Maximum Performance with Maximum Security - Protecting Redis Data Stores with Zettaset XCrypt™ Full Disk Encryption

Redis is an in-memory database platform powering real-time applications with the highest throughput, lowest latencies, and the least resources. Open-source Redis has gained popularity among users for its incomparable high performance and ease of use.

Redis Enterprise (Redis^e) enhances open-source deployments with a technology layer that makes scaling effortless and transparent to the user. Redis^e also adds unmatched resilience, with high availability that protects against every failure scenario and is benchmarked to recover within seconds without losing data. Performance optimizations within Redis^e ensure that applications that use it achieve flawless high performance under any load.

Redis^e is optimized for maximum performance and simplicity *but relies on users to maximize its security to protect sensitive information*

Redis^e was designed to be accessed by trusted clients inside trusted environments. However, Redis does not include a built-in security component. Exposing the Redis^e instance directly to the internet or to an environment where untrusted clients can directly access the Redis TCP port or UNIX socket carries a high risk. SSL using Stipes provides only basic security between the client and the data store, but Redis lacks built-in data-at-rest encryption to protect the data store.

If your Redis^e instance contains sensitive information like personally identifiable information (PII) that contains customer names, addresses, and payment information and is not properly secured, you could be in violation of data protection compliance regulations.

Zettaset has partnered with Redis Labs to provide maximum security for users running Redis Enterprise in production at scale. As Redis Enterprise usage continues to grow exponentially, major enterprises now utilize Redis Labs to power mission- and business-critical applications. Virtually every vertical of every industry utilizes Redis^e to a certain extent to power their big data initiatives.

In this age of unabated data breaches, we know that a determined cybercriminal can break through the periphery of almost any database environment. And the risk of insider threats through misconfigurations or deliberate actions continues to increase. Best security practices dictate that any access to your Redis Labs deployment, trusted or untrusted, must be mediated with ACLs and the data store itself must be encrypted.

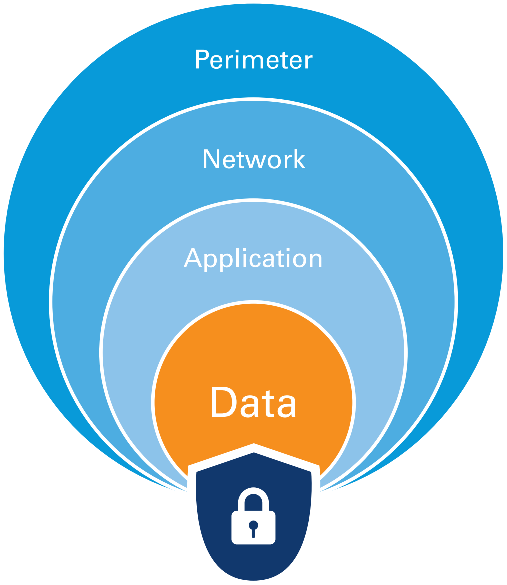

Fig. 1 - Layered Security Model. Outer layers are protected by firewalls, IDS, IPS, and IAM, but can and will be hacked. Only encryption provides proven privacy and protection for the data store.

The Best of Both Worlds: Redis and Zettaset - An industry leading database optimized for maximum performance and maximum security

Zettaset XCrypt Full Disk is a high-performance, partition-level encryption solution which, because of its high speed and extremely low latency, is ideal for encryption and decryption of in-memory stored data. Even if the periphery of the Redis Labs environment is breached, the data store itself remains securely protected.

XCrypt Full Disk can be applied to both data-at-rest, and data-in-motion, which also simplifies protection of a Redis Enterprise deployment. Unlike legacy encryption technologies, XCrypt Full Disk is has been designed from the ground up for optimal performance and scalability in high volume data stores and distributed architectures, and can be transparently applied in NoSQL environments similar to Redise, as well as in Relational/SQL, Object, and Hadoop data stores.

High-Performance Data Encryption for High Performance Data Stores

The industry-leading performance of XCrypt Full Disk makes it the ideal match for Redis^e, especially when snap-shotting, dumping data to disk, or holding your Redis data in Flash memory. XCrypt Full Disk is optimized for superior performance in in-memory and scale-out distributed computing environments, with negligible impact on application performance: approximately 3%* for data-at-rest encryption and 7%* for data-in-motion encryption. (*Measured using TeraSort MapReduce Benchmark).

Zettaset XCrypt Full Disk includes a policy engine for highly granular management and can be configured to align with the frequency of the Redis snap-shotting process and to encrypt the snapshots as they are saved to disk. Because XCrypt Full Disk works transparently across data environments, you can choose to store the snapshots in Relational, NoSQL, or Object data stores. In any case, XCrypt Full Disk provides encryption that does not inhibit Redise performance.

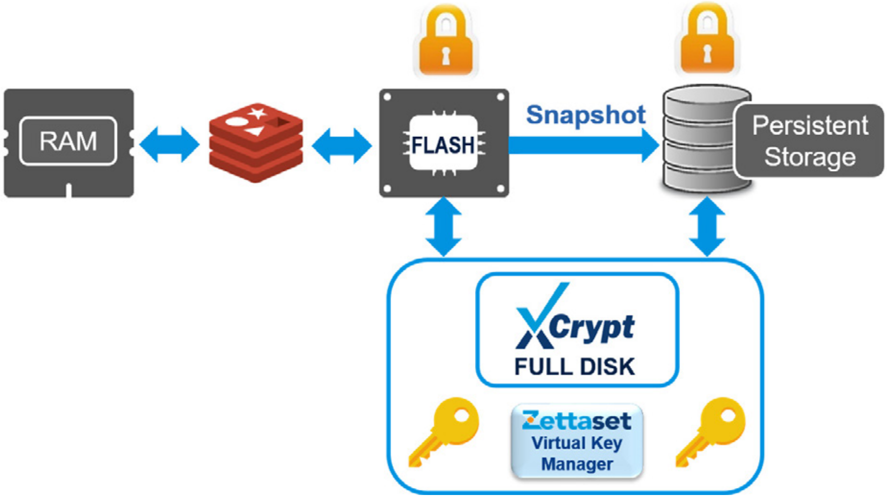

Fig. 2 - Data-at-rest protection for the Redis database. Redis performs point-in-time "snapshots" of in-memory dataset at specified intervals. Zettaset XCrypt Full Disk high-performance encryption protects the snapshots and secures flash and persistent storage.

A Complete Encryption Solution for Protecting Sensitive, High-Risk Data Environments

The XCrypt Full Disk solution delivers a complete encryption package that includes a software-based virtual enterprise key manager (V-EKM) and virtual hardware security module (V-HSM). XCrypt Full Disk adheres to OASIS encryption open standards, making it compatible with any KMIP-compliant key management system and PKCS#11-compliant hardware security module (HSM). This makes Zettaset XCrypt Full Disk fit easily into existing enterprise data security frameworks.

Zettaset XCrypt Full Disk provides a proven defense in regulated industries such as healthcare, financial services, and retail from the accelerating frequency and scope of data breaches. When integrated into a strategic IT security initiative, XCrypt Full Disk can help bring Redis Enterprise data stores into compliance with corporate and regulatory data protection initiatives including GDPR, SOX and HIPAA.

Redis Labs and Zettaset are working together to provide joint customers with the best of both worlds: An industry leading database that is **optimized for maximum performance and maximum security.**