Managing feature settings

Active IQ Unified Manager 9.12

NetApp
February 12, 2024

This PDF was generated from https://docs.netapp.com/us-en/active-iq-unified-manager-912/config/concept_policy_based_storage_management.html on February 12, 2024. Always check docs.netapp.com for the latest.

Table of Contents

Managing feature settings . . . 1
- Enabling policy-based storage management . . . 1
- Enabling API Gateway . . . 1
- Specifying inactivity timeout . . . 2
- Enabling Active IQ portal events . . . 2
- Enabling and disabling security settings for compliance . . . 3
- Enabling and disabling scripts upload . . . 4
- Adding login banner . . . 4

Managing feature settings

The Feature Settings page allows you to enable and disable specific features in Active IQ Unified Manager. This includes creating and managing storage objects based on policies, enabling the API Gateway and Login Banner, uploading scripts for managing alerts, timing out a web UI session based on inactivity time, and disabling receipt of Active IQ platform events.

The Feature Settings page is only available for users with Application Administrator role.

For information about Scripts Upload, see Enabling and disabling scripts upload.

Enabling policy-based storage management

The **Policy-based storage management** option allows storage management based on service level objectives (SLOs). This option is enabled by default.

On activating this feature, you can provision storage workloads on the ONTAP clusters added to your Active IQ Unified Manager instance, and manage these workloads based on the assigned Performance Service Levels and Storage Efficiency Policies.

You can choose to activate or deactivate this feature from **General** > **Feature Settings** > **Policy-based storage management**. On activating this feature, the following pages are available for operation and monitoring:

- Provisioning (storage workload provisioning)
- **Policies** > **Performance Service Levels**
- **Policies** > **Storage Efficiency**
- Workloads Managed by Performance Service Level column on the Clusters Setup page
- Workload Performance panel on the **Dashboard**

You can use the screens to create Performance Service Levels and Storage Efficiency Policies, and provision storage workloads. You can also monitor the storage workloads that conform to the assigned Performance Service Levels, as well as the nonconforming ones. The Workload Performance and Workload IOPS panel also enables you to assess the total, available, and used capacity and performance (IOPS) of the clusters across your data center based on the storage workloads provisioned on them.

After activating this feature, you can run the Unified Manager REST APIs to perform some of these functions from **Menu Bar** > **Help button** > **API Documentation** > **storage-provider** category. Alternatively, you can enter the host name or IP address and the URL to access the REST API page in the format https://<hostname>/docs/api/

For more information about the APIs, see Getting started with Active IQ Unified Manager REST APIs.

Enabling API Gateway

The API Gateway feature allows Active IQ Unified Manager to be a single control plane from which you can manage multiple ONTAP clusters, without logging in to them

individually.

You can enable this feature from the configuration pages that appear when you first log in to Unified Manager. Alternatively, you can enable or disable this feature from **General** > **Feature Settings** > **API Gateway**.

Unified Manager REST APIs are different from the ONTAP REST APIs, and not all the functionalities of ONTAP REST APIs can be availed by using the Unified Manager REST APIs. However, if you have a specific business requirement of accessing the ONTAP APIs for managing specific features that are not exposed to Unified Manager, you can enable the API Gateway feature and execute the ONTAP APIs. The gateway acts as a proxy to tunnel the API requests by maintaining the header and body requests in the same format as in the ONTAP APIs. You can use your Unified Manager credentials and execute the specific APIs to access and manage the ONTAP clusters without passing individual cluster credentials. Unified Manager performs as a single point of management for running the APIs across the ONTAP clusters managed by your Unified Manager instance. The response returned by the APIs is the same as the response returned by the respective ONTAP REST APIs executed directly from ONTAP.

After enabling this feature, you can execute the Unified Manager REST APIs from **Menu Bar** > **Help button** > **API Documentation** > **gateway** category. Alternatively, you can enter the host name or IP address and the URL to access the REST API page in the format `https://<hostname>/docs/api/`

For more information about the APIs, see Getting started with Active IQ Unified Manager REST APIs.

Specifying inactivity timeout

You can specify the inactivity timeout value for Active IQ Unified Manager. After an inactivity of the specified time, the application is automatically logged out. This option is enabled by default.

You can deactivate this feature or modify the time from **General** > **Feature Settings** > **Inactivity Timeout**. Once you activate this feature, you should specify the time limit of inactivity (in minutes) in the **LOGOUT AFTER** field, after which the system automatically logs out. The default value is 4320 minutes (72 hours).

This option is not available if you have enabled Security Assertion Markup Language (SAML) authentication.

Enabling Active IQ portal events

You can specify whether you want to enable or disable Active IQ portal events. This setting allows the Active IQ portal to discover and display additional events about system configuration, cabling, and so forth. This option is enabled by default.

On enabling this feature, Active IQ Unified Manager displays events discovered by the Active IQ portal. These events are created by running a set of rules against AutoSupport messages generated from all monitored storage systems. These events are different from the other Unified Manager events, and they identify incidents or risks related to system configuration, cabling, best practice, and availability issues.

You can choose to activate or deactivate this feature from **General** > **Feature Settings** > **Active IQ Portal Events**. In sites with no external network access, you must upload the rules manually from **Storage Management** > **Event Setup** > **Upload Rules**.

This feature is enabled by default. Disabling this feature stops the Active IQ events from being discovered or displayed on Unified Manager. When disabled, enabling this feature allows Unified Manager to receive the

Active IQ events on a cluster at a predefined time of 00:15 for that cluster timezone.

Enabling and disabling security settings for compliance

By using the **Customize** button on the **Security Dashboard** panel of the Features Settings page, you can enable or disable the security parameters for compliance monitoring on Unified Manager.

The settings that are enabled or disabled from this page govern the overall compliance status of the clusters and storage VMs on Unified Manager. Based on the selections, the corresponding columns are visible in the **Security: All Clusters** view of the Clusters inventory page and the **Security: All Storage VMs** view of the Storage VMs inventory page.

Only users with administrator role can edit these settings.

The security criteria for your ONTAP clusters, storage VMs, and volumes are evaluated against the recommendations defined in the Security Hardening Guide for NetApp ONTAP 9. The Security panel on the dashboard and the Security page display the default security compliance status of your clusters, storage VMs, and volumes. Security events are also generated and management actions enabled for the clusters and storage VMs that have security violations.

Customizing security settings

To customize the settings for compliance monitoring as applicable to your ONTAP environment, follow these steps:

Steps

1. Click **General > Feature Settings > Security Dashboard > Customize**. The **Customize Security Dashboard Settings** pop-up appears.

   The security compliance parameters that you enable or disable can directly affect the default security views, reports, and scheduled reports on the Clusters and Storage VMs screens. If you had uploaded an excel report from these screens before modifying the security parameters, the downloaded excel reports might be faulty.

2. To enable or disable the custom settings for your ONTAP clusters, select the required general setting under **Cluster**. For information on the options for customizing cluster compliance, see Cluster compliance categories.
3. To enable or disable the custom settings for your storage VMs, select the required general setting under **Storage VM**. For information on the options for customizing storage VM compliance, see Storage VM compliance categories.

Customizing AutoSupport and authentication settings

On the **AutoSupport Settings** section, you can specify whether HTTPS transport is to be used for sending AutoSupport messages from ONTAP.

From the **Authentication Settings** section, you can enable Unified Manager alerts to be raised for the default ONTAP administrator user.

Enabling and disabling scripts upload

The ability to upload scripts to Unified Manager and run them is enabled by default. If your organization does not want to allow this activity because of security reasons, you can disable this functionality.

What you'll need

You must have the Application Administrator role.

Steps

1. In the left navigation pane, click **General** > **Feature Settings**.
2. In the **Feature Settings** page, disable or enable scripting by choosing one of the following options:

If you want to…	Then do this…
Disable scripts	In the **Script Upload** panel, move the slider button to the left.
Enable scripts	In the **Script Upload** panel, move the slider button to the right.

Adding login banner

Adding a login banner enables your organization to display any information, such as, who is permitted access to the system and the terms and conditions of use during login and logout.

Any user, such as storage operators or administrators can view this login banner pop-up during login, logout, and session timeout.

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.