HPE Shadowbase Data Protection

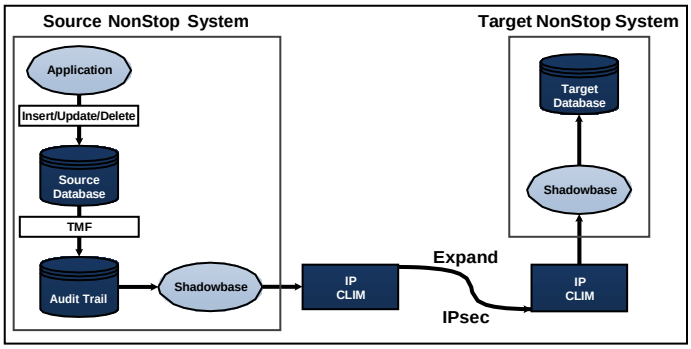
Encryption for Data Replication

Businesses today are driven by data, and the quality of the business depends upon the quality of that data. Consequently, data has become one of a company's most valuable assets, and other people want it. Stealing or corruption of this data can result in significant business losses, pose serious security threats, put life and limb at risk, and result in legal violations. As hackers become increasingly sophisticated, protection of data from unauthorized access is a number one priority for any IT department.

HPE Shadowbase replication solutions involve moving data between systems in real-time, for the purposes of business continuity, application and data integration, real-time business intelligence, and more. To provide these services, Shadowbase replication moves a copy of the source data to the target environment, often across the network, and may make copies of some or all of the data in intermediate files along the way. With its sophisticated encryption capabilities, Shadowbase software ensures that your data is never exposed during this process, whether at rest or in motion.

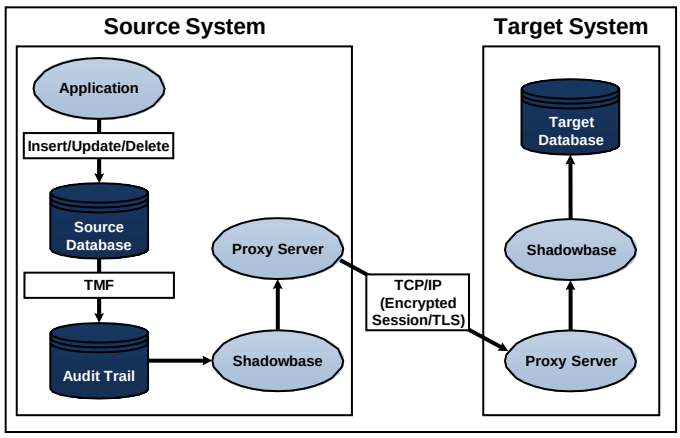
HPE Shadowbase Solutions Protect Your Data in Motion

To protect data in motion, HPE Shadowbase software uses various techniques depending upon the type of source and target systems, and the communications protocol between them. Intra-system communications are not typically encrypted by Shadowbase replication; however, inter-system communications can be encrypted, as described below.



1. When using Expand for communications between HPE NonStop servers as shown in the figure on the left, Shadowbase software will not directly encrypt the data messages. To have encrypted Expand communications, use Expand-over-IP and then the secure IPsec protocol support available with the HPE IP CLIM NonStop network I/O adapter. With IPsec, each data packet transferred by Shadowbase replication between HPE NonStop systems is authenticated and encrypted.

2. When using TCP/IP for communications between HPE NonStop servers, as well as between NonStop servers and other server platforms (e.g., Linux, Unix, Windows) as shown in the figure on the right, Shadowbase software can be configured to use proxy servers to encrypt the network traffic. In this architecture, the message traffic between Shadowbase replication and the proxy server is unencrypted; however, the connection across the network between the proxy servers is encrypted (using SSH connections and the TLS protocol).



3. Between any Shadowbase-supported system type using any supported communications protocol – Shadowbase architecture offers customizable user exit programming which can be used to encrypt, tokenize, or obfuscate specific data items at the field/column level before send, and optionally decrypt, detokenize, or unobfuscate the data items on receipt. This capability also supports using the format-preserving encryption technologies.
4. Regardless of the system type and communications protocol, if the source data being replicated is already encrypted, tokenized, or obfuscated, it will remain encrypted, tokenized, or obfuscated by Shadowbase end-to-end, including when sent across the network.

HPE Shadowbase Solutions Protect Your Data at Rest

Depending on the replication configuration, HPE Shadowbase software solutions may store data in intermediatequeue files during the replication process, and protects this data at rest in the following ways:

1. If the source data being replicated is already encrypted, tokenized, or obfuscated, it will remain encrypted, tokenized, or obfuscated by Shadowbase end-to-end, including when at rest in intermediate queue files.
2. Shadowbase user exits can be customized to encrypt, tokenize, or obfuscate replicated data before it is written to the queue file, and to optionally decrypt, detokenize, or unobfuscate it when read from the queue file.
3. HPE NonStop Volume Level Encryption (VLE) and other server encrypting file systems can be used in most cases for data at rest encryption of Shadowbase queue files.

Summary

Data is one of a company's most valuable assets, and cyber thieves want it. Whenever data is moved between systems, a window of opportunity for data theft opens, which opportunistic hackers will be quick to exploit. But whether it is data at rest or data in motion, HPE Shadowbase replication provides protection so that window of opportunity for data theft remains firmly closed. Take advantage of the capabilities of HPE Shadowbase replication solutions for business continuity, data and application integration, real-time business intelligence, and more, without having to worry that your data security could be compromised in the process.

Hewlett Packard Enterprise globally sells and supports Shadowbase solutions under the name HPE Shadowbase. For more information, please contact your local HPE Shadowbase representative or visit our website. For additional information, please view our Shadowbase solution videos: https://vimeo.com/shadowbasesoftware.

Learn more:
shadowbasesoftware.com
hpe.com

Contact us:
Gravic, Inc.
17 General Warren Blvd
Malvern, PA 19355-1245 USA
Tel: +1.610.647.6250
Fax: +1.610.647.7958
Email Sales: shadowbase@gravic.com
Email Support: sbsupport@gravic.com

Please follow: