This article provides an overview of end-to-end data protection as provided by implementing the T10 standard data integrity field (DIF). In addition, it provides configuration information and restrictions based on the current implementation for Power Systems. Reading this article provides the information required to set up a Power System for T10 DIF within the current constraints and an overview of how it is implemented.

Overview

The ANSI T10 standard provides a way to check the integrity of data read and written from the host bus adapter to the disk and back through the SAN fabric. This check is implemented through the data integrity field (DIF) defined in the T10 standard.

AIX has implemented the Type 1 DIF in AIX 6.1 TL6 SP5 and AIX 7.1 SP3. In the Type 1 implementation the 8 byte DIF consists of a Ref Tag, an App Tag, and a CRC. A Type 1 DIF is defined as having a 2 byte CRC, a 2 byte App tag, and a 4 byte Ref tag, which consists of the lower 32 bits of the logical block address. See Figure 1 below as an example.

Figure 1. Type 1 DIF definition

Figure 1 shows a data block (for example, a 512 byte sector) with the 8-byte footer attached to the end. The contents of the 8-byte footer are shown with the fields which make up the Type 1 DIF, the CRC, the App Tag, and the Ref Tag.

On a write, the DIF is generated by the host bus adapter (HBA), based on the block data and logical block address. The DIF field is added to the end of the data block, and the data is sent...
through the fabric to the storage target. The storage target validates the CRC and Ref tag and, if correct, stores both the data block and DIF on the physical media. If the CRC does not match the data, then the data was corrupted during the write. The write op is returned back to the host with a write error code. The host records the error and retransmits the data to the target. In this way, data corruption is detected immediately on a write and never committed to the physical media.

On a read, the DIF is returned along with the data block to the host, which validates the CRC and Ref tags. This validation adds a very small amount of latency—sub millisecond—per IO and potentially could impact overall response time on smaller block transaction < 4K.

Figure 2 illustrates the path taken by the data.

**Figure 2. Data flow with DIF**

![Diagram of data flow with DIF]

Figure 2 shows the read data block flow from the system processor/memory/OS/App to the HBA; the HBA through the SAN fabric to the target port on the storage; and inside the storage from the target port to the storage processor/memory/application and to the disk. The path from the system processor/memory/OS/App to the HBA contains only the read data block. The DIF is attached to the read data block at the HBA. The read data and DIF are sent through the SAN fabric to the target port on the storage then to the storage processor/memory/application and written to the disk.

For the initial implementation of T10 DIF, the following restrictions apply:

- AIX is the only host with the T10 DIF implementation on POWER.
  - Type 1 DIF is supported.
  - App Tag is always 0x4149 (ASCII “AI”).
  - AIX 6.1 TL6 SP5 or AIX 7.1 SP3 is required.
  - Not supported on virtual fibre channel devices.
- The 2 port, 8Gb PCIe Fibre Channel Adapted must be used.
  - 200307 level of firmware or higher is required.
  - Feature code 5735 or low profile feature code 5273 is required.
  - No support on Power Blades.
- IBM DS3950, DS5020, DS5100 or DS5300 storage must be used as target storage.
Subsequent releases incorporate expansion of coverage as part of the overall Power Systems end-to-end data protection initiative.

**Setup**

The following setup steps assume that all restrictions have been followed.

1. **Find all paths to the disks.**
   a. Run `lspath -l hdisk#` on all hdisks where DIF protection is desired. The fscsi# devices (FC protocol devices) is returned from this command.
   b. Run `lsdev -l fscsi# -F'name parent'` to find the parent of a fscsi# device.

2. **Enable protection on the FC adapter (DIF_enabled attribute of fcs device).** Step 2 should be done on all the FC adapters from which the disk has paths.
   a. Run command `rmdev –Rdl fscsi#` to allow changing of attributes on fcs
   b. To enable protection on FC adapter, run `chdev -l fcs# -a DIF_enabled=yes`  
      `(DIF_enabled=no disables protection.)`
   c. Run command `cfgmgr` to rediscover disks.
   d. The `smit fcsa` command can also be used to enable/disable protection on fcs#

3. **Enable T10 protection on a disk.** To enable protection on a disk the disk also must support "Type 1" T10 protection.
   a. To enable T10 protection on a disk, run `chdev -l hdisk# -a DIF_protection=yes"`  
      `(DIF_protection=no disables protection).
   b. The `smit disk` command can also be used to enable/disable protection on hdisk#.
   c. User has to check current value of this attribute after enabling protection using the `lsattr -El hdisk#` command.
   d. If this attribute has a values of unsupported it means one of the following:
      i. Some or all paths to disk do not support protection.
      ii. The disk does not support protection.
Related topics

- See [T10 Technical Committee](https://www.ibm.com/developerWorks/ibm/trademarks/) for more information about I/O interfaces.
- Read what Martin K. Petersen said about [Proactively preventing data corruption](https://www.ibm.com/developerWorks/ibm/trademarks/).

© Copyright IBM Corporation 2011
[Trademarks](https://www.ibm.com/developerworks/ibm/trademarks/)