Introduction to minimizing risk in thin provisioning

OnCommand Insight

NetApp
March 08, 2024

This PDF was generated from https://docs.netapp.com/us-en/oncommand-insight/howto/monitoring-the-storage-pool.html on March 08, 2024. Always check docs.netapp.com for the latest.

Table of Contents

Introduction to minimizing risk in thin provisioning 1
- Monitoring the storage pool 1
- Monitoring the Datastores 1
- Create dashboards to monitor thin provisioned environments 2
- Using performance policies to reduce risk in thin provisioning 4
- Creating performance policies for Storage Pools 5
- Creating performance policies for Datastores 6

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.

OnCommand Insight 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.

- **Summary**

  Use this 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.
- **Storage resources and Disks sections**

  The storage resources section shows the LUN utilization.

  The disks section shows the individual disks that make up the storage pool.
- **Resources**

  Use this section to understand the VMDKs to LUNs correlation and understand the storage to VM application path.
- **Violations section**

  The violations section identifies any 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.

- **Summary**

  Use this section to understand:

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

  The VMDKs section shows virtual disk capacity and performance.
- **Storage resources**

  This section shows the capacity used and the performance metrics for the internal volume correlated to the Datastore.
- **Resources**

  Use this section to understand the VMDKs to LUNs correlation, and understand the storage to VM application path.
- **Violations section**

  The violations section identifies any breaches to performance policies that have been set for the Datastore.

Create dashboards to monitor thin provisioned environments

OnCommand Insight's 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.

Overcommit Subscription %

Name	Capacity - Total (GB)	Capacity - Used (GB)	Capacity - Provisioned (GB)	Capacity ratio - Over commit (%)	Capacity ratio - Used (%)
dc14_1407_...1_prd_cl03	5,008.00	4,091.04	12,876.38	257.12	81.69
dc14_1407_...2_prd_cl03	6,936.69	5,872.31	14,633.80	210.96	84.66
dc14_1407_...3_prd_cl03	9,437.03	7,951.36	17,639.86	186.92	84.26
dc14_1407_...4_prd_cl03	7,911.09	6,627.00	17,891.24	226.15	83.77

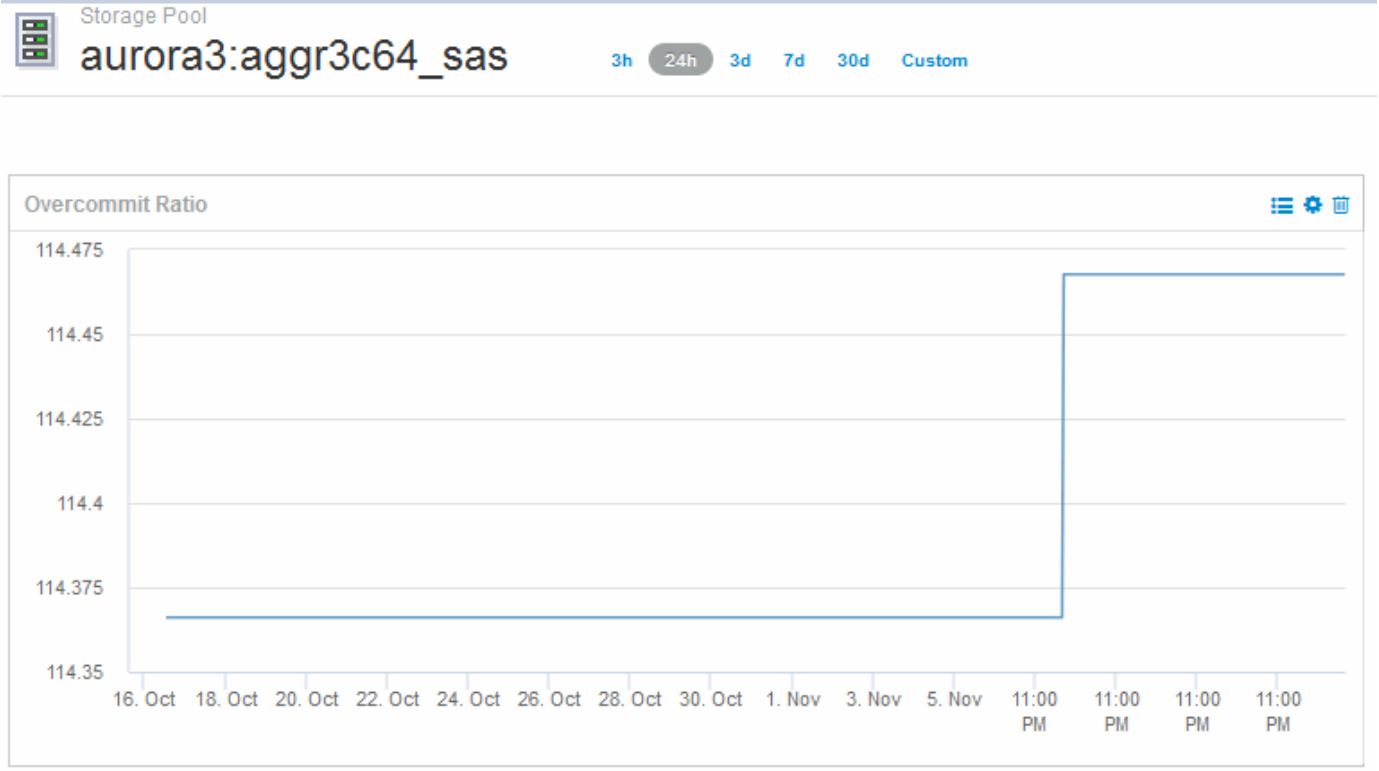
4 items found

Additional widgets that could be used to monitor your thin-provisioned environment could include some of the following information:

- VMDK capacities correlated to Datastores
- VM capacities
- Data store capacity used trending

Using dashboards to access Storage pool information

A dashboard could include widgets similar to the following, identifying the amount of physical storage capacity used, or identifying the overcommitted capacity for a Storage Pool.



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 could use the following policies on the Datastore:

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

- **Storage pool**

  The following policies can protect against storage related 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, including:

- 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 within defined policies can help to further 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. Open OnCommand Insight in your browser.
2. Select **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. If notifications are enabled (**Admin** > **Notifications**), you can configure Insight to send email when performance policies are breached.

3. Click **+Add**to create a new policy.
4. In **Policy Name** enter a policy name for the Storage Pool.
5. In **Apply to objects of type** select Storage Pool.
6. In **Apply after window of** enter First occurrence.
7. In **With severity** enter Critical
8. 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.

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

Results

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.

Create additional Storage Pool policies

About this task

Create an additional “Capacity ratio - Used” policy that raises a warning message when the Storage Pool capacity used exceeds 75%. If notifications are enabled (**Admin** > **Notifications**), you can configure Insight to send email when performance policies are breached.

Creating performance policies for Datastores

You can create performance policies with thresholds for metrics associated with the datastores 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.

Before you begin

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

About this task

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 or a policy using annotations might also work if you annotate your Datastores.

Steps

1. From the Insight toolbar, select **Manage** > **Performance Policies**

   The performance policies page is displayed. Review any existing performance policies to identify existing policies that address the metrics for thresholds you want to monitor.

2. Click **+Add** to add a new 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 data store. 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”

   The First occurrence option triggers an alert when a threshold is exceeded on the first sample of data. All other options trigger an alert when the threshold is crossed once and is continuously crossed for at least the specified amount of time.

6. Click “Warning”
7. For “Create alert”, select **Capacity ratio - Over commit** and set the value to **> 150**

   You might want to create additional capacity related alerts, such as **Capacity total**and **Capacity used**.

Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.