Technical Support Bulletin

Background Verifies Mandatory on All SFA Installations

ALERT! All SFA storage arrays running any version of SFA OS must be configured with **BACKGROUND VERIFIES ENABLED** on all virtual disks or pools.

Determination of Best Practice

DDN has determined that, during normal operation, background verify scans must be enabled on all virtual disks (VDs) or storage pools on all SFA storage arrays running any version of SFA OS. This requirement applies to all configurations in all application environments, including test environments, and to NVMe and SAS SSDs and SAS and SATA HDDs without exception.

If background verifies are turned off briefly for diagnostic purposes at the direction of a DDN engineer, they must be resumed immediately thereafter.

Background verifies discover and repair on-disk errors before the data is needed by an application. When enabled, each background verify job continuously scans its designated VD or storage pool for medium errors, recovered errors, and inconsistencies between data and parity or DIF checksums. Errors are automatically repaired in the background if sufficient redundancy exists on the VD or pool. A user-configurable verify policy number allows customers to manage the overhead imposed by the verification process and minimize its impact on performance.

Potential consequences of failure to enable continuous background verifies on all SFA VDs or pools include:

- **Uncorrected medium errors** on individual drives
- **Risk of data loss** if a pool gets into a nonredundant state

Exception Requests

Customers who prefer not to enable background verifies on *all* VDs or pools on *all* SFA equipment must advise

DDN of their *request for an exception in writing*. This exception request should be directed to the Vice President of Global Services and Support at DDN, and must explicitly acknowledge your understanding of the risks above.

Determining Current Verify Status

Background verifies are enabled at two levels on SFA storage platforms: (1) globally for the subsystem as a whole; and (2) locally for each VD or pool on the subsystem. Background verify status must be checked at both levels.

DETERMINING GLOBAL VERIFY STATUS FOR THE SUBSYSTEM

To determine whether the background verify feature is enabled globally for the SFA subsystem, log in to either controller using SSH and enter the following command at the SFA command line:

```
show subsystem
```

The resulting output should show the **Verify Policy** value as `ENABLED`. For example:

```
*********************
*     Subsystem     *
*********************
                                                   |   Locate    |   Fast   | Verify
Name          |Time                      | Licences | Dwell Time | Timeout | Policy | UUID
--------------------------------------------------------------------------------------------
L1_7700SFX     Thu May 28 17:45:46 2015  R D X E    120 seconds    OFF     ENABLED  ...
```

DETERMINING LOCAL VD VERIFY STATUS UNDER SFA OS DECLUSTERED RAID

Under SFA OS with declustered RAID (versions 11.0.x and later), background verify jobs execute against VDs, not storage pools. The verify status of each VD on the subsystem must be checked individually.

A given VD is protected by background verify scans only if both of the following conditions are met:

- *Verify scans* are enabled for that particular VD.
- *Verify jobs* for that VD are running continuously and successfully.

To determine whether verify scans are locally enabled for each VD, enter the following command:

```
show vd
```

If verify scans are enabled correctly, the **Settings** and **Jobs** columns in the command output will both show a “V” entry for every VD on the SFA subsystem. For example:

```
***************************
* Virtual Disk(s) *
***************************
                                                            |      Home
 Idx|Name       | State |Pool|RAID|Capacity|Settings|  Jobs |Current|Preferred
------------------------------------------------------------------------------
   1 vd-1_1       READY     1   1    1.8 TiB   T V WM     V    0(L) 0   0(L) 0
   2 vd-2_2       READY     2   6   82.3 TiB   T V WM     V    0(L) 1   0(L) 1
   3 vd-3_3       READY     3   6   82.3 TiB   T V WM     V    1(R) 0   1(R) 0
   4 vd-4_4       READY     4   6   82.3 TiB   T V WM     V    1(R) 1   1(R) 1

Total Virtual Disks: 4
```

Next, check the status of the verify jobs themselves. Enter the command:

```
show job
```

The command output will look similar to the following:

```
***************************
* Jobs *
***************************
                                         |Fraction|
Idx|Type          |Target (Sub) |State   |Complete|Priority|Status    ...
------------------------------------------------------------------------------
 84 VERIFY         VD:1   (NA)   RUNNING     99%      70%             ...
 85 VERIFY         VD:2   (NA)   RUNNING     65%      70%             ...
 86 VERIFY         VD:3   (NA)   RUNNING     65%      70%             ...
 87 VERIFY         VD:4   (NA)   RUNNING     65%      70%             ...

Total Background Jobs: 4
```

Ensure that all of the following are true:

- A verify job is running *for every VD* (see the job Type, Target and State columns).
- No error conditions for the verify jobs appear in the Status column.
- The Fraction Complete increments at least *daily.*
- 100% completion is seen periodically for each VD as expected from the scan cycle time established by the verify policy number (which is shown in the Priority column above).

NOTE Jobs with a value of `VERIFY ONCE` or `VRFY NOCORRECT` in the **Type** column are not ordinary, repeating background verify jobs. They are one-time variants of the verify function. Only the value `VERIFY` in the **Type** column designates a repeating background verify job.

Repeating background verify jobs must be enabled on the affected VDs following the completion of any `VERIFY ONCE` or `VRFY NOCORRECT` jobs.

DETERMINING LOCAL POOL VERIFY STATUS UNDER LEGACY SFA OS

Under SFA OS legacy versions (3.x.x and earlier), background verify jobs execute against storage pools, not VDs. The verify status of each pool must be checked individually.

A given pool is protected by background verify scans only if both of the following conditions are met:

- *Verify scans* are enabled for that particular pool.
- *Verify jobs* for that pool are running continuously and successfully.

To determine whether verify scans are locally enabled for each storage pool, enter the following command:

```
show pool
```

If verify scans are enabled correctly, the Settings and Jobs columns in the command output will *both* show a "V" entry *for every pool* on the SFA subsystem. For example:

```
*****************
*     Pools     *
*****************
                                             |Total  |Free  |Max   |                  |Disk|
Idx |Name     |State     |Chunk|Raid| Faults |cap GB|cap GB|VD GB | Settings | Jobs |T/O |...
----------------------------------------------------------------------------------------------
  1  pool-1    NORMAL      128K  6            9040      0      0  DWMR IV        V     10  ...
  2  pool-2    NORMAL      128K  6            9040      0      0  DWMR IV        V     10  ...
  3  pool-3    NORMAL      128K  6            9040      0      0  DWMR IV        V     10  ...
  4  pool-4    NORMAL      128K  6            9040      0      0  DWMR IV        V     10  ...

Total Storage Pools: 4
```

Next, check the status of the verify jobs themselves. Enter the command:

```
    show job
```

Refer to the **Background Jobs** section of the command output, which will look similar to the following:

```
***************************
*     Background Jobs     *
***************************
                                                         |Fraction|
Idx|Type         |Target  (Sub)    |State        |Complete|Priority|Status               ...
----------------------------------------------------------------------------------------------------
  0 VERIFY        POOL:0  (NA)      RUNNING          99%       10%                      ...
  1 VERIFY        POOL:1  (NA)      RUNNING          97%       10%                      ...
  2 VERIFY        POOL:2  (NA)      RUNNING          97%       10%                      ...
  3 VERIFY        POOL:3  (NA)      RUNNING          97%       10%                      ...

Total Background Jobs: 4
```

Ensure that all of the following are true:

- A verify job is running for *every* pool (see the job **Type**, **Target** and **State** columns).
- No error conditions for those jobs appear in the **Status** column.
- The **Fraction Complete** increments at least *daily.*
- 100% completion is seen periodically for each pool as expected from the scan cycle time established by the verify policy number (which is shown in the **Priority** column above).

Prerequisites for Enabling Verifies After a Period of Disuse

If background verifies have been disabled for some time on any SFA VD or storage pool, *you may have experienced data corruption without knowing it.* Potential data corruption should be resolved before enabling background verifies. DDN strongly recommends the following procedure prior to enabling background verifies for the first time after a period of background verify disuse.

1. First run *two full passes of force verifies* on each affected VD or pool. Running force verifies twice enables the *second* pass to take advantage of corrections made during the *first* pass to find more redundancies that can be used to recover more corrupted data.

SFA OS WITH DECLUSTERED RAID

For SFA OS 11.0.x and later, issue the following force verify command against each affected VD:

```
verify vd <vd-idx> force_consistency priority <policy-number>
```

where

<pool-idx> is the index of the pool to be verified (wild card * not allowed)

<policy-number> see Choosing a Verify Policy Number (or “Priority”) or contact DDN Support

`force_consistency` causes the verify job to immediately correct any errors it finds based on the current redundancy in the pool

LEGACY SFA OS

For SFA OS 3.x.x and earlier, issue the following force verify command against each affected storage pool:

```
verify pool <pool-idx> force_consistency priority <policy-number>
```

where

<pool-idx> is the index of the pool to be verified (wild card * not allowed)

<policy-number> see Choosing a Verify Policy Number (or “Priority”) or contact DDN Support

`force_consistency` causes the verify job to immediately correct any errors it finds based on the current redundancy in the pool

2. If medium errors or uncorrected bad blocks remain after the second force verify job completes, *contact DDN Support for assistance with data recovery*.
3. Once the second (or a subsequent) force verify job completes cleanly, with no medium errors or uncorrected bad blocks reported, enable background verifies on the pool.
4. Repeat Steps 1-3 on all pools which have not been running background verifies.

ALERT! ***Do NOT update SFA OS firmware, drive firmware*, or major storage component firmware if background verifies have been suspended on any storage pool for a substantial length of time. Perform the above procedure on all affected pools first before updating SFA firmware.**

Enabling Background Verifies

Background verifies must be enabled at two levels on SFA storage platforms: (1) globally for the SFA subsystem as a whole; and (2) locally for each VD or pool on the subsystem.

ENABLING VERIFIES GLOBALLY FOR THE SUBSYSTEM

To enable the background verify feature globally for the SFA subsystem, log in to either controller using SSH and enter the following command at the SFA command line:

```
set subsystem verify_policy true
```

ENABLING LOCAL VIRTUAL DISK VERIFIES UNDER SFA OS DECLUSTERED RAID

Under SFA OS with DCR, background verify jobs execute against VDs, not storage pools. Verifies must be enabled for each VD on the subsystem.

For each VD on the subsystem, enable background verifies by setting the pool verify policy number (also known as “priority” in some SFA OS reports) to an integer value *from 1 to 98*. The syntax for the line command that sets the VD verify policy is:

```
set vd <vd-idx> verify_policy <policy-number>
```

where

<vd-idx> = index of the VD to be enabled, or the asterisk (*) wildcard for all VDs

<policy-number> = integer from 1 - 98 (or 0 to disable, or 99 for non-background maximum speed)

For example, to enable background verifies on VD 3 with a low-resource, long-duration verify policy number of 70:

```
set vd 3 verify_policy 70
```

Under SFA OS with DCR, VDs are created by default with background verifies enabled and a verify policy number of 70. *A verify policy number of 70* is suggested for DCR VDs as a rule of thumb in the absence of more specific information. This value will scan an entire VD over the course of about 58 days. Background verifies will cycle through repeated verify scans of this duration in the background with little impact to overall performance. See Choosing a Verify Policy Number (or "Priority") for more information.

ENABLING LOCAL POOL VERIFIES UNDER LEGACY SFA OS

Under legacy SFA OS, background verify jobs execute against storage pools, not VDs. Verifies must be enabled individually for each storage pool on the subsystem.

For each pool on the subsystem, enable background verifies by setting the pool verify policy number (also known as "priority" in some SFA OS reports) to an integer value *from 1 to 98*. The syntax for the line command that sets the pool verify policy is:

```
set pool <pool-idx> verify_policy <policy-number>
```

where

<pool-idx>	= index of the pool to be enabled
<policy-number>	= integer from 1 - 98 (or 0 to disable, or 99 for non-background maximum speed)

For example, to enable background verifies on pool 3 with a low-resource, long-duration verify policy number of 5:

```
set pool 3 verify_policy 5
```

A verify policy number from 5 to 10 is suggested for legacy SFA OS pools as a rule of thumb in the absence of more specific information. These values will verify an entire pool over the course of about 44.5 to 47 days. Background verifies will cycle through repeated verify scans of this duration in the background with little impact to overall performance. See Choosing a Verify Policy Number (or "Priority") for more information.

Choosing a Verify Policy Number (or "Priority")

The verify policy number (or "priority") determines the duration of a verify scan cycle. Higher verify policy numbers enable verifies to complete each scan cycle in less time, but the jobs use more system resources to do it and have more impact on application I/O performance. Lower verify policy numbers have less impact on application I/O performance, but take longer to complete.

Verify policy numbers for SFA OS with DCR cannot be compared to verify policy numbers for legacy SFA OS. These values are calculated differently for the two SFA architectures and mean different things. For example, if you set the verify policy number to 5 on a legacy SFA OS storage system, the verify scan cycle would complete in about 47 days (about a month and a half), while on SFA OS with DCR, it would take about 188 days (more than 6 months). Conversely, if you wanted a verify scan cycle to complete about every 30 days, you would set the verify policy number to 39 on legacy SFA OS, but on SFA OS with DCR you would set it to 84.

ALERT! **Much larger verify policy values are needed with declustered RAID versions of SFA OS (11.0.x and later) than with legacy SFA OS (3.x.x and earlier) in order to achieve the same scan cycle times.**

CALCULATING THE VERIFY POLICY NUMBER FOR SFA OS WITH DECLUSTERED RAID

For SFA OS with DCR, verify policy numbers from 1 to 98 correspond to a verify scan time in multiples of 48 hours. Incrementing the verify policy number by 1 increases verify scan time by about 48 hours, while decrementing the verify policy number by 1 decreases verify scan time by about 48 hours. As expected verify completion time speeds up, application I/O performance slows down.

- **To estimate the days to verify scan completion** for a DCR verify policy number, use the following formula:

  Days = (99 - Policy Number) × 2

  For example, a verify policy of 84 would set the verify scan cycle time to (99 - 84) x 2 = 30 days.

- **To find the verify policy number** needed to complete a DCR verify scan in a given number of days, use the formula:

  Policy Number = 99 - (0.5 × Days)

  For example, if you want verify scans to complete every 45 days, set the verify policy number to 99 - (0.5 x 45) = 76.5 ≈ 77.

CALCULATING THE VERIFY POLICY NUMBER FOR LEGACY SFA OS

For legacy SFA OS, verify policy numbers from 1 to 98 correspond to resource utilizations from 1% to 98% of the maximum. As resource utilization goes up, verify scan cycle times go down but application I/O performance takes more of a hit.

- **To estimate the days to verify scan completion** for a legacy RAID verify policy number, use the following formula:

  Days = (99 - Policy Number) ÷ 2

  For example, a verify policy number of 5 would set the verify scan cycle time to (99 - 5) ÷ 2 = 47 days.

- **To find the verify policy number** needed to complete a legacy RAID verify scan in a given number of days, use the formula:

  Policy Number = 99 - (2 x Days)

  For example, if you want scans to complete every 45 days, choose a legacy RAID verify policy number equal to 99 - (2 x 45) = 9.

Contacting DDN Technical Support

Please contact DDN Technical Support at any time if you have questions or need assistance. Support can be reached online, by email, or by phone as listed below.

Web

DDN Community Support Portal	https://community.ddn.com/login
Portal Assistance	webportal.support@ddn.com

Email

Support Email	support@ddn.com

Telephone

DDN Support Worldwide Directory	https://www.ddn.com/support/global-services-overview/

Bulletins & Notices

Support Bulletins	http://www.ddn.com/support/technical-support-bulletins
End-of-Life Notices	http://www.ddn.com/support/end-of-life-notices
Release Notes	https://community.ddn.com/login
Subscription Requests	support-tsb@ddn.com