BROCADE

VALIDATION TEST REPORT

Brocade Self-Certification Replication over Brocade IP Extension Test Plan

53-1004216-01
17 May 2016

Contents

Introduction

Brocade has adopted the guidelines defined in IEEE 829.1991, *Standard for Software Test Documentation*. A *test plan* is the hierarchical top-level document among the test documents that is required by the standard.

The purpose of such a test plan is to define, at a very high level, the scope, approach (strategy), resources, and schedule of the testing activities. The test plan also identifies the related features to be tested, the testing tasks to be performed, the personnel responsible for the tasks, and the associated risks.

This test plan defines the scope and approach necessary to release the test item(s) identified in this document. It also identifies related features to be tested.

Objective

This document gives an overview of the test cases as they pertain to Brocade switching products, their corresponding operating system, and storage device specified configurations/applications.

This document is generated from internal SQA test specs, internal and external defect logs, engineering specs, product release notes, previous storage device qualifications, and TSE communications and recommendations.

Strategy

Testing is performed with GA versions of Brocade Fabric OS (FOS) in a heterogeneous environment. Testing is at the system level, including interoperability of storage devices with Brocade Fabric switches.

General Test Case Setup, Monitoring, and Expectations

The test engineer should follow all of these procedures while executing the test cases. Test cases generally follow the same setup procedure for the topology, device configurations for ports, storage devices, and so on. While executing each test case, the tester should monitor the fabric activity and verify the outcome against the general expectations.

General Test Case Setup Procedures

1. Verify that switches and storage devices are operating with the latest testing code and that they are set to pre-determined configuration settings.
2. Ensure that all Ethernet, ISL, adapter, and target ports are physically connected as described in the device list or test case procedures.
3. Check that all devices under test are online. Verify port states, port types, port configurations, speeds, and trunks.
4. Verify that no critical conditions exist on switches, hosts, and targets. On switches, check memory, panic and core dumps, and high availability (HA). Resolve all errors before continuing.
5. Reset all event logs. Additionally, clear all statistics, core files, and port logs on switches.
6. Start switch serial console monitoring for errors and recording to a log.
7. Verify that the fabric is properly formed.
8. If I/O is required, use all available initiators and targets for this test.
9. If I/O is required, use the appropriate tool to check that initiators can see *all* and *only* their designated targets per the host configuration. Depending on the test and setup conditions, host reboot/reset may be required. Check that host failover software can see these targets from all its assigned paths.

10. If I/O is required, run read/write/compare-based I/O from the initiators to their designated targets.

General Monitoring Procedures During Test Case Execution

1. Closely watch the timing and completeness of initialization processes, target discovery, and switch memory and CPU utilization.
2. Monitor the behavior of initiators during fabric events where appropriate.
3. Check fabrics using both console and syslog monitoring.
4. Clear or archive all previous logs (archive test logs, archive support files, reset console logs).
5. Check and log the status of all fabrics in the test bed if required (fabric state, device state, log pre-test date).
6. Initialize all fabrics in the test bed if required (clear logs, clear core files, reset counters).

General Expectations During and After Test Case Execution

1. Expect the fabric to show complete information on the correct number of switches with one principal. ISLs and trunks should form correctly with the correct speed and port type.
2. Expect no critical or unexpected errors in the application, host, and switch logs. However, expect errors to be logged in the switch log when created by appropriate test procedures.
3. Expect events to complete correctly and on time with no excessive retries.
4. Expect I/O to resume with minimum interruption where routes are changed or the path is blocked. Expect no interruption or stoppage in I/O where routes are not expected to change or where paths are not blocked. Verify by viewing protocol traces where appropriate.
5. Expect no effect in I/O on other hosts in the fabric that do not share the same path to the target.
6. Expect no switch panic, incorrect process termination, flash corruption, core file, software watchdog expiration, or hardware watchdog code shutting down the system, memory leaks, or HA unexpectedly out of sync.
7. If a failover application is used on a host, expect access to storage to remain when a multipath drive loses a single path.

Test Configuration

Test Bed Diagram

Please provide a comprehensive network diagram demonstrating the physical and logical test bed used for testing. The diagram must include all storage array connections, Brocade 7840 connections, and host connections. Interface labels on both sides of each connection must be included.

<INSERT NETWORK TOPOLOGY DIAGRAM HERE.>

DUT Descriptions

1. Please provide the following details of the storage array tested. The DUT ID should match the network topology diagram provided above.

TABLE 1 Storage Array

DUT ID	Vendor	Model	Description

2. Please provide the following details of the Brocade 7840 switches tested. The DUT ID should match the network topology diagram provided above.

TABLE 2 Brocade 7840 Switches

DUT ID	Software Version

3. Please provide the following details of the server hosts used for I/O generation. The DUT ID should match the network topology diagram provided above.

TABLE 3 Server Hosts

DUT ID	Servers	RAM	Processor	Operating System

4. Please provide the following details of the server host adapters used for I/O generation. The DUT ID should match the network topology diagram provided above.

TABLE 4 Server Host Adapters

DUT ID	Adapter	Driver Version

5. Please provide the following details of the hardware or software used for I/O generation and/or monitoring used during testing.

TABLE 5 Test Equipment

Device/Software Tool	Version

Configure DUT and Test Equipment

Task 1. Brocade 7840 Configuration

1. Set both Brocade 7840 switches to hybrid mode, and verify the mode change. By default, the Brocade 7840 is in FCIP mode and does not support IPEX.

```
; 7840 EAST and WEST
extncfg hybrid

; Verify mode change:
extncfg --show
```

2. Configure IPIF interfaces and verify L3 connectivity. One IP address per GE and circuit.

```
; These configurations assume the following physical WAN connections:
; 7840 EAST ge10 < --- > 7840 WEST ge2
; 7840 EAST ge11 < --- > 7840 WEST ge3

; 7840 EAST
portcfg ipif ge10.dp0 create 192.168.1.1/28 mtu 9216
portcfg ipif ge10.dp1 create 192.168.1.3/28 mtu 9216
portcfg ipif ge11.dp0 create 192.168.1.17/28 mtu 9216
portcfg ipif ge11.dp1 create 192.168.1.19/28 mtu 9216

; 7840 WEST
portcfg ipif ge2.dp0 create 192.168.1.2/28 mtu 9216
portcfg ipif ge2.dp1 create 192.168.1.4/28 mtu 9216
```

```
portcfg ipif ge3.dp0 create 192.168.1.18/28 mtu 9216
portcfg ipif ge3.dp1 create 192.168.1.20/28 mtu 9216
```

3. Create the IPsec policy.

```
; 7840 EAST and WEST
portcfg ipsec-policy test_policy create --preshared-key 1234567890abcdef
```

4. Create and verify IPEX tunnel and second circuit. First tunnel creation automatically creates circuit 0.

```
; 7840 EAST
portcfg fciptunnel 24 create --fastwrite --tape-pipelining --compression deflate --ipsec test_policy
-S 192.168.1.1 -D 192.168.1.2 -b 10000000 -B 10000000 --ipext enable --local-ha-ip 192.168.1.3 --
remote-ha-ip 192.168.1.4
portcfg fcipcircuit 24 create 1 -S 192.168.1.17 -D 192.168.1.18 -b 10000000 -B 10000000 --local-ha-
ip 192.168.1.19 --remote-ha-ip 192.168.1.20

; 7840 WEST
portcfg fciptunnel 24 create --fastwrite --tape-pipelining --compression deflate --ipsec test_policy
-S 192.168.1.2 -D 192.168.1.1 -b 10000000 -B 10000000 --ipext enable --local-ha-ip 192.168.1.4 --
remote-ha-ip 192.168.1.3
portcfg fcipcircuit 24 create 1 -S 192.168.1.18 -D 192.168.1.17 -b 10000000 -B 10000000 --local-ha-
ip 192.168.1.20 --remote-ha-ip 192.168.1.19

; Verify tunnel operation:
portshow fciptunnel -c
portshow fciptunnel -ch
portshow fciptunnel -chi
```

5. Set physical ports to LAN mode. By default, all ports are in FCIP mode.

```
; These configurations assume the following physical LAN connections:
; 7840 EAST ge4 < --- > EAST LAN L2 device
; 7840 EAST ge5 < --- > EAST LAN L2 device
; 7840 EAST ge14 < --- > WEST LAN L2 device
; 7840 EAST ge15 < --- > WEST LAN L2 device

; 7840 EAST
portcfgge ge4 --set -lan
portcfgge ge5 --set -lan

; 7840 WEST
portcfgge ge14 --set -lan
portcfgge ge15 --set -lan

; Verify LAN port config:
portcfgge –show
```

6. Create and verify the Gigabit Ethernet port static LAG.

```
; These configurations assume the following physical LAN connections:
; 7840 EAST ge4 < --- > EAST LAN L2 device
; 7840 EAST ge5 < --- > EAST LAN L2 device
; 7840 EAST ge14 < --- > WEST LAN L2 device
; 7840 EAST ge15 < --- > WEST LAN L2 device

; 7840 EAST
portcfg lag to_L2_LAN --create ge4-ge5
y
portenable ge4
portenable ge5

; 7840 WEST
portcfg lag to_L2_LAN --create ge14-ge15
y
portenable ge14
portenable ge15

; Verify LAG creation:
```

```
portcfgge --show

; Verify LAG operation:
portshow lag -detail
```

7. Create the SVI. This assigns an IP address to the LAN side of the 7840 and acts as the LAN gateway for the local subnets.

```
; 7840 EAST
portcfg ipif lan.dp0 create 192.168.100.1/24 mtu 9216

; 7840 WEST
portcfg ipif lan.dp0 create 192.168.200.1/24 mtu 9216
```

8. Create the TCL. This permits replication traffic between the storage array IP addresses across the IPEX tunnel.

```
; These configurations assume the following storage device IP addresses:
; storage device EAST: 192.168.200.10
; storage device WEST: 192.168.100.10

; 7840 EAST
portcfg tcl storage_data create --priority 50 --admin-status enable --action allow --src-addr
192.168.200.10/32 --dst-addr 192.168.100.10/32 --target 24

; 7840 WEST
portcfg tcl storage_data create --priority 50 --admin-status enable --action allow --src-addr
192.168.100.10/32 --dst-addr 192.168.200.10/32 --target 24

; Verify TCL creation:
portshow tcl
```

Task 2. LAN Configuration

Please provide the device details and configuration for the L2 device used to connect hosts, storage array, and Brocade 7840 on each side of the network topology.

<*INSERT L2 DETAILS AND CONFIGURATION HERE*>

Task 3. Storage Array Configuration

Please provide the device details and configuration for the L2 storage array used on each side of the network topology.

<*INSERT STORAGE ARRAY DETAILS AND CONFIGURATION HERE*>

Test Cases

1.1 Replication Events

1.1.1 Replication with No IPEX Advanced Features Enabled

Test Objective

Verify that replication is successful with no Brocade 7840 IPEX advanced features enabled and no concurrent FCIP traffic across the Brocade 7840 WAN link.

Setup

Remove all Brocade 7840 IPEX tunnel advanced features.

```
<7840-BOTH>
portcfg fciptunnel <port> modify --fastwrite disable --tape-pipelining disable --compression none --ipsec
none
```

Test Steps

1. View IPEX tunnel status.

   ```
   portshow fciptunnel -c
   ```

2. Perform the replication event.

   Use an I/O generator to create a 100-GB file with 100-percent random data on the replication source storage file system from each host. Confirm that file replication completes by verifying that files are present on the replication destination storage file system and that the destination file sizes match the source file sizes.

Validation

1. IPEX tunnel OpStatus is "Up".
2. Storage replication is successful.

   Perform MD5 checksum on all source and destination files. MD5 checksum values should be identical.

Results

<PROVIDE PASS OR FAIL RESULT HERE>

<PROVIDE EVIDENCE TO SUPPORT TEST RESULT HERE>

<EVIDENCE CAN INCLUDE CONSOLE OUTPUT OR SCREENSHOTS TO VALIDATE TEST RESULT>

1.1.2 Replication with All IPEX Advanced Features Enabled

Test Objective

Verify that replication is successful with all Brocade 7840 IPEX advanced features enabled and no concurrent FCIP traffic across the Brocade 7840 WAN link.

Setup

Restore Brocade 7840 IPEX tunnel advanced features.

```
<7840-BOTH>
portcfg fciptunnel <port> modify --fastwrite enable --tape-pipelining enable --compression deflate --ipsec
<policy>
```

Test Steps

1. View the IPEX tunnel status.

   ```
   portshow fciptunnel -c
   ```

2. Perform the replication event.

Use an I/O generator to create a 100-GB file with 100-percent random data on the replication source storage file system from each host. Confirm that file replication completes by verifying that files are present on the replication destination storage file system and that the destination file sizes match the source file sizes.

Validation

1. IPEX tunnel OpStatus is "Up".
2. Storage replication is successful.

   Perform MD5 checksum on all source and destination files. MD5 checksum values should be identical.

Results

<*PROVIDE PASS OR FAIL RESULT HERE.*>

<*PROVIDE EVIDENCE TO SUPPORT TEST RESULT HERE.*>

<*EVIDENCE CAN INCLUDE CONSOLE OUTPUT OR SCREENSHOTS TO VALIDATE TEST RESULT.*>

1.1.3 Multiple IPEX Circuits on a Single Physical Interface

Test Objective

Verify that replication is successful with IPEX advanced features enabled and no concurrent FCIP traffic on multiple circuits on a single physical interface. The test configuration is set as IPsec enabled, QoS is set to High, and compression is set to Deflate.

Setup

1. Add a second circuit to the first physical interface on the Brocade 7840 switches.

```
<7840-EAST>
portcfg ipif ge10.dp0 create 192.168.1.5/28 mtu 9216
portcfg fcipcircuit 24 modify 0 -b 5000000 -B 5000000
portcfg fcipcircuit 24 create 2 -S 192.168.1.5 -D 192.168.1.6 -b 5000000 -B 5000000

<7840-WEST>
portcfg ipif ge2.dp0 create 192.168.1.6/28 mtu 9216
portcfg fcipcircuit 24 modify 0 -b 5000000 -B 5000000
portcfg fcipcircuit 24 create 2 -S 192.168.1.6 -D 192.168.1.5 -b 5000000 -B 5000000
```

2. Modify the Brocade 7840 TCL to QoS High.

```
<7840-EAST>
portcfg tcl storage_data modify --admin-status disable
portcfg tcl storage_data modify --target 24-high
portcfg tcl storage_data modify --admin-status enable

<7840-WEST>
portcfg tcl storage_data modify --admin-status disable
portcfg tcl storage_data modify --target 24-high
portcfg tcl storage_data modify --admin-status enable
```

3. Disable the second physical interface on both Brocade 7840 switches.

```
<7840-EAST>
portdisable ge11

<7840-WEST>
portdisable ge3
```

Test Steps

1. View the IPEX tunnel status.

```
portshow fciptunnel -c
```

2. View the IPEX TCL status.

```
portshow tcl
```

3. Perform the replication event.

   Use an I/O generator to create a 100-GB file with 100-percent random data on the replication source storage file system from each host. Confirm that file replication completes by verifying that files are present on the replication destination storage file system and that the destination file sizes match the source file sizes.

4. During replication transfer, view TxMBps and RxMBps of both circuits on the first physical interface.

```
portshow fciptunnel -c
```

Validation

1. The IPEX tunnel OpStatus is "Degrade". The IPEX circuit OpStatus is "Up" for both circuits on the first physical interface. The IPEX circuit OpStatus is "InProg" for the circuit on the second physical interface. CommRt for both circuits on the first physical interface is 5000.
2. The IPEX TCL target is 24-High.
3. Storage replication is successful.

   Perform MD5 checksum on all source and destination files. MD5 checksum values should be identical.

4. TxMBps and RxMBps of both circuits on the first physical interface show traffic load split.

Results

<PROVIDE PASS OR FAIL RESULT HERE:>

<PROVIDE EVIDENCE TO SUPPORT TEST RESULT HERE:>

<EVIDENCE CAN INCLUDE CONSOLE OUTPUT OR SCREENSHOTS TO VALIDATE TEST RESULT:>

1.1.4 Multiple IPEX Circuits on Multiple Physical Interfaces

Test Objective

Verify that replication is successful with IPEX advanced features enabled and no concurrent FCIP traffic on multiple circuits on multiple physical interfaces. The test configuration is set as IPsec enabled, QoS is set to High, and compression is set to Deflate.

Setup

1. Enable the second physical interface on both Brocade 7840 switches.

```
<7840-EAST>
portenable ge11

<7840-WEST>
portenable ge3
```

2. Add a second circuit to the second physical interface on the Brocade 7840 switches.

```
<7840-EAST>
portcfg ipif ge11.dp0 create 192.168.1.21/28 mtu 9216
portcfg fcipcircuit 24 modify 1 -b 5000000 -B 5000000
portcfg fcipcircuit 24 create 3 -S 192.168.1.21 -D 192.168.1.22 -b 5000000 -B 5000000

<7840-WEST>
portcfg ipif ge3.dp0 create 192.168.1.22/28 mtu 9216
portcfg fcipcircuit 24 modify 1 -b 5000000 -B 5000000
portcfg fcipcircuit 24 create 3 -S 192.168.1.22 -D 192.168.1.21 -b 5000000 -B 5000000
```

Test Steps

1. View the IPEX tunnel status.

```
portshow fciptunnel -c
```

2. Perform the replication event.

   Use an I/O generator to create a 100-GB file with 100-percent random data on the replication source storage file system from each host. Confirm that file replication completes by verifying that files are present on the replication destination storage file system and that the destination file sizes match the source file sizes.

3. During replication transfer, view TxMBps and RxMBps of both circuits on the first and second physical interfaces.

```
portshow fciptunnel -c
```

Validation

1. The IPEX tunnel OpStatus is "Up". The IPEX circuit OpStatus is "Up" for both circuits on the first and second physical interfaces. CommRt for both circuits on the first and second physical interfaces is 5000.
2. Storage replication is successful.

   Perform MD5 checksum on all source and destination files. MD5 checksum values should be identical.

3. TxMBps and RxMBps of both circuits on the first and second physical interfaces show traffic load split.

Results

<*PROVIDE PASS OR FAIL RESULT HERE:*>

<*PROVIDE EVIDENCE TO SUPPORT TEST RESULT HERE:*>

<*EVIDENCE CAN INCLUDE CONSOLE OUTPUT OR SCREENSHOTS TO VALIDATE TEST RESULT:*>

1.1.5 Replication and Concurrent FCIP Traffic (Optional)

Test Objective

Verify that replication is successful with Brocade 7840 IPEX advanced features enabled and concurrent FCIP traffic across the Brocade 7840 WAN link. The test configuration is set as IPsec enabled, QoS is set to Low, and compression is set to Aggr-Deflate.

Setup

1. Delete all circuits and tunnels on the Brocade 7840 switches.

```
<7840-EAST>
portcfg fcipcircuit 24 delete 2
portcfg fcipcircuit 24 delete 0
portcfg tcl storage_data delete
portcfg fciptunnel 24 delete

<7840-WEST>
portcfg fcipcircuit 24 delete 3
portcfg fcipcircuit 24 delete 1
portcfg tcl storage_data delete
portcfg fciptunnel 24 delete
```

2. Create a new IPEX tunnel with QoS Low, a second circuit, and a new TCL.

```
<7840-EAST>
portcfg fciptunnel 24 create --fastwrite --tape-pipelining --compression aggr-deflate --ipsec
test_policy -S 192.168.1.1 -D 192.168.1.2 -b 10000000 -B 10000000 --ipext enable --local-ha-ip
192.168.1.3 --remote-ha-ip 192.168.1.4
portcfg fcipcircuit 24 create 1 -S 192.168.1.17 -D 192.168.1.18 -b 10000000 -B 10000000 --local-ha-
ip 192.168.1.19 --remote-ha-ip 192.168.1.20
portcfg tcl storage_data create --priority 50 --admin-status enable --action allow --src-addr
192.168.200.54/32 --dst-addr 9.79.70.1/32 --target 24-low

<7840-WEST>
portcfg fciptunnel 24 create --fastwrite --tape-pipelining --compression aggr-deflate --ipsec
test_policy -S 192.168.1.2 -D 192.168.1.1 -b 10000000 -B 10000000 --ipext enable --local-ha-ip
192.168.1.4 --remote-ha-ip 192.168.1.3
portcfg fcipcircuit 24 create 1 -S 192.168.1.18 -D 192.168.1.17 -b 10000000 -B 10000000 --local-ha-
ip 192.168.1.20 --remote-ha-ip 192.168.1.19
portcfg tcl storage_data create --priority 50 --admin-status enable --action allow --src-addr
9.79.70.1/32 --dst-addr 192.168.200.54/32 --target 24-low
```

Test Steps

1. View the IPEX tunnel status.

```
portshow fciptunnel -c
```

2. View the IPEX TCL status.

```
portshow tcl
```

3. Initiate FC traffic across the Brocade 7840 switches.
4. Perform the replication event.

   Use an I/O generator to create a 100-GB file with 100-percent random data on the replication source storage file system from each host. Confirm that file replication completes by verifying that files are present on the replication destination storage file system and that the destination file sizes match the source file sizes.

Validation

1. The IPEX tunnel OpStatus is "Up".
2. The IPEX TCL target is 24-Low.
3. FC traffic passes successfully.
4. Storage replication is successful.

   Perform MD5 checksum on all source and destination files. MD5 checksum values should be identical.

Results

<PROVIDE PASS OR FAIL RESULT HERE>

<PROVIDE EVIDENCE TO SUPPORT TEST RESULT HERE>

<EVIDENCE CAN INCLUDE CONSOLE OUTPUT OR SCREENSHOTS TO VALIDATE TEST RESULT>

1.1.6 Multiple IPEX Circuits on a Single Physical Interface with Concurrent FCIP Traffic (Optional)

Test Objective

Verify that replication is successful with IPEX advanced features enabled and concurrent FCIP traffic on multiple circuits on a single physical interface. The test configuration is set as IPsec enabled, QoS is set to Low, and compression is set to Aggr-Deflate.

Setup

1. Add a second circuit to the first physical interface on the Brocade 7840 switches.

```
<7840-EAST>
portcfg fcipcircuit 24 modify 0 -b 5000000 -B 5000000
portcfg fcipcircuit 24 create 2 -S 192.168.1.5 -D 192.168.1.6 -b 5000000 -B 5000000

<7840-WEST>
portcfg fcipcircuit 24 modify 0 -b 5000000 -B 5000000
portcfg fcipcircuit 24 create 2 -S 192.168.1.6 -D 192.168.1.5 -b 5000000 -B 5000000
```

2. Disable the second physical interface on both Brocade 7840 switches.

```
<7840-EAST>
portdisable ge11

<7840-WEST>
portdisable ge3
```

Test Steps

1. View the IPEX tunnel status.

```
portshow fciptunnel -c
```

2. Initiate FC traffic across the Brocade 7840 switches.
3. Perform the replication event.

   Use an I/O generator to create a 100-GB file with 100-percent random data on the replication source storage file system from each host. Confirm that file replication completes by verifying that files are present on the replication destination storage file system and that the destination file sizes match the source file sizes

4. During replication transfer, view TxMBps and RxMBps of both circuits on the first physical interface.

```
portshow fciptunnel -c
```

Validation

1. The IPEX tunnel OpStatus is "Degrade". The IPEX circuit OpStatus is "Up" for both circuits on the first physical interface. The IPEX circuit OpStatus is "InProg" for the circuit on the second physical interface. CommRt for both circuits on the first physical interface is 5000.

2. FC traffic passes successfully.
3. Storage replication is successful.

   Perform MD5 checksum on all source and destination files. MD5 checksum values should be identical.
4. TxMBps and RxMBps of both circuits on the first physical interface show traffic load split.

Results

<PROVIDE PASS OR FAIL RESULT HERE>

<PROVIDE EVIDENCE TO SUPPORT TEST RESULT HERE>

<EVIDENCE CAN INCLUDE CONSOLE OUTPUT OR SCREENSHOTS TO VALIDATE TEST RESULT>

1.1.7 Multiple IPEX Circuits on Multiple Physical Interfaces with Concurrent FCIP Traffic (Optional)

Test Objective

Verify that replication is successful with IPEX advanced features enabled and concurrent FCIP traffic on multiple circuits on multiple physical interfaces. The test configuration is set as IPsec enabled, QoS is set to Low, and compression is set to Aggr-Deflate.

Setup

1. Enable the second physical interface on both Brocade 7840 switches.

```
<7840-EAST>
portenable ge11

<7840-WEST>
portenable ge3
```

2. Add a second circuit to the second physical interface on the Brocade 7840 switches.

```
<7840-EAST>
portcfg fcipcircuit 24 modify 1 -b 5000000 -B 5000000
portcfg fcipcircuit 24 create 3 -S 192.168.1.21 -D 192.168.1.22 -b 5000000 -B 5000000

<7840-WEST>
portcfg fcipcircuit 24 modify 1 -b 5000000 -B 5000000
portcfg fcipcircuit 24 create 3 -S 192.168.1.22 -D 192.168.1.21 -b 5000000 -B 5000000
```

Test Steps

1. View the IPEX tunnel status.

```
portshow fciptunnel -c
```

2. Initiate FC traffic across Brocade 7840 switches.
3. Perform the replication event.

   Use an I/O generator to create a 100-GB file with 100-percent random data on the replication source storage file system from each host. Confirm that file replication completes by verifying that files are present on the replication destination storage file system and that the destination file sizes match the source file sizes.
4. During replication transfer, view TxMBps and RxMBps of both circuits on the first and second physical interfaces.

```
portshow fciptunnel -c
```

Validation

1. The IPEX tunnel OpStatus is "Degrade". The IPEX circuit OpStatus is "Up" for both circuits on the first and second physical interfaces. CommRt for both circuits on the first and second physical interfaces is 5000.
2. FC traffic passes successfully.
3. Storage replication is successful.

   Perform MD5 checksum on all source and destination files. MD5 checksum values should be identical.
4. TxMBps and RxMBps of both circuits on the first and second physical interfaces show traffic load split.

Results

<*PROVIDE PASS OR FAIL RESULT HERE.*>

<*PROVIDE EVIDENCE TO SUPPORT TEST RESULT HERE.*>

<*EVIDENCE CAN INCLUDE CONSOLE OUTPUT OR SCREENSHOTS TO VALIDATE TEST RESULT.*>

1.1.8 Hot Code Load During Replication with Optional Concurrent FCIP Traffic

Test Objective

Verify that HCL does not interrupt concurrent FCIP traffic while IPEX traffic resumes successfully after HCL completes on a single IPEX circuit.

Setup

1. Delete all circuits and tunnels on the Brocade 7840 switches.

```
<7840-EAST>
portcfg fcipcircuit 24 delete 2
portcfg fcipcircuit 24 delete 0
portcfg tcl storage_data delete
portcfg fciptunnel 24 delete

<7840-WEST>
portcfg fcipcircuit 24 delete 3
portcfg fcipcircuit 24 delete 1
portcfg tcl storage_data delete
portcfg fciptunnel 24 delete
```

2. Create a new IPEX tunnel with QoS High, a second circuit, and a new TCL.

```
<7840-EAST>
portcfg fciptunnel 24 create --fastwrite --tape-pipelining --compression aggr-deflate --ipsec
test_policy -S 192.168.1.1 -D 192.168.1.2 -b 10000000 -B 10000000 --ipext enable --local-ha-ip
192.168.1.3 --remote-ha-ip 192.168.1.4
portcfg fcipcircuit 24 create 1 -S 192.168.1.17 -D 192.168.1.18 -b 10000000 -B 10000000 --local-ha-
ip 192.168.1.19 --remote-ha-ip 192.168.1.20
portcfg tcl storage_data create --priority 50 --admin-status enable --action allow --src-addr
192.168.200.54/32 --dst-addr 9.79.70.1/32 --target 24-high

<7840-WEST>
portcfg fciptunnel 24 create --fastwrite --tape-pipelining --compression aggr-deflate --ipsec
test_policy -S 192.168.1.2 -D 192.168.1.1 -b 10000000 -B 10000000 --ipext enable --local-ha-ip
192.168.1.4 --remote-ha-ip 192.168.1.3
portcfg fcipcircuit 24 create 1 -S 192.168.1.18 -D 192.168.1.17 -b 10000000 -B 10000000 --local-ha-
ip 192.168.1.20 --remote-ha-ip 192.168.1.19
```

```
portcfg tcl storage_data create --priority 50 --admin-status enable --action allow --src-addr
9.79.70.1/32 --dst-addr 192.168.200.54/32 --target 24-high
```

3. Downgrade the Brocade 7840 switches to the previous GA version.

```
<7840-EAST>
firmwaredownload 10.38.2.25,anonymous,/pub/sre/SQA/fos/v7.4.0/v7.4.0,none

<7840-WEST>
firmwaredownload 10.38.2.25,anonymous,/pub/sre/SQA/fos/v7.4.0/v7.4.0,none
```

Test Steps

1. View the IPEX tunnel status.

```
portshow fciptunnel -c
```

2. View the IPEX TCL status.

```
portshow tcl
```

3. (Optional) Initiate FC traffic across the Brocade 7840 switches.
4. Initiate HCL on both Brocade 7840 switches from the previous GA version to the current GA version.

```
<7840-EAST>
firmwaredownload 10.38.2.25,anonymous,/pub/sre/SQA/fos/v7.4.1/v7.4.1,none

<7840-WEST>
firmwaredownload 10.38.2.25,anonymous,/pub/sre/SQA/fos/v7.4.1/v7.4.1,none
```

5. Perform the replication event while HCL is in progress.

   Use an I/O generator to create a 100-GB file with 100-percent random data on the replication source storage file system from each host. Confirm that file replication completes by verifying that files are present on the replication destination storage file system and that the destination file sizes match the source file sizes.

Validation

1. The IPEX tunnel OpStatus is "Up".
2. The IPEX TCL target is 24-High.
3. (Optional) FC traffic passes successfully, even through the HCL event.
4. HCL completes successfully.

```
<7840-EAST>
firmwaredownloadstatus
firmwareshow

<7840-WEST>
firmwaredownloadstatus
firmwareshow
```

5. Storage replication is interrupted by Brocade 7840 HCL, but resumes and completes successfully once HCL is finished.

   Perform MD5 checksum on all source and destination files. MD5 checksum values should be identical.

Results

<PROVIDE PASS OR FAIL RESULT HERE>

<PROVIDE EVIDENCE TO SUPPORT TEST RESULT HERE:>

<EVIDENCE CAN INCLUDE CONSOLE OUTPUT OR SCREENSHOTS TO VALIDATE TEST RESULT:>

1.1.9 Hot Code Load with Multiple IPEX Circuits on a Single Physical Interface with Optional Concurrent FCIP Traffic

Test Objective

Verify that HCL does not interrupt concurrent FCIP traffic while IPEX traffic resumes successfully after HCL completes using multiple IPEX circuits on a single physical interface.

Setup

1. Add a second circuit to the first physical interface on the Brocade 7840 switches.

```
<7840-EAST>
portcfg fcipcircuit 24 modify 0 -b 5000000 -B 5000000
portcfg fcipcircuit 24 create 2 -S 192.168.1.5 -D 192.168.1.6 -b 5000000 -B 5000000

<7840-WEST>
portcfg fcipcircuit 24 modify 0 -b 5000000 -B 5000000
portcfg fcipcircuit 24 create 2 -S 192.168.1.6 -D 192.168.1.5 -b 5000000 -B 5000000
```

2. Disable the second physical interface on both Brocade 7840 switches.

```
<7840-EAST>
portdisable ge11

<7840-WEST>
portdisable ge3
```

3. Downgrade Brocade 7840 switches to the previous GA version.

```
<7840-EAST>
firmwaredownload 10.38.2.25,anonymous,/pub/sre/SQA/fos/v7.4.0/v7.4.0,none

<7840-WEST>
firmwaredownload 10.38.2.25,anonymous,/pub/sre/SQA/fos/v7.4.0/v7.4.0,none
```

Test Steps

1. View the IPEX tunnel status.

```
portshow fciptunnel -c
```

2. (Optional) Initiate FC traffic across the Brocade 7840 switches.
3. Initiate HCL on both Brocade 7840 switches from the previous GA version to the current GA version.

```
<7840-EAST>
firmwaredownload 10.38.2.25,anonymous,/pub/sre/SQA/fos/v7.4.1/v7.4.1,none

<7840-WEST>
firmwaredownload 10.38.2.25,anonymous,/pub/sre/SQA/fos/v7.4.1/v7.4.1,none
```

4. Perform the replication event while HCL is in progress.

Use an I/O generator to create a 100-GB file with 100-percent random data on the replication source storage file system from each host. Confirm that file replication completes by verifying that files are present on the replication destination storage file system and that destination file sizes match the source file sizes.

Validation

1. The IPEX tunnel OpStatus is "Degrade". The IPEX circuit OpStatus is "Up" for both circuits on the first physical interface. The IPEX circuit OpStatus is "InProg" for the circuit on the second physical interface. CommRt for both circuits on the first physical interface is 5000.
2. (Optional) FC traffic passes successfully, even through the HCL event.
3. HCL completes successfully.

```
<7840-EAST>
firmwaredownloadstatus
firmwareshow

<7840-WEST>
firmwaredownloadstatus
firmwareshow
```

4. Storage replication is interrupted by Brocade 7840 HCL, but resumes and completes successfully once HCL is finished.

   Perform MD5 checksum on all source and destination files. MD5 checksum values should be identical.

Results

<PROVIDE PASS OR FAIL RESULT HERE>

<PROVIDE EVIDENCE TO SUPPORT TEST RESULT HERE>

<EVIDENCE CAN INCLUDE CONSOLE OUTPUT OR SCREENSHOTS TO VALIDATE TEST RESULT>

1.1.10 Hot Code Load with Multiple IPEX Circuits on Multiple Physical Interfaces with Optional Concurrent FCIP Traffic

Test Objective

Verify that HCL does not interrupt concurrent FCIP traffic while IPEX traffic resumes successfully after HCL completes using multiple IPEX circuits on multiple physical interfaces.

Setup

1. Enable the second physical interface on both Brocade 7840 switches.

```
<7840-EAST>
portenable ge11

<7840-WEST>
portenable ge3
```

2. Add a second circuit to the second physical interface on the Brocade 7840 switches.

```
<7840-EAST>
portcfg fcipcircuit 24 modify 1 -b 5000000 -B 5000000
portcfg fcipcircuit 24 create 3 -S 192.168.1.21 -D 192.168.1.22 -b 5000000 -B 5000000

<7840-WEST>
```

```
portcfg fcipcircuit 24 modify 1 -b 5000000 -B 5000000
portcfg fcipcircuit 24 create 3 -S 192.168.1.22 -D 192.168.1.21 -b 5000000 -B 5000000
```

3. Downgrade the Brocade 7840 switches to the previous GA version.

```
<7840-EAST>
firmwaredownload 10.38.2.25,anonymous,/pub/sre/SQA/fos/v7.4.0/v7.4.0,none

<7840-WEST>
firmwaredownload 10.38.2.25,anonymous,/pub/sre/SQA/fos/v7.4.0/v7.4.0,none
```

Test Steps

1. View the IPEX tunnel status.

```
portshow fciptunnel -c
```

2. (Optional) Initiate FC traffic across the Brocade 7840 switches.
3. Initiate HCL on both Brocade 7840 switches from the previous GA version to the current GA version.

```
<7840-EAST>
firmwaredownload 10.38.2.25,anonymous,/pub/sre/SQA/fos/v7.4.1/v7.4.1,none

<7840-WEST>
firmwaredownload 10.38.2.25,anonymous,/pub/sre/SQA/fos/v7.4.1/v7.4.1,none
```

4. Perform the replication event while HCL is in progress.

   Use an I/O generator to create a 100-GB file with 100-percent random data on the replication source storage file system from each host. Confirm that file replication completes by verifying that files are present on the replication destination storage file system and that the destination file sizes match the source file sizes.

Validation

1. The IPEX tunnel OpStatus is "Up". The IPEX circuit OpStatus is "Up" for both circuits on the first and second physical interfaces. CommRt for both circuits on the first and second physical interfaces is 5000.
2. (Optional) FC traffic passes successfully, even through the HCL event.
3. HCL completes successfully.

```
<7840-EAST>
firmwaredownloadstatus
firmwareshow

<7840-WEST>
firmwaredownloadstatus
firmwareshow
```

4. Storage replication is interrupted by Brocade 7840 HCL, but resumes and completes successfully once HCL is finished.

   Perform MD5 checksum on all source and destination files. MD5 checksum values should be identical.

Results

<PROVIDE PASS OR FAIL RESULT HERE>

<PROVIDE EVIDENCE TO SUPPORT TEST RESULT HERE>

<EVIDENCE CAN INCLUDE CONSOLE OUTPUT OR SCREENSHOTS TO VALIDATE TEST RESULT>

1.1.11 Iterative Compression (Optional)

Test Objective

Verify that iterative compression from both storage and 7840 does not increase transfer sizes.

Setup

1. Insert a packet analyzer in the network topology both before and after the first 7840.
2. Disable the interface on the source 7840 to force all replication traffic over the LAN interface with the packet analyzer connected.

```
<7840 EAST>
portdisable ge4
```

3. Disable the interface on the source 7840 to force all replication traffic over the WAN interface with the packet analyzer connected.

```
<7840 EAST>
portdisable ge11
```

Test Steps

1. Modify the 7840 configurations for compression **none**.

```
<7840 EAST>
portcfg fciptunnel 24 modify --compression none

<7840 WEST>
portcfg fciptunnel 24 modify --compression none
```

2. Begin recording on both pairs of packet analyzer ports.
3. Perform the replication event.

   Use an I/O generator to create a 100-GB file with 100-percent random data on the replication source storage file system from each host. Confirm that file replication completes by verifying that files are present on the replication destination storage file system and that the destination file sizes match the source file sizes.
4. Stop recording on both packet analyzer ports to document bandwidth usage before and after the 7840 switches during the replication event.
5. Modify the 7840 configurations for compression **deflate**.

```
<7840 EAST>
portcfg fciptunnel 24 modify --compression deflate

<7840 WEST>
portcfg fciptunnel 24 modify --compression deflate
```

6. Begin recording on both pairs of packet analyzer ports.
7. Perform the replication event.

   Use an I/O generator to create a 100-GB file with 100-percent random data on the replication source storage file system from each host. Confirm that file replication completes by verifying that files are present on the replication destination storage file system and that the destination file sizes match the source file sizes

8. Stop recording on both packet analyzer ports to document bandwidth usage before and after the 7840 switches during the replication event.
9. Modify the 7840 configurations for compression **aggr-deflate**.

```
<7840 EAST>
portcfg fciptunnel 24 modify --compression aggr-deflate

<7840 WEST>
portcfg fciptunnel 24 modify --compression aggr-deflate
```

10. Begin recording on both pairs of packet analyzer ports.
11. Perform the replication event.

    Use an I/O generator to create a 100-GB file with 100-percent random data on the replication source storage file system from each host. Confirm that file replication completes by verifying that files are present on the replication destination storage file system and that the destination file sizes match the source file sizes
12. Stop recording on both packet analyzer ports to document bandwidth usage before and after the 7840 switches during the replication event.

Validation

1. 7840 tunnel modification is successful.

```
portshow fciptunnel –c
```

2. Packet analyzer recording begins successfully.
3. Storage replication is successful.

   Perform MD5 checksum on all source and destination files. MD5 checksum values should be identical.
4. The sum of all bandwidth recordings on the WAN side of the packet analyzer is equal to the sum of all bandwidth recordings on the LAN side of the packet analyzer.
5. 7840 tunnel modification is successful.

```
portshow fciptunnel –c
```

6. Packet analyzer recording begins successfully.
7. Storage replication is successful.

   Perform MD5 checksum on all source and destination files. MD5 checksum values should be identical.
8. The sum of all bandwidth recordings on the WAN side of the packet analyzer is less than or equal to the sum of all bandwidth recordings on the LAN side of the packet analyzer.
9. 7840 tunnel modification is successful.

```
portshow fciptunnel –c
```

10. Packet analyzer recording begins successfully.
11. Storage replication is successful.

    Perform MD5 checksum on all source and destination files. MD5 checksum values should be identical.
12. The sum of all bandwidth recordings on the WAN side of the packet analyzer is less than or equal to the sum of all bandwidth recordings on the LAN side of the packet analyzer.

Results

<PROVIDE PASS OR FAIL RESULT HERE.>

<PROVIDE EVIDENCE TO SUPPORT TEST RESULT HERE.>

<EVIDENCE CAN INCLUDE CONSOLE OUTPUT OR SCREENSHOTS TO VALIDATE TEST RESULT.>

1.1.12 File Replication Performance Testing

Test Objective

Benchmark file replication performance with and without Brocade 7840 switches using a variety of delay and packet-loss impairment combinations.

Latency ms RTT	No Packet Drop		0.1% Packet Drop		0.5% Packet Drop	
0	X MBps	Y MBps				
5						
10						
25						
50						
100						
200						
250						
DUT with IPEX						
DUT Native						
Results in MBps						

Latency ms RTT	No Packet Drop		0.1% Packet Drop		0.5% Packet Drop	
0	320	320	320	33	320	16
5	320	320	320	18	320	10
10	320	262	320	8	320	6
25	320	178	320	6	320	6
50	320	62	320	6	320	6
100	320	40	320	6	320	6
200	310	5	310	4	260	3
250	200	4	195	2	170	2
DUT Storage Array with IPEX						
DUT Storage Array Native						
Results in MBps						

Setup

Insert a network impairment tool in the network topology in between the Brocade 7840 switches. One pair of packet analyzer ports must be connected inline with the network impairment tool to record traffic after network impairment.

[REPLICATION SOURCE] ---> [PACKET ANALYZER] ---> [BROCADE 7840] ---> [NETWORK IMPAIRMENT] ---> [PACKET ANALYZER] ---> [BROCADE 7840] ---> [REPLICATION DESTINATION]

Test Steps

1. Configure the network impairment tool for the first combination of delay and packet loss.
2. Begin recording on both pairs of packet analyzer ports.
3. Perform the replication event.

   Use an I/O generator to create a 100-GB file with 100-percent random data on the replication source storage file system from each host. Confirm that file replication completes by verifying that files are present on the replication destination storage file system and that the destination file sizes match the source file sizes.
4. Stop recording on both packet analyzer ports to document performance before and after the Brocade 7840 switches during the replication event.
5. Repeat Steps 1 through 4 for all desired delay and packet loss combination configurations.
6. Reconfigure the network topology so that the Brocade 7840 switches are no longer present in between the file replication source and destination.

   [REPLICATION SOURCE] ---> [PACKET ANALYZER] ---> [NETWORK IMPAIRMENT] ---> [PACKET ANALYZER] ---> [REPLICATION DESTINATION]
7. Repeat Steps 1 through 5 to record performance without the Brocade 7840 switches.

Validation

1. Network impairment tool configuration is successful.
2. Packet analyzer recording begins successfully.
3. Storage replication is successful.

   Perform MD5 checksum on all source and destination files. MD5 checksum values should be identical.
4. Packet analyzer recordings are successful.
5. Packet analyzer recordings demonstrate increased transfer time and decreased throughput values as impairment and/or delay values increase.
6. Network reconfiguration is successful.
7. Packet analyzer recordings demonstrate increased transfer time and decreased throughput values as impairment and/or delay values increase greater than the results recorded with Brocade 7840 switches in the network configuration.

Results

<*PROVIDE PASS OR FAIL RESULT HERE.*>

<*PROVIDE EVIDENCE TO SUPPORT TEST RESULT HERE.*>

<*EVIDENCE CAN INCLUDE CONSOLE OUTPUT OR SCREENSHOTS TO VALIDATE TEST RESULT.*>

1.1.13 Jumbo Frames

Test Objective

Verify that replication is successful with jumbo frames configured on all IP devices between storage clusters.

Setup

Configure LAN switches and all hosts for the maximum MTU size.

Test Steps

1. Clear packet statistics on both Brocade VCS fabrics.

   ```
   clear counters all
   ```

2. View the IPEX tunnel status.

   ```
   portshow fciptunnel -c
   ```

3. Perform the replication event.

   Use an I/O generator to create a 100-GB file with 100-percent random data on the replication source storage file system from each host. Confirm that file replication completes by verifying that files are present on the replication destination storage file system and that the destination file sizes match the source file sizes.

4. View Brocade VCS Fabric interface statistics.

   ```
   show interface port-channel <number>
   ```

Validation

1. Interface statistics are successfully cleared.
2. The IPEX tunnel OpStatus is "Up".
3. Storage replication is successful.

   Perform MD5 checksum on all source and destination files. MD5 checksum values should be identical.

4. Interface statistics show a majority of receive traffic is counted as "Over 1518-byte pkts (Jumbo)."

Results

<PROVIDE PASS OR FAIL RESULT HERE>

<PROVIDE EVIDENCE TO SUPPORT TEST RESULT HERE>

<EVIDENCE CAN INCLUDE CONSOLE OUTPUT OR SCREENSHOTS TO VALIDATE TEST RESULT>

1.2 Error Recovery

1.2.1 LAN Network Impairment

Test Objective

Verify that replication is successful with network impairment on the LAN and no concurrent FCIP traffic.

- CRC errors
- Packet errors
- Packet drops

Setup

Insert a network impairment device on the LAN side of the replication source setup.

Test Steps

1. View the IPEX tunnel status.

```
portshow fciptunnel -c
```

2. Initiate CRC error impairment up to LAN-device supported values, not to exceed 1 percent total.
3. Perform the replication event.

   Use an I/O generator to create a 100-GB file with 100-percent random data on the replication source storage file system from each host. Confirm that file replication completes by verifying that files are present on the replication destination storage file system and that the destination file sizes match the source file sizes.
4. Change impairment to packet errors up to LAN-device supported values, not to exceed 1 percent total. Do not correct the TCP checksum.
5. Perform the replication event.

   Use an I/O generator to create a 100-GB file with 100-percent random data on the replication source storage file system from each host. Confirm that file replication completes by verifying that files are present on the replication destination storage file system and that the destination file sizes match the source file sizes.
6. Change impairment to packet drops up to LAN-device supported values, not to exceed 1 percent total.
7. Perform the replication event.

   Use an I/O generator to create a 100-GB file with 100-percent random data on the replication source storage file system from each host. Confirm that file replication completes by verifying that files are present on the replication destination storage file system and that the destination file sizes match the source file sizes.

Validation

1. The IPEX tunnel OpStatus is "Up".
2. The CRC impairment configuration is successful.
3. Storage replication is successful.

   Perform MD5 checksum on all source and destination files. MD5 checksum values should be identical.
4. The packet error impairment configuration is successful.
5. Storage replication is successful.

   Perform MD5 checksum on all source and destination files. MD5 checksum values should be identical.
6. The packet drop impairment configuration is successful.
7. Storage replication is successful.

   Perform MD5 checksum on all source and destination files. MD5 checksum values should be identical.

Results

<PROVIDE PASS OR FAIL RESULT HERE>

<PROVIDE EVIDENCE TO SUPPORT TEST RESULT HERE>

<EVIDENCE CAN INCLUDE CONSOLE OUTPUT OR SCREENSHOTS TO VALIDATE TEST RESULT>

1.2.2 WAN Network Impairment on a Single IPEX Circuit

Test Objective

Verify that replication is successful with network impairment on a single IPEX circuit WAN and no concurrent FCIP traffic.

- CRC errors
- Packet errors

Setup

1. Insert a network impairment device on the WAN side of the setup.
2. Delete all circuits and tunnels on the Brocade 7840 switches.

```
<7840-EAST>
portcfg fcipcircuit 24 delete 2
portcfg fcipcircuit 24 delete 0
portcfg tcl storage_data delete
portcfg fciptunnel 24 delete

<7840-WEST>
portcfg fcipcircuit 24 delete 3
portcfg fcipcircuit 24 delete 1
portcfg tcl storage_data delete
portcfg fciptunnel 24 delete
```

3. Create a new IPEX tunnel with QoS High and a new TCL.

```
<7840-EAST>
portcfg fciptunnel 24 create --fastwrite --tape-pipelining --compression aggr-deflate --ipsec
test_policy -S 192.168.1.1 -D 192.168.1.2 -b 10000000 -B 10000000 --ipext enable --local-ha-ip
192.168.1.3 --remote-ha-ip 192.168.1.4
portcfg tcl storage_data create --priority 50 --admin-status enable --action allow --src-addr
192.168.200.54/32 --dst-addr 9.79.70.1/32 --target 24-high

<7840-WEST>
portcfg fciptunnel 24 create --fastwrite --tape-pipelining --compression aggr-deflate --ipsec
test_policy -S 192.168.1.2 -D 192.168.1.1 -b 10000000 -B 10000000 --ipext enable --local-ha-ip
192.168.1.4 --remote-ha-ip 192.168.1.3
portcfg tcl storage_data create --priority 50 --admin-status enable --action allow --src-addr
9.79.70.1/32 --dst-addr 192.168.200.54/32 --target 24-high
```

Test Steps

1. View the IPEX tunnel status.

```
portshow fciptunnel -c
```

2. Initiate CRC error impairment (1%).
3. Perform the replication event.

   Use an I/O generator to create a 100-GB file with 100-percent random data on the replication source storage file system from each host. Confirm that file replication completes by verifying that files are present on the replication destination storage file system and that the destination file sizes match the source file sizes.
4. Change impairment to packet errors (1%). Do not correct the TCP checksum.

5. Perform the replication event.

   Use an I/O generator to create a 100-GB file with 100-percent random data on the replication source storage file system from each host. Confirm that file replication completes by verifying that files are present on the replication destination storage file system and that the destination file sizes match the source file sizes.

Validation

1. The IPEX tunnel OpStatus is "Up".
2. The CRC impairment configuration is successful.
3. Storage replication is successful.

   Perform MD5 checksum on all source and destination files. MD5 checksum values should be identical.
4. The packet error impairment configuration is successful.
5. Storage replication is successful.

   Perform MD5 checksum on all source and destination files. MD5 checksum values should be identical.

Results

<PROVIDE PASS OR FAIL RESULT HERE>

<PROVIDE EVIDENCE TO SUPPORT TEST RESULT HERE>

<EVIDENCE CAN INCLUDE CONSOLE OUTPUT OR SCREENSHOTS TO VALIDATE TEST RESULT>

1.2.3 WAN Network Impairment on Multiple IPEX Circuits on a Single Physical Interface

Test Objective

Verify that replication is successful with network impairment on multiple IPEX circuits on a single interface WAN and no concurrent FCIP traffic.

- CRC errors
- Packet errors

Setup

1. Insert a network impairment device on the WAN side of the setup.
2. Add a second circuit to the first physical interface on the Brocade 7840 switches.

```
<7840-EAST>
portcfg fcipcircuit 24 modify 0 -b 5000000 -B 5000000
portcfg fcipcircuit 24 create 2 -S 192.168.1.5 -D 192.168.1.6 -b 5000000 -B 5000000

<7840-WEST>
portcfg fcipcircuit 24 modify 0 -b 5000000 -B 5000000
portcfg fcipcircuit 24 create 2 -S 192.168.1.6 -D 192.168.1.5 -b 5000000 -B 5000000
```

3. Disable the second physical interface on both Brocade 7840 switches.

```
<7840-EAST>
portdisable ge11

<7840-WEST>
portdisable ge3
```

Test Steps

1. View IPEX tunnel status.

```
portshow fciptunnel -c
```

2. Initiate CRC error impairment (1%).
3. Perform the replication event.

   Use an I/O generator to create a 100-GB file with 100-percent random data on the replication source storage file system from each host. Confirm that file replication completes by verifying that files are present on the replication destination storage file system and that the destination file sizes match the source file sizes.
4. Change impairment to packet errors (1%). Do not correct the TCP checksum.
5. Perform the replication event.

   Use an I/O generator to create a 100-GB file with 100-percent random data on the replication source storage file system from each host. Confirm that file replication completes by verifying that files are present on the replication destination storage file system and that the destination file sizes match the source file sizes.

Validation

1. The IPEX tunnel OpStatus is "Up".
2. The CRC impairment configuration is successful.
3. Storage replication is successful.

   Perform MD5 checksum on all source and destination files. MD5 checksum values should be identical.
4. The packet error impairment configuration is successful.
5. Storage replication is successful.

   Perform MD5 checksum on all source and destination files. MD5 checksum values should be identical.

Results

<PROVIDE PASS OR FAIL RESULT HERE>

<PROVIDE EVIDENCE TO SUPPORT TEST RESULT HERE>

<EVIDENCE CAN INCLUDE CONSOLE OUTPUT OR SCREENSHOTS TO VALIDATE TEST RESULT>

1.2.4 WAN Network Impairment on Multiple IPEX Circuits on Multiple Physical Interfaces

Test Objective

Verify that replication is successful with network impairment on multiple IPEX circuits on multiple WAN interfaces and no concurrent FCIP traffic.

- CRC errors
- Packet errors

Setup

1. Insert a network impairment device on the WAN side of the setup.
2. Enable the second physical interface on both Brocade 7840 switches.

```
<7840-EAST>
portenable ge11

<7840-WEST>
portenable ge3
```

3. Add a second circuit to the second physical interface on the Brocade 7840 switches.

```
<7840-EAST>
portcfg fcipcircuit 24 modify 1 -b 5000000 -B 5000000
portcfg fcipcircuit 24 create 3 -S 192.168.1.21 -D 192.168.1.22 -b 5000000 -B 5000000

<7840-WEST>
portcfg fcipcircuit 24 modify 1 -b 5000000 -B 5000000
portcfg fcipcircuit 24 create 3 -S 192.168.1.22 -D 192.168.1.21 -b 5000000 -B 5000000
```

Test Steps

1. View the IPEX tunnel status.

```
portshow fciptunnel -c
```

2. Initiate CRC error impairment (1%).
3. Perform the replication event.

   Use an I/O generator to create a 100-GB file with 100-percent random data on the replication source storage file system from each host. Confirm that file replication completes by verifying that files are present on the replication destination storage file system and that the destination file sizes match the source file sizes.
4. Change impairment to packet errors (1%). Do not correct the TCP checksum.
5. Perform the replication event.

   Use an I/O generator to create a 100-GB file with 100-percent random data on the replication source storage file system from each host. Confirm that file replication completes by verifying that files are present on the replication destination storage file system and that the destination file sizes match the source file sizes.

Validation

1. The IPEX tunnel OpStatus is "Up".
2. The CRC impairment configuration is successful.
3. Storage replication is successful.

   Perform MD5 checksum on all source and destination files. MD5 checksum values should be identical.
4. The packet error impairment configuration is successful.
5. Storage replication is successful.

   Perform MD5 checksum on all source and destination files. MD5 checksum values should be identical.

Results

<PROVIDE PASS OR FAIL RESULT HERE>

<PROVIDE EVIDENCE TO SUPPORT TEST RESULT HERE>

<EVIDENCE CAN INCLUDE CONSOLE OUTPUT OR SCREENSHOTS TO VALIDATE TEST RESULT>

1.2.5 LAN and WAN Cable Pulls

Test Objective

Verify that replication is successful during failover events as a result of LAN and WAN cable pulls.

Test Steps

1. Run the replication event. During the replication event, pull a WAN cable to force a failover.

   Use an I/O generator to create a 100-GB file with 100-percent random data on the replication source storage file system from each host. Confirm that file replication completes by verifying that files are present on the replication destination storage file system and that the destination file sizes match the source file sizes.

2. Run the replication event. During the replication event, pull a LAN cable to force a failover.

   Use an I/O generator to create a 100-GB file with 100-percent random data on the replication source storage file system from each host. Confirm that file replication completes by verifying that files are present on the replication destination storage file system and that the destination file sizes match the source file sizes.

Validation

1. Pulling a WAN cable results in no temporary replication suspension since there is a redundant WAN path to fail over to.
2. Pulling a LAN cable results in no temporary replication suspension since there is a redundant LAN path to fail over to.

Results

<PROVIDE PASS OR FAIL RESULT HERE>

<PROVIDE EVIDENCE TO SUPPORT TEST RESULT HERE>

<EVIDENCE CAN INCLUDE CONSOLE OUTPUT OR SCREENSHOTS TO VALIDATE TEST RESULT>

1.2.6 Device Reboot

Test Objective

Verify that replication is successful during failover events as a result of device reboots simulating power outages.

Test Steps

1. Run the replication event. During the replication event, reboot a Brocade 7840.

   Use an I/O generator to create a 100-GB file with 100-percent random data on the replication source storage file system from each host. Confirm that file replication completes by verifying that files are present on the replication destination storage file system and that the destination file sizes match the source file sizes.

2. Run the replication event. During the replication event, reboot a LAN switch.

Use an I/O generator to create a 100-GB file with 100-percent random data on the replication source storage file system from each host. Confirm that file replication completes by verifying that files are present on the replication destination storage file system and that the destination file sizes match the source file sizes.

3. Run the replication event. During the replication event, reboot the destination storage system.

   Use an I/O generator to create a 100-GB file with 100-percent random data on the replication source storage file system from each host. Confirm that file replication completes by verifying that files are present on the replication destination storage file system and that the destination file sizes match the source file sizes.

Validation

1. Rebooting a Brocade 7840 results in a temporary replication suspension since there is no redundant WAN path to fail over to. Storage replication is successful.

   Perform MD5 checksum on all source and destination files. MD5 checksum values should be identical.

2. Rebooting a LAN switch results in no temporary replication suspension since there is a redundant LAN path to fail over to. Storage replication is successful.

   Perform MD5 checksum on all source and destination files. MD5 checksum values should be identical.

3. Rebooting the destination storage system results in a temporary replication suspension. Storage replication is successful.

   Perform MD5 checksum on all source and destination files. MD5 checksum values should be identical.

Results

<PROVIDE PASS OR FAIL RESULT HERE>

<PROVIDE EVIDENCE TO SUPPORT TEST RESULT HERE>

<EVIDENCE CAN INCLUDE CONSOLE OUTPUT OR SCREENSHOTS TO VALIDATE TEST RESULT>

1.3 Stress Testing

1.3.1 Replication with IPEX Advanced Features Enabled for Extended Run

Test Objective

Verify that replication is successful with all Brocade 7840 IPEX advanced features enabled and no concurrent FCIP traffic across the Brocade 7840 WAN link over an 8-hour period.

Setup

Restore Brocade 7840 IPEX tunnel advanced features.

```
<7840-BOTH>
portcfg fciptunnel <port> modify --fastwrite enable --tape-pipelining enable -compression deflate --ipsec
<policy>
```

Test Steps

1. View the IPEX tunnel status.

   ```
   portshow fciptunnel -c
   ```

2. Perform the replication event.

   Use an I/O generator to write continuously for 8 hours with 100-percent random data on the replication source storage file system from each host. Confirm that file replication completes by verifying that files are present on the replication destination storage file system and that the destination file sizes match the source file sizes.

Validation

1. The IPEX tunnel OpStatus is "Up".
2. Storage replication is successful.

   Perform MD5 checksum on all source and destination files. MD5 checksum values should be identical.

Results

<PROVIDE PASS OR FAIL RESULT HERE>

<PROVIDE EVIDENCE TO SUPPORT TEST RESULT HERE>

<EVIDENCE CAN INCLUDE CONSOLE OUTPUT OR SCREENSHOTS TO VALIDATE TEST RESULT>

1.3.2 WAN Network Impairment for Extended Run

Test Objective

Verify that replication is successful with network impairment on the WAN and no concurrent FCIP traffic over a 3-hour period.

- CRC errors
- Packet errors

Setup

Insert the network impairment device on the WAN side of the setup.

Test Steps

1. View the IPEX tunnel status.

   ```
   portshow fciptunnel -c
   ```

2. Initiate CRC error impairment (0.1%).
3. Run the replication event for 3 hours.

   Use an I/O generator to write continuously for 3 hours with 100-percent random data on the replication source storage file system from each host. Confirm that file replication completes by verifying that files are present on the replication destination storage file system and that the destination file sizes match the source file sizes.

4. Change impairment to packet errors (0.1%). Do not correct the TCP checksum.
5. Run the replication event for 3 hours.

   Use an I/O generator to write continuously for 3 hours with 100-percent random data on the replication source storage file system from each host. Confirm that file replication completes by verifying that files are present on the replication destination storage file system and that the destination file sizes match the source file sizes.

Validation

1. The IPEX tunnel OpStatus is "Up".
2. The CRC impairment configuration is successful.
3. Storage replication is successful.

   Perform MD5 checksum on all source and destination files. MD5 checksum values should be identical.
4. The packet error impairment configuration is successful.
5. Storage replication is successful.

   Perform MD5 checksum on all source and destination files. MD5 checksum values should be identical.

Results

<PROVIDE PASS OR FAIL RESULT HERE:>

<PROVIDE EVIDENCE TO SUPPORT TEST RESULT HERE:>

<EVIDENCE CAN INCLUDE CONSOLE OUTPUT OR SCREENSHOTS TO VALIDATE TEST RESULT:>

1.3.3 LAN Network Impairment for Extended Run

Test Objective

Verify that replication is successful with network impairment on the LAN and no concurrent FCIP traffic over a 3-hour period.

- CRC errors
- Packet errors
- Packet drops

Setup

Insert a network impairment device on the LAN side of the setup.

Test Steps

1. View the IPEX tunnel status.

   ```
   portshow fciptunnel -c
   ```

2. Initiate CRC error impairment up to LAN-device supported values, not to exceed 1 percent total.
3. Run the replication event for 3 hours.

   Use an I/O generator to write continuously for 3 hours with 100-percent random data on the replication source storage file system from each host. Confirm that file replication completes by verifying that files are present on the replication destination storage file system and that the destination file sizes match the source file sizes.
4. Change impairment to packet errors up to LAN-device supported values, not to exceed 1 percent total. Do not correct the TCP checksum.
5. Run the replication event for 3 hours.

   Use an I/O generator to write continuously for 3 hours with 100-percent random data on the replication source storage file system from each host. Confirm that file replication completes by verifying that files are present on the replication destination storage file system and that the destination file sizes match the source file sizes.

6. Change impairment to packet drops up to LAN-device supported values, not to exceed 1 percent total.
7. Run the replication event for 3 hours.

   Use an I/O generator to write continuously for 3 hours with 100-percent random data on the replication source storage file system from each host. Confirm that file replication completes by verifying that files are present on the replication destination storage file system and that the destination file sizes match the source file sizes.

Validation

1. The IPEX tunnel OpStatus is "Up".
2. The CRC impairment configuration is successful.
3. Storage replication is successful.

   Perform MD5 checksum on all source and destination files. MD5 checksum values should be identical.
4. The packet error impairment configuration is successful.
5. Storage replication is successful.

   Perform MD5 checksum on all source and destination files. MD5 checksum values should be identical.
6. The packet drop impairment configuration is successful.
7. Storage replication is successful.

   Perform MD5 checksum on all source and destination files. MD5 checksum values should be identical.

Results

<PROVIDE PASS OR FAIL RESULT HERE>

<PROVIDE EVIDENCE TO SUPPORT TEST RESULT HERE>

<EVIDENCE CAN INCLUDE CONSOLE OUTPUT OR SCREENSHOTS TO VALIDATE TEST RESULT>