NetBackup™ 11.2 Anomaly Detection Extensions Guide

VERITAS
now part of Cohesity

NetBackup™ Anomaly Detection Extensions Guide

Last updated: 2026-05-29

Legal Notice

Cohesity, Inc.
2625 Augustine Drive.
Santa Clara, CA 95054

https://www.cohesity.com

Cohesity Support

Reach Cohesity Support

There are several ways to create a Cohesity support case.

- Go to Cohesity Support, to search in our knowledge base; or contact us by phone - United States and Canada: 1-855-9CO-HESI (926-4374), option 2.
- Log in to the Cohesity Support Portal to create a new case.
- Click the (**?**) icon on the Cohesity UI and select Support Portal.

Support/Service Assistance

First, contact the Service Provider that you have contracted for service and support. If you work directly with Cohesity and have a product warranty/entitlement, repair pricing, or technical support-related question, see your options below:

- To find solutions to your product issues or for suggestions or best practices, visit the Cohesity Knowledge Base.
- Log in to the Cohesity Support Portal to create a new case.
- To monitor your open cases, log in to the portal and click the **Cases** tab on the home page. This page should have all the case statuses and updates. You can also view individual case status.

Cohesity Software Running on Partner Hardware

For Cohesity software running on qualified third-party hardware, the following support workflow applies:

1. The customer may contact Cohesity Support first if the issue cannot be determined as a hardware issue.

   Note: Cohesity cannot process hardware replacement requests for partner hardware.

2. Cohesity Support triages the issue. If it is a software issue, Cohesity Support continues to work on it.
3. If it is a hardware/firmware issue or is suspected to be a hardware/firmware issue, Cohesity provides information about the issue to the customer and requests that the customer open a support ticket with the appropriate partner.
4. If needed, Cohesity Support can join a three-way call with the partner and the customer.
5. The customer informs Cohesity Support on the progress of the partner’s case.

Contents

Chapter 1

About detecting system anomalies in NetBackup

This chapter includes the following topics:

About system anomaly detection (extensions)

NetBackup can detect system anomalies (also called anomaly detection extensions) during critical operations as follows:

- Rule-based system anomaly
  See "Configure rules-based anomaly detection" on page 8.
- Risk engine-based system anomaly
  See "Configure risk engine-based anomaly detection" on page 9.

See "View system anomalies" on page 12.

NetBackup utilizes the Cohesity REDLab research outcome to add new anomaly detection capabilities and provide industry-leading ransomware protection.

See "About the Cohesity REDLab" on page 5.

About the Cohesity REDLab

Based on the severity and high number of ransomware attacks across large institutions, it is imperative for Cohesity to keep its ransomware solutions updated and to introduce new capabilities quickly and efficiently. To cater to this critical

requirement, Cohesity has developed an isolated security lab, called REDLab that is equipped to create the required environment in-house and carry out the necessary experimentations with NetBackup.

Important notes

- The new extension analyses the image expiry data of the last 3 months from audit records. Only the manual operations are considered.
- It also analyses the image expiry date modifications if the date is pre-poned.
- Once the historical data is captured, the extension keeps analyzing new expiry audit data from the audit API every few minutes.
- If there are any expirations by a user that are beyond the threshold, an anomaly is detected.

Chapter 2

System anomalies

This chapter includes the following topics:

Configure system anomaly detection settings

After you enable anomaly detection, anomaly data gathering, detection service, and events are enabled. You can configure specific settings to detect system anomalies in your domain.

To configure system anomaly detection settings

1. On the left, click **Detection and reporting > Anomaly detection.**
2. On the top right, click **Anomaly detection settings > System anomaly detection configuration**.
3. On the **System anomaly detection configuration** screen, configure the following settings:
   - **Risk engine-based anomaly detection**
     See "Configure risk engine-based anomaly detection" on page 9.
   - **System anomaly detection > Monitor database corruption in workloads during job failures**
     This anomaly monitors database corruption in workloads like Microsoft SQL Server and Oracle during backup job failures.

Select the checkbox to generate an anomaly alert when NetBackup detects backup job failures because of database corruption in workloads like Microsoft SQL Server and Oracle.

If database corruption in a workload is detected, status code 5464 is attributed to the parent job that is displayed in the **Activity monitor** > **Jobs** tab.

Click the status code number to view information about this status code in the Cohesity Knowledge Base.

See the NetBackup Status Codes Reference Guide.

Note: For detecting database corruption in Microsoft SQL Server, the 'Microsoft SQL Server checksum' option must be set to 'Fail on Error' during MS SQL Server policy configuration.

- **Rules-based anomaly detection**
  See "Configure rules-based anomaly detection" on page 8.

Configure rules-based anomaly detection

Rules engine-based anomaly detection allows you to define certain rules. If the threshold values that are defined in the rule are exceeded, anomalies are generated. For example, an anomaly is generated if a certain number of failed login attempts occur in a specified time period.

For each rule, you can configure the following parameters: execution frequency, query period, and threshold.

To modify the rule parameters, use the `/security/anomaly/rules/{ruleId}` API.

To configure rules-based anomaly detection

1. On the left, click **Detection and reporting** > **Anomaly detection**.
2. On the top right, click **Anomaly detection settings** > **System anomaly detection configuration**.
3. On the **System anomaly detection configuration** screen, expand **Rules-based anomaly detection** and select the **Detect anomalies using NetBackup anomaly detection rules** check box.

   The following details for each of the predefined rules are displayed:

   - Rule name
   - Description
   - Severity

- Version
- Enabled

For the latest rules file, go to the Cohesity Download Center and download the rules file (`.zip`) for which you want to generate anomalies.

Select **Upload rules** to select the rules file that you have downloaded. All the latest rules are listed in the **Rules-based anomaly detection** section.

4 Select the rules that you want to enable and for which you want to generate anomalies.

Select **Enable**.

NetBackup generates anomalies for the conditions that meet the rule criteria.

Configure risk engine-based anomaly detection

The NetBackup risk engine detects certain system anomalies in a proactive manner and sends appropriate alerts. It helps you take corrective action before you face any security threat in your environment.

You can configure the following options that the risk engine uses to detect anomalies for the given operations:

Detect suspicious image expiration

Use this option to detect when images are expired in an unusual or a suspicious manner.

By default, a system anomaly is generated when the risk engine detects an unusual or a suspicious image expiration attempt and allows the operation to proceed.

However, for additional security, you can configure multiperson authorization for such image expiration attempts, where an MPA approver needs to approve the operation.

Important notes on the Detect suspicious image expiration option

- If the audit retention period is set to less than 3 months, this option accumulates data of 3 months and then becomes active.
- This option supports full backup schedules. Other types of schedule are not considered. The retention level of an image is also not considered for this rule.
- Images are expired by media ID, server name, or by recalculating the retention period.

Select **Edit** and select the **Generate multiperson authorization ticket if images are deleted in a suspicious manner** option.

Note: To successfully review the multiperson authorization tickets, ensure that one or more MPA approvers are available in your environment.

Detect unusual user sign in

Use this option to detect when a user attempts to sign in to the NetBackup web UI at an unusual time. NetBackup identifies deviations in user sign-in patterns, and flags them.

A notification is generated when an unusual user login is detected.

For additional security, you can configure multiperson authorization for such unusual login attempts, where an MPA approver needs to approve the operation.

- If an unusual login attempt is detected on a NetBackup host earlier that 11.0, the request is rejected. Carry out the operation on a NetBackup 11.0 host.
- If an unusual login request is detected in the **NetBackup Administration Console**, the request is rejected. Use the web UI to carry out the operation.
- If none of the users can login and they are placed on hold because of unusual login pattern, the NetBackup administrator can disable the unusual login detection to allow the users to sign in to the NetBackup web UI using the following command:

  NBU_INSTALL_PATH/netbackup/bin/admincmd/nbseccmd -disableLoginAnomalyDetection
- User logins that are based on the authentication types such as SAML, smart card, and API keys do not support login anomaly detection.

Click **Edit** and use the **Place user's sign in on hold and generate multiperson authorization ticket if a user signs in at an unusual time** option to enable multiperson authentication.

- To successfully review the multiperson authorization tickets, ensure that one or more MPA approvers are available in your environment.
- If multiperson authorization is enabled and an unusual user login is detected, the user’s login is placed on hold.
- A ticket is generated and requires approval for the user to proceed. Until the ticket is approved, the user shall not be able to login from the device.
- If the ticket is approved, the user is allowed login and granted a free pass for the next 24 hours. During the free pass period, the user is not subjected to further scrutiny for unusual login attempts.
- If the ticket is rejected, the user cannot log in for the current session but can try again with their credentials.

- The user can choose to cancel their login request.

Detect unusual updates to policies

By default, a system anomaly is generated when the risk engine detects an unusual deletion or update of a policy. An alert is generated and the operation proceeds.

For additional security, you can configure multiperson authorization for such unusual policy update or deletion attempts, where an MPA approver needs to approve the operation.

Click **Edit** and use the **Generate multiperson authorization ticket if policy is being modified or deleted in an unusual manner** option to enable multiperson authorization for the **Detect unusual updates to policies** type of anomaly.

- To successfully review the multiperson authorization tickets, ensure that one or more MPA approvers are available in your environment.
- Two alerts are generated for unusual updates to a policy for the next 48 hours. After the second alert, no alert is generated for the next 48 hours even if the policy is modified.
- If multiperson authorization is enabled, a ticket is generated for modification of a policy.
- Approving two consecutive tickets for the same policy does not generate new tickets for the next 48 hours for the same policy.
- If multiperson authorization is enabled for the policy operations on the global level, the **Detect unusual updates to policies** option is disabled.

Note: If multiperson authorization is enabled for the **Detect unusual updates to policies** option, you cannot update or delete policies using the **NetBackup Administration Console** or the command-line interface.

Alternatively, use the `nbcmdrun` command to update or delete policies. For more information on the commands, see the NetBackup Commands Reference Guide.

Secure critical operations

Use this option to protect critical operations such as modifying global security settings and creating API key. When you select this option, you are required to reautneticate yourself by entering the one-time password that you see in the authenticator application on your smart device before you perform the given critical operations.

Ensure that you have configured multifactor authentication for your user account. If multifactor authentication is not configured, you are not prompted to reauthenticate.

Note: It is strongly recommended that you configure multifactor authentication in your environment to prevent security threats by malicious sources.

Detect possible session hijack

Use this option to detect if there is a possible user session hijack by a malicious source.

The risk engine detects if the same user session token is used by another IP address, and sends a maximum of 10 alerts per day.

Select **Edit** and select the check box to terminate the user session when the risk engine detects that there is a possible session hijack.

View system anomalies

NetBackup can detect system anomalies. This anomaly detection is enabled by default for all policy types.

To view system anomalies

1. On the left, select **Detection and reporting > Anomaly detection > System anomalies**.

   The following columns are displayed:

   - Detected on - The date when the anomaly is detected
   - Review status - Anomaly status that indicates whether the detected anomaly is reported as a false positive or an actual anomaly, or it can be ignored.
   - Anomaly type - Type of the anomaly
   - Severity - Severity of the anomaly
   - Description - Additional information about the anomaly
   - Anomaly ID - ID of the anomaly record

2. Expand a row to see the details of the selected anomaly.
3. You can perform the following actions on the anomaly record:
   - Select **Report as false positive** if the anomaly is a false positive. Similar anomaly conditions are not reported in the future.
   - Select **Confirm as anomaly** when you want to take some action on the anomaly condition.
   - Select **Mark as ignore** when you can ignore the anomaly condition.