

# Data Replication

in Privileged  
Credential Vaults



# Contents

- 1 Background: Securing Privileged Accounts** **2**
  
- 2 The Business Challenge** **3**
  
- 3 Solution Approaches** **4**
  - 3.1 Sensitive data . . . . . 4
  - 3.2 Business interruption . . . . . 4
  - 3.3 Constant change . . . . . 4
    - 3.3.1 Periodic Backups . . . . . 4
    - 3.3.2 Local Replication . . . . . 4
    - 3.3.3 Remote Replication . . . . . 5
  
- 4 Replication Architecture** **6**
  
- 5 Limitations of Native DBMS Replication** **7**
  - 5.1 Oracle Database Replication . . . . . 7
    - 5.1.1 Cost . . . . . 7
    - 5.1.2 Complexity . . . . . 7
    - 5.1.3 Security / Encrypted Transmission . . . . . 8
    - 5.1.4 Bandwidth / Latency Requirements . . . . . 8
  - 5.2 Microsoft SQL Server Replication . . . . . 8
    - 5.2.1 Cost . . . . . 8
    - 5.2.2 Complexity . . . . . 8
    - 5.2.3 Security / Encrypted Transmission . . . . . 8
    - 5.2.4 Bandwidth / Latency Requirements . . . . . 8
  
- 6 Privileged Access Manager Replication Features** **9**
  - 6.1 High Availability and Replication . . . . . 9
  - 6.2 Architecture Overview . . . . . 9

## Key Findings:

---

Privileged password storage must be:

1. Encrypted.
2. Replicated.

Replication must:

1. Span at least two sites.
2. Include all passwords.
3. Happen in real time.
4. Be inexpensive and easy to manage.

The replication protocol must:

1. Be encrypted.
2. Tolerate low bandwidth.
3. Tolerate high packet latency.
4. Recover from network interruptions.

Native replication features in Oracle and Microsoft databases do not meet all of the above conditions, so application-level replication is preferable. Privileged Access Manager includes appropriate replication technology out of the box.

## 1 Background: Securing Privileged Accounts

Consider an organization which operates 1000 servers and where there are 5 administrator-level accounts on each server. To secure these, a privileged access management system may choose a new, random password for each of the 5000 accounts daily. This process improves security by:

1. Ensuring that users only know the sensitive passwords they need to do their jobs.
2. Compromise of a single password / login ID / system does not lead to compromise of any other systems.
3. Limiting the time period during which a user has administrative access.

In other words, randomizing privileged passwords daily supports basic security principles:

1. **Authentication:**  
Users who need access to a privileged account must first authenticate themselves, before connecting to the application or server in question.
2. **Authorization:**  
The privileged access management system has an opportunity to apply access control rules and/or approval processes before connecting the session.
3. **Accountability:**  
All sessions are logged, making IT users accountable for changes made on systems to which they had privileged access.

## 2 The Business Challenge

Privileged passwords must be protected more vigorously than any other data in an organization:

1. **Sensitive data:**

Privileged passwords and the encryption keys used to protect them are arguably the most sensitive data in an organization, since they unlock all other data. Inappropriate disclosure can be catastrophic.

2. **Business interruption:**

Loss of access to privileged passwords means that the systems which the privileged passwords control cannot be managed, at least until they are powered down and “hacked into.” Consider the impact on IT support of a disaster where every `root` or `Administrator` password in a company is permanently lost.

3. **Constant change / data backup:**

If privileged passwords are changed regularly, then scheduled backups will contain mostly historical data rather than current passwords and so provide little value. It is therefore important to replicate this data in real time.

## 3 Solution Approaches

The challenges presented above must be addressed as follows:

### 3.1 Sensitive data

Privileged passwords must be encrypted. Various schemes may be used to manage encryption keys and of course various encryption algorithms may be used. Encryption and key management are outside the scope of this white paper.

### 3.2 Business interruption

Servers fail – disks crash, power supplies burn out and CPUs overheat, all of which can cause data loss. This means that, at a minimum, privileged password data must be backed up frequently.

### 3.3 Constant change

#### 3.3.1 Periodic Backups

Modern backup software is implemented using full and incremental backups. Each backup represents a snapshot of the data being protected at a point in time. For example, a full backup of a database may be made weekly, and incremental changes may be backed up daily. Data may be restored from backup by combining the most recent full backup with a series of subsequent incremental backups.

This strategy – of backups made regularly, at a frequency of approximately once per day, is inadequate where a significant subset of the data being protected changes every day. This is the case in a privileged access management system which randomizes every password daily.

Consider a situation where backups are made at 3AM and where 5000 privileged passwords are randomized daily, at random times of the day. If a single database contains all privileged passwords, and the database server crashes at 2:59AM, then every password changed in the last 24 hours – which is almost every password – will be irretrievably lost. If the database crashes at 3PM then we might expect 50% of the passwords to be lost.

#### 3.3.2 Local Replication

To reduce the risk of a single server crashing and taking every privileged password with it, it makes sense to copy every password to two servers. Whenever a new password is committed to the database, it should actually be committed to two databases, so that loss of one server would be inconvenient rather than catastrophic.

This is certainly better than relying on backups of mostly-obsolete data, but it still leaves open mechanisms for catastrophic data loss. If there is a facility failure, such as a fire, flood or earthquake, then every server at a single site may be destroyed, and every password will be lost. If the server housing the privileged access management software simply loses connectivity (a more likely event), then users at other sites will be unable to get access to servers at other sites.

Loss of access to all privileged passwords at all sites because of a problem at a single data center is a major and unnecessary business risk.

### **3.3.3 Remote Replication**

To avoid disasters where a major problem at one facility or a hardware failure on a single server trigger loss of all passwords, it makes sense to copy all privileged passwords to at least two servers, located in at least two sites.

Moreover, it makes sense to put the servers as far apart as possible – so that natural disasters or regional infrastructure failures, such as the Kobe earthquake of 1995, the Katrina hurricane that hit New Orleans in 2005 or the Northeast power blackout of 2003 do not knock out access to all privileged passwords in a large organization.

## 4 Replication Architecture

To summarize the previous sections, privileged passwords are sensitive and loss of access to them would be disastrous. Since they change constantly, they should be protected as follows:

1. Encrypted storage and transmission.
2. Copies stored on multiple servers.
3. Servers located at separate, physically distant sites.

Failure to provide all of these protections may lead to catastrophic failures, not only of the privileged access management system, but of the entire IT infrastructure support and management function.

Given the above, we must consider important technical characteristics that the replicated password storage system should have:

1. Replication should be near-real-time, since data (privileged passwords) changes constantly.
2. Replication should be encrypted, since servers are far apart and the network segments connecting them may be insecure.
3. Replication must work well over a wide area network, where:
  - (a) Connectivity may be unreliable (i.e., sometimes lost).
  - (b) Bandwidth may be limited.
  - (c) Packet transmission latency may be high.
4. Replication should be of all data, not just a subset. Replicating only some privileged passwords means that those not replicated could be lost.
5. Every server should be able to function independently, randomizing passwords and processing access disclosure independently. This allows an organization to continue to function when a server crashes or a data center goes offline.

There are also business characteristics that replication should have:

1. Replication should be inexpensive, otherwise organizations may be tempted to defer implementing it.
2. Replication should be easy to configure and manage, otherwise administrators may avoid it or make mistakes setting it up.

## 5 Limitations of Native DBMS Replication

The latest versions of the major RDBMS products (Oracle, Microsoft SQL Server, IBM DB2/UDB) already provide replication features. Naturally, the first option to consider for replicating storage of privileged passwords is to use the native replication features in these products.

Following is a clear overview of replication technologies and some design choices:

[http://research.microsoft.com/~gray/WICS\\_99\\_TP/18\\_Philbe%20Replication%20Stanford99.ppt](http://research.microsoft.com/~gray/WICS_99_TP/18_Philbe%20Replication%20Stanford99.ppt)

Another useful reference is Oracle specific:

[http://www.wikibon.org/Best\\_practice\\_in\\_Oracle\\_11G\\_remote\\_replication](http://www.wikibon.org/Best_practice_in_Oracle_11G_remote_replication)

While native replication features are very powerful, unfortunately they do not map well to the requirements of a privileged access management system:

### 5.1 Oracle Database Replication

#### 5.1.1 Cost

In order to effectively manage replication, Oracle Enterprise Edition is required, as it includes the Advanced Replication Management Module. The Enterprise edition is significantly more expensive than the Standard Edition.

Data encryption is not included in the Oracle Enterprise Edition. To add it, Oracle Advanced Security must also be purchased and deployed.

#### 5.1.2 Complexity

Oracle's replication feature is very complex. It supports filtering what is replicated by object type, table, row and column. Different replicas may be configured to receive different data sets. Replicas may be read/write or read-only. A single server may replicate different subsets of its data to different peers.

This complexity comes at a cost. Again from Oracle documentation,<sup>1</sup> multi-master replication (MMR) is described as follows: "Significant increases in administration requirements. When problems appear in the database, the DBA must insure that replication is not the cause or that the cause is not replicated to other databases. Database performance tuning and problem resolution becomes more complicated by an order of magnitude."

Another cost can be performance. The type of replication that is most appropriate to the privileged password management problem space is multi-master replication. According to Oracle documentation, "MMR involves the use of triggers and procedures, and this can result in a database performance hit. Depending on how much data you are replicating, this performance hit can be substantial."

<sup>1</sup>[http://www.oracle.com/technology/books/pdfs/book\\_rep\\_chap6\\_ce2.pdf](http://www.oracle.com/technology/books/pdfs/book_rep_chap6_ce2.pdf)

### 5.1.3 Security / Encrypted Transmission

By default, Oracle replication sends data in plaintext. Changing this to encrypt data is possible, but requires purchase, deployment and management of another product: Oracle Advanced Security.

### 5.1.4 Bandwidth / Latency Requirements

From the same Oracle, documentation: “Potentially large network bandwidth requirements. Not only does multi-master push and pull changes between sites, it also sends acknowledgements and quite a bit of administrative data.”

In other words, MMR may not be appropriate to WAN deployment, especially where the WAN does not guarantee high bandwidth and low latency.

## 5.2 Microsoft SQL Server Replication

### 5.2.1 Cost

Replication requires SQL Server Standard Edition or higher – significantly more expensive than the Express or Workgroup editions of SQL Server.

### 5.2.2 Complexity

The most appropriate model of SQL Server replication is the Merge type using Push rather than Pull mode.

From <http://technet.microsoft.com/en-us/magazine/cc162477.aspx>:

“Replication requires specialized knowledge, which is a big concern for environments that don’t have a dedicated DBA. Replication can be somewhat complex to troubleshoot and it does require a more involved design if it’s to be used as a high-availability option.”

### 5.2.3 Security / Encrypted Transmission

Microsoft SQL Server replication is plaintext. Organizations are expected to add encryption at the transport layer if it is required at all. This means that by itself, SQL Server replication is not appropriate for secure WAN deployment.

### 5.2.4 Bandwidth / Latency Requirements

Microsoft SQL Server replication consumes about three times the bandwidth as the rate at which SQL Server generates log data, which can be too much if bandwidth between sites is limited.

## 6 Privileged Access Manager Replication Features

### 6.1 High Availability and Replication

Once deployed, Hitachi ID Privileged Access Manager becomes an essential part of an organization's IT infrastructure, since it alone has access to privileged passwords for thousands of networked devices. An interruption to the availability of Privileged Access Manager or its password vault would mean that administrative access to a range of devices is interrupted – a major IT service disruption.

Since servers occasionally break down, Privileged Access Manager supports load balancing and data replication between multiple physical servers and multiple credential vaults. Any updates written to one database instance are automatically replicated, in real time, over an encrypted communication path, to all other Privileged Access Manager servers and all other credential vaults.

In short, Privileged Access Manager incorporates a highly available, replicated, multi-master architecture for both the application and the credential vault.

To provide out-of-the-box data replication, Privileged Access Manager includes a database service that replicates updates across multiple database instances. This service can be configured use either Oracle or Microsoft SQL Server databases for physical storage. Hitachi ID Systems recommends one physical database per Privileged Access Manager server, normally on the same hardware as the Privileged Access Manager application.

The Privileged Access Manager data replication system makes it both simple and advisable for organizations to build a highly-available Privileged Access Manager server cluster, spanning multiple servers, with each server placed in a different data center. Replication traffic is encrypted, authenticated, bandwidth-efficient and tolerant of latency, making it suitable for deployment over a WAN.

This multi-site, multi-master replication is configured at no additional cost, beyond that of the hardware for additional Privileged Access Manager servers, and with minimal manual configuration.

### 6.2 Architecture Overview

To secure privileged accounts on servers – i.e., IT assets attached to the network at fixed addresses, each Hitachi ID Privileged Access Manager server runs a password updating service. This service periodically runs a connector, also on the Privileged Access Manager server, that communicates with a single target server and changes a single password. Upon successfully setting the new password, the service updates the Privileged Access Manager server with the new password, thus making it available to IT staff. The new password is automatically, immediately and securely replicated to all other Privileged Access Manager servers.

This process is repeated thousands of times daily, for different types of servers (Windows, Unix, Linux, DBMS, mainframe, application, etc.), using different types of connectors. Connectors for over 110 types of servers and applications are included with Privileged Access Manager.

The Privileged Access Manager network architecture is illustrated in [Figure 1](#).

To secure privileged accounts on servers – i.e., IT assets attached to the network at fixed addresses, each

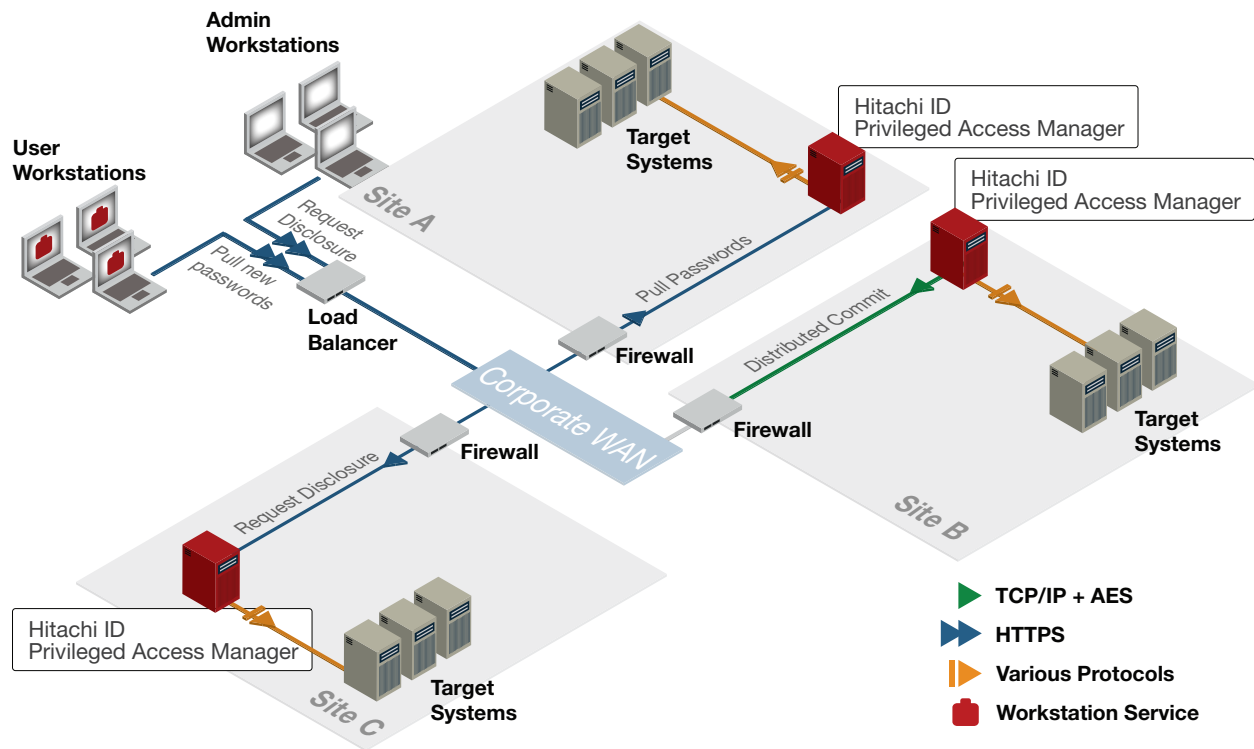


Figure 1: Privileged Access Manager Network Architecture Diagram

Privileged Access Manager server runs a password updating service. This service periodically runs a connector, also on the Privileged Access Manager server, that communicates with a single target server and changes a single password. Upon successfully setting the new password, the service updates the Privileged Access Manager server with the new password, thus making it available to IT staff. The new password is automatically, immediately and securely replicated to all other Privileged Access Manager servers.

This process is repeated thousands of times daily, for different types of servers (Windows, Unix, Linux, DBMS, mainframe, application, etc.), using different types of connectors. Connectors for over 110 types of servers and applications are included with Privileged Access Manager.