Local and extended datastores

Published: 2024-05-15

The ExtraHop system includes a self-contained, streaming datastore for storing and retrieving performance and health metrics in real time. This local datastore bypasses the operating system and accesses the underlying block devices directly, rather than going through a conventional relational database.

The local datastore maintains entries for all devices discovered by the ExtraHop system as well as metrics for those devices. By storing this information, the ExtraHop system is able to provide both quick access to the latest network capture and historic and trend-based information about selected devices.

Extended datastore

The ExtraHop system can connect to an external storage device to expand your metric storage. By default, the ExtraHop system stores fast (30-second), medium (5-minute), and slow (1-hour) metrics locally. However, you can store 5-minute, 1-hour, and 24-hour metrics on an extended datastore.

To store metrics externally, you must first mount an external datastore ⬈, and then configure the ExtraHop system to store data in the mounted directory. You can mount an external datastore through NFS v4 (with optional Kerberos authentication) or CIFS (with optional authentication).

Note that you can configure only one active extended datastore at a time to collect all configured metric cycles. For example, if you configure your extended datastore to collect 5-minute, 1-hour, and 24-hour metrics, all three metric cycles are stored in the same extended datastore. In addition, you can archive an extended datastore and those metrics are available for read-only requests from multiple ExtraHop systems.

Here are some important things to know about configuring an external datastore:

- If an extended datastore contains multiple files with overlapping timestamps, the metrics will be incorrect.
- If an extended datastore has metrics committed by an ExtraHop system running a later firmware version, the system with the older firmware cannot read those metrics.
- If an extended datastore becomes unreachable, the ExtraHop system buffers metrics until the allocated memory is full. After the memory is full, the system overwrites older blocks until the connection is restored. When the mount reconnects, all of the metrics stored in memory are written to the mount.
- If an extended datastore file is lost or corrupted, metrics contained in that file are lost. Other files in the extended datastore remain intact.
- As a security measure, the system does not allow access to the stored plaintext password for the datastore.