DELL Technologies

MODULE 3 SCALABILITY, PERFORMANCE, AND COMPLIANCE FEATURES

PARTICIPANT GUIDE

Table of Contents

FAST Cache 5

FAST Cache Overview 6
FAST Cache Components 8
FAST Cache Operations 10
Supported Drives and Configurations 11
Create FAST Cache 12
Enable FAST Cache 13
Expand FAST Cache 15
Expand FAST Cache Management 18
Shrink FAST Cache 19
Shrink FAST Cache Management 21
Delete FAST Cache 22
Demonstration 23

Host I/O Limits 24

Host I/O Limits Overview 25
Host I/O Limit Use Cases 26
Host I/O Limit Policy Types 27
Host I/O Limit Policy – Examples 28
Shared Policies 30
Shared Density-Based Host I/O Limits 31
Multiple Resources Within a Single Policy 32
Density-Based Host I/O Limits Values 34
Burst Feature Overview 35
Burst Creation 36
Burst Configuration 37
Burst Calculation Example 38
Burst Scenarios 39
Burst Scenario 1 40
Animation - Burst Scenario 1 47
Burst Scenario 2 48

Animation - Burst Scenario 2 54
Policy Level Controls 55
Policy Level Controls Defined 56
Host I/O Limits System Pause – Settings 58
Host I/O Limits Policy Pause – Unisphere 60
Demonstration 63

UFS64 File System Extension and Shrink 64

File System Extension Overview 65
Manual UFS64 File System Extension 66
Automatic UFS64 File System Extension 67
Storage Space Reclamation Overview 68
UFS64 Thin File System Manual Shrink 69
UFS64 File System Automatic Shrink 71
File System Extension and Shrink Operations 72

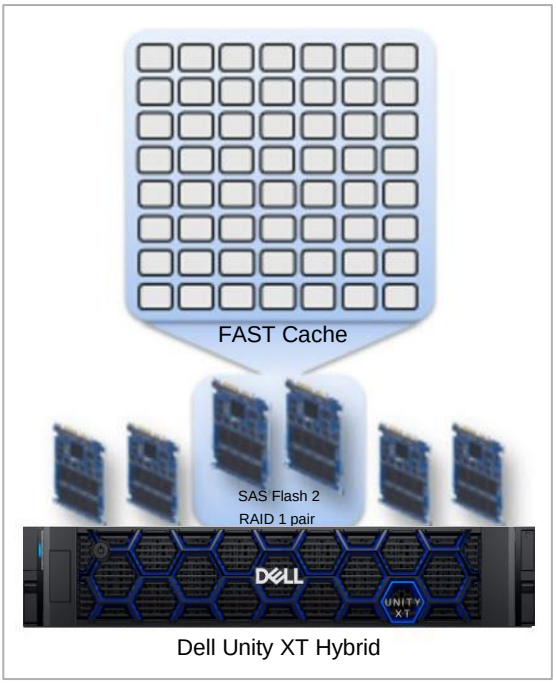
File-level Retention (FLR) 73

FLR Overview 74
FLR Capabilities and Interoperability 77
Process to Enable and Manage FLR 79
Enable FLR on a File System 81
Enable writeverify for FLR-C 82
Define FLR Retention Periods 83
Set File State - NFS 85
Set File State - FLR Toolkit for SMB 87
Set File State - Automated 89
Scalability, Performance and Compliance Key Points 90

FAST Cache

FAST Cache

FAST Cache Overview

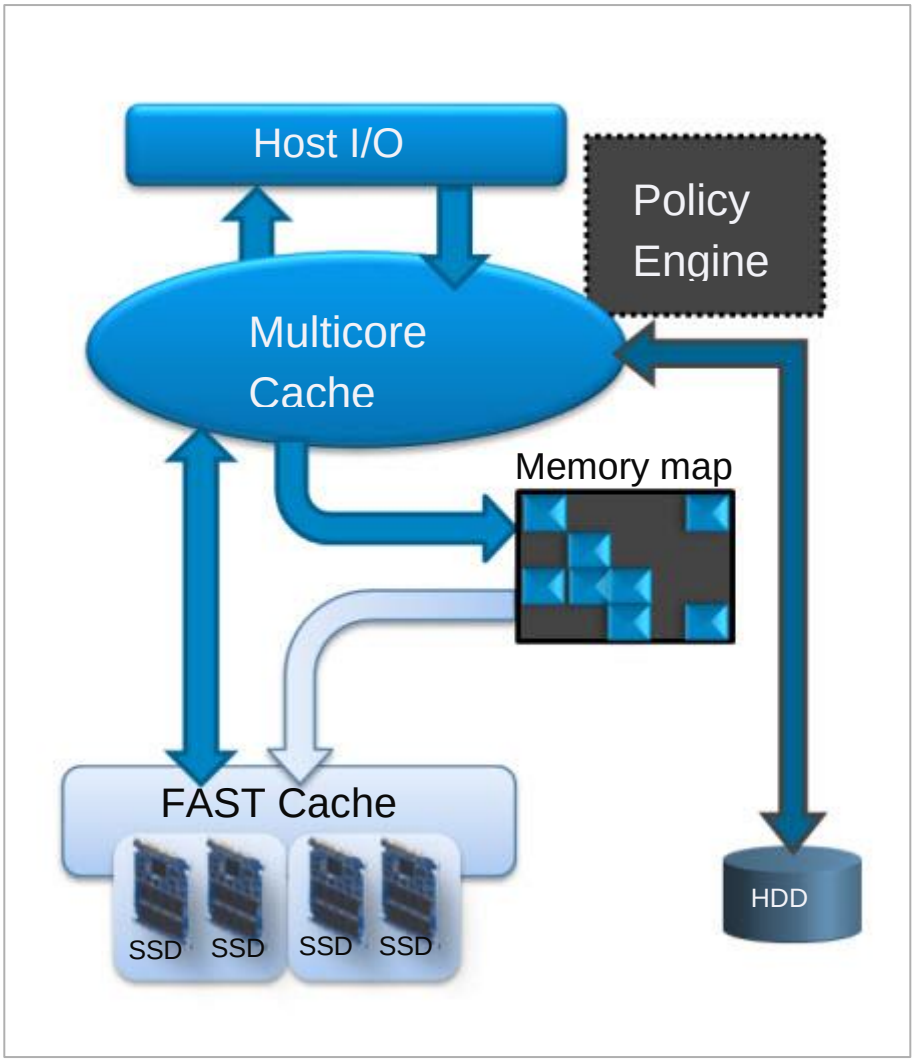


FAST Cache using SAS Flash 2 drives in RAID 1 pair.

- FAST Cache is a performance feature for Hybrid Unity XT systems that extends the existing caching capacity.
- FAST Cache can scale up to a larger capacity than the maximum DRAM Cache capacity.
- FAST Cache consists of one or more RAID 1 pairs [1+1] of SAS Flash 2 drives.
  - Provides both read and write caching.
    - For reads, the FAST Cache driver copies data off the disks being accessed into FAST Cache.
    - For writes, FAST Cache effectively buffers the data waiting to be written to disk.
- At a system level, FAST Cache reduces the load on back-end hard drives by identifying when a chunk of data on a LUN is accessed frequently.
- The system copies the frequently accessed data temporarily to FAST Cache.
- The storage system then services any subsequent requests for this data faster from the Flash disks that make up FAST Cache.

- FAST Cache reduces the load on the disks that the LUN is formed from which will ultimately contain the data.
- The data is flushed out of cache when it is no longer accessed as frequently as other data.
- Subsets of the storage capacity are copied to FAST Cache in 64 KB chunks of granularity.

FAST Cache Components



FAST Cache components

Policy Engine - The FAST Cache Policy Engine is the software which monitors and manages the I/O flow through FAST Cache. The Policy Engine keeps statistical information about blocks on the system and determines what data is a candidate for promotion. A chunk is marked for promotion when an eligible block is accessed from spinning drives three times within a short amount of time. The block is then copied to FAST Cache, and the Memory Map is updated. The policies that

are defined in the Policy Engine are system-defined and cannot be modified by the user.

Memory Map - The FAST Cache Memory Map contains information of all 64 KB blocks of data currently residing in FAST Cache. Each time a promotion occurs, or a block is replaced in FAST Cache, the Memory Map is updated. The Memory Map resides in DRAM memory and on the system drives to maintain high availability. When FAST Cache is enabled, SP memory is dynamically allocated to the FAST Cache Memory Map. When an I/O reaches FAST Cache to be completed, the Memory Map is checked. The I/O is either redirected to a location in FAST Cache or to the pool to be serviced.

FAST Cache Operations

- **Host read/write operation**
  - During FAST Cache operations, the application gets the acknowledgment for an I/O operation after it is serviced by FAST Cache. FAST Cache algorithms are designed such that the workload is spread evenly across all the Flash drives that have been used for creating the FAST Cache.
- **FAST Cache promotion**
  - During normal operation, a promotion to FAST Cache is initiated after the Policy Engine determines that 64 KB block of data is being accessed frequently. For consideration, the 64 KB block of data must have been accessed by reads and/or writes multiple times within a short amount of time.
- **FAST Cache flush**
  - A FAST Cache Flush is the process in which a FAST Cache page is copied to the HDDs and the page is freed for use. The **Least Recently Used** [LRU] algorithm determines which data blocks to flush to make room for the new promotions.
- **FAST Cache cleaning**
  - FAST Cache performs a cleaning process which proactively copies dirty pages to the underlying physical devices during times of minimal back-end activity.

Supported Drives and Configurations

FAST Cache is only supported on the Dell Unity XT hybrid models. This is because the data is already on flash drives on the All-Flash models. Dell Unity hybrid models support 200 GB, 400 GB, or 800 GB SAS Flash 2 drives in FAST Cache, dependent on the model. The Dell Unity XT hybrid models support 400 GB SAS Flash 2 drives only. See the Dell Unity Drive Support Matrix documentation for more information.

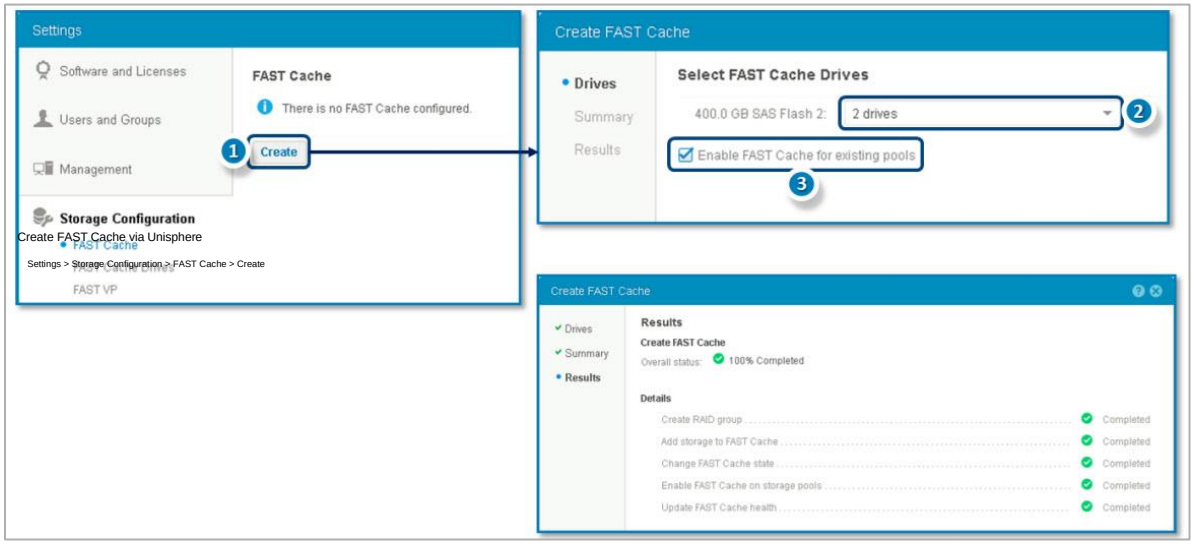
The table shows each Unity XT hybrid model, the SAS Flash 2 drives supported for that model, the maximum FAST Cache capacities and the total Cache.

Hybrid System Model	System Memory (Cache) per Array	Supported SAS Flash 2 Drives	Maximum FAST Cache Capacity	Total Cache
Dell Unity XT 380	128 GB	Only the 400 GB SAS Flash 2	800 GB	928
Dell Unity XT 480	192 GB		1.2 TB	1.39 TB
Dell Unity XT 680	384 GB		3.2 TB	3.58 TB
Dell Unity XT 880	768 GB		6.0 TB	6.76

FAST Cache specifications

Create FAST Cache

FAST Cache can only be created on physical Dell Unity XT hybrid systems with available SAS Flash 2 drives. In Unisphere, FAST Cache is created from the Initial Configuration Wizard, or from the system Settings page. In this example, there is no existing FAST Cache configuration on the system and it is being created from the system Settings page in the Storage Configuration section. From the FAST Cache page, the **Create** button is selected. The Create FAST Cache wizard is launched to configure FAST Cache. The system has 400 GB SAS FLASH 2 drives available for creating FAST Cache. The drop-down list shows the total number of eligible drives for the FAST Cache configuration. In this example, two drives are selected for the FAST Cache configuration. The **Enable FAST Cache for existing pools** option is checked in this example. Thus, FAST Cache will be enabled on all existing pools on the system. Leave the option unchecked if you want to customize which pools to have FAST Cache enabled and disabled on. The wizard continues the FAST Cache creation process, creating the RAID group for the FAST Cache configuration, then enables FAST Cache on the existing storage pools. The status of the used disks can be seen from the FAST Cache Drives page.



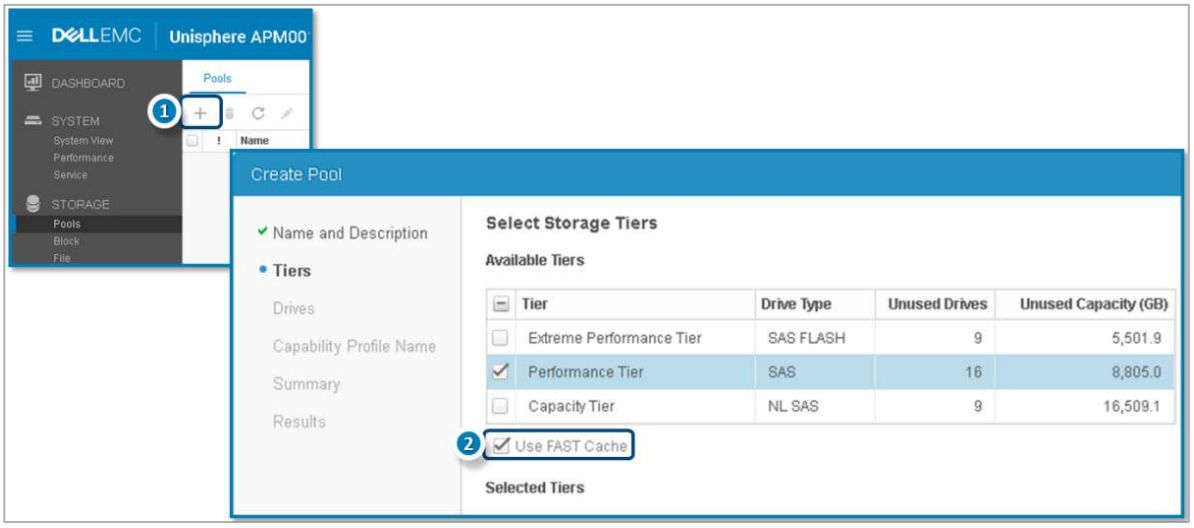
Create FAST Cache via Unisphere

Settings > Storage Configuration > FAST Cache > Create

Enable FAST Cache

Pool Creation Wizard

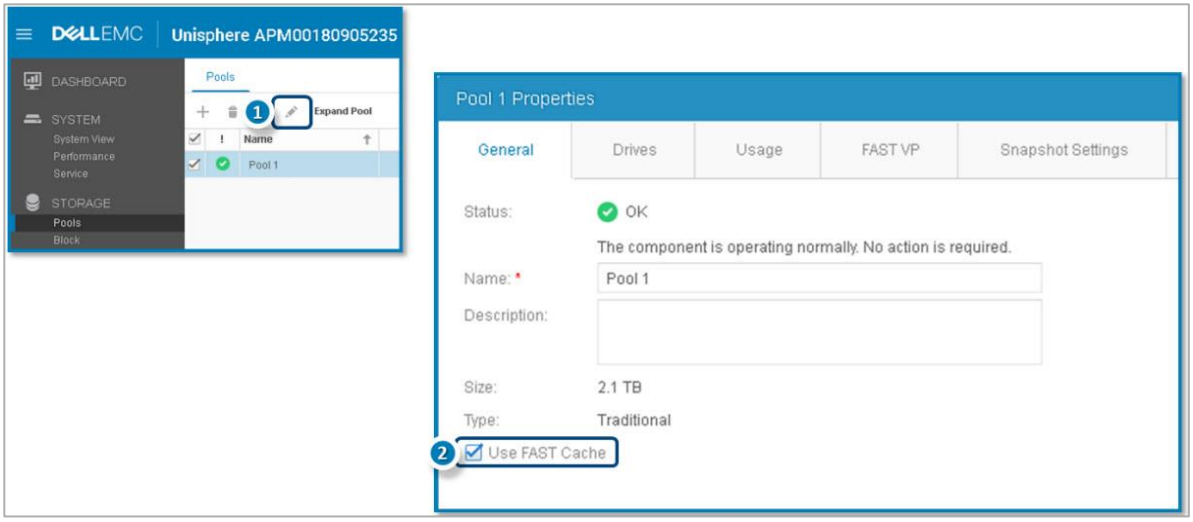
Although FAST Cache is a global resource, it is enabled on a per pool basis. You can enable a pool to use FAST Cache during pool creation. The Create Pool wizard Tiers step has a checkbox option **Use FAST Cache** to enable FAST Cache on the pool being created. The option is disabled if FAST Cache is not created on the system. If FAST Cache is created on the system, the **Use FAST Cache** option is checked by default.



Pool Properties

If FAST Cache was created on the system without the Enable FAST Cache on existing pools option checked, it can be selectively enabled on a per-pool basis. Select a specific pool to enable FAST Cache on and go to its Properties page. From the General tab, check the **Use FAST Cache** option checkbox to enable FAST Cache on the pool.

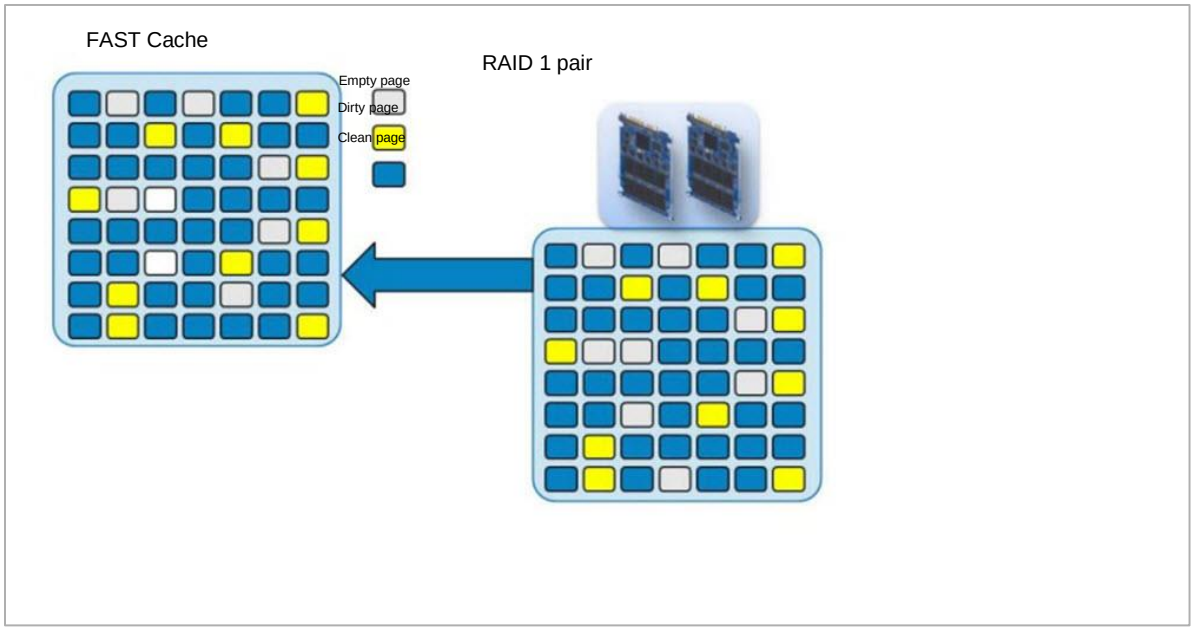
FAST Cache



Expand FAST Cache

Expand Fast Cache Overview

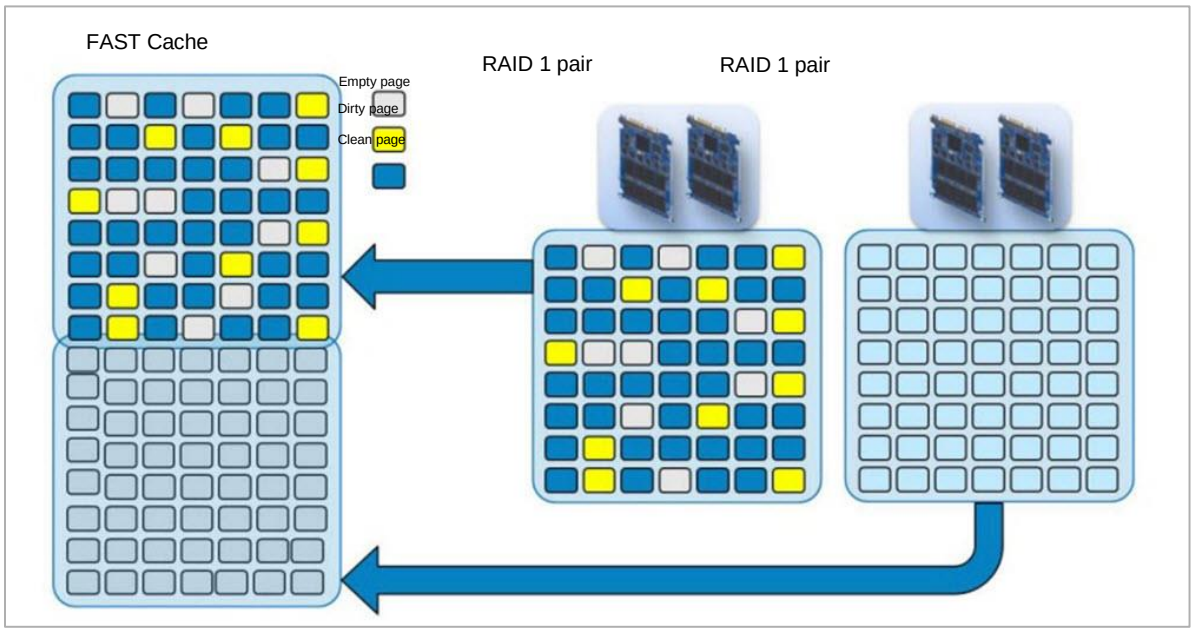
FAST Cache can be expanded online with the Dell Unity XT system. The expansion is used to increase the configured size of FAST Cache online, without impacting FAST Cache operations on the system. The online expansion provides an element of system scalability, enabling a minimal FAST Cache configuration to service initial demands. FAST Cache can later be expanded online, growing the configuration as demands on the system are increased. Each RAID 1 pair is considered a FAST Cache object. In the example shown, the system is configured with a single RAID 1 pair providing the FAST Cache configuration.



Start Fast Cache Expansion

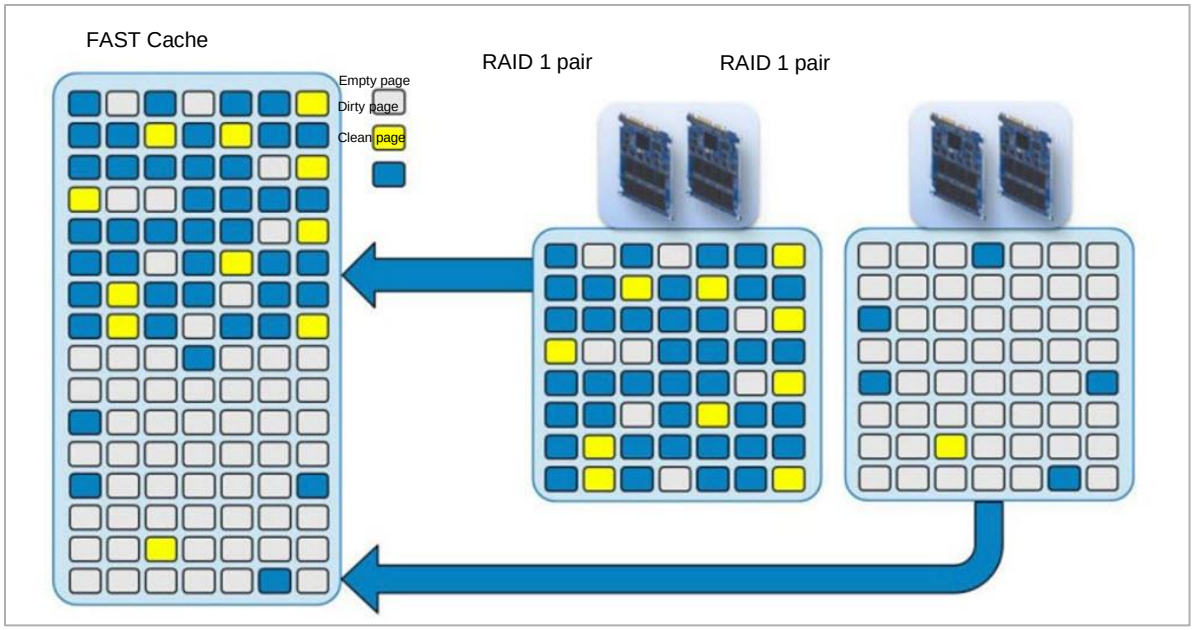
To expand FAST Cache, free drives of the same size and type currently used in FAST Cache must exist within the system. FAST Cache is expanded in pairs of drives and can be expanded up to the system maximum. In the example shown, an extra pair of SSD drives is being added to the existing FAST Cache configuration.

When a FAST Cache expansion occurs, a background operation is started to add the new drives into FAST Cache. This operation first configures a pair of drives into a RAID 1 mirrored set. The capacity from this set is then added to FAST Cache and is available for future promotions. These operations are repeated for all remaining drives being added to FAST Cache. During these operations, all FAST Cache reads, writes, and promotions occur without impact from the expansion. The amount of time the expand operation takes to complete depends on the size of drives used in FAST Cache. The number of drives being added to the configuration also impact the expansion time.



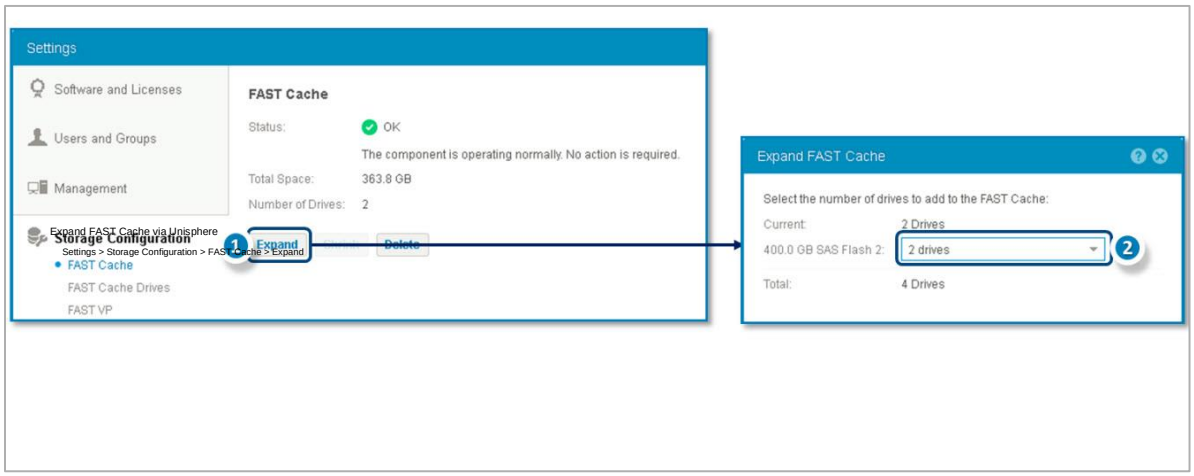
Fast Cache Expansion Completed

The example shows the completion of the FAST Cache expansion. The reconfiguration provides the new space to FAST Cache and is available for its operations.



Expand FAST Cache Management

When FAST Cache is enabled on the Dell Unity XT system, FAST Cache can be expanded up to the system maximum. To expand FAST Cache from Unisphere, go to the FAST Cache page found under Storage Configuration in the Settings window. From this window, select **Expand** to start the Expand FAST Cache wizard. Only free drives of the same size and type currently configured in FAST Cache are used to expand FAST Cache. In this example, only 400 GB SAS Flash 2 drives are available to be selected because FAST Cache is currently configured with those drives. From the drop-down list, you can select pairs of drives to expand the capacity of FAST Cache up to the system maximum. In this example, two drives are being added to the current two drive FAST Cache configuration. After the expansion, FAST Cache is configured with four drives arranged in two RAID 1 drive pairs.

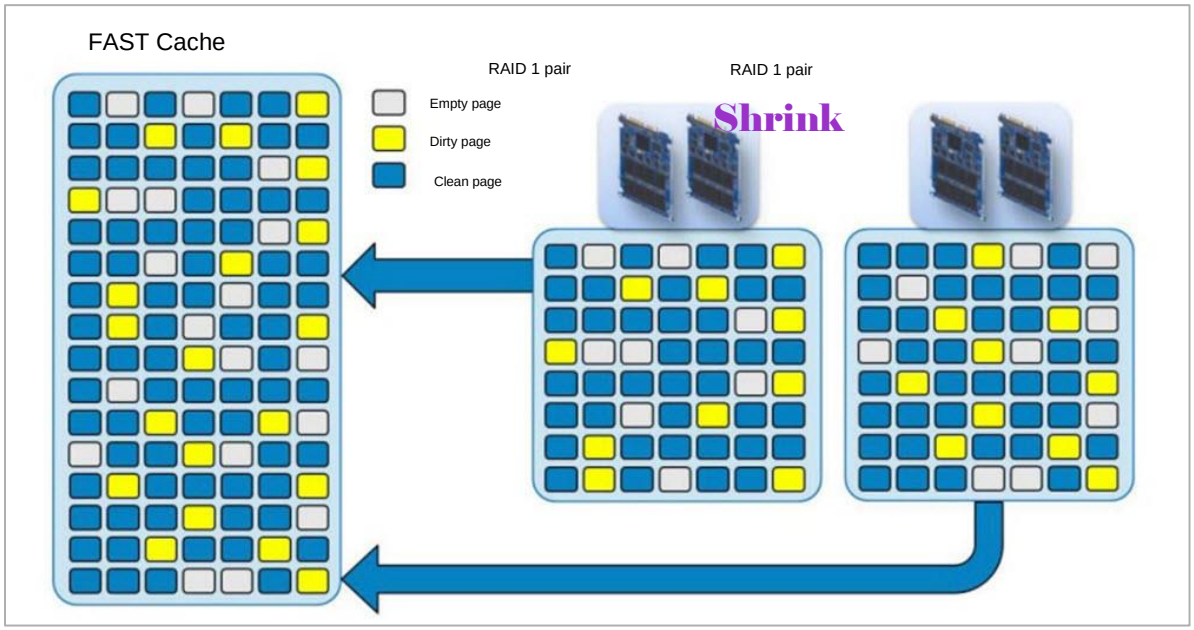


Shrink FAST Cache

FAST Cache Shrink Overview

FAST Cache can be shrunk online with the Dell Unity XT system. Shrinking FAST Cache is performed by removing drives from the FAST Cache configuration and can be performed while FAST Cache is servicing I/O. In the following series of examples, FAST Cache is shrunk by removing an existing pair of drives from the FAST Cache configuration.

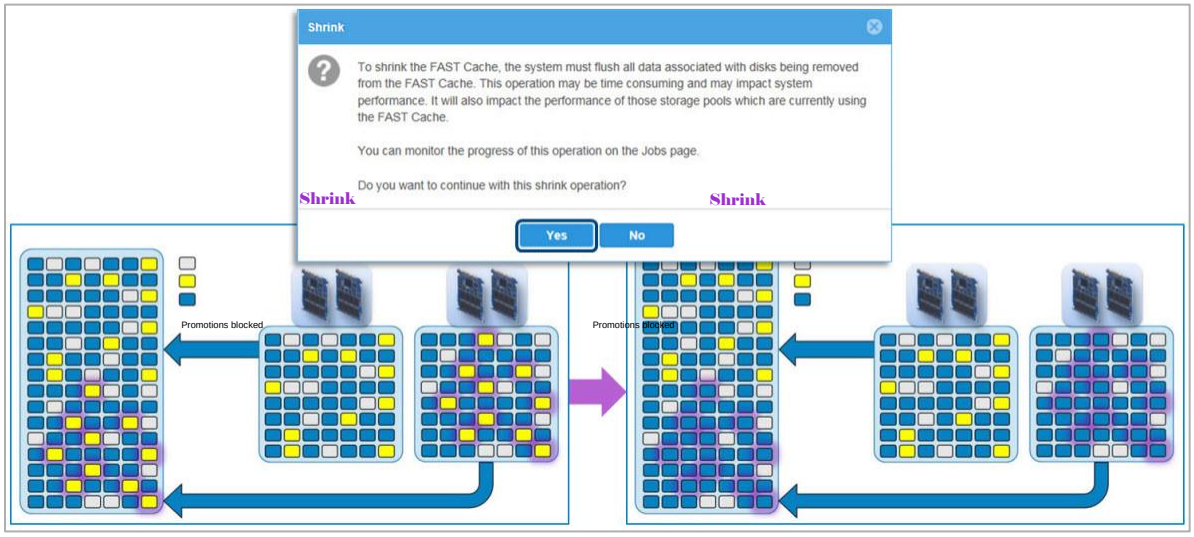
A FAST Cache shrink operation can be initiated at any time and is issued in pairs of drives. A shrink operation allows the removal of all but two drives from FAST Cache. Removing drives from FAST Cache can be a lengthy operation and can impact system performance.



Start FAST Cache Shrink

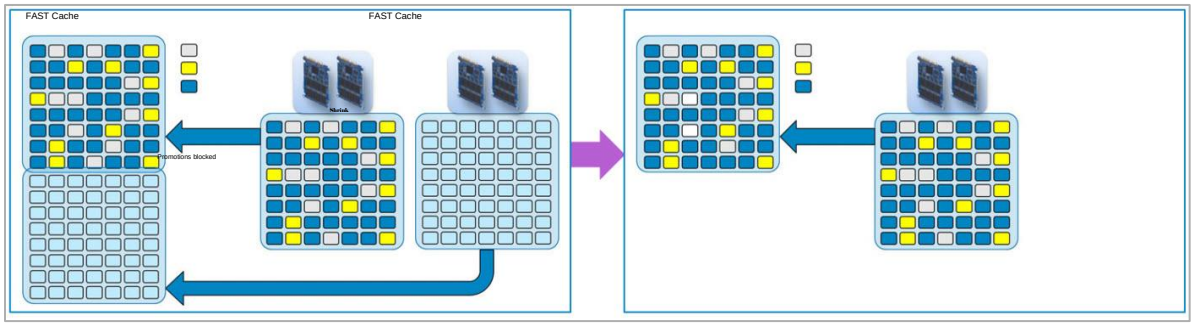
When a FAST Cache shrink occurs, a background operation is started to remove drives from the current FAST Cache configuration. After a shrink operation starts,

new promotions are blocked to each pair of drives selected for removal from FAST Cache. Next, the FAST Cache dirty pages within the drives being removed are cleaned. The dirty page cleaning ensures that data is flushed to the LUN back-end disks.



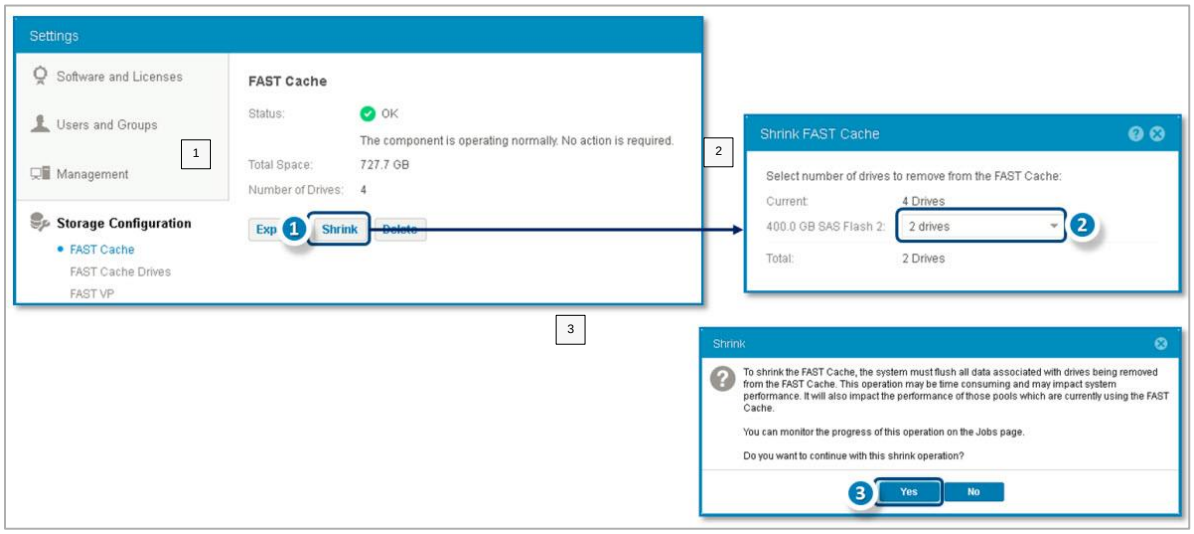
FAST Cache
Shrink Completed

After all dirty pages are cleaned within a set of drives, the capacity of the set is removed from the FAST Cache configuration. For this example, the FAST Cache configuration has been shrunk from two drive pairs down to a single drive pair. Data which existed on FAST Cache drives that were removed may be promoted to FAST Cache again through the normal promotion mechanism.



Shrink FAST Cache Management

FAST Cache supports online shrink by removing drives from its configuration. It is possible to remove all but one RAID 1 pair – each RAID 1 pair is considered a FAST Cache object.



1: To shrink the FAST Cache, select the system Settings option in Unisphere and navigate to the Storage Configuration section.

Select the **Shrink** option and the Shrink FAST Cache window opens.

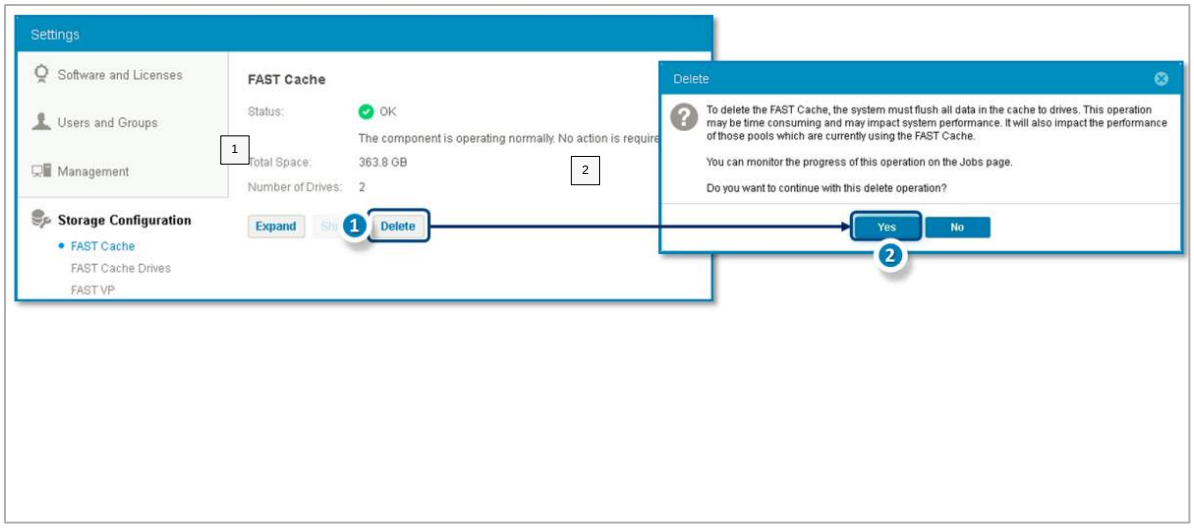
2: In the drop-down list, select the number of drives to remove from the configuration. In this example, the current FAST Cache configuration includes four drives and two drives are being removed.

3: A message is displayed stating that removing the drives from FAST Cache requires the flushing of dirty data from each set being removed to disk.

Click **Yes** to confirm the shrink operation.

Delete FAST Cache

To remove all drives from FAST Cache, the Delete operation is used. FAST Cache delete is often used when drives must be repurposed to a pool for expanded capacity. The delete operation is similar to a shrink operation in that any existing dirty pages must be flushed from FAST Cache to back-end disks. Then the disks are removed from FAST Cache. The delete operation can consume a significant amount of time, and system performance is impacted.



1: To Delete FAST Cache, select the system **Settings** option in Unisphere and go to the Storage Configuration section. Select the **Delete** option and the Delete message window opens.

2: The message states that deleting FAST Cache requires the flushing all data from the FAST Cache drives. Click **Yes** to confirm the delete operation.

Demonstration

This demonstration covers FAST Cache management. It begins by creating FAST Cache on a Dell Unity XT hybrid system. Then the system's FAST Cache capacity is increased by performing an expand operation. Next, a FAST Cache shrink is performed to reduce its capacity. Finally, FAST Cache is removed from the system by performing a delete operation.

Movie:

The web version of this content contains a movie.

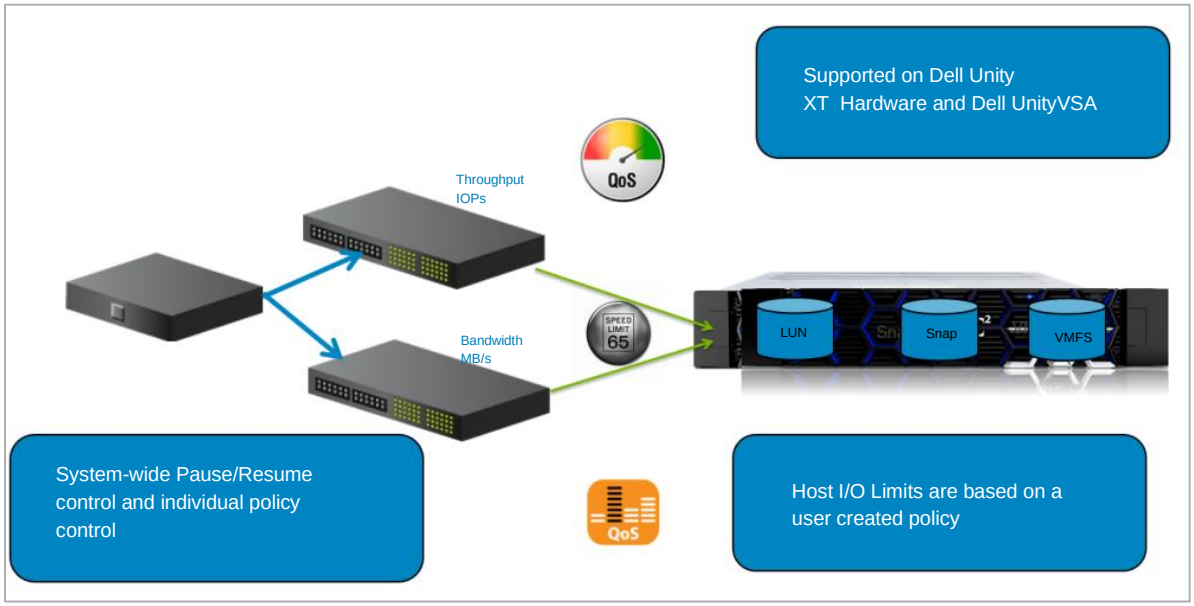
Host I/O Limits

Host I/O Limits Overview

Dell Unity XT Host I/O Limits, also referred to Quality of Service [QoS], is a feature that limits I/O to storage resources: LUNs, attached snapshots, VMFS, and vVol [Block] datastores. Host I/O Limits can be configured on physical or virtual deployments of Dell Unity XT systems. Limiting I/O throughput and bandwidth provides more predictable performance in system workloads between hosts, applications, and storage resources.

Host I/O Limits are Active when the global feature is enabled, policies are created, and assigned to a storage resource. Host I/O Limits provides a system-wide or a specific host pause and resume control feature. Limits can be set by throughput, in IOs per second [IOPS], or bandwidth, defined by Kilobytes or Megabytes per second [KBPS or MBPS], or a combination of both types of limits. If both thresholds are set, the system limits traffic according to the threshold that is reached first.

Only one I/O limit policy can be applied to a storage resource. For example, an I/O limit policy can be applied to an individual LUN or to a group of LUNs. When an I/O limit policy is applied to a group of LUNs, it can also be shared. When a policy is shared, the limit applies to the combined activity from all LUNs in the group. When a policy is not shared, the same limit applies to each LUN in the group.

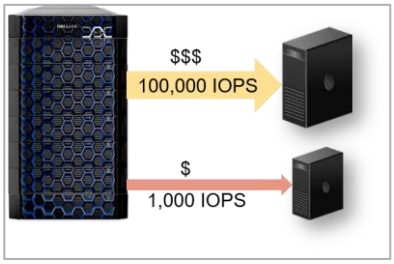


Host I/O overview

Host I/O Limit Use Cases

The Host I/O Limit feature is useful for service providers to control service level agreements.

- Mechanism to control the maximum level of service
  - If a customer wants to have an SLA that specifies 500 IOPS, a limit can be put in place that allows a maximum of 500 IOPS. A service provider can create host I/O policies that meet their requests.
- Storage administrators can limit I/O for followings:
  - **Billing Rates:** Billing rates can be set up for customers or departments dependent on how much I/O each host requires.
  - **Run-away Processes and Busy Users – "Noisy" neighbors:** These processes take resources away from other processes.
  - **Test and Development Environment:** A LUN with a database on it may be used for testing. Administrators can create a snapshot of the LUN and mount it. Putting a limit on the snapshot would be useful to limit I/O on the snap since it is not a production volume.



Host I/O Limits use cases

Host I/O Limit Policy Types

Two Host I/O Limit policy types: **Absolute** and **Density**

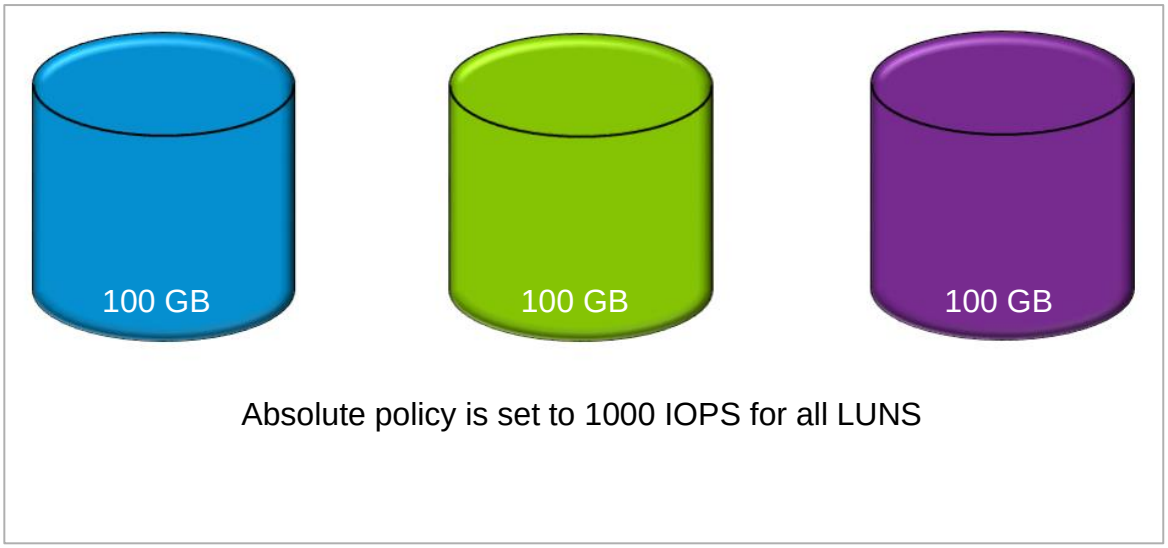
- **Absolute:**
  - An absolute limit applies a maximum threshold to a storage resource regardless of its size.
    - It can be configured to limit the amount of I/O traffic up to a threshold amount based on IOPS, bandwidth or both. If both thresholds are set, the storage system limits traffic according to the threshold that is reached first. The limit is also shared across resources.
    - Burst configuration supported
- **Density-based:**
  - A Host I/O Limit policy is configured based on a capacity of a given storage resource.
    - A density-based host I/O limit scales with the amount of storage that is allocated to the resource. As with the absolute limit, a policy is shared with other resources. When a density-based policy is in place, the IOPS and bandwidth are based on a GB [KBPS or MBPS] value, not a maximum value as with an absolute policy.
    - Burst configuration supported

Host I/O Limit Policy – Examples

Two Host I/O Limit policy examples:

Absolute

In the example, there are three LUNs under the same policy. Setting an absolute policy for the LUNs would limit each LUN to 1000 IOPS regardless of LUN size.

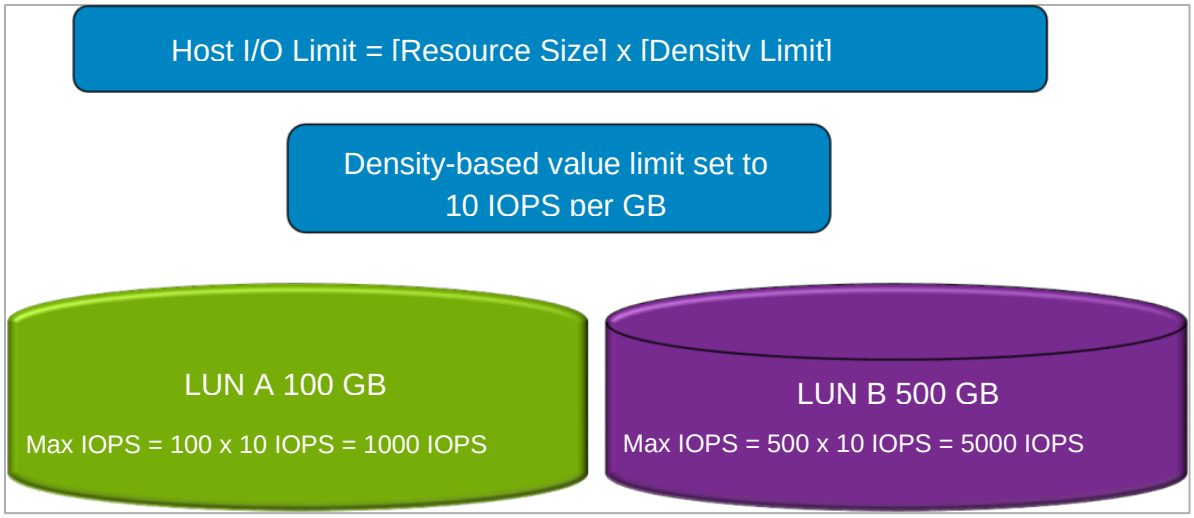


Absolute-based policies limit I/O regardless of resource size

Density-Based

The density-based Host I/O Limit configuration is calculated by taking the Resource Size x [multiplied by] the Density Limit that is set by the Storage Administrator. After set, the Host I/O Limits driver throttles the IOPS based on the calculation.

- LUN A is a 100 GB LUN, so the calculation is 100 [Resource Size] x 10 [Density Limit]. This calculation sets the maximum number of IOPS to 1000.
- LUN B is 500 GB so the calculation is 500 [Resource Size] x 10 [Density Limit]. This calculation sets the maximum number of IOPS to 5000.
- A Service Provider can add both LUNs under a single density-based Host I/O Limit to implement the policy.

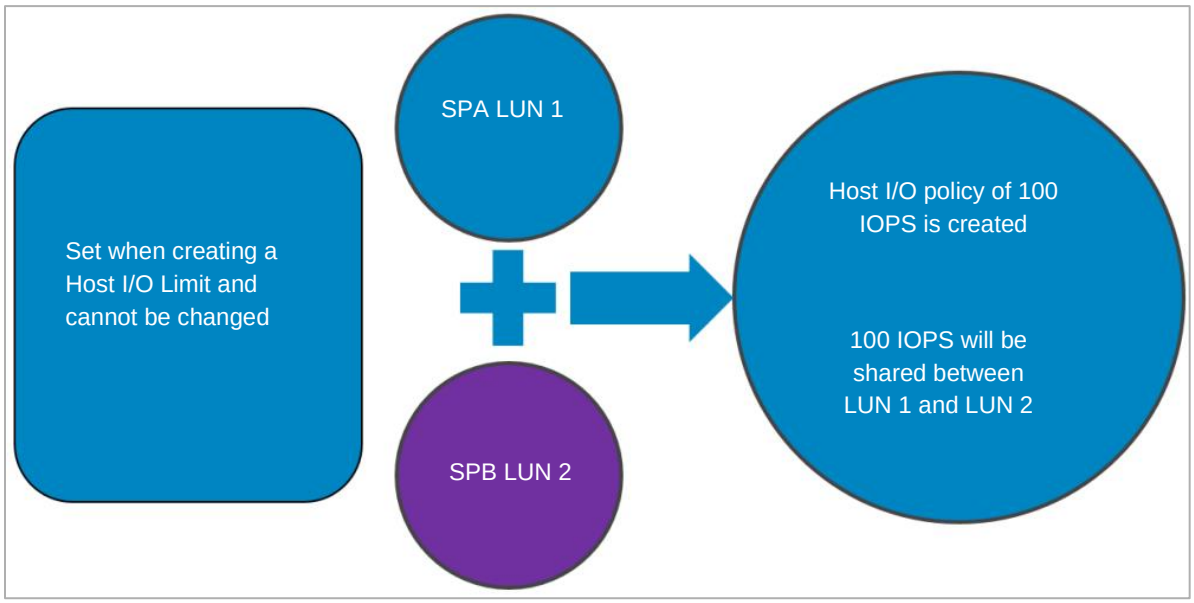


Density-based policies limit I/O based on resource size

Shared Policies

Host I/O Limit allows administrators to implement a shared policy when the initial Host I/O policy is created. The policy is in effect for the life of that policy and cannot be changed. Administrators must create another policy with the Shared check box cleared if they want to disable the setting. When the Shared check box is cleared, each individual resource is assigned a specific limit or limits. When the Shared check box is selected, the resources are treated as a group, and all resources share the limits that are applied in the policy.

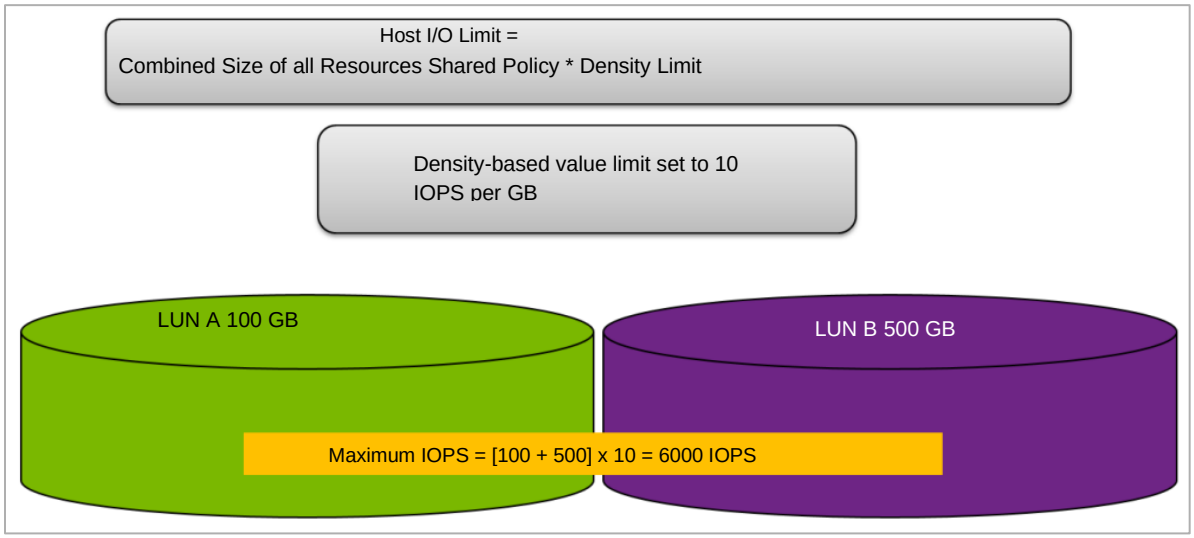
In the example, a Host I/O Limit policy has been created to limit the number of hosts IOPS to 100. In this case, both LUN 1 and LUN 2 share this limit. Shared limits do not guarantee the limits are distributed evenly. From the example with a shared limit of 100 IOPS, LUN 1 can service I/O at 75 IOPS and LUN 2 can service 25 IOPS. Also, if limits are shared across Storage Processors, it does not matter if the LUNs are owned by different SPs. The policy applies to both.



Host I/O limit shared between resources

Shared Density-Based Host I/O Limits

The Density-based Shared Host I/O Limit calculation takes the combined size of all resources sharing the policy multiplied by the Density Limit set by the Storage Administrator. After it is set, the Host I/O Limits driver throttles the IOPS based on the calculation. In the example, LUN A is a 100 GB LUN, LUN B is 500 GB, so the calculation is 100 + 500 [combined resource size] x 10 [Density Limit]. This sets the maximum number of IOPS to 6000.



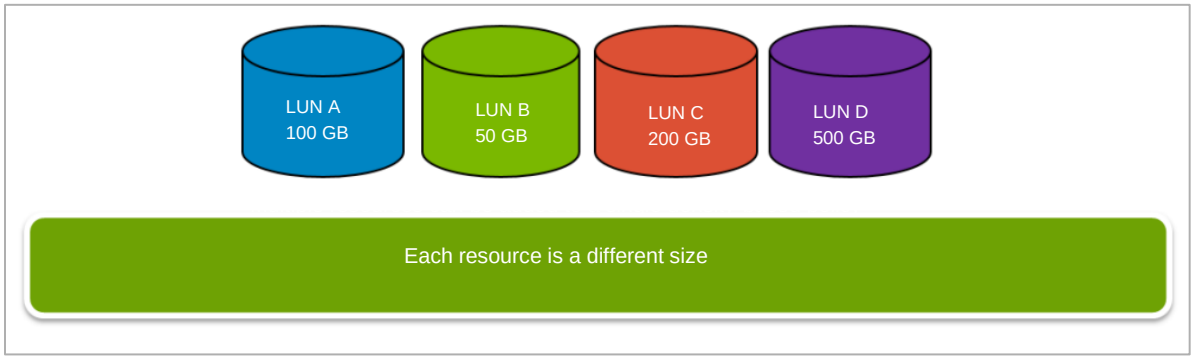
Example of shared Density-based Host I/O Limit policy

Multiple Resources Within a Single Policy

Multiple resources can be added to a single density-based Host I/O Limit policy. Each resource in that policy can have a different limit that is based on the capacity of the resource. If a Storage Administrator decides to change the capacity of a given resource, the new capacity is now used in the calculation when configuring the IOPS.

Multiple Resources on a Single Policy

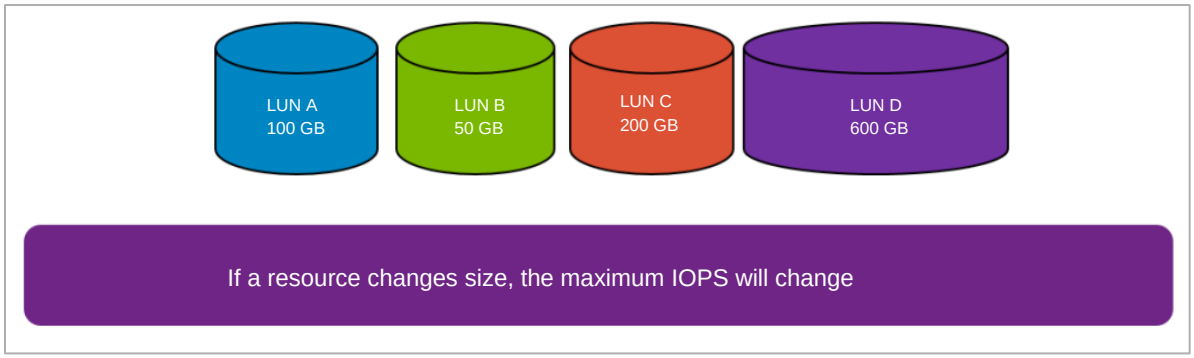
In this example, a LUN resource is configured at 500 GB at initial sizing and the density-based limit is configured a 10 IOPS. The IOPS is 5000 based on the calculation [500 x 10 = 5000].



Example of multiple resources under a single density-based policy

IOPS Change with Resource Size

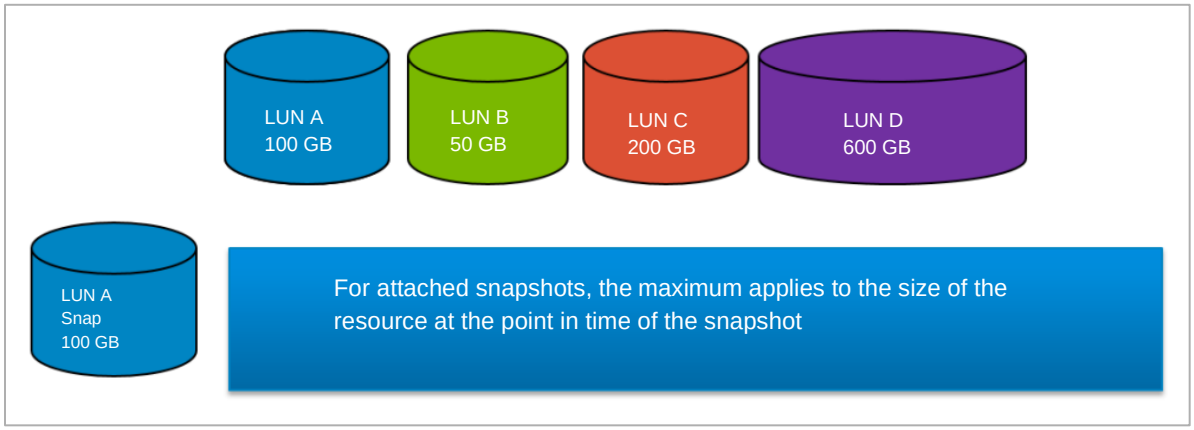
Expanding the LUN by an additional 100 GB results in a new calculation of 6000 IOPS [600 x 10 = 6000].



Example of a resource size change under a single density-based policy

Snapshots and I/O Limits

For attached snapshots, the maximum IOPS is determined by the size of the resource [LUN] at the point in time that the snapshot was taken. In the example, a snapshot was created for LUN A. Using the same density limit of 10 the maximum number of IOPS would be 1000 for the snapshot. [100 x 10 = 1000 IOPS].

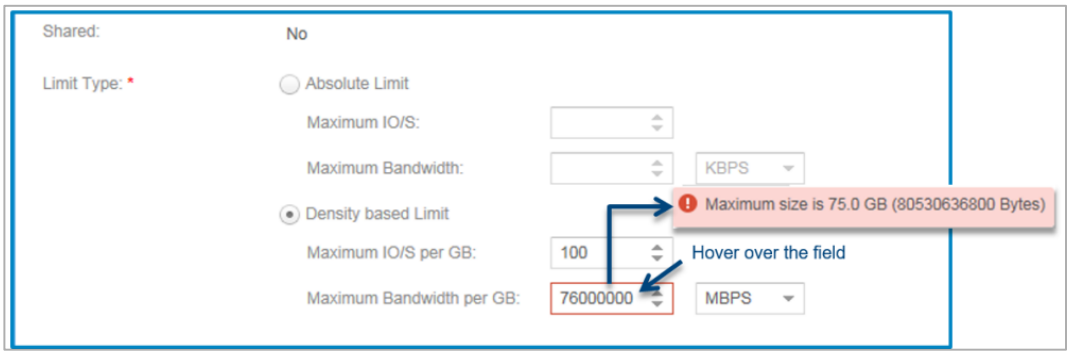


Example of how snapshots are handled

Density-Based Host I/O Limits Values

When configuring density-based limits, there are minimum and maximum values the user interface accepts. The values are shown below. If a user tries to configure a value outside the limits, the box is highlighted in Red to indicate that the value is incorrect. An example is shown below. Hover over the box to view the max allowed value.

Settings	Value Range
Maximum IOPS per GB	1 -> 1,000,000 IOPS
Maximum Bandwidth per GB	1.0 KBPS -> 75 GBPS



With Host I/O Limits, maximum values can be set

Burst Feature Overview

The Burst feature typically allows for one-time exceptions that are set at some user-defined frequency. This allows for circumstances such as boot storms, to periodically occur. For example, if a limit setting was configured to limit IOPS in the morning, you may set up an I/O Burst policy for some period to account for possible increased login traffic. The Burst feature provides Service Providers with an opportunity to upsell an existing SLA. Service Providers can afford end users the opportunity to use more IOPS than the original SLA called for. If applications are constantly exceeding the SLA, they can go back to the end user and sell additional usage of the extra I/Os allowed.

- Allows for one-time exceptions
  - Allow applications with a backlog to catch up periodically
    - Example: Boot storms
- Provides the ability for service providers to upsell
  - Provides insight into how much more I/O the end user is consuming
    - Usage of extra I/Os allowed may warrant a higher limit

Burst Creation

Users can select the **Optional Burst Settings** from the **Configuration** page of the wizard when creating a Host I/O Limit policy. Also, if there is an existing policy in place, users can edit that policy anytime to create a Burst configuration. Users can configure the duration and frequency of when the policy runs. This timing starts from when the Burst policy is created or edited. It is not tied in any way to the system or NTP server time. Having the timing run in this manner prevents several policies from running simultaneously, say at the top of the hour. Burst settings can be changed or disabled at any time by clearing the Burst setting in Unisphere.

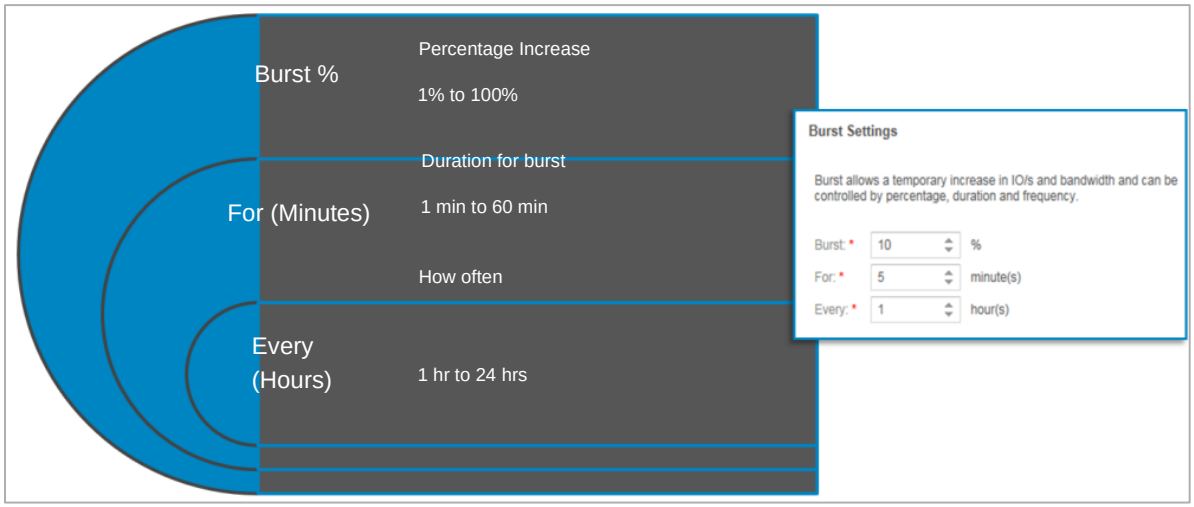
- Burst parameters are configurable:
  - At time of policy creation
  - Anytime by editing an existing policy
- A created or edited policy dictates the timing or scheduling of the Bursts.
  - For example, not just at the top of the hour
- Burst is disabled by clearing the Burst setting in Unisphere
  - Can be changed or disable at any time

Burst Configuration

Host Burst configuration parameters can be set at creation or when an existing policy is edited. The **Burst** % option is the amount of traffic over the base I/O limit in percent that can occur during the burst time. This value is configurable from 1% to 100%.

The **For** option is the duration in minutes to allow burst to run. This setting is not a hard limit and is used only to calculate the extra I/O operations that are allocated for bursting. The actual burst time depends on I/O activity and can be longer than defined when activity is lower than the allowed burst rate. The For option configurable values are 1 to 60 minutes.

The **Every** option is the frequency to allow the burst to occur. The configurable setting is 1 hour to 24 hours. The example shows a policy that is configured to allow a 10% increase in IOPS and Bandwidth. The duration of the window is 5 minutes, and the policy will run every 1 hour.



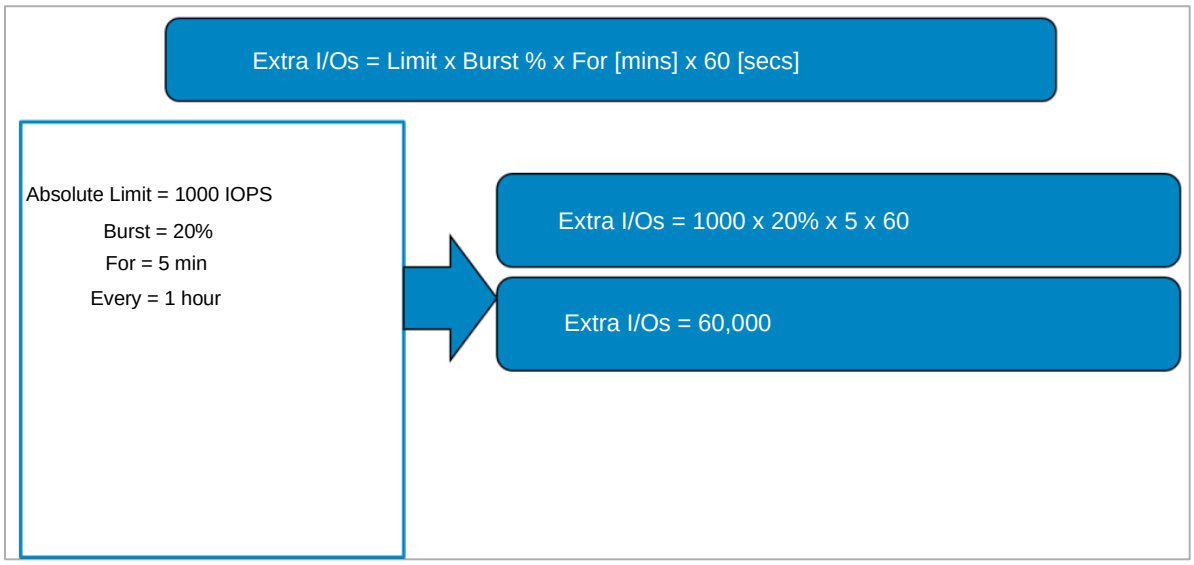
Burst settings

Burst Calculation Example

The example shows how an I/O burst calculation is configured. What the policy does is allow X number of extra I/O operations to occur based on the percentage and duration the user input.

In this case, the absolute limit is 1000 IOPS with a burst percentage of 20%. The policy is allowed for a five-minute period and will reset at 1-hour intervals. The number of extra I/O operations in this case is calculated as: 1000 x 0.20 x 5 x 60 = 60,000. The policy will never allow the IOPS to go above this 20% limit, 1200 IOPS in this case. After the additional I/O operations allocated for bursting are depleted, the limit returns to 1000 IOPS. The policy cannot burst again until the 1-hour interval ends.

Note that the extra number of burst I/O operations are not allowed to happen all at once. The system will only allow the 20% increase to the configured I/O limit of 1000 IOPS for the burst. In this case, the system would allow a maximum of 1200 IOPS for the burst duration of 5 minutes.

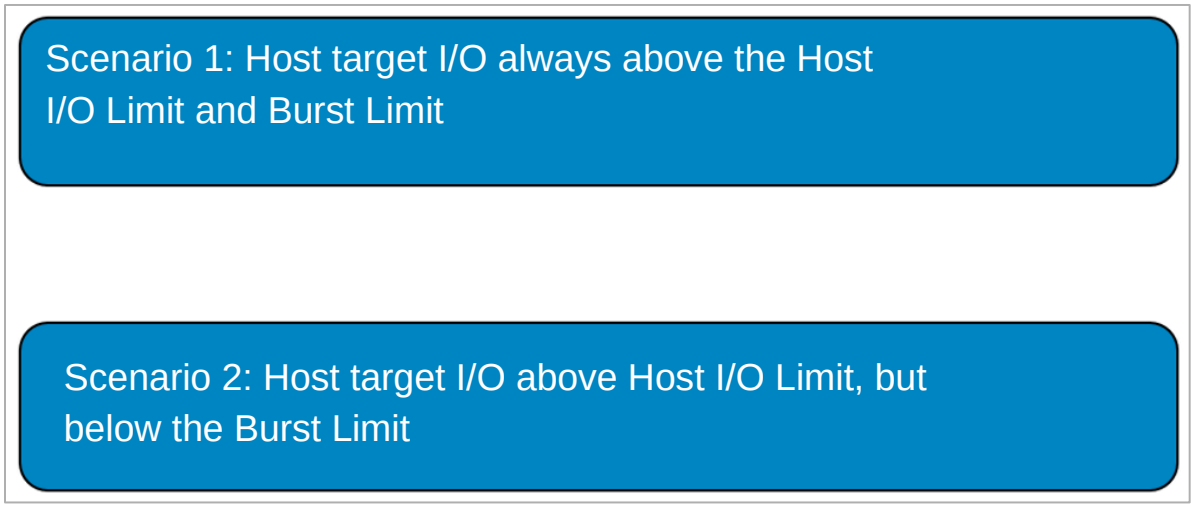


Burst setting example

Burst Scenarios

Shown here are two scenarios that may be encountered when configuring a Burst limit. In the first case, the Host target I/O is always above the Host I/O limit and Burst limit. There are both a Host I/O Limit and Burst Limit that is configured, but the incoming Host target I/O continually exceeds these values.

In the second scenario, the Host target I/O is above Host I/O Limit, but below the Burst Limit. The Host IOPS generated are somewhere in between these two limits.



Introduction to two Burst scenarios

Burst Scenario 1

Host target I/O is always above the Host I/O limit and Burst limit. There is both a Host I/O Limit and a Burst Limit that is configured, but the incoming Host target I/O continually exceeds these values.

Target I/O, Host Limit, Burst Limit

Host target I/O stays above the Host I/O Limit and Burst Limit

- IOPS will never go above the Burst Limit ceiling
  - If Burst is 20%, then only 20% more IOPS allowed at any point in time
- Duration of the extra IOPS matches the “For” setting
  - Note: This is not a set window
- Once all Extra IOPS has been consumed, burst allowance ends
  - Extra IOPS refreshed once next Burst is allowed

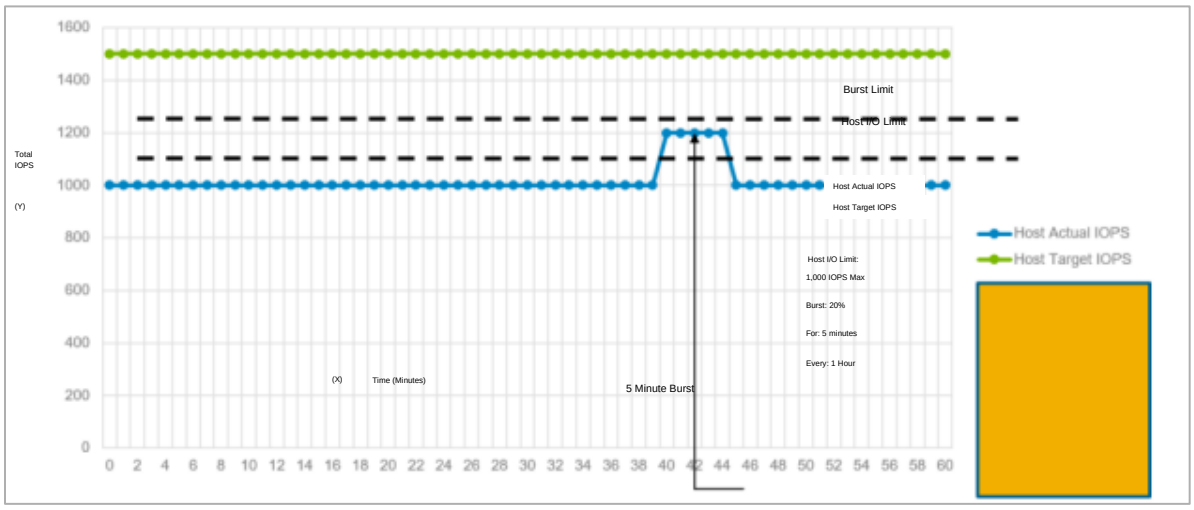
In this scenario, the Host I/O being sent is always greater than the Host I/O Limit and Burst Limit values. When a Burst limit policy is configured, it throttles the Host I/O as to never allow IOPS to go above the Burst Limit ceiling. If the Burst Limit is 20%, then only 20% more IOPS are allowed at any point in time.

For this scenario, the duration of the extra IOPS matches the “For” setting. For the scenario where the host target I/O is below the burst limit, the burst duration window will be longer. Once all the extra I/O operations have been consumed, the burst allowance ends and only the Host I/O Limit is applied for the remainder of the defined burst limit policy period. Extra burst I/O will be available again in the next burst limit policy period.

Total IOPS in 60 Minutes

Here is a graph showing the Total incoming IOPS on the “Y” axis and the time in minutes (60 min) on the “X” axis. The Host I/O Limits are configured to be a maximum of 1000 IOPS with a burst percentage of 20 (1200 IOPS). The duration of the burst is 5 minutes and will refresh every hour. The graphics show that the Host

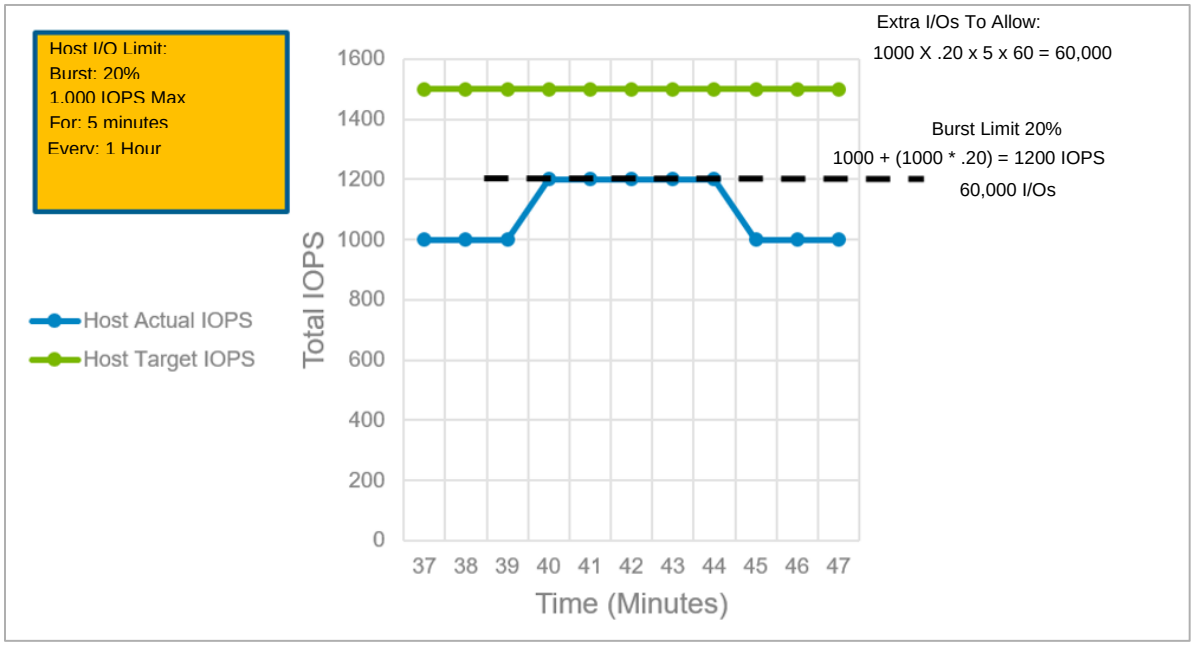
target IOPS is around 1500, well above the Host I/O and Burst Limit settings. This is the I/O that the host is performing. The blue line is what the Host I/O limit is, so we will try to keep the I/O rate at this limit of 1000 IOPS. The Burst Limit is the limit that was calculated from the user input and is at 1200 IOPS. The policy will never allow the IOPS to go above the burst limit. It also means that you will match the “For” window for the duration period since the Host I/O is always above the other limits. The I/O comes in and are throttled by the Host I/O Limit of 1000 IOPS. I/O continues up until the 42-minute mark where it comes to the 5-minute window. During this period, the I/O is allowed to burst to 1200 IOPS.



Total IOPS in 60 Minutes

Burst Limit and Extra IOPS

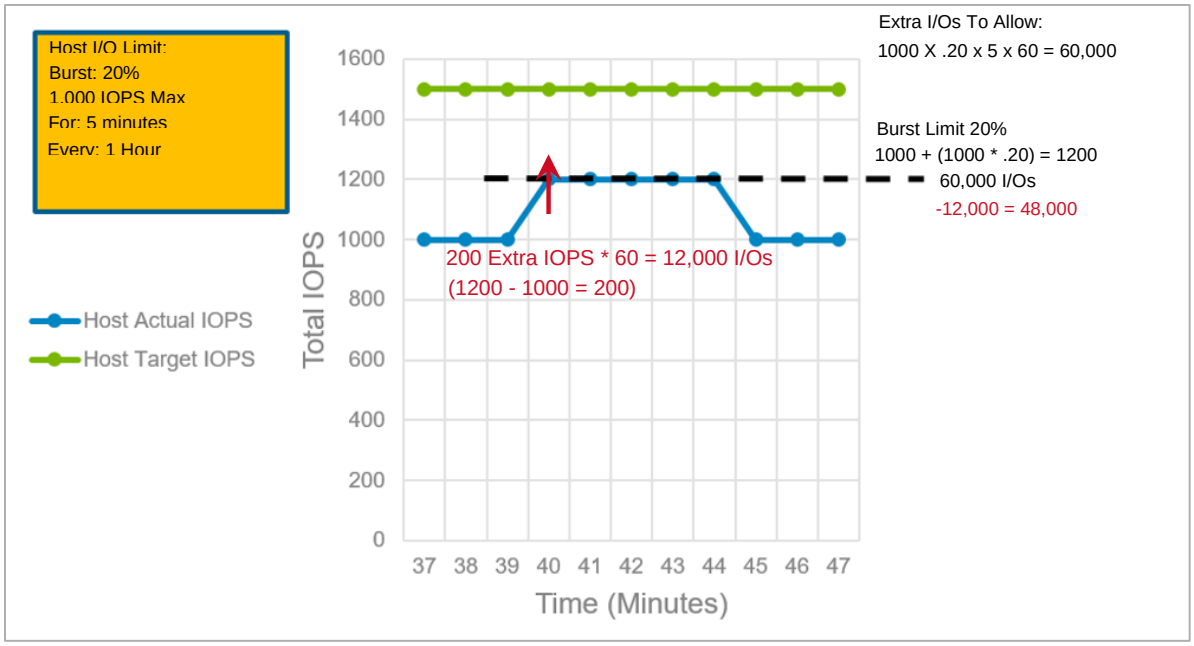
Let us look a bit closer at how the Burst feature throttles the I/Os. The calculations are the same as the previous scenario where the total number of extra I/O operations was based on the Limit x % x For x Frequency. So, we calculated 60,000. The I/O burst period starts, and a calculation is taken between minute 39 and 40 (60 seconds). In that 60 seconds, an extra 200 IOPS is allowed (1200 – 1000), so 200 x 60 produces the value of 12,000 I/O operations. So, every 60-second sample period allows 12,000 I/O operations.



Burst Limit and Extra IOPS

Minute 1

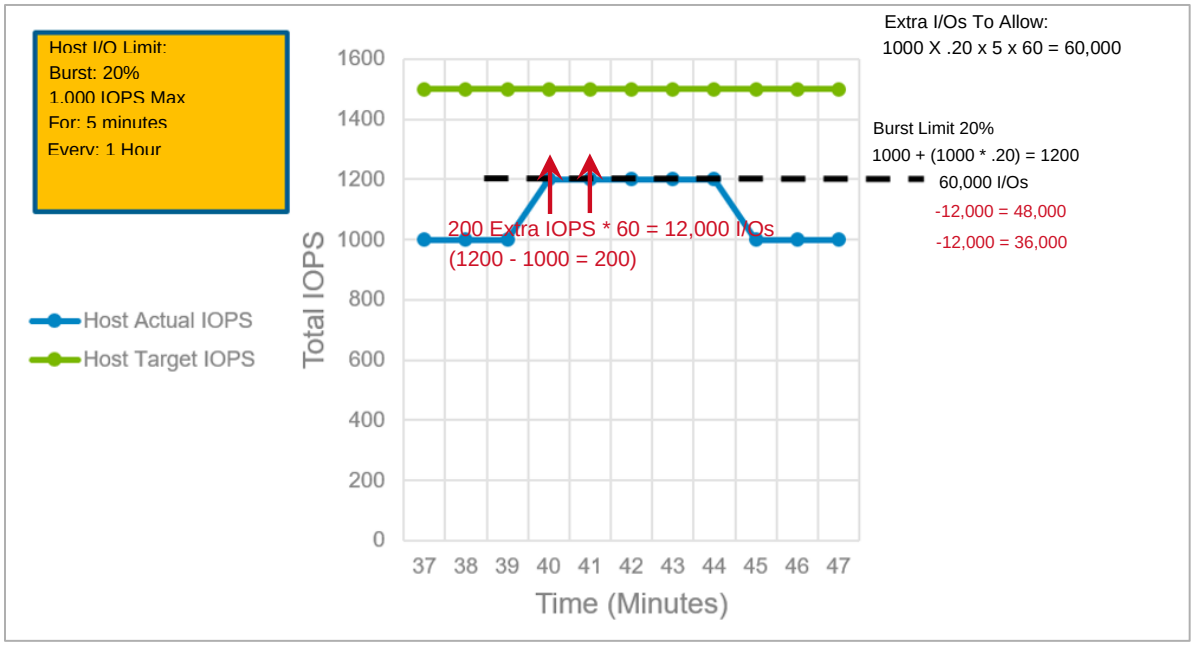
Our “For” value is 5 minutes, so in a 5-minute period we should use our 60,000 extra I/O operations. (12000 * 5 = 60,000). The 12,000 is subtracted from our total of 60,000 for each 60 sec. period (60,000 – 12,000 = 48,000). This continues for the frequency of the burst. Every 60-second period subtracts an additional 12,000 I/O operations until the allotted extra I/O operations value is depleted.



Burst Limit and Extra IOPS at minute 1

Minute 2

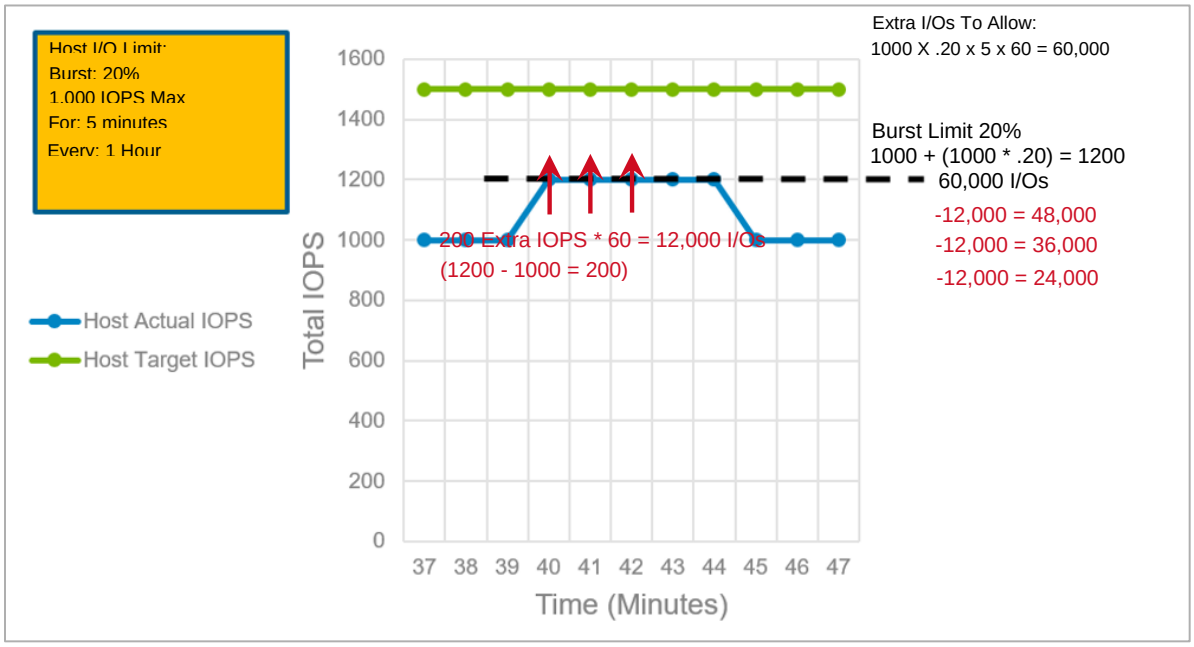
Again, this continues for the frequency of the burst. Every 60-second period subtracts an additional 12,000 I/O operations until the allotted extra I/O value is depleted. Here, another 12,000 is subtracted from our total of 60,000 for this 60 sec. period (60,000 – 12,000 – 12,000 = 36,000).



Burst Limit and Extra IOPS at minute 2

Minute 3

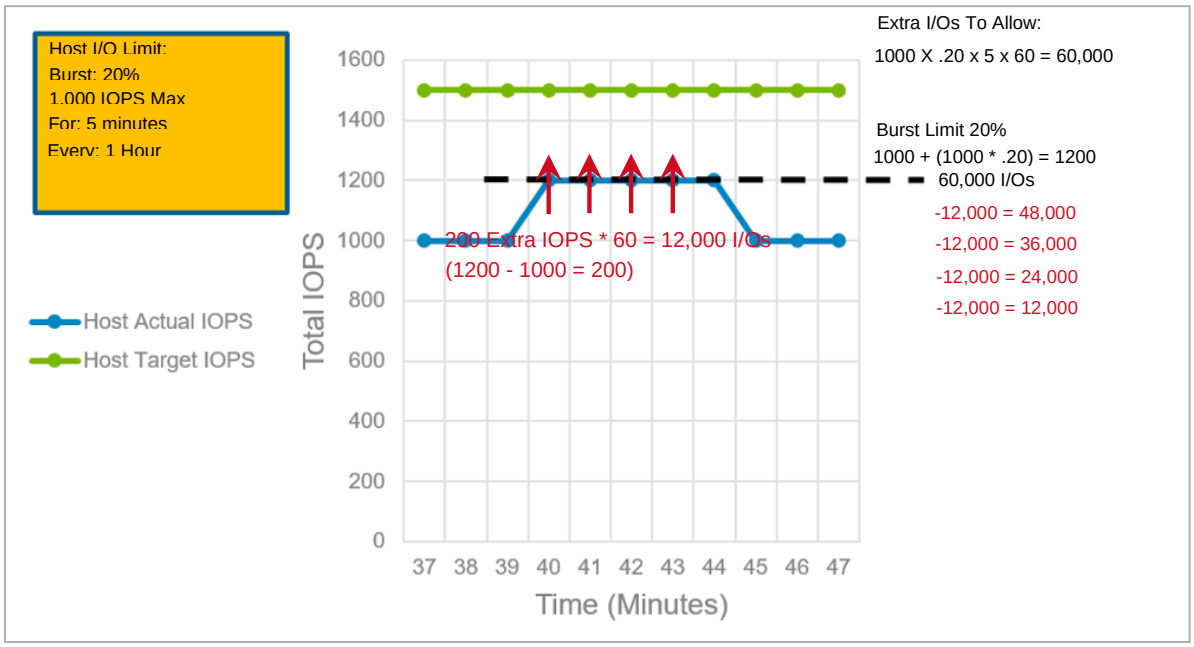
The burst is continuing therefore another 12,000 is subtracted from our total of 60,000 (60,000 – 12,000 – 12,000 -12,000 = 24,000).



Burst Limit and Extra IOPS at minute 3

Minute 4

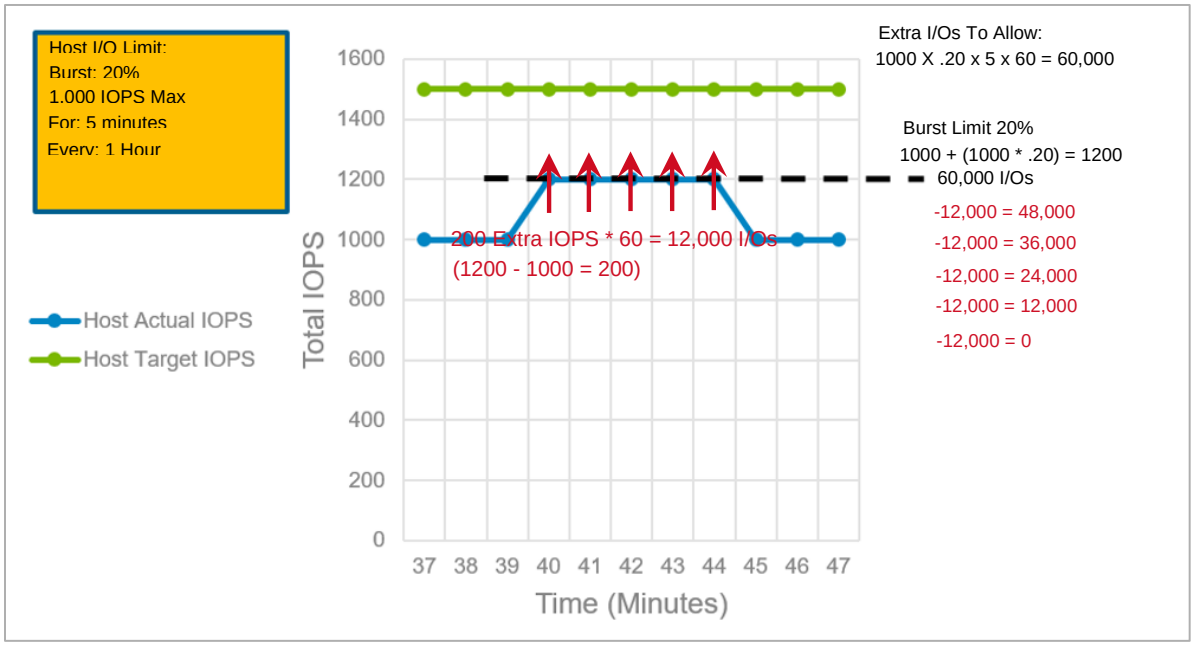
Since the burst continues, another 12,000 is subtracted from our total of 60,000 (60,000 – 12,000 – 12,000 -12,000 – 12,000 = 12,000). This happens as long as the Host I/O rate is above our calculated values during the period. The extra I/O operations are used within the 5-minute window.



Burst Limit and Extra IOPS at minute 4

Minute 5

Since the burst is still continuing, an additional and final 12,000 I/O operations are subtracted and now the allotted extra I/O value is depleted. During the burst, since the Host I/O rate was always above our calculated values during this period, the extra I/O operations were used within the 5-minute window. Once the burst frequency ends, it will start again in 1 hour as determined by the “Every” parameter.



Burst Limit and Extra IOPS at minute 5

Animation - Burst Scenario 1

In this scenario, a Host I/O Limit and Burst Limit are configured, and the incoming Host target I/O continually exceeds these values.

Movie:

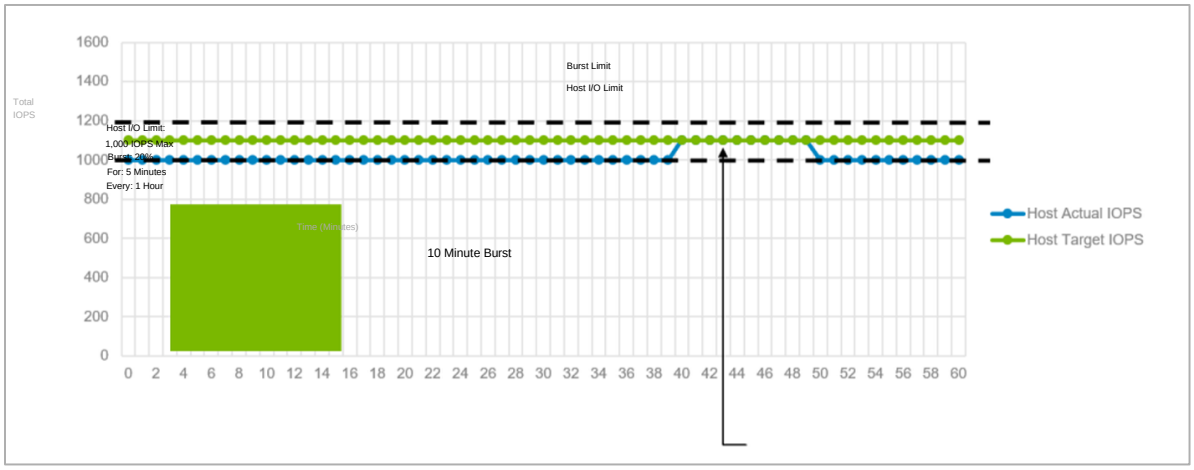
The web version of this content contains a movie.

Burst Scenario 2

In this case where the Host target I/O is above Host I/O Limit, but below the Burst Limit. The Host IOPS generated are somewhere in between these two limits.

Target I/O, Host Limit, Burst Limit

In this second scenario, the same calculations are used as in the previous slides however the Host I/O being generated is around 1100 IOPS, right between our two limits of 1000 and 1200. As Host I/O continues, we see at the 39-minute mark the start of the I/O burst that in this case is a 10-minute period. The thing to note is the I/O does not cross the 1100 IOPS since this is all the I/O the host was attempting to do. Also, since the number of IOPS is smaller, it continues to run for a longer period before the total Extra I/O count is reached.



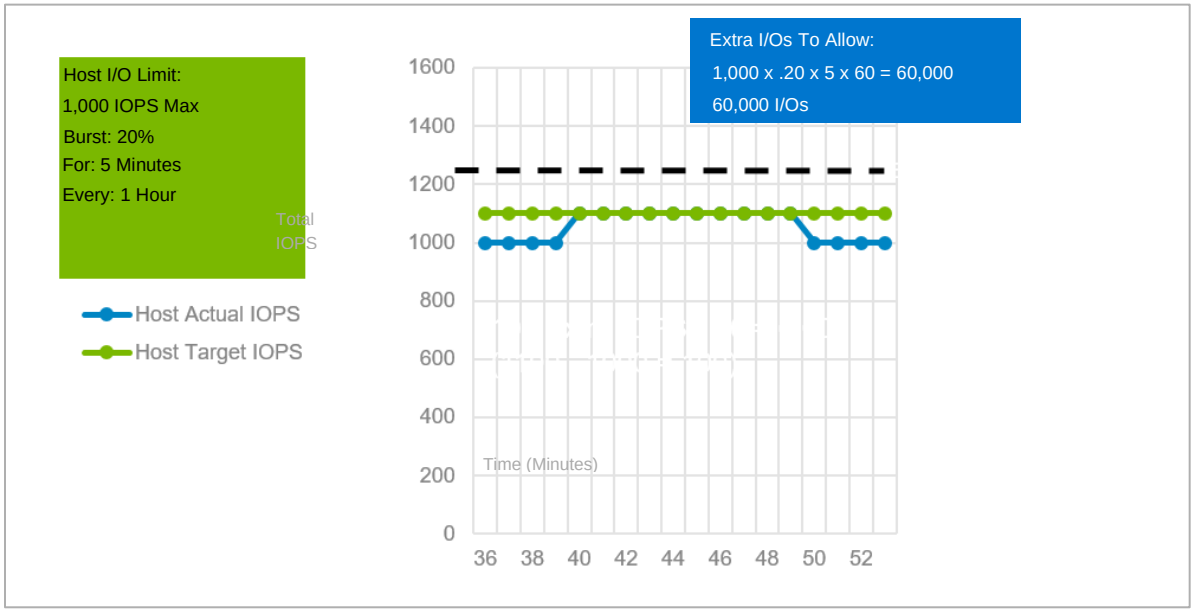
Target I/O, Host Limit, and Burst Limit

Total IOPS in 60 Minutes

Look at the calculations for this scenario. The Host I/O is between the two limits and is only generating 1100 IOPS. The difference between the Host I/O Limit of 1000 and the actual Host I/O is 100 IOPS. So, the calculation is based on 100 x 60 = 6,000 I/O operations.

The total number of I/O operations calculated based on the original numbers is 60,000 I/O operations. So, for each 60-second period 6,000 I/O operations get subtracted from the 60,000 I/O operation total. Effectively, this doubles the “For”

time since it will take 10 minutes to deplete the 60,000 I/O operations that the burst limit allows. So even though the “For” period was 5 minutes, the number of IOPS allowed were smaller, thus allowing for a longer period of the burst than the configured time.

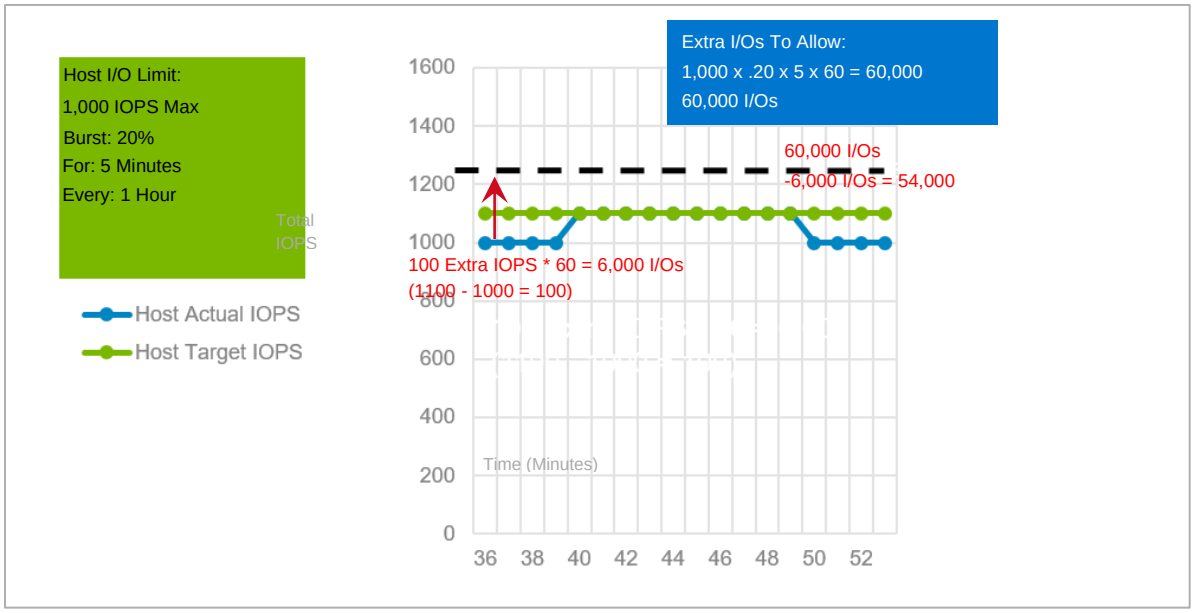


Burst Limit and Extra IOPS

Minute 1

Since the “For” period is set for 5 minutes, and that the number of IOPS allowed were smaller this allows for a longer period of 10 minutes of burst than the configured 5 minutes.

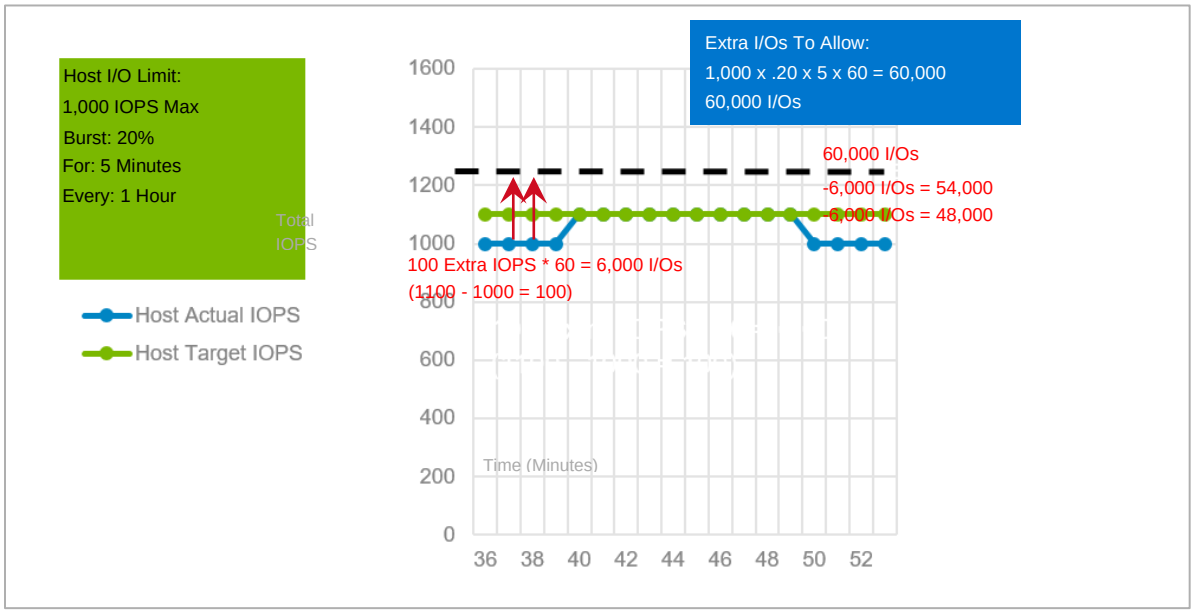
Therefore, for a 10-minute period we should use our 60,000 extra I/O operations. (12000 x 5 = 60,000). Now only 6,000 is subtracted from our total of 60,000 for each 60-second period (60,000 – 6,000 = 54,000). This continues for the frequency of the burst. Every 60-second period will subtract an additional 6,000 I/O operations until the allotted extra I/O value is depleted.



Burst Limit and Extra IOPS at minute 1

Minute 2

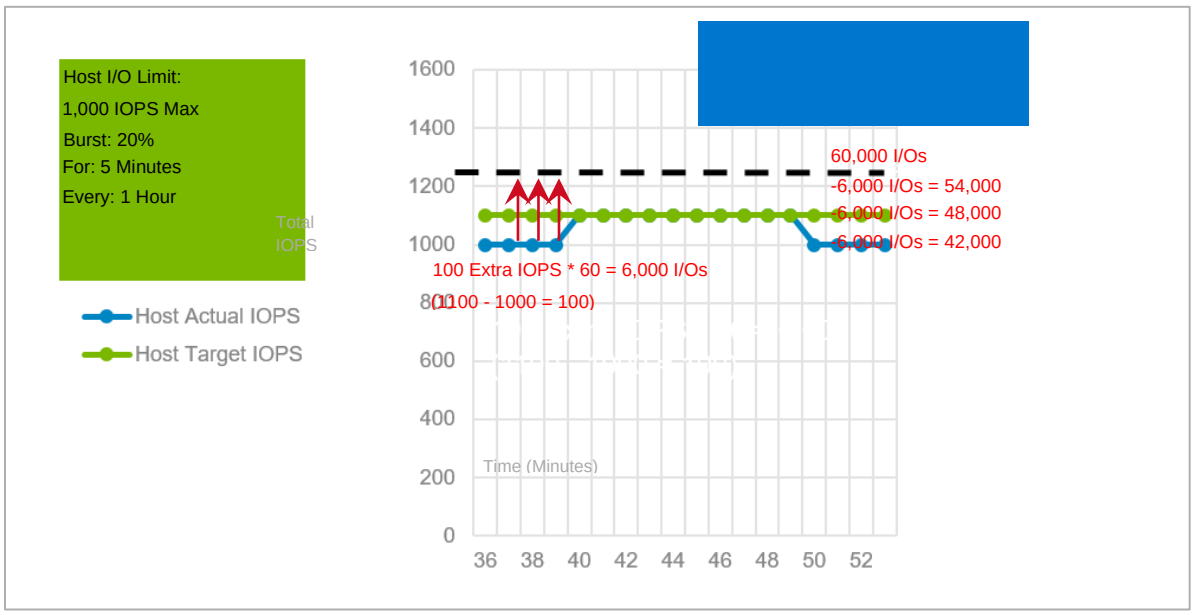
Here, another 6,000 is subtracted from our total of 60,000 for this 60-second period [60,000 – 6,000 – 6,000 = 48,000].



Burst Limit and Extra IOPS at minute 2

Minute 3

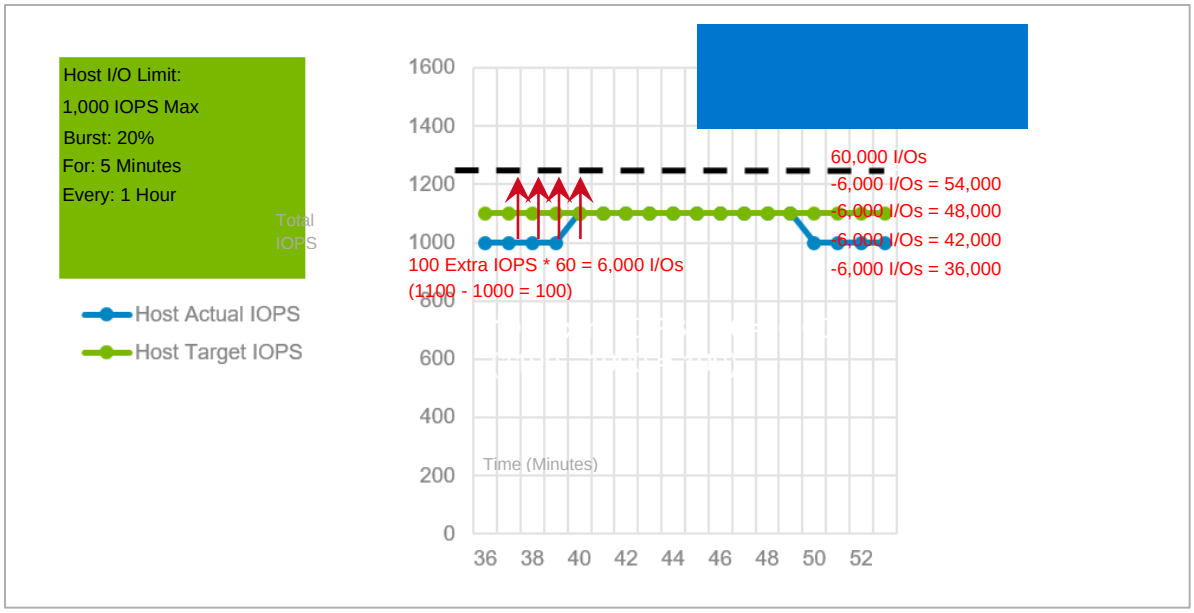
Another 6,000 is subtracted from our total of 60,000 for this 60-second period (60,000 – 6,000 – 6,000 – 6000 = 42,000).



Burst Limit and Extra IOPS at minute 3

Minute 4

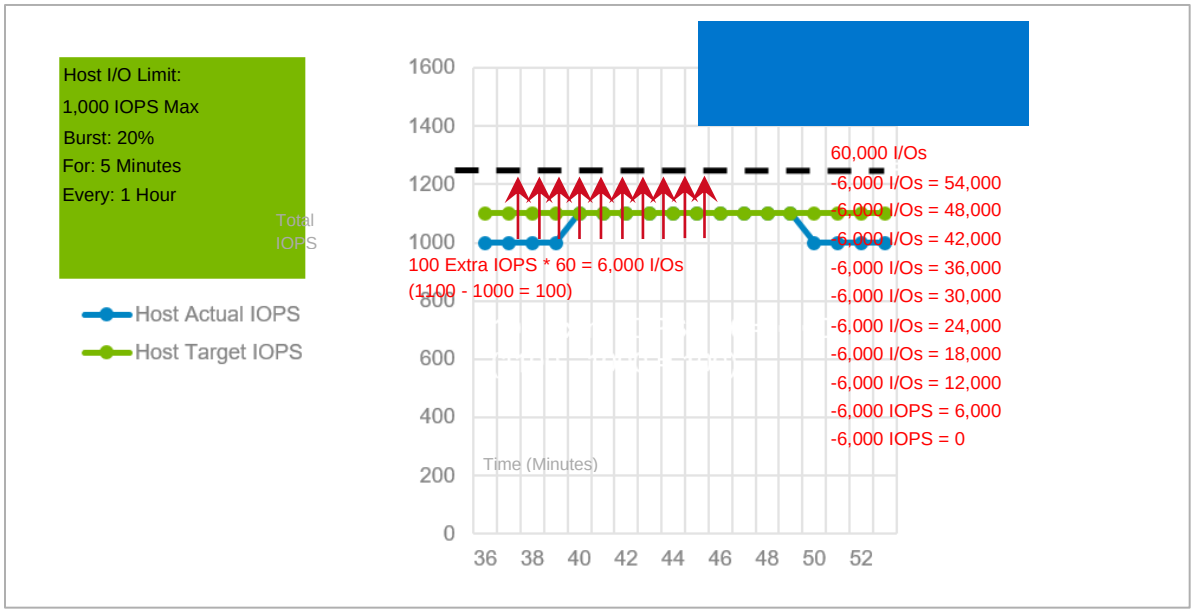
Another 6,000 is subtracted from our total of 60,000 for this 60-second period (60,000 – 6,000 – 6,000 – 6000 – 6000 = 36,000).



Burst Limit and Extra IOPS at minute 4

Minutes 5 through 10

This continues until the extra I/O operations for the burst are depleted. As you can see, even though the “For” period was 5 minutes, the number of I/O operations per 60 seconds were smaller and allowed for a longer period of burst than the configured time.



Burst Limit and Extra IOPS at minutes 5-10

Animation - Burst Scenario 2

In this scenario, the Host target I/O is above the Host I/O Limit, but below the Burst Limit.

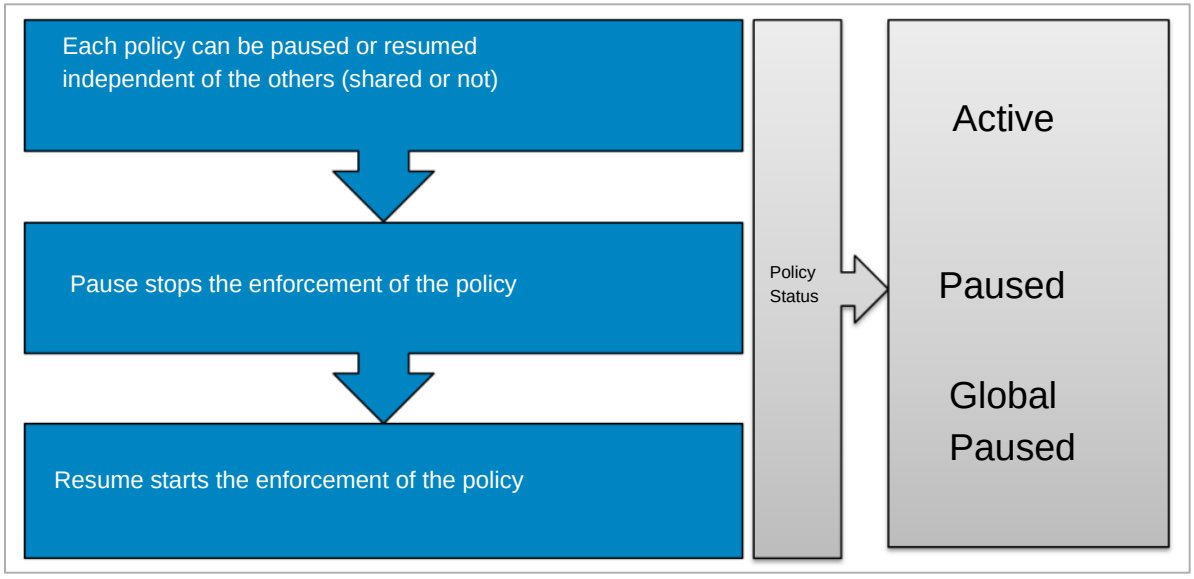
Movie:

The web version of this content contains a movie.

Policy Level Controls

Here are the available policy level controls and status conditions that are displayed in Unisphere.

Host I/O Limits provides the ability to pause and resume a specific host I/O limit. This feature allows each configured policy to be paused or resumed independently of the others, whether or not the policy is shared. Pausing the policy stops the enforcement of that policy. Resuming the policy immediately starts the enforcement of that policy and throttles the I/O accordingly. There are three status conditions for Host I/O Limit policies: Active, Paused, or Global Paused.

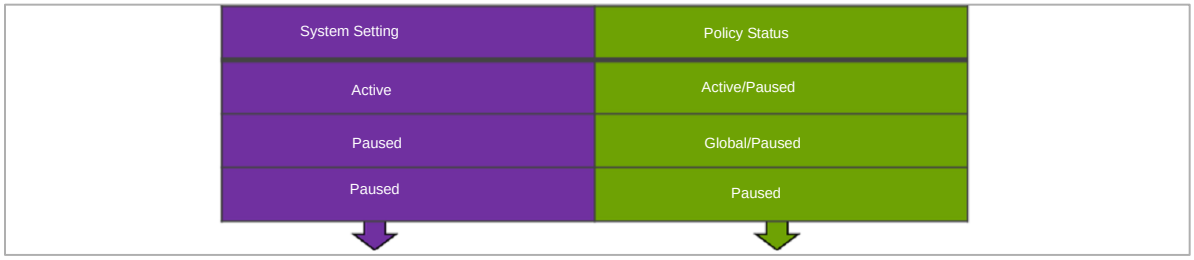


Policies can be paused, resumed, or global paused

Policy Level Controls Defined

System Settings and Policy Status

The table looks at the policies and their relationship for both System Settings and Policy Status. When a policy is created, the policy is displayed as Active by default. System Settings are global settings and are displayed as either Active or Paused. When the System Settings are displayed as Active, the Policy Status will be displayed as “Active” or “Paused” depending on the status of the policy when the System Settings were changed.



System settings and policy status

Changing System Settings to Paused

For example, if the System Setting was “Active” and the user had configured three policies A, B and C. A user could pause A, and the system would update the status of “A” to “Paused.” The other two policies B and C would still display an “Active” status. At this point if the user decided to change the System settings to “Pause” the Policy status will be displayed as “Global Paused” on policies B and C but “Paused” on A.

Changing System settings to paused

Changing Policy Settings to Paused

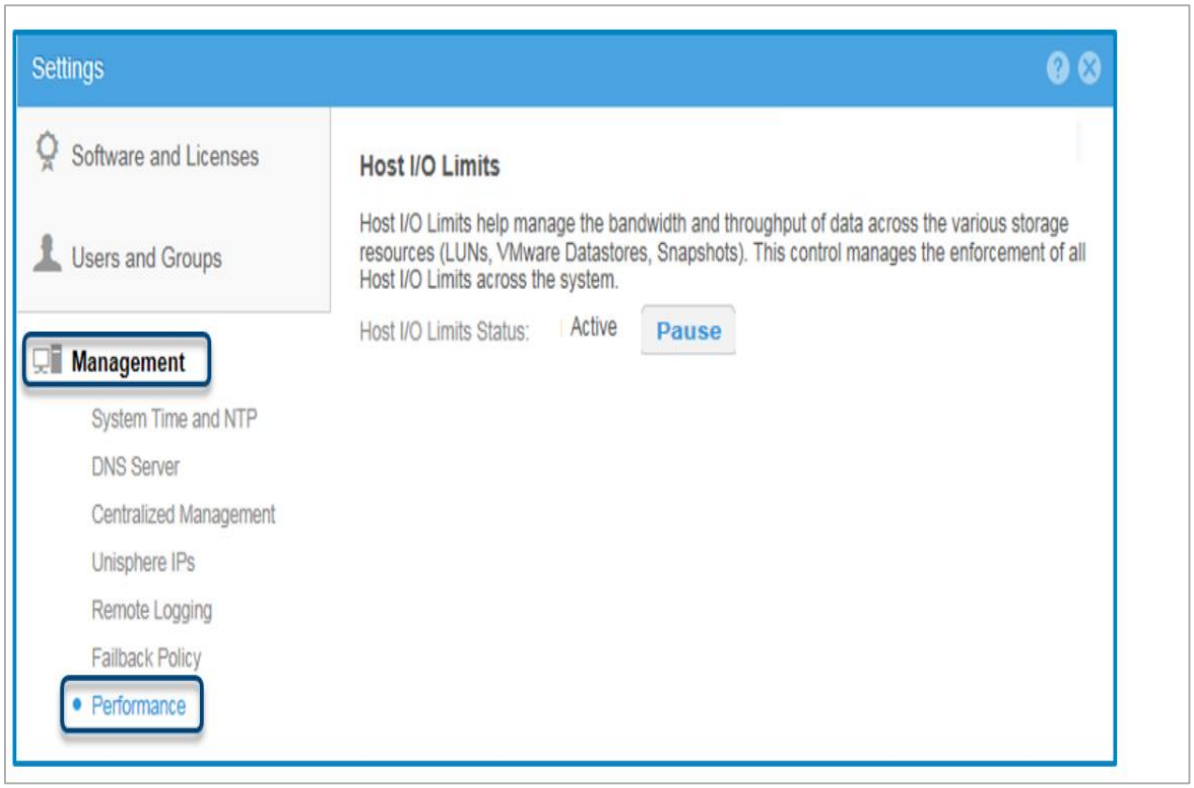
When both the System setting and Policy Setting are “Paused,” the Policy Status will be shown as “Paused.”

Changing Policy settings to paused

Host I/O Limits System Pause – Settings

Host I/O - System Level Settings

To set a Host I/O Limit at the **System level**, click the **Settings** icon then go to **Management > Performance**. The Host I/O Limits Status is **Active**. All host I/O limits are being enforced now. The limits can be temporarily lifted by clicking **Pause**.

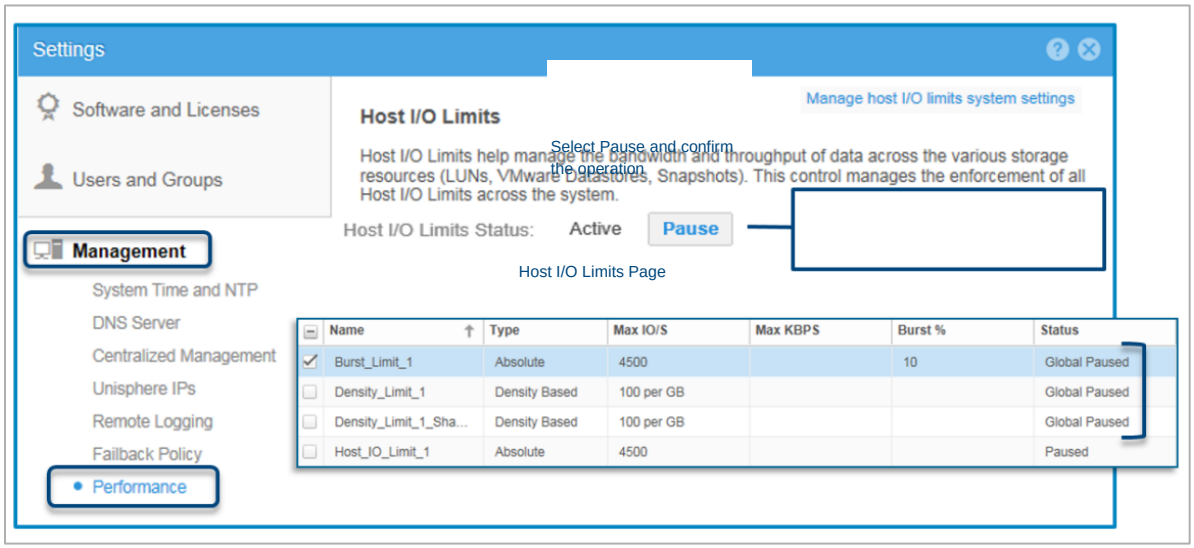


Host I/O - System Level Settings

Pausing Host I/O Limits

If there are “Active” policies, you can pause the policies on a system-wide basis. Once you select “Pause,” you will be prompted to confirm the operation. (Not shown)

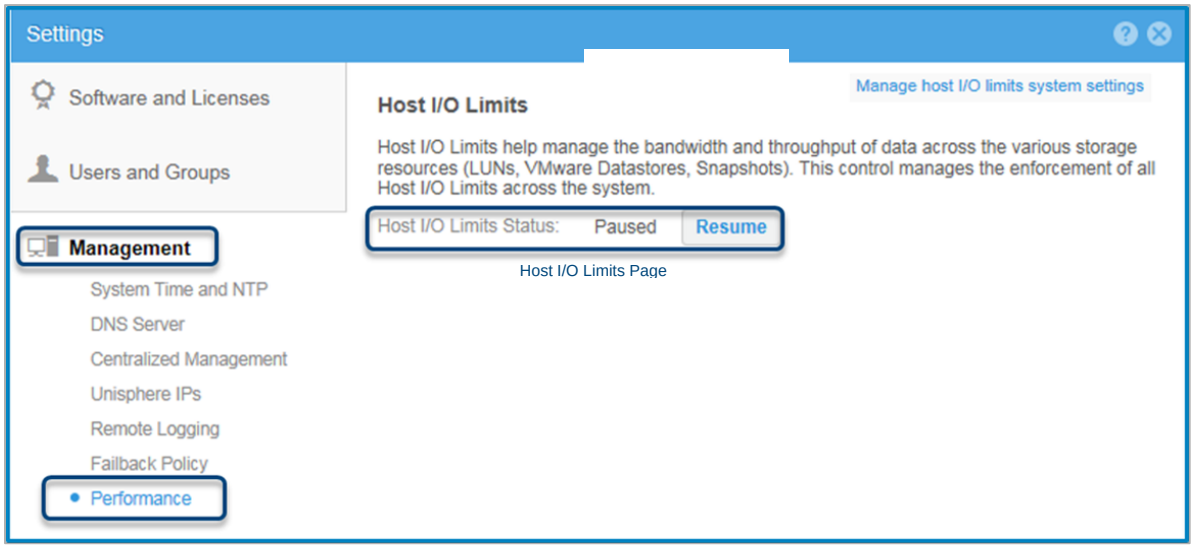
The **Performance > Host I/O Limits** page shows the policies that are affected by the Pause. In the example, three policies display a Status of “Global Paused” indicating a System-wide enforcement of those policies.



Pausing Host I/O Limits

Resuming Host I/O Limits

The Host I/O Limits Status now displays a “Paused” Status, and users can “Resume” the policy. Select **Resume** to allow the system to continue with the throttling of the I/O according to the parameters in the policies.

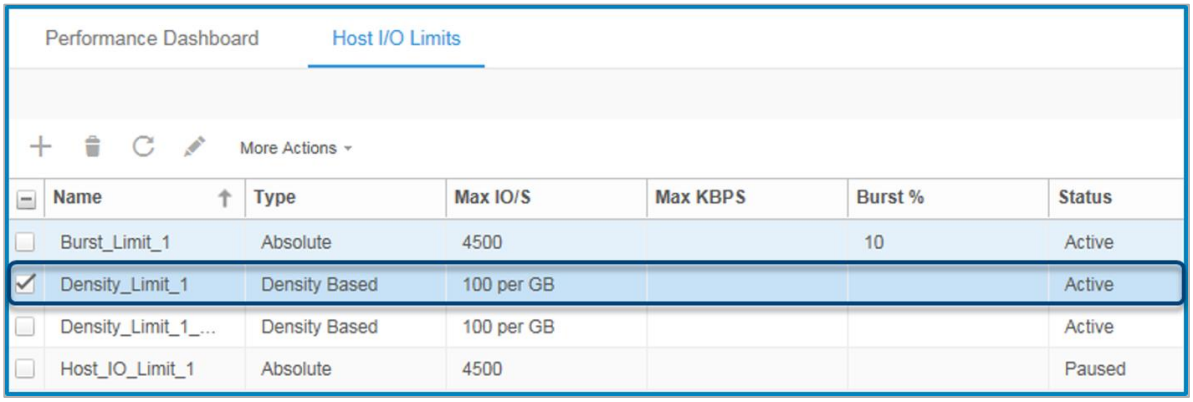


Resuming Host I/O Limits

Host I/O Limits Policy Pause – Unisphere

1 - Select Policy

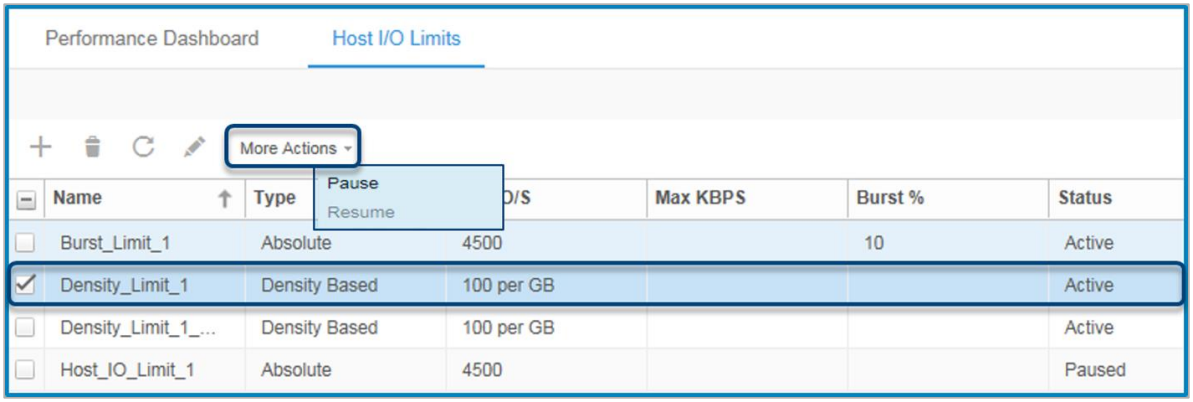
The example displays the Host I/O Limits policies from Unisphere under **System > Performance > Host I/O Limits** window. There are several policies that are created, three of which show a default status of Active. The Density_Limit_1 policy is selected.



Select policy

2 - Pause Policy

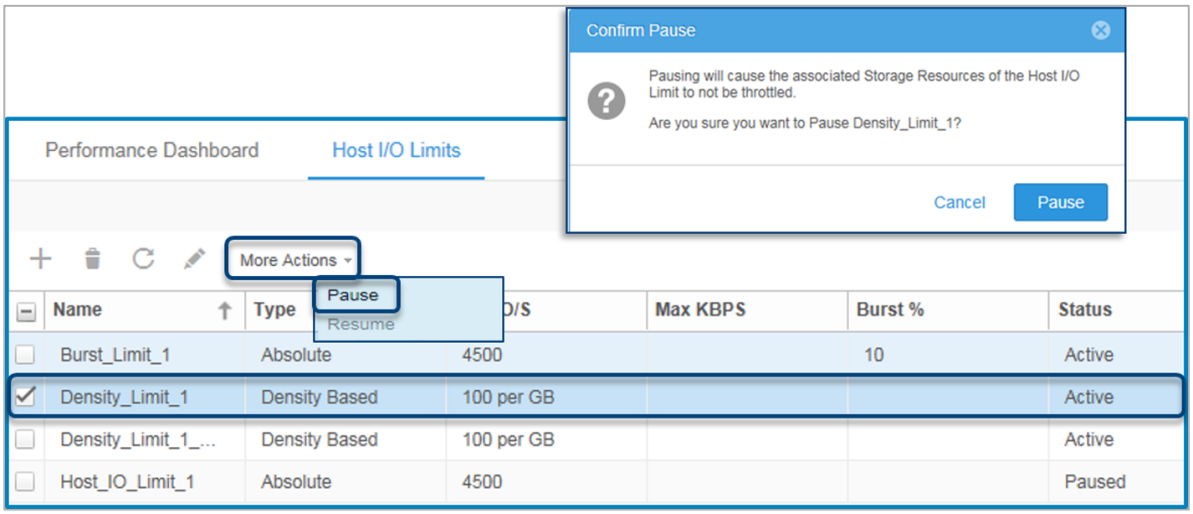
From the More Actions tab, users have a chance to Pause an Active session (resume will be unavailable).



Pause policy

3 - Confirm Pause

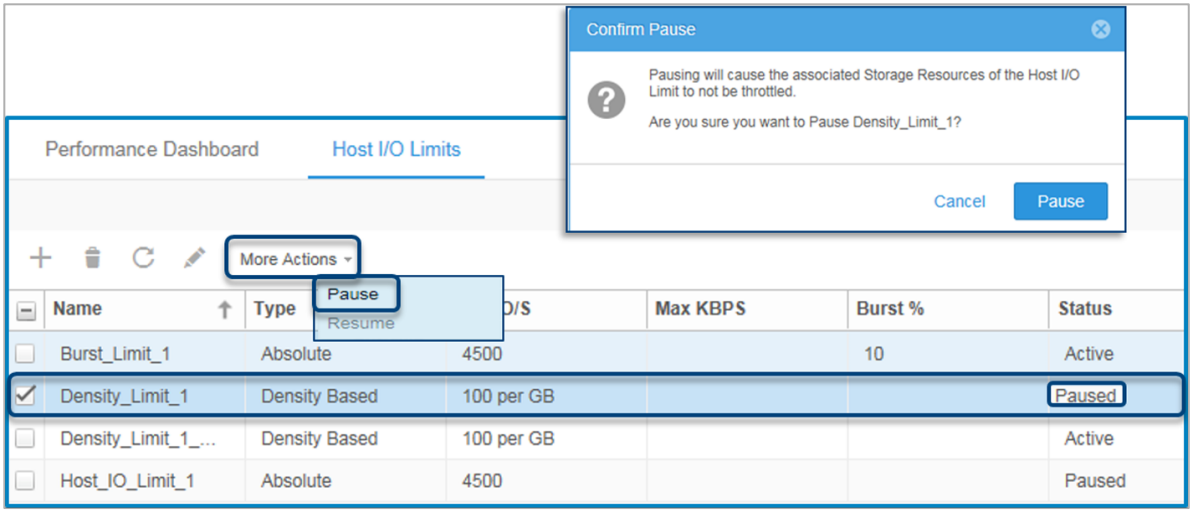
Once the **Pause** option is selected, a warning message is issued to the user to confirm the Pause operation.



Confirm pause

4 - Verify Pause

Selecting **Pause** will start a background job and after a few seconds, causes the Status of the policy to be displayed a Paused. All other policies are still Active since the pause was done at the Policy level, not the System level.



Verify pause

Demonstration

These demos show how to setup different types of host I/O limit policies. Click the associated links to view the videos.

Topics	Link
Creating an Absolute Host I/O Limit policy	Launch
Creating a shared Absolute Host I/O Limit policy	Launch
Creating a shared Density-based Host I/O Limit policy	Launch
Configuring I/O Burst settings for an Absolute Host I/O Limit policy	Launch

UFS64 File System Extension and Shrink

File System Extension Overview

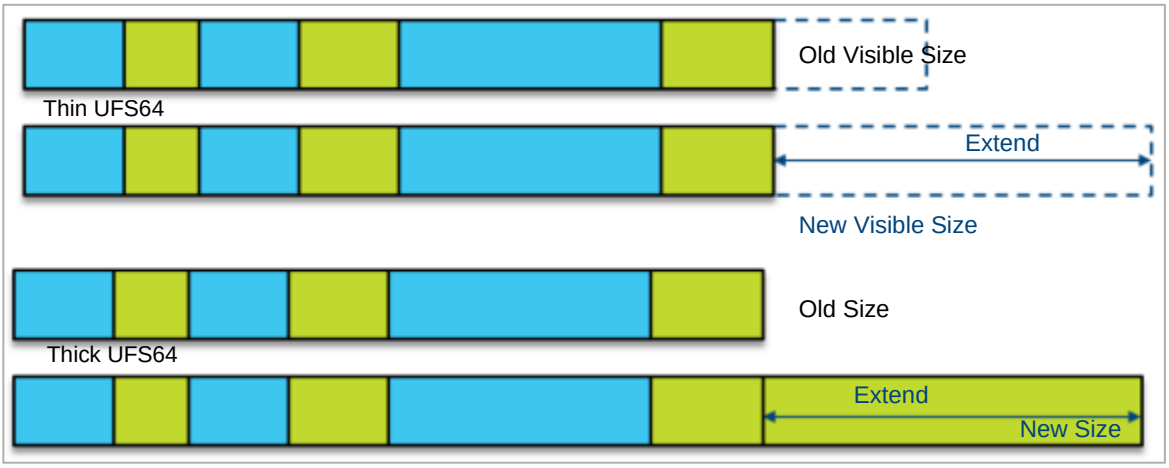
In Dell Unity XT systems, the UFS64 architecture allows users to extend file systems. Performing UFS64 file system extend operations is transparent to the client meaning the array can still service I/O to a client during extend operations.

- On a physical Dell Unity XT systems, the maximum size a file system can be extended to is 256 TB
  - The maximum file system size on Dell UnityVSA is defined by its license.
- The capacity of thin and thick file systems can be extended by manually increasing their total size.
- Auto-extension works only on thin file systems
  - Thin file systems are automatically extended by the system based on the ratio of used-to-allocated space.
  - File systems automatically extend when used space exceeds 75% of the allocated space.
  - Auto-extension operation happens without user intervention and does not change the advertised capacity.

Manual UFS64 File System Extension

For thin-provisioned file systems, the manual extend operation increases visible or virtual size without increasing the actual size allocated to the file system from the storage pool.

For thick file systems, the manual extend operation increases the actual space allocated to the file system from the storage pool.

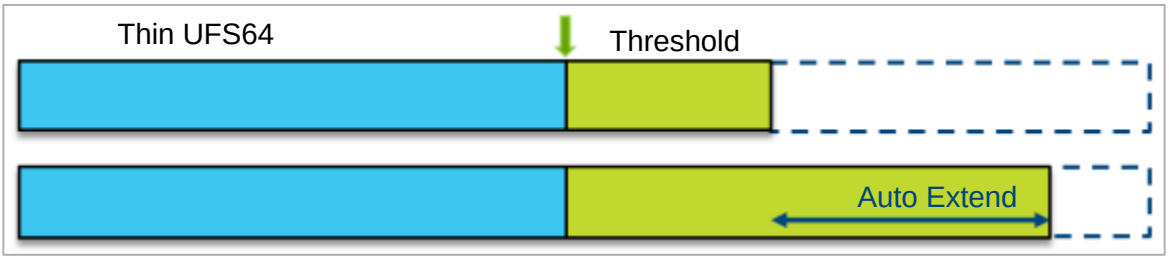


Comparison of manual extension on thick and thin provisioned file systems

Automatic UFS64 File System Extension

Thin-provisioned file systems are automatically extended by the system when certain conditions are met. A thin-provisioned file-based storage resource may appear full when data copied or written to the resource is greater than the space available at that time. When this occurs, the system begins to automatically extend the storage space and accommodate the write operation. If there is enough extension space available, this operation will complete successfully.

The system automatically allocates space for a thin UFS64 file system along with space consumption. Auto extend happens when the space consumption threshold is reached. The threshold is the percentage of used space in the file system allocated space (system default value is 75%). It cannot exceed the file system visible size. Only allocated space increases, not the file system provisioned size. The file system cannot auto-extend past the provisioned size.



Thin provisioned file system automatic extension

Storage Space Reclamation Overview

In Dell Unity XT, the UFS64 architecture enables the reduction of the space the file system uses from a storage pool.

- UFS64 architecture allows the underlying released storage of the file system to be reclaimed.
- The storage space reclamation is triggered by the UFS64 file system shrink operations.
- UFS64 shrink operations can be:
  - Manually initiated by user for both thin and thick file systems.
  - Automatic initiated only on thin file systems when the storage system identifies allocated, but unused, storage space that can be reclaimed back to the storage pool.

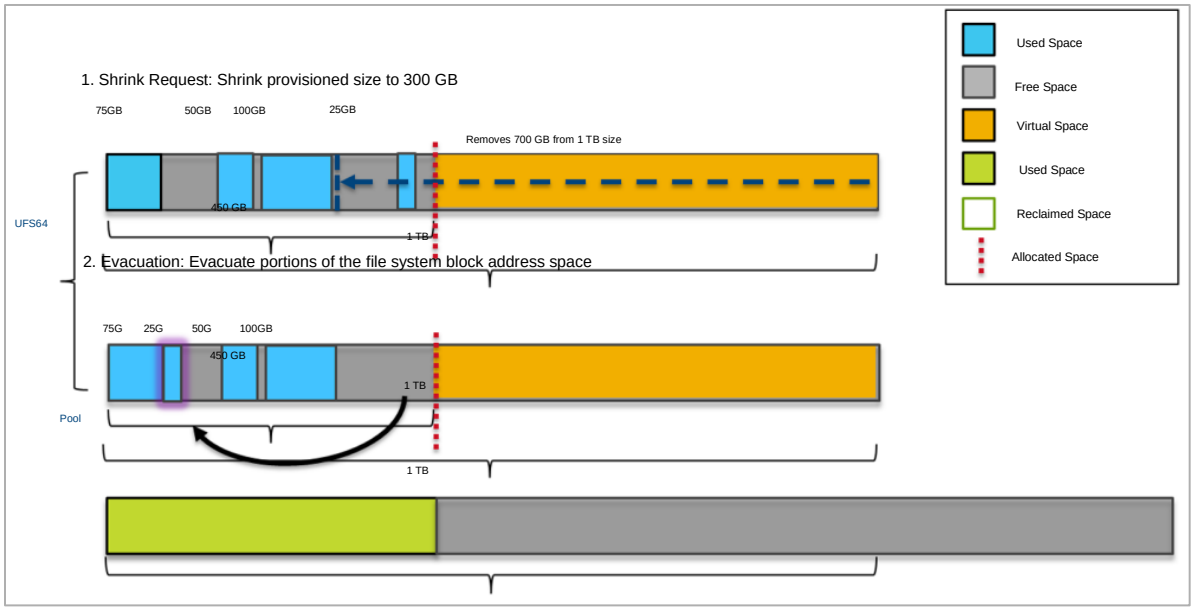
UFS64 Thin File System Manual Shrink

A storage administrator can manually shrink the provisioned size of a thin or thick-provisioned file system into, or within, the allocated space.

In this example, a thin-provisioned 1 TB file system is being shrunk by 700 GB to a new thin-provisioned size of 300 GB. A thick-provisioned file system can be shrunk in a similar manner.

Thin FS Manual Shrink Overview

The thin-provisioned file system currently has 450 GB of space allocated from the storage pool. The allocated space consists of 250 GB of Used Space and 200 GB of Free Space. The system performs any evacuation that is necessary to allow the shrinking process on the contiguous free space.

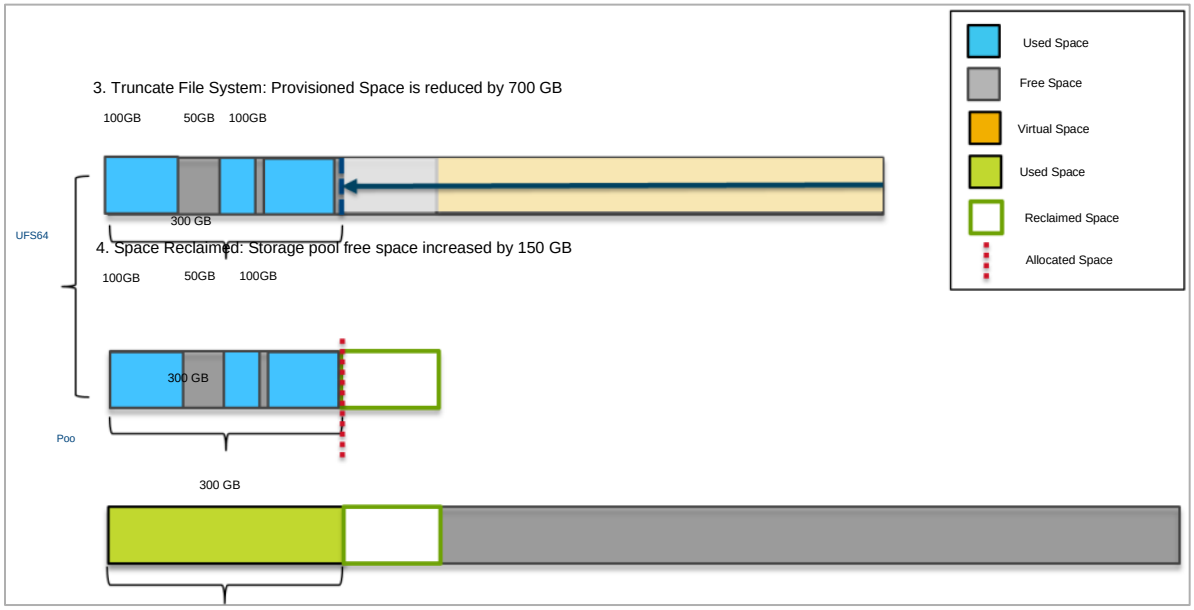


Thin-provisioned file System shrink operation

Thin FS Manual Shrink Completed

In the example, the provisioned space for the thin-provisioned file system is reduced by 700 GB. The total storage pool free space is increased by 150 GB. The file system Allocated Space and Pool Used Space is decreased. The Allocated space after the shrink drops below the original allocated space, enabling the

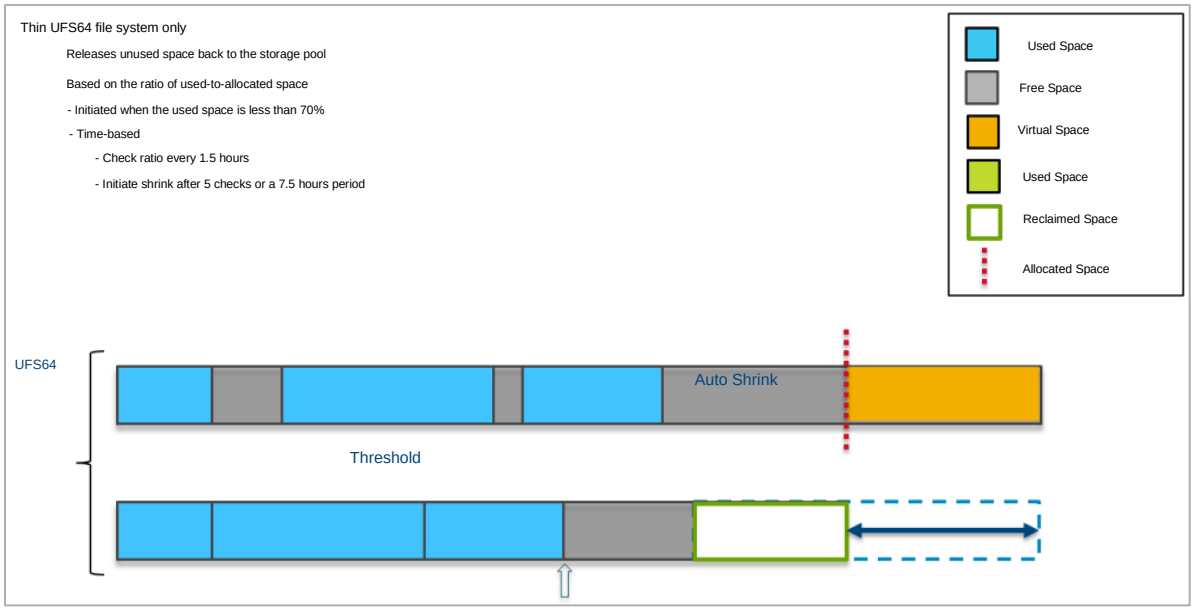
storage pool to reclaim the space. Observe that the only space that is reclaimed is the portion of the shrink that was in the original allocated space of 450 GB. This is because the remaining 550 GB of the original thin file system was virtual space that is advertised to the client.



Storage pool space reclamation after file system shrink operation

UFS64 File System Automatic Shrink

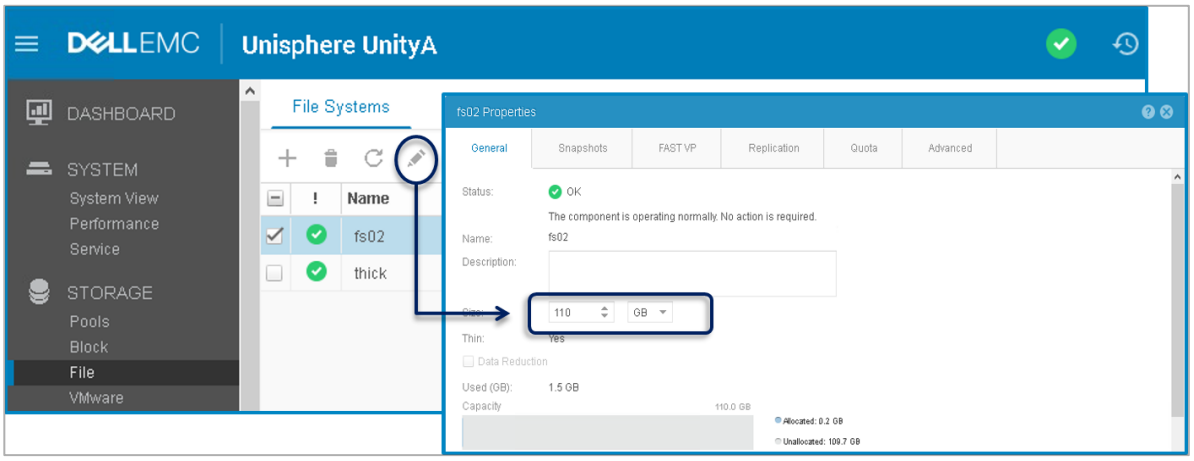
Thin-provisioned file systems are automatically shrunk by the system when certain conditions are met. Automatic shrink improves space allocation by releasing any unused space back to the storage pool. The file system is automatically shrunk when the used space is less than 70% [system default value] of the allocated space after a period of 7.5 hours. The file system provisioned size does not shrink, only the allocated space decreases.



Thin-provisioned file system automatic shrink

File System Extension and Shrink Operations

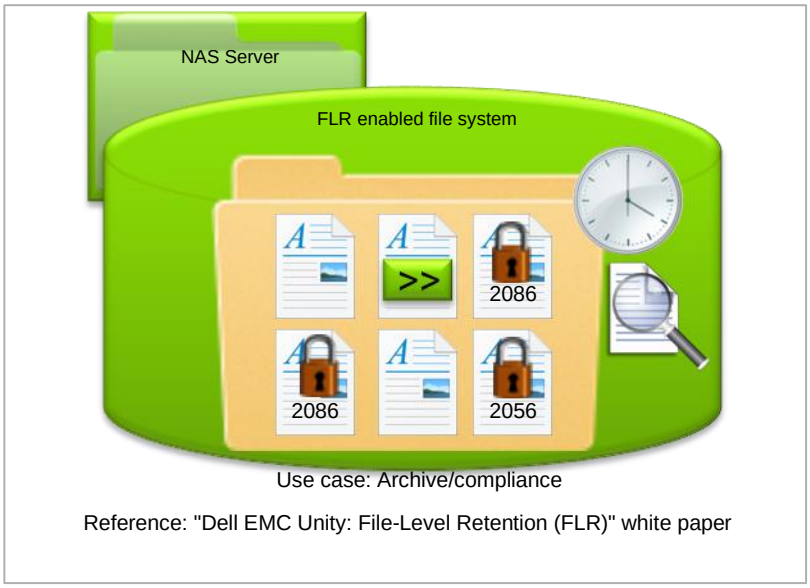
To change the size of a file system, select the File page under the Storage section in Unisphere. Then select the File System tab from the top menu. The properties of the File System can be launched by double-clicking the File System from the list or by clicking the pencil icon from the menu on the top of the File Systems list. From the General tab, the size of the file system can be extended by increasing the Size field. To shrink the file system, you must decrease the Size field. The Apply button must be selected to commit the changes. The change to the file system configuration [size and percentage of allocation space] will be displayed in the list. In this example, the fs02 file system size is manually set to 110 GB.



Unisphere file system properties window

File-level Retention (FLR)

FLR Overview



File-Level Retention is enabled at the file system level

- Locks files to protect from deletion/modification
  - SMB, NFS, or FTP clients
  - For specified retention date and time
- Enabled at file system creation
  - Cannot be disabled
  - FLR clock and activity log
- Two different retention types
  - FLR-E (Enterprise)
  - FLR-C (Compliance)
    - SEC rule 17a-4(f)
- FLR file states
  - Not locked
  - Append-only
  - Locked (WORM)

– Expired

File-level Retention (FLR) protects files from modification or deletion through SMB, NFS, or FTP access based on a specified retention date and time. The retention period can be increased but cannot be reduced. The FLR use case is for file data content archival and compliance needs. FLR is also beneficial in preventing users from accidental file modification and deletion.

For full details of the FLR feature, reference the *Dell EMC Unity: File-Level Retention (FLR)* white paper available on Dell EMC Online Support.

FLR can only be enabled during the creation of a file system. Once FLR is enabled for a file system, it cannot be disabled after the file system is created. Therefore, it is critical to know if FLR is required at file system creation time. When a file system is enabled for FLR, a nonmodifiable FLR clock is started on the file system. The FLR clock is used to track the retention date. An FLR activity log is also created on the file system when it is FLR enabled. The activity log provides an audit record for files stored on the file system.

There are two different types of FLR; FLR-E (Enterprise) and FLR-C (Compliance).

FLR-E protects file data that is locked from content changes that are made by SMB and NFS users regardless of their administrative rights and privileges. An appropriately authorized Dell EMC Unity administrator (with the Unisphere Administrator or Storage Administrator role) can delete an FLR-E enabled file system, even if it contains locked files.

FLR-C protects file data that is locked from content changes that are made by SMB and NFS users regardless of their administrative rights and privileges. File systems containing locked files cannot be deleted by any authorized Dell EMC Unity administrative role. FLR-C enabled file systems are compliant the Securities and Exchange Commission (SEC) rule 17a-4(f) for digital storage. FLR-C also includes a data integrity check for files that are written to an FLR-C enabled file system. The data integrity check affects write performance to an FLR-C enabled file system.

Files within an FLR enabled file system have different states; Not Locked, Append-only, Locked and Expired.

Not Locked: All files start as not locked. A not locked file is an unprotected file that is treated as a regular file in a file system. In an FLR file system, the state of an unprotected file can change to Locked or remain as not locked.

Append-only: Users cannot delete, rename, and modify the data in an append-only file, but users can add data to it. A use case for an append-only file is to archive logfiles that grow over time. The file can remain in the append-only state forever. However, a user can transition it back to the Locked state by setting the file status to read-only with a retention date.

Locked: Also known as “Write Once, Read Many” (WORM). A user cannot modify, extend, or delete a locked file. The path to locked files is protected from modification. That means a user cannot delete or rename a directory containing locked files. The file remains locked until its retention period expires. An administrator can perform two actions on a locked file: 1. Increase the file retention date to extend the existing retention period. 2. If the locked file is initially empty, move the file to the append-only state.

Expired: When the retention period ends, the file transitions from the locked state to the expired state. Users cannot modify or rename a file in the expired state, but can delete the file. An expired file can have its retention period extended such that the file transitions back to the locked state. An empty expired file can also transition to the append-only state.

FLR Capabilities and Interoperability

- Supported on entire Dell Unity Family of storage systems
  - Dell Unity XT platform
  - Dell UnityVSA
- Supports Replication
  - Destination FLR type must match source
  - FLR changes at source are replicated to destination
- Supports NDMP
  - Backups include retention period and permissions but not lock status
  - Restores lock read-only files
  - Append-only files are normal files after restore
- Supports Data Reduction
- Supports CTA tiering as a destination
  - Cannot be a tiering source
- Supports File Import from VNX
  - If source VNX file system is FLR enabled, target Dell EMC Unity file system is FLR type matched
  - VNX is DHSM enabled
- Supports Snapshots
  - FLR-C supports read-only snapshots
  - FLR-C does not support snapshot restores
  - FLR-E supports read-only and R/W snapshots
  - FLR-E supports snapshot restores
- VMware NFS datastores not supported

The FLR feature is supported on the entire Dell Unity family of storage systems. It is available on all physical Dell Unity XT models and the Dell UnityVSA.

The Dell Unity Replication feature supports FLR. When replicating an FLR enabled file system, the destination file system FLR type must match the source. If the replication session is created with the Unisphere GUI, the system automatically creates the destination file system to match the source file system FLR type. If the replication session is being created with UEMCLI, the destination file system provisioning and FLT type selection are done manually.

FLR enabled file systems are supported with NDMP backup and restore operations. The retention period and permissions of files are captured in the backup but the file lock status is not. When an FLR enabled file system is restored with NDMP, read-only files are restored as locked files. Append-only files are restored as normal files.

FLR fully supports the Dell Unity Data Reduction feature.

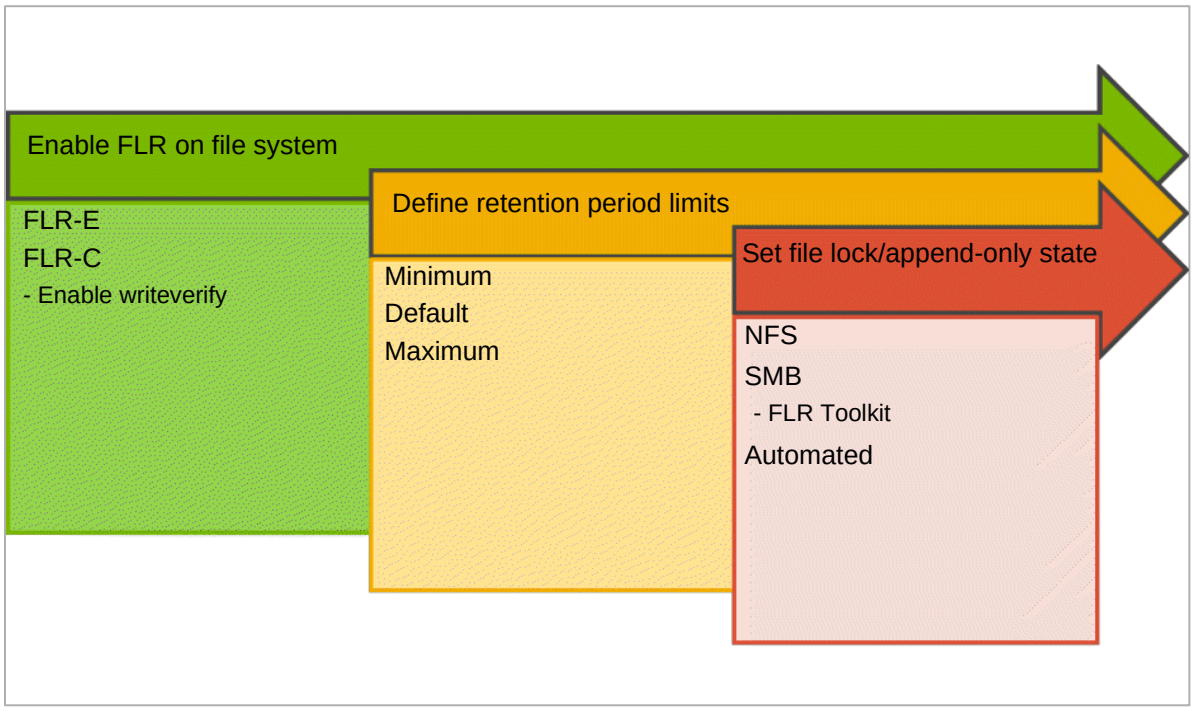
FLR is supported as a tiering destination for CTA archive operations. However, FLR enabled file system are not supported as a CTA tiering source.

FLR supports the Dell EMC File Import feature. If the source VNX file system imported is FLR enabled, the target Dell Unity file system is migrated as a type matched FLR enabled file system. The source VNX must be DHSM enabled. The DHSM credentials are used when the import session is created on the Dell Unity system.

FLR supports the Dell Unity Snapshots feature. FLR-C file systems support read-only snapshots but do not support snapshot restore operations. FLR-E file systems support read-only and R/W snapshots, and support snapshot restores. When an FLR-E file system is restored from a snapshot, the FLR file system clock is set back in time, corresponding to the snapshot time. Note that the change to the FLR clock effectively extends the retention period of locked files.

FLR is not supported on VMware NFS datastores.

Process to Enable and Manage FLR



Process to enabled and manage FLR on a file system

There is a process to enable and manage FLR on a file system.

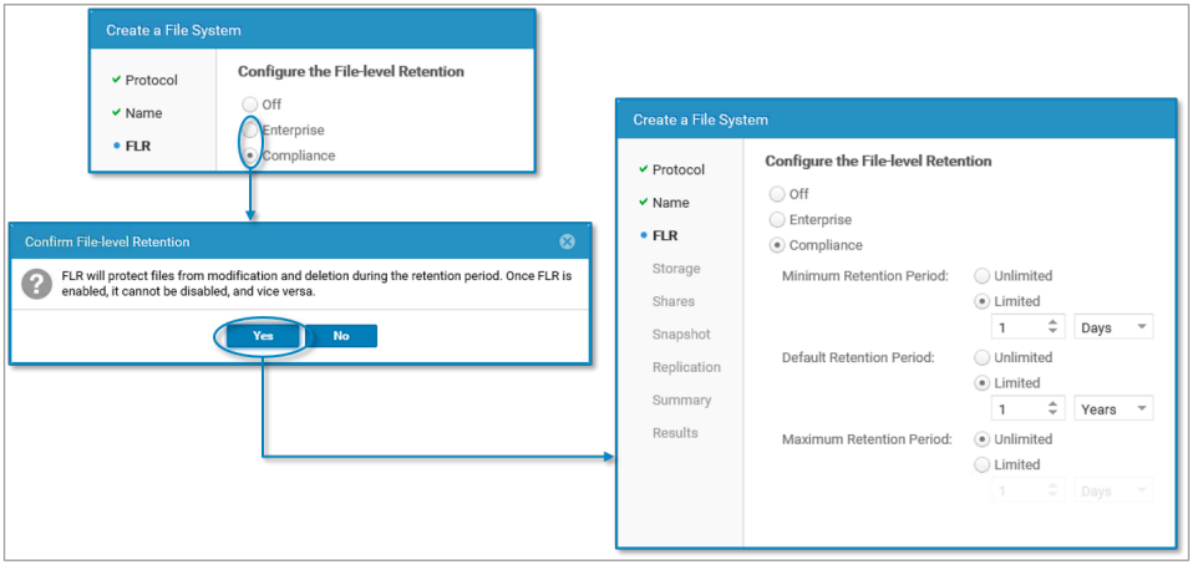
The first step in the process is to enable FLR on the file system. It must be done at file system creation time. The file system creation wizard includes a step to enable FLR where either the FLR-E or FLR-C type can be selected. If FLR-C is selected, there is a separate step to enable its data integrity check. The data integrity check is controlled by the *writeverify* NAS Server parameter.

The next step is to define retention period limits for the file system and is done within the FLR step of file system creation wizard. The retention period limits can also be defined after the file system is created from the FLR tab of the file system Properties. A minimum limit, a default limit, and a maximum limit are defined for the FLR enabled file system.

The next step is to set a lock or append-only state for files on the file system. There is a process to set a file to the lock state and a process to set a file to the append-only state. For NFS files, setting the file state is done from an NFS client. For SMB

files, setting the file state is done using the FLR Toolkit application. A retention time can also be placed on files in an automated fashion by the system. This is enabled from the FLR tab of the file system Properties.

Enable FLR on a File System



Unisphere Create File System wizard step to enable FLR

Enabling a file system for FLR is only done during the creation of the file system in the Create File System wizard. The FLR step of the wizard by default has the FLR option Off. Select either Enterprise to enable FLR-E or select Compliance to enable FLR-C. The example illustrates FLR-C being enabled for the file system.

When either type is selected, a confirmation window is displayed indicating to the user that FLR will protect files from modification and deletion. The message also informs the user that once enabled FLR cannot be disabled or enabled later.

When the user confirms to enable FLR, options are exposed for defining the minimum, default, and maximum retention periods for FLR. Shown in the example are the default retention periods for FLR-C. The retention period values can also be defined after the file system creation from the FLR tab of the file system Properties. The retention periods for the file system are covered on a following slide.

Enable writeverify for FLR-C

```
spa:~/user# svc_nas nas04 -param -f FLRCompliance -i writeverify
nas04 :
name            = writeverify
facility_name   = FLRCompliance
default_value   = 0
current_value   = 0 ←— writeverify disabled ~
description     = Set the writeVerify flag for FLR Compliance File Systems

spa:~/user# svc_nas nas04 -param -f FLRCompliance -m writeverify   -v 1
nas04 : done

spa:~/user# svc_nas nas04 -param -f FLRCompliance -i writeverify
nas04 :
name            = writeverify
facility_name   = FLRCompliance
default_value   = 0
current_value   = 1 ←— writeverify disabled ~
description     = Set the writeVerify flag for FLR Compliance File Systems
```

CLI command to enable data integrity check

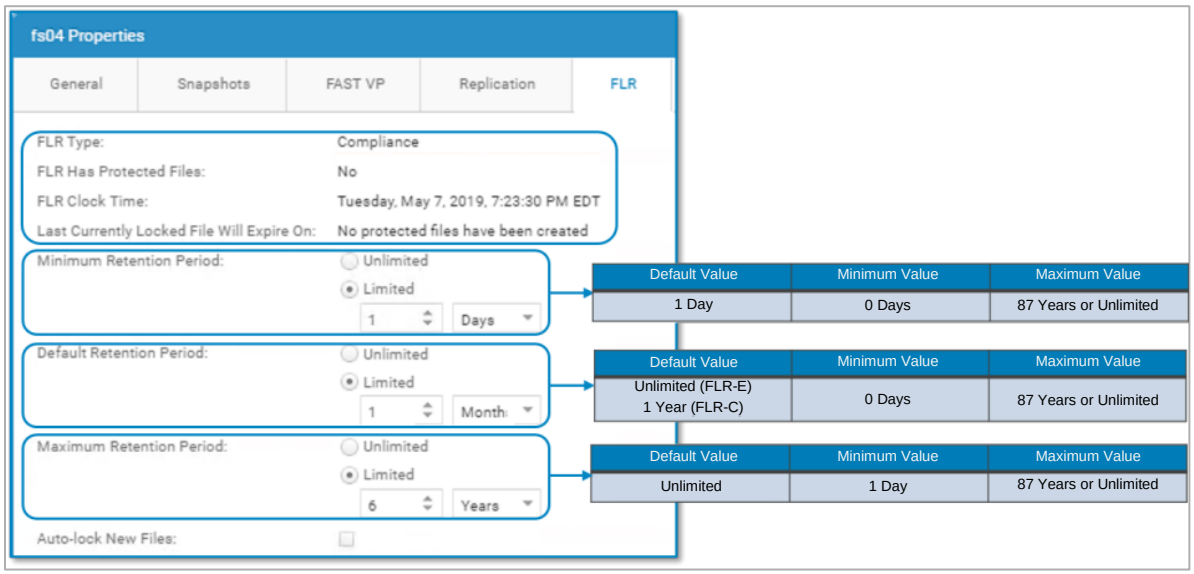
When FLR-C is enabled on a file system, the user must also turn on the data integrity check. It is required for compliance before files are locked on the file system. The NAS Server `FLRCompliance.writeverify` parameter controls the data integrity check. The parameter is set using the **svc_nas** CLI command from an SSH session to the system. When the parameter is enabled, all write operations on all FLR Compliance file systems mounted on the NAS Server are read back and verified. The integrity check ensures that the data has been written correctly. The system performance may degrade during this procedure due to the amount of work being performed.

In the example, the first **svc_nas** command is used to check if the parameter is enabled. From its output, the current value is set to **0** indicating that *writeverify* is disabled.

The second **svc_nas** command sets the value of the parameter to **1**, to enable *writeverify*.

The third **svc_nas** command verifies that *writeverify* is enabled.

Define FLR Retention Periods



File system properties FLR tab with FLR retention periods

This example illustrates the information and retention period configuration available from the FLR tab of the file system Properties.

The FLR Type for the file system is shown. In this example,, the file system has been enabled for Compliance. Also displayed are the number of protected files. In this example file system has no protected files. The FLR clock time is displayed. The tab also displays the date when the last protected file expires.

An FLR enabled file system has retention period limits that can be customized to user needs. Retention periods define how short or long a user can define a file to be locked. The retention periods can be set within the FLR step of the File System Creation wizard as seen previously. The Retention periods can also be configured any time after the file system is created. This example illustrates the retention periods that are defined for the file system. The respective tables show the default, minimum and maximum values for each of the retention periods.

The Minimum Retention Period value specifies the shortest time period a user can specifically lock files for. The value of the Minimum Retention Period must be less than or equal to the Maximum Retention Period value.

The Default Retention Period specifies the time period a file is locked for when the user does not explicitly set a retention time for files. The Default Retention Period is also used when automation is configured to lock files on the file system. The Default Retention Period value must be greater than or equal to the Minimum Retention Period value. It must also be less than or equal to the Maximum Retention Period value.

The Maximum Retention Period specifies the longest time period that files can be locked for. The value must be greater than of equal to the Minimum Retention Period value.

Note: The FLR retention periods can be modified at any time. The modification only affects the retention times for newly locked files by the user or automation. Previously locked files remain unchanged.

Set File State - NFS

Set file Lock state

```
[root@linux15a nfs_mp]# touch -at 202412312359 lockedfile

[root@linux15a nfs_mp]# ls -lu --time-style=long-iso
-rw-r--r--. 1 root root 5 2024-12-31 23:59 lockedfile

[root@linux15a nfs_mp]# chmod -w lockedfile

[root@linux15a nfs_mp]# ls -l
-r--r--r--. 1 root root 5 May 6 2019 lockedfile
```

Set file Append-only state

```
[root@linux15a nfs_mp]# touch append-only

[root@linux15a nfs_mp]# chmod -w append-only

[root@linux15a nfs_mp]# chmod +w append-only
```

CLI command to set file state to locked or append-only

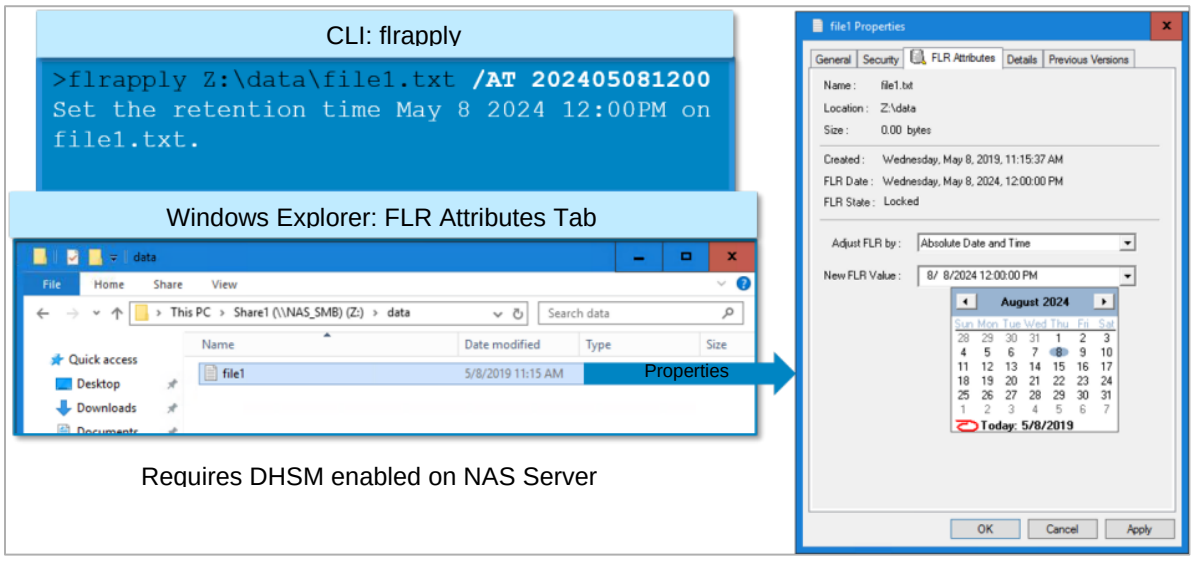
The file state of locked or append-only is set using an NFS client that is mounted to the exported file system.

A file lock state is achieved by setting the last access time of the file to the wanted file retention date and time, and then change the file permission bits to read-only. To set the file last access date and time, use the `touch` command with the `-at` option and the wanted retention date and time. In the example, a file that is named *lockedfile* has its last access time set to 23:59, Dec 31, 2024 as shown in the `ls` output for the file. Then the file is set to read-only using the `chmod` command with the `-w` option to remove the write permission.

When setting the locked file retention date and time, it must be equal to or less than the Maximum Retention Period defined on the file system. Any attempt to set a file retention date and time greater than the Maximum Retention Period results in the retention date and time setting equal to the Maximum Retention Period setting. In a similar manner, any attempt to set a file retention date and time less than the Minimum Retention Period results in the retention date and time setting equal to the Minimum Retention Period setting. Files that are locked without specifying a

retention date and time results in the retention date and time setting equal to the Default Retention Period setting.

Set File State - FLR Toolkit for SMB



Setting file state using FLR toolkit

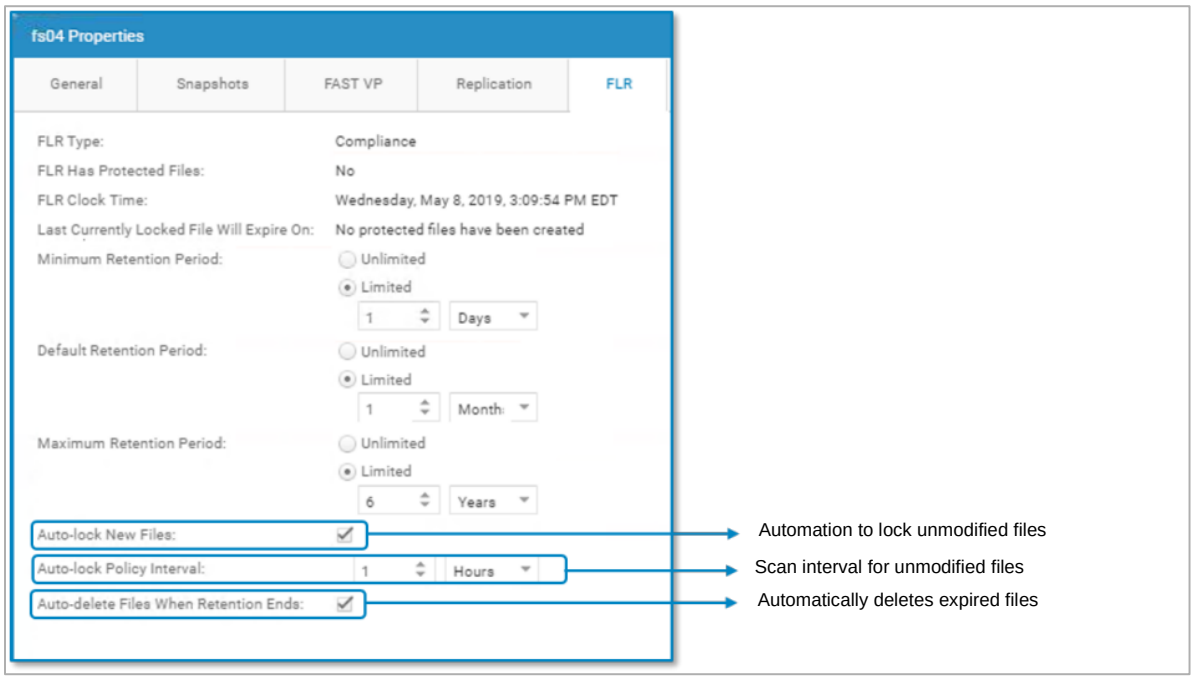
Windows does not have a native UI/CLI to set retention date and time to lock files. The **Dell FLR Toolkit** is an application available for download from Dell Online Support. Install the application on a Windows client in the same domain as the FLR enabled file system to be accessed. The application uses the Windows API *SetFileTime* function for setting retention date and time to lock files on FLR enabled file systems. The toolkit includes a CLI function called **flrapply**. Another aspect of the FLR toolkit is an enhancement to Windows Explorer. An **FLR Attributes** tab is available in Windows Explorer file Properties. The FLR toolkit also has an FLR Explorer which has FLR related reporting and retention time capabilities. FLR Explorer is not shown in this training.

FLR Toolkit requires that DHSM be enabled on the NAS Server that is associated with the FLR enabled file system. Do not check **Enforce HTTP Secure** when enabling DHSM on the NAS Server.

The examples illustrate setting retention date and time on a file to set its lock state. In the flrapply CLI example, an SMB file is set to the lock state with a retention data and time of 12:00 PM May 8, 2024. The second example illustrates the Windows Explorer **FLR Attributes** tab enhancement in the file properties window. The tab displays the FLR expiration date of the file. The example illustrates the retention

date and time being extended on the file to 12:00 PM Aug 8, 2024. As with NFS, when specifying file retention dates and times, they must be within the Minimum and Maximum Retention Period values. If not, the settings defined for the Retention Period are used to lock the file.

Set File State - Automated



Setting automatic lock and delete

Files can be locked through automation on FLR enabled file systems using options available on the FLR tab of the file system Properties. The automation options are disabled by default.

When the Auto-lock New Files option is enabled, the Auto-lock Policy Interval configuration is exposed. The system automatically locks files if they are not modified for a user specified time period, defined by the Auto-lock Policy Interval. Automatically locked files use the Default Retention Period setting. Files in append-only mode are also subject to automatic locking.

When enabled, the Auto-delete Files When Retention Ends option automatically deletes locked files after their retention date and time have expired. The auto-delete happens at 7-day intervals. Its timer starts when the auto-delete option is enabled.

Scalability, Performance and Compliance Key Points

1. **FAST Cache**
   a. FAST Cache is a secondary cache created from SAS Flash 2 drives that extends the storage system caching capacity.
   b. The storage system identifies LUN data that that is more frequently accessed and service any subsequent requests from the FAST Cache.
   c. FAST Cache operations includes host reads/writes, FAST Cache promotion, FAST Cache flush, and FAST Cache cleaning. In addition, the FAST Cache can be expanded, shrunk or deleted.
2. **Host I/O Limits**
   a. Dell Unity XT Host I/O Limits is a feature that limits I/O to storage resources: LUNs, attached snapshots, and VMFS datastores.
   b. Only one Host I/O limit policy can be applied to a storage resource. Policies can be set by:
      - Throughput, in IOs per second (IOPS)
      - Bandwidth, defined by Kilobytes or Megabytes per second (KBPS or MBPS)
      - A combination of both types of limits
   c. There are two Host I/O Limit policy types: Absolute and Density-based. In addition, a policy can share the same limit(s) with all assigned storage resources.
   d. The Burst feature allows for one-time exceptions to Host I/O Limits. The feature can be set at some user-defined frequency for each Host I/O Limit policy.
3. **UFS64 File System Extension and Shrink**
   a. In Dell Unity XT systems, the UFS64 architecture enables the extension of file systems.
      - A storage administrator can manually extend the size of a provisioned file system.
      - Thin file systems are automatically extended by the system based on the ratio of used-to-allocated space.

b. In Dell Unity XT, the UFS64 architecture enables the reduction of the space the file system uses from a storage pool.
   - A storage administrator can manually shrink the size of a provisioned file system.
   - Thin-provisioned file systems are automatically shrunk by the system when the used space is less than 70%.

4. **File-level Retention (FLR)**

a. Dell Unity XT supports the configuration of File-level Retention (FLR) during the creation of a file system.

b. File-level Retention (FLR) protects files from modification or deletion through SMB, NFS, or FTP access based on a specified retention date and time.

c. There are two different types of FLR; FLR-E (Enterprise) and FLR-C (Compliance).

d. Files within an FLR enabled file system have different states; Not Locked, Append-only, Locked and Expired.

For more information, see the **Dell EMC Unity Family Configuring Pools**, **Dell EMC Unity: NAS Capabilities**, and **Dell EMC Unity: File-Level Retention (FLR)** on the Dell Technologies Support site.