 2 attempt to log into Target 1.
- Following these failed attempts to log into the targets that the VLAN configuration has made inaccessible, attempt to have Initiator 1 log into Target 1 and Initiator 2 log into Target 2.
- C4 and C5: Verify that the failure to log into the previously attempted Target does not affect the ability of either Initiator 1 to log into Target 1 or Initiator 2 to log into Target 2.

Observable Results:

- C1: Verify that both target Storage Nodes were visible from the server after the target started.
- C2: Verify that both initiator Storage Nodes become visible from the server after the initiators are started.
- C3: Verify that both Initiator 1 and Initiator 2 can see the advertisement of both Target 1 and Target 2 from the Server.
- C4: Verify that Initiator 1 can log into Target 1 after the failure to log into Target 2.
- C5: Verify that Initiator 2 can log into Target 2 after the failure to log into Target 1.

Possible Problems:

- Some management interfaces, especially GUI-based ones, are implemented in a reactive manner, which do not reflect the latest information until the tester explicitly commands to update the information.
- Some ways of updating the information invoke iSNS DevAttrQry command. This prevents the tester from verifying the initiator can automatically detect the target.
- If the initiator device has firewall functionality, SCN message sent by server should be dropped. This results in the initiator being unable to detect the targets startup and stop.
- Dependent on whether the Discovery Domain the Storage Nodes belong to is Default DD or others, some server implementations change its behavior in SCN propagation, which affects results of some verification.
- It may be difficult to get an iSCSI session to stay open long enough for the initiator to be removed from the DD while the session is active. Care must be taken to ensure that the Session is active when the initiator is removed from the DD.

APPENDICES

Overview: Appendices give some additional information to analyze problems that would occur during the interoperability tests.

Appendix A: Registration

Purpose: To show proper methods for an initiator or target client to register with an iSNS server.

Reference: iSNS standard clause 5.6.5

Resource Requirements:

- An iSNS server.
- The client of interest (COI).

Last Modification: October 31, 2006

Discussion: In order for a client to register with an iSNS server it must transmit a ‘Device Attribute Registration Request’ to the iSNS server containing the client type, IP address, port number. The replace bit in the DevAttrReg defines whether the request will update an existing entry or create a new entry.

Test setup: The iSNS server, two clients, and the monitoring facility are connected. The server and the monitoring facility are started up while two clients are not yet.

Procedure:

- Startup COI and the peer client.
- Using a monitoring station capture the DevAttrReg.

Observable Results:

- Verify that the payload of the DevAttrReg contains all Valid Source Attributes, either the iSCSI Name or the FC Port Name WWPN.
- Verify that the payload of the DevAttrReg contains all necessary Message Key Attributes of the registering device.
- Verify that the Delimiter Attribute is set to all 0’s.
- Verify that the payload of the DevAttrReg contains all of the necessary Operating Attributes of the registering device.

Appendix B: Deregistration

Purpose: To show proper methods for an initiator or target client to deregister with an iSNS server.

Reference: iSNS standard clause 5.6.5.4

Resource Requirements:

- An iSNS server.
- The client of interest (COI).

Last Modification: October 31, 2006

Discussion: In order for a client to deregister with an iSNS server it must transmit a 'Device Deregistration Request' to the iSNS server containing the client type, IP address, port number entries to be removed from the iSNS database.

Test setup: The iSNS server, two clients, and the monitoring facility are connected. The server and the monitoring facility are started up while two clients are not yet.

Procedure:

- Startup COI and the peer client.
- Allow the client to register and deregister with the server.
- Using a monitoring station capture the DevDeReg.

Observable Results:

- Determine whether deregistration resulted in SCNs being delivered to all affected client nodes.
- Verify that valid Operating Attributes are contained in the payload of the DevDeReg including Entity Identifier, Portal IP Address, Portal TCP/UDP Port, Portal Index, iSCSI Name, iSCSI Index.

Appendix C: Information Retrieval

Purpose: To show the proper use of DevAttrQry and DevGetNext.

Reference: iSNS standard clause 5.6.5.2, 5.6.5.3

Resource Requirements:

- An iSNS server.
- The client of interest (COI).

Last Modification: October 31, 2006

Discussion: In order for a client to obtain information about other clients registered with an iSNS server it must transmit a ‘Device Attribute Query Request’ or a ‘Device Get Next Request’ to the iSNS server.

Test setup: The iSNS server, two clients, and the monitoring facility are connected. The server and the monitoring facility are started up while two clients are not yet.

Procedure:

- Startup COI and the peer client.
- Allow the client to register and with the server.
- Using a monitoring station capture the DevAttrQry and/or DevGetNext from the COI.

Observable Results:

- If the COI transmits a DevGetNext
  - Determine that the Message Key Attribute is one of the following: an Entity Identifier (EID), iSCSI Name, iSCSI Index, Portal IP Address and TCP/UDP Port, Portal Index, PG Index, FC Node Name WWNN, or FC Port Name WWPN.
  - Verify that the Source Attribute identifies the node initiating the request.
  - Verify that provided Operating Attributes are attributes of the object type identified by the Message Key.
- If the COI transmits a DevAttrQry
  - Verify that provided Operating Attributes are attributes of the object type identified by the Message Key.
  - Verify that DD restrictions are used in the information provided when no Message Key is provided in the DevAttrQry.

Appendix D: Detection of Client Addition and Removal

Purpose:
- To determine supported methods for a client to detect that other client is started / stopped.
- To analyze possible problems in the methods.

Reference: iSNS standard

Resource Requirements:
- An iSNS server.
- The client of interest (COI).
- A peer client: a client of different type than COI, that is, if COI is an initiator, this should be a target, vice versa.
- Monitoring facilities capable of capturing and decoding iSCSI PDUs.

Last Modification: July 21, 2006

Discussion: In order to allow COI to take an action when a peer client is added or removed, COI should detect the change without any user operation intervening. If COI is an initiator, the action could be automatic iSCSI login / logout, for instance. For the automatic detection, implementers can select two methods: State Change Notification and query repetition.

On the other hand, in cases such as an initiator always controlled by human operator, manual detection should be enough. In this case, the operator initiates queries to detect addition / removal of other clients.

This optional test helps the tester determine which method COI supports for the detection and analyze possible problems therein.

Test setup: The iSNS server, two clients, and the monitoring facility are connected. The server and the monitoring facility are started up while two clients are not yet.

Procedure:
- Startup COI.
- Startup the peer client.
- Wait until the peer client becomes visible from COI up to *5 minutes*.
- If expired, manually initiate a query and check the visibility.
- Stop the peer client
- Wait until the peer client becomes invisible from COI up to *5 minutes*.
- If expired, manually initiate a query and check the invisibility.
- Stop COI.

Observable Results:
- Verify that COI properly registers with the server. See Appendix A.
- Determine if COI supports SCN, by checking:
  - that *DevAttrReg* PDU from COI contains "*SCN Port = p*," where the least significant 16 bits of *p* represent a TCP or UDP port number; and
  - that COI sends *SCNReg* PDU.
- Determine if COI supports query repetition, by checking:
  - that COI sends *DevAttrQry* or *DevGetNext* PDUs in a certain interval and the PDUs have "*iSCSI Node Type = t*," where *t* is type of the peer client; and
  - that all of the *DevAttrQry* PDUs do not follow SCN from the server (if all follow, they are stimulated by the SCN).
- If none of SCN and query repetition was verified, COI does not support automatic detection.

CASE 1: SCN supported.

- Verify that COI properly requests SCN, by checking:
  - that, in *DevAttrReg* PDUs, each Storage Node is associated with at least one Portal registered with an *SCN Port* declaration, by using implicit or explicit Portal Group definition;
  - that, for each Storage Node, one *SCNReg* PDU is sent; and
  - that each *SCNReg* PDU has a Source attribute and Message Key attribute whose content is "*iSCSI Name = n*," where *n* is the Storage Node's name and an Operating attribute whose content is "*SCN Bitmap = b*," where *b* is formatted properly to be notified of interesting event.
- Note that SCNReg for a Storage Node that is not associated with any Portal having an SCN Port registered violates the RFC and will be responded with an error in *SCNRegRsp* PDU.

- Verify that the server responds to each *SCNReg* PDU with an *SCNRegRsp* PDU with status code of "*SUCCESS*" and no attributes.

- Verify that the peer client properly registers to the server just after it is started up. See Appendix A.

- Verify that the server sends one or more *SCN* PDUs to each Storage Node registered by COI (i.e., destination Storage Node) just after the peer client was started and the server received *DevAttrReg* PDUs.

- Verify that each set of the *SCN* PDUs for a destination Storage Node have this Storage Node's name in their destination attribute and contain all Storage Nodes newly registered by the peer client (i.e., source Storage Node) in their source attributes.

- Verify that COI sends an *SCNRsp* PDU to the server for each received *SCN* PDU.

- Verify that COI successfully retrieves the information of all of the source Storage Nodes for each of the destination Storage Nodes. See Appendix C.

- Verify that the peer client properly deregisters from the server just after it is stopped. See Appendix B.

- Verify that the server sends one or more *SCN* PDUs to each Storage Node registered by COI (i.e., destination Storage Node) just after the peer client was stopped and the server received *DevAttrDereg* PDUs.

- Verify that each set of the *SCN* PDUs for a destination Storage Node have this Storage Node's name in their destination attribute and contain all Storage Nodes newly deregistered by the peer client (i.e., source Storage Node) in their source attributes.

- Verify that COI sends an *SCNRsp* PDU to the server for each received *SCN* PDU.

- CASE 2: Query repetition supported.
- Verify that COI sends a *DevAttrQry* or *DevGetNext* PDU for each Storage Node COI registered in a certain interval.

- Verify that the DevAttrQry or DevGetNext PDU for a Storage Node has the Storage Node's name in source attribute and an operational attribute of "*iSCSI Node Type = t*," where *t* is type of the peer client.

- Verify that each query is successful. See Appendix C.

- CASE 3: Manual detection.
- Verify that COI sends a *DevAttrQry* or *DevGetNext* PDU for each Storage Node COI registered just after the tester initiates a query.

- Verify that the DevAttrQry or DevGetNext PDU for a Storage Node has the Storage Node's name in source attribute and an operational attribute of "*iSCSI Node Type = t*," where *t* is type of the peer client.

- Verify that each query is successful. See Appendix C.

Possible Problems:

- The management consoles can be implemented in a reactive manner, which do not reflect the latest information until the tester refreshes the console.
- Some ways of refreshing the console can invoke queries to acquire the latest information. This prevents the tester from verifying the initiator can automatically detect the target.
- There can be no management console provided. In such cases, using other interface like command-line interface and system log file should be considered. Those options can be considered also for getting the latest information if the console does not display the latest information.
- If a client supports ESI, it sends *DevAttrReg* PDU with "*ESI Port = n*" where *n* is a port number. Otherwise, it sends *DevAttrReg* PDU with "*Registration Period = s*" where *s* is an interval in seconds in which the client must send requests to the server.