Introduction to minimizing risk in thin provisioning

Cloud Insights

Dave Grace
February 27, 2020

NetApp®

Table of Contents

Introduction to minimizing risk in thin provisioning

In today's hybrid IT data centers, administrators are pressured to stretch resource utilization beyond physical bounds by employing capacity efficiency technologies such as thin provisioning to control over allocation and leverage what was once unavailable capacities.

Cloud Insights provides near real time capacity usage and utilization details historically across multiple thin provisioned layers within the IT service stack. Failing to properly manage oversubscription risk could result in untimely downtime to the business.

Monitoring the storage pool

Each storage pool landing page provides over-subscription ratios, identifies correlated resources, LUN and disk utilization, as well as policy breaches and violations that have occurred with the storage pool.

Use the storage pool landing page to identify any potential problems with the physical assets supporting your virtual infrastructure. You can track capacity and capacity ratios trending over 30 days or use a custom time frame. Pay attention to data in the following sections to monitor the status of the storage pool.

Use the **Summary** section to understand:

- Storage pool capacity information including physical capacity and the overcommitted capacity.
- Whether the aggregate is oversubscribed, and by how much
- Any policy violations that have occurred
- Use the **Storage resources** section to understand the LUN utilization
- Use the **Disks** sections to understand the individual disks that make up the storage pool
- Use the **Resources** section to understand the VMDKs to LUNs correlation and understand the storage to VM application path
- Use the **Violations** section to identify breaches to performance policies that have been set for the storage pool.

Monitoring the Datastores

The Datastore landing page identifies over-subscription ratios, LUN and disk utilization, correlated resources, and shows policy breeches and violations that have occurred with the Datastore.

Use this landing page to identify problems with your virtual infrastructure. You can track capacity and

capacity ratio trending to anticipate changes in your capacity.

Use the **Summary** section to understand:

- Datastore capacity information including physical capacity and the overcommitted capacity.
- The percentage of overcommitted capacity.
- Metrics for latency, IOPS, and throughput.

The **VMDKs** section shows virtual disk capacity and performance.
The **Storage resources** section shows the capacity used and the performance metrics for the internal volume correlated to the Datastore.
Use the **Resources** section to understand the VMDKs to LUNs correlation, and understand the storage to VM application path.

Create dashboards to monitor thin provisioned environments

loud Insights flexible dashboard widget design and display charting options allow deep analysis into capacity usage and utilization, strategic information for minimizing risks in thin provisioned data center infrastructures.

You can create dashboards that provide access to Datastore and Storage pool information that you want to monitor.

Using dashboards to access Datastore information

You might want to create dashboards that provide quick access to the data you want to monitor in your virtual infrastructure. A dashboard could include widgets similar to the following to identify the top 10 Datastores based on their overcommitted % and a widget showing the capacity data for Datastores. The dashboards use variables to highlight Datastores that are overcommitted by more than 150% and Datastores that have exceeded more than 80% used capacity.

image::top_10_overcommit.png

Using performance policies to reduce risk in thin provisioning

You should create performance policies to raise alerts when thresholds in your virtual infrastructure have been breached. The alerts allow you to respond to changes in your environment before they cause interruptions or outages in operations.

Policies that help in monitoring the virtual infrastructure include the following:

Datastore

You can create policies that closely monitor Datastore capacity:

- Capacity ratio - Overcommit
- Capacity ratio - Used
- Capacity - Used
- Capacity - Total

Storage pool
You can create policies that that protect against Storage Pool capacity outages in thin provisioned environments:

- Capacity provisioned
- Capacity used
- Capacity ratio - Overcommit
- Capacity ratio - Used

You can expand from these policies to monitor capacity in the virtual infrastructure by creating additional policies for these assets:

- Internal volumes
- LUNs
- Disks
- VMDKs
- VMs

You can configure policies using annotations. You assign the same annotation to the specific assets that support an application. For example, you can assign annotations to the Datastores and the Storage pools of a thin provisioned application.

You might have annotations named Production for the production environment, Development for the development environment, and so on. You can change the thresholds and criticality of warnings depending on the type of application the assets are supporting.

For example, a breach of a threshold for a production application’s DataStore might raise a critical warning, while the same breach for a development environment might only raise a warning.

Incorporating annotations into defined policies can reduce unwanted alerting noise for non-critical assets.

Creating performance policies for Storage Pools

You can create performance policies that trigger alerts to notify you when thresholds for Storage Pool assets have been exceeded.

- Before you begin

This procedure assumes that you have thin provisioned the storage pool.

- About this task

You want to create policies that monitor and report changes in a storage pool that could contribute to outages. For the thin provisioned physical storage pool, you want to monitor the physical capacity and monitor the overcommit ratio.

- Steps
  1. In the Cloud Insights menu, click **Manage** > **Performance Policies**

     The Performance Policies page is displayed. Policies are organized by object, and are evaluated in the order in which they appear in the list. When notifications are enabled (**Admin** > **Notifications**), you can configure Insight to send email when performance policies are breached.

  2. Click + **Performance Policy** to create a new policy
  3. In **Policy Name** enter a unique name for the policy
  4. In **Apply to objects of type** select Storage Pool
  5. In **Apply after window of** enter First occurrence.
  6. In **With severity** enter Critical
  7. Configure the Email recipients that you want notified when thresholds are breached.

     By default, email alerts on policy violations are sent to the recipients in the global email list. You can override these settings so that alerts for a particular policy are sent to specific recipients.

     Click the link to open the recipients list, then click the + button to add recipients. Violation alerts for this policy will be sent to all recipients in the list.

  8. In **Create alert if any of the following are true** enter Capacity ratio - Used > 85%
- Result

This configuration results in the system sending a critical warning message when more than 85% of the physical capacity of the storage pool is used. Using 100% of the physical memory will result in application failure.

Creating performance policies for Datastores

You can create performance policies with thresholds for metrics associated with the data stores that correlate to the storage pools you are monitoring.

By default, performance policies apply to all devices of the specified type when you create them. You

can create an annotation to include only a specific device or a set of devices in the performance policy.

1. Before you begin

When using an annotation in a performance policy, the annotation must exist before the policy is created.

You create a performance policy that provides notification when one or more Datastores you are monitoring exceeds a threshold you set. Your system might already contain a global policy that meets your needs. With a policy using annotations you can provide more focus on specific Datastores.

Steps

1. In the Cloud Insights toolbar, click **Manage** > **Performance Policies**
2. Click + **Performance Policy**
3. Add a "Policy Name"

   You must use a name that is different from all the other policy names for the object. For example, you cannot have two policies named "Latency" for an internal volume; however, you can have a "Latency" policy for an internal volume and another "Latency" policy for a Datastore. The best practice is to always use a unique name for any policy, regardless of the object type.

4. Select "Datastore" as the Object Type
5. Click "First Occurrence"
6. In **Policy Name** enter a unique name for the policy
7. In **Apply to objects of type** select Datastore
8. In **With Annotation** select the name of the annotation
9. In **Annotation Value** select the desired value
10. In **Apply after window of** enter First occurrence
11. In **With severity** enter Critical
12. Configure Email recipients
13. In **Create alert** enter Capacity Ratio - Over Commit > 150
14. Click + **Threshold** to add additional thresholds, such as Capacity total and Capacity used.