

NetBackup Detection

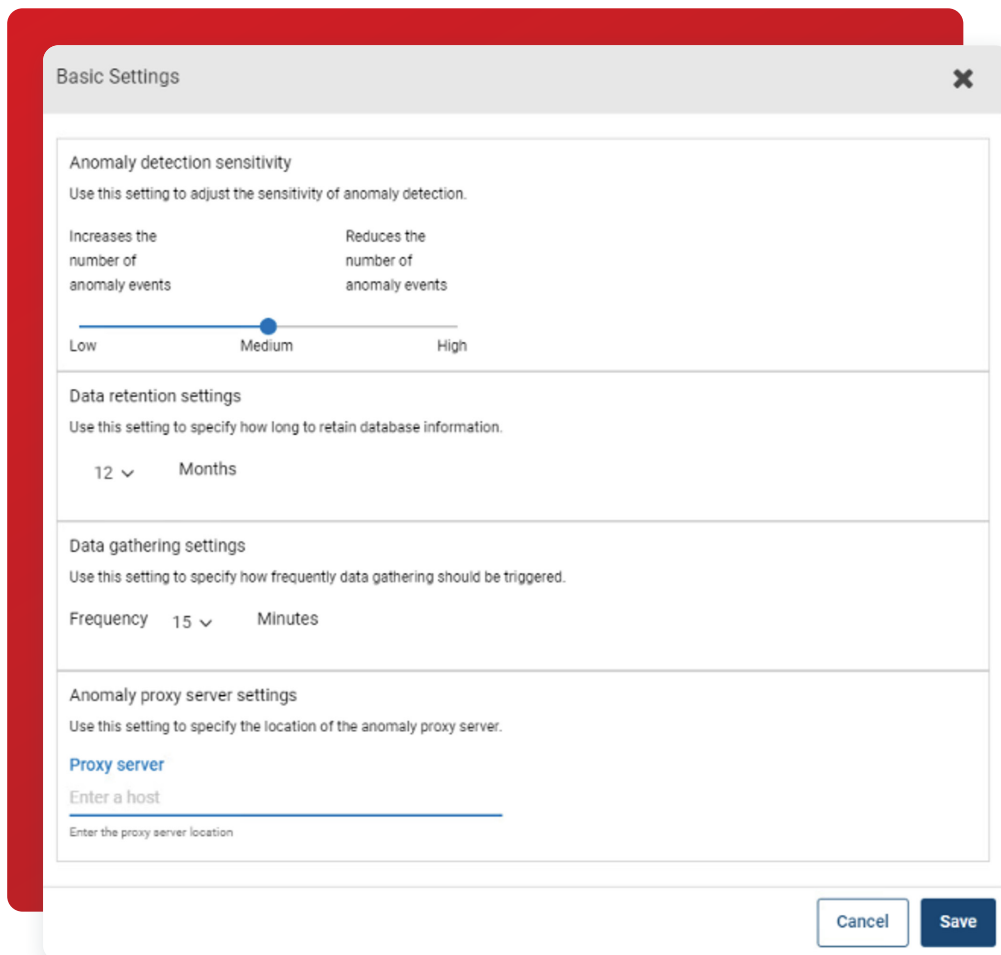
Continuously monitor, detect, and mitigate potential threats and vulnerabilities.

Overview

Detecting anomalies in backup images gives backup administrators an important metric to both play a role in the organization's security posture and understand trends and deviations in its data protection footprint. Anomaly detection was previously only possible through rigorous manual analysis of the Veritas NetBackup™ Activity Monitor, but this process is now automated with the Anomaly Detection engine. Introduced in NetBackup 9.1, anomaly detection uses metadata already available to key in on likely indicators of issues. An anomaly is any significant change in backup image size, number of backup files, data that is transferred in KB, deduplication rate, or backup job completion time. NetBackup uses machine learning (ML) to detect anomalies, based on statistical data clustering analysis, to form an anomaly's score. A higher score is more significant and reflects how different one set of data is compared to previous sets of data to form a baseline.

To access the anomaly detection settings, open the NetBackup web UI and log in as the backup administrator, the account with permissions to all aspects of the web UI. You can find anomaly detection under "Detection and reporting" on the left-hand menu.

You can tune the level of sensitivity to changes under the Anomaly detection settings in the NetBackup web UI, depending on the needs of your organization. Negative values reduce the deviation tolerance, resulting in more detected anomalies. Conversely, positive values increase the tolerance, allowing for small to medium deviations without alerts and only alerting for significantly large deviations. By default, the sensitivity is set in the exact middle, labeled "Medium" (see Figure 1).



The screenshot shows a 'Basic Settings' dialog box with a close button (X) in the top right corner. The dialog is divided into several sections:

- Anomaly detection sensitivity:** Includes a description 'Use this setting to adjust the sensitivity of anomaly detection.' and a slider. The slider has three labels: 'Low', 'Medium', and 'High'. A blue dot is positioned exactly in the middle, corresponding to 'Medium'. Text above the slider indicates that moving left 'Increases the number of anomaly events' and moving right 'Reduces the number of anomaly events'.
- Data retention settings:** Includes a description 'Use this setting to specify how long to retain database information.' and a dropdown menu set to '12 Months'.
- Data gathering settings:** Includes a description 'Use this setting to specify how frequently data gathering should be triggered.' and a dropdown menu set to '15 Minutes'.
- Anomaly proxy server settings:** Includes a description 'Use this setting to specify the location of the anomaly proxy server.' and a text input field labeled 'Proxy server' with the placeholder text 'Enter a host' and 'Enter the proxy server location'.

At the bottom right of the dialog are two buttons: 'Cancel' and 'Save'.

Figure 1. The basic anomaly detection sensitivity settings in the NetBackup web UI.

Anomaly detection can run on NetBackup's primary server or optionally on a media server by defining the parameter ANOMALY_PROXY_SERVER. The anomaly proxy server does not alter the flow of the backup data but only offloads the ML process.

It takes several data points to establish a usable baseline from which to detect anomalies.

For each of the categories tracked, the backup admin can leverage anomaly detection in several ways. The significant changes detected can help the admin contribute to the overall health of the infrastructure by detecting unforeseen impacts, system performance issues, forecasting future storage needs, and detecting possible compromised systems. These indicators reveal important changes in the environment sooner.

Any anomaly should prompt investigative questions and adoption of the Zero Trust model to address malignant issues as quickly as possible. Keep in mind that changes in the environment do not always indicate a bad actor or infection but should always elicit a response to maintain confidence by asking:

- Is this a predictable change from standard events or an unknown event suggesting unscrupulous action?
- When did this change happen?
- What is driving this anomaly?
- How could this change be explained? Is it a patch, a change in nature of the data, or a breach?

Look for symptoms of unhealthy changes. Leveraging anomaly detection from deduplication rates can highlight fundamental changes to data that require prompt attention. If the normal deduplication rate is dropping, it indicates that more unique data is entering the backup, which becomes useful information for the backup administrator. Identifying reasonable and unreasonable causes for this kind of anomaly can elicit a more thorough investigation of that data. Significantly lower deduplication rates will use more backup storage, which can have ramifications for other NetBackup operations. When the data protection footprint increases in size, number of files, or time, you need to eliminate the possibility the anomaly is caused by harmful data or harmful activities on the system manifesting as performance issues. The integration of several malware scanners in NetBackup 10.0 provides a more purposeful malware scan of a backup image that can be another defense against malicious software breaching your servers.

Answering "Why did this happen?" will help optimize other workloads. Understanding anomalies helps avoid detecting events that are simply reflecting how an organization's data lives and works.

Is the anomaly a false positive? Is this anomaly truly an expected outcome for that data set? By flagging false positives and confirming true anomalies, NetBackup's ML can refactor future scores using that feedback. Alternatively, you can opt to ignore an anomaly and use the event as an opportunity for tuning more strict or lenient detection settings.

Why is Malware Scanning Important?

These days, it's a "when-not-if" attack scenario, so it's important to take the right steps to protect every system and practice good data hygiene.

With malware scanning, NetBackup can use Microsoft Defender or Symantec Protection Engine (SPE) to scan the backup image to ensure a "last-known-good" image is available for restores. This powerful feature combines NetBackup deduplication with Universal Shares and endpoint security to bolster business continuity plans. (See Figure 2.) NetBackup's anomaly detection offers admins an exceptional opportunity to scan backup images, and with the appropriate detection settings, highlight issues to streamline the workflow and use automation.

We all know security is everyone's responsibility, and bad actors and attackers will take advantage of the smallest mistakes and oversights. NetBackup's malware detection and anomaly detection provide powerful tools for the backup administrator on the front lines of the organization's data protection.

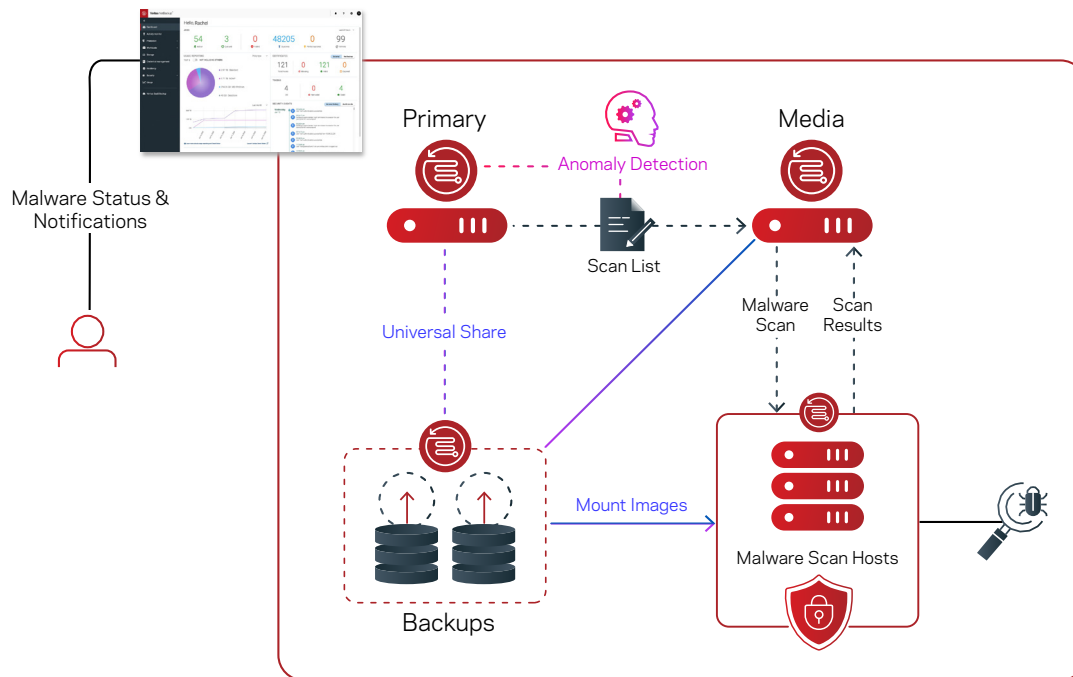


Figure 2. An overview of how to use NetBackup to create a last-known-good image for restores.

NetBackup Appliances will immediately support this feature as will NetBackup media servers using MSDP with the required components for Universal Shares.

Scan hosts are a new entity in the backup infrastructure that allows the scan to be offloaded to a location where the anti-malware engine resides and then filters the results back to the NetBackup web interface. You can deploy malware scanners on one or more hosts, depending on concurrent scanning requirements. These scan hosts are grouped together into a scan pool that is capable of inspecting unstructured data of either MS-Windows or Standard data types.

Taking further advantage of NetBackup deduplication beyond the storage savings, and using Universal Share technology, the scan host temporarily mounts the image to perform the malware scan.

Where anomaly detection scores “High,” you can automate the malware scanning process to respond to these higher-risk situations.

For organizations that do not have a malware scanning engine immediately available to their backup environment, Veritas has partnered to provide an option from the Veritas Download Center, with installation files for SUSE Linux, Red Hat Enterprise Linux, and Windows x64. The installation files provided by Veritas do not require additional licenses. This is an optional, separate step to download and set up. The NetBackup 10 release also includes integration with leading malware scanners such as Microsoft Defender and Symantec Protection Engine.

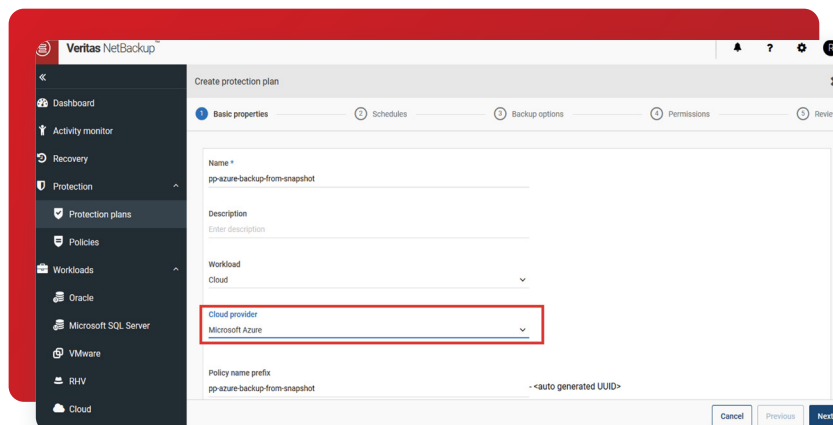


Figure 3. An overview of events detected by malware scanning in the NetBackup web UI.

In a recovery scenario, malware detection is building business continuity confidence with last-known-good backup images. You can see an image's infection status to know which backup is the last-known-good image in the NetBackup web UI (see Figure 3).

The backup administrator can also use another NetBackup feature to restore only clean files. If a file selected for restore is marked as infected, the clean restore will restore that file from an uninfected backup, allowing a safe and effective way to recover from that point in time without re-infecting the target machine. The command-line interface (CLI) option for this newly added feature is `bpcleanrestore`. This command's options will be familiar because it parallels the often-used `bprestore` command. For recovery at scale, using the CLI is popular because it lends itself to scripts and reduces clicks in the graphical user interface (GUI).

Conclusion

Data protection is an attractive target for bad actors and malware. They know it's an organization's safety net, so they work systematically to weaken the backup solution. Bad actors assume the solution is an unmonitored gap and admins won't notice changes until it is too late. With anomaly detection, you can discover where the environment is deviating from expectations and then take action to protect your valuable IT infrastructure. Ultimately, detecting anomalies in backup images offers additional insight into the broad range of data protected by NetBackup. To leverage even more data-driven analysis, consider adding NetBackup IT Analytics to your backup infrastructure. And most important, respond to anomalies with an integrated malware detection configuration that supports a strong security posture within the entire infrastructure, not just the edges.

About Veritas

Veritas Technologies is a global leader in data protection and availability. Over 80,000 customers—including 87 percent of the Fortune Global 500—rely on us to abstract IT complexity and simplify data management. The Veritas Enterprise Data Services Platform automates the protection and orchestrates the recovery of data everywhere it lives, ensures 24/7 availability of business-critical applications, and provides enterprises with the insights they need to comply with evolving data regulations. With a reputation for reliability at scale and a deployment model to fit any need, Veritas Enterprise Data Services Platform supports more than 800 different data sources, over 100 different operating systems, more than 1,400 storage targets, and more than 60 different cloud platforms. Learn more at www.veritas.com. Follow us on Twitter at [@veritastechllc](https://twitter.com/veritastechllc).

VERITAS™

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For global contact
information visit:
veritas.com/company/contact