ManageEngine
PAM360

High Availability and Disaster Recovery Models in PAM360

High Availability and Disater Recovery Models in PAM360

PAM360 offers comprehensive High Availability (HA) and Disaster Recovery (DR) models for both PostgreSQL and MS SQL databases, ensuring seamless access to privileged enterprise data while protecting critical information for sustained business continuity.

This guide provides an in-depth exploration and traverse you with the various HA and DR models supported by PAM360, detailing how each framework functions. Additionally, it highlights the differences in database behavior across HA instances during access interruptions, offering clear insights into how PAM360 ensures resilience and minimizes downtime in the event of failures or disruptions.

High Availability Models

Disater Recovery

6. Instant and Scheduled Database Backups
7. Data Restoration

We highly recommend Failover Service for MS SQL databases and Read-Only Server Model for PostgreSQL databases in PAM360 for ensuring high availability, data redundancy, and optimized performance across distributed environments, thereby minimizing downtime and enhancing system reliability.

1. Failover Service Model

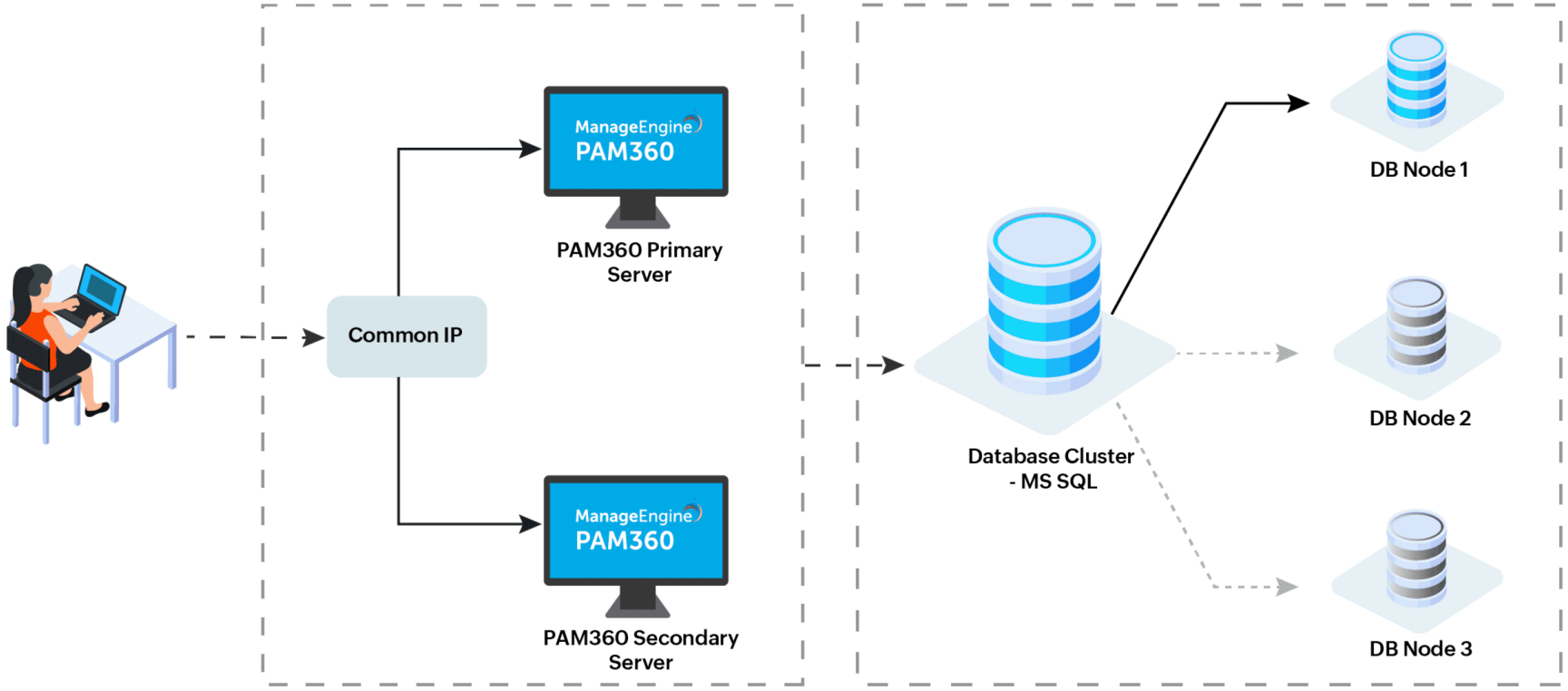
Note: PAM360 supports the Failover Service model only in MS SQL databases.

PAM360's Failover Service supplements HA by ensuring continuous access to privileged resources through redundant PAM360 server instances connected to a shared database cluster with multiple database instances. This redundancy minimizes service disruptions, thereby enhancing system reliability and privileged access.

Both primary and standby PAM360 instances are deployed on separate servers connected to a shared database cluster with multiple database instances using SQL server clustering. The primary instance grants full access, while the standby (secondary) instance monitors the primary. In the event of primary server failure, the standby instance assumes control. Upon the primary server's restoration, it transitions to standby status, with the former standby instance becoming the primary. Both servers utilize a shared public IP address, facilitating uninterrupted access through the PAM360 web interface.

Server and Database Behavior - MS SQL		
Operations	**Primary Server**	**Secondary Server**
Operates with a dedicated database	No (Database Cluster)	No (Database Cluster)
Server is continuously up and operational	Yes	Yes

Server's database remains synchronized with the primary server's database 24/7	-	Yes
Secondary server takes over response handling in the event of primary server downtime	-	Yes
Server's web interface is accessible and fully functional	Yes	No
Creation or modification of entities (such as users, resources, accounts, and client organizations) is supported	Yes	No
Password retrieval is supported	Yes	No
Access control workflow is fully functional	Yes	No
Session initiation supported	Yes	No
Password reset functionality is available	Yes	No
Scheduled task execution supported	Yes	No
Report generation capabilities are available	Yes	No
Personal tab is accessible	Yes	No
Password provisioning is supported for the ticketing systems	Yes	No
RESTful API responses	Yes	No


ManageEngine
PAM360
PAM360 Primary
Server
Common IP
ManageEngine
PAM360
PAM360 Secondary
Server
Database Cluster
- MS SQL
DB Node 1
DB Node 2
DB Node 3

2. Read-Only Server Model

Note: PAM360 supports the Read-Only Server model only in the PostgreSQL databases.

The Read-Only Server functionality enhances PAM360's high availability strategy by adding a critical layer of resilience. Configurable across multiple locations, Read-Only servers are dedicated to executing read operations, thereby preserving data integrity by preventing modifications. These servers operate in synchronization with the primary server, effectively functioning as mirror servers.

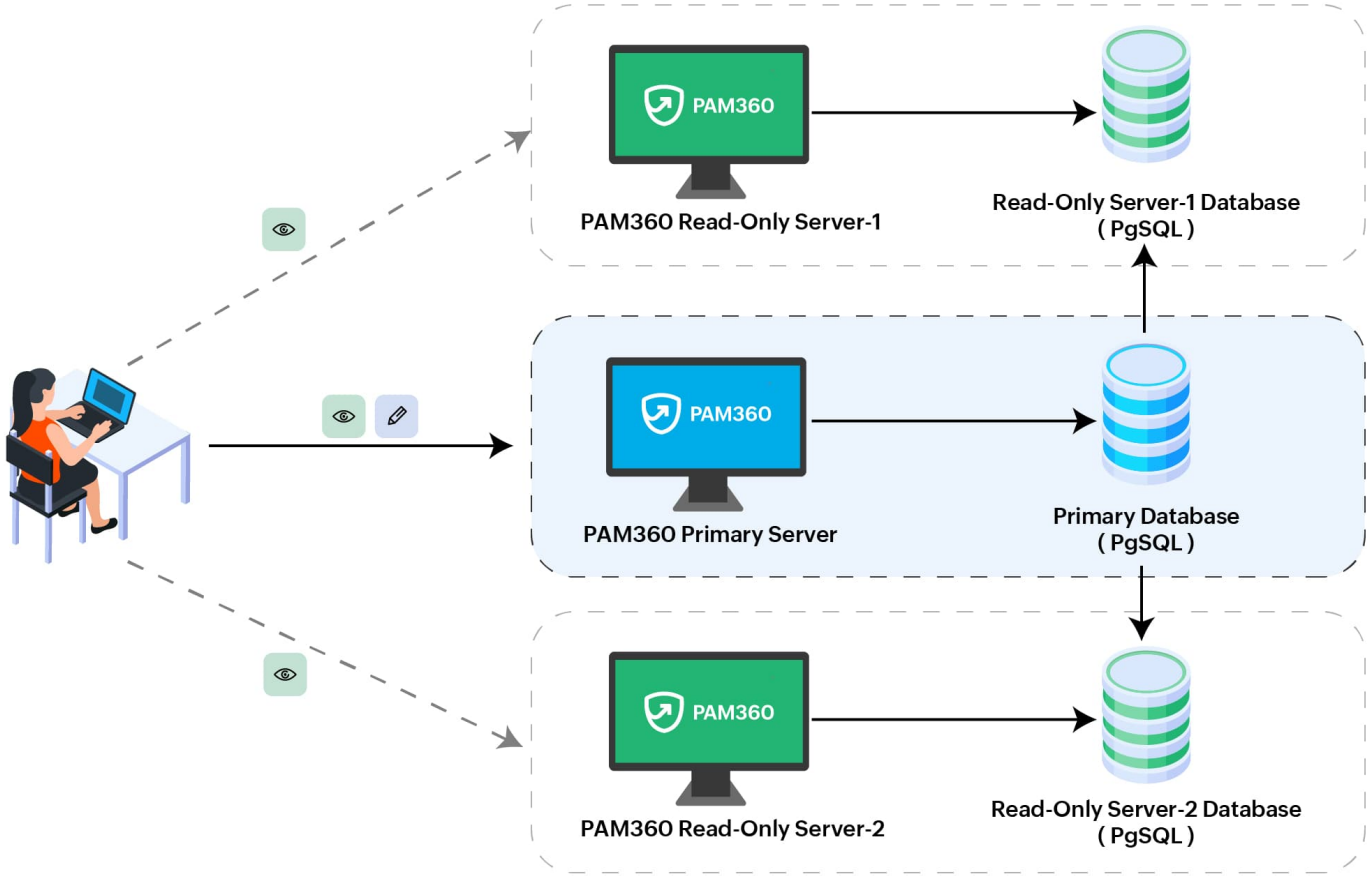
In the event of a primary server failure or catastrophic incident, any Read-Only server can seamlessly transition to assume the role of the primary server, ensuring uninterrupted operational continuity. Unlike other high availability configurations, which allow for only one secondary server, organizations can configure multiple Read-Only servers in various locations, offering greater flexibility.

When the primary server fails, administrators can easily convert any Read-Only server into the primary server, reconfiguring the remaining servers to point to the new primary instance. This capability ensures that PAM360 remains resilient and operational, even in the face of unexpected disruptions.

However, PAM360 enables users to retrieve passwords exclusively through Read-Only servers. All operations conducted on these servers are logged and audited by the primary server, with records replicated to other Read-Only servers.

Server and Database Behavior - PostgreSQL		
Operates with a dedicated database	Yes	Yes
Server is continuously up and operational	Yes	Yes
Server's database remains synchronized with the primary server's database 24/7	-	Yes
Read-Only server takes over response handling in the event of primary server downtime	-	Yes
Server's web interface is accessible	Yes	Yes
Creation or modification of entities (such as users, resources, accounts, and client organizations) is supported	Yes	No
Password retrieval is supported	Yes	Yes
Access control workflow is fully functional	Yes	No
Session initiation supported	Yes	No
Password reset functionality is available	Yes	No
Scheduled task execution supported	Yes	No
Report generation capabilities are available	Yes	No

Personal tab is accessible	Yes	Yes
Password provisioning is supported for the ticketing systems	Yes	Yes
RESTful API responses	Yes	No



3. Application Scaling Model

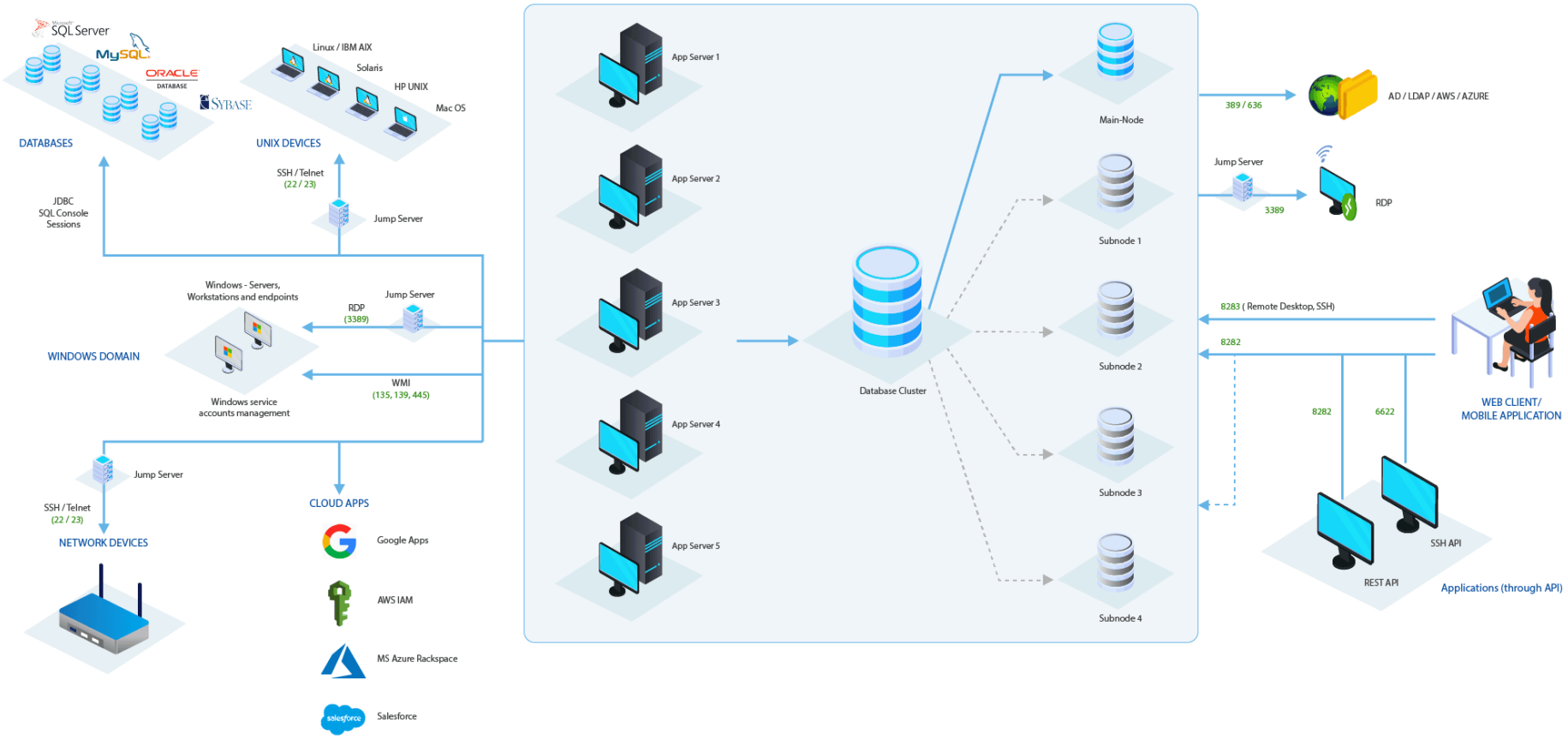
To meet scalability demands, PAM360's Application Scaling model boosts performance while upholding service levels. A primary PAM360 node and multiple sub-nodes (up to 4) linked to a singular database cluster through SQL server clustering enable organizations to manage complexity adeptly, ensuring uninterrupted access to privileged resources. Any sub-node can swiftly transition into a primary PAM360 server node in the event of the existing primary node's failure.

Initially, a PAM360 instance is installed on a server connected to a database cluster, serving as the primary node. Additional instances on other servers, interconnected with the same cluster, operate as secondary nodes. Requests are routed to the database cluster through numerous servers to efficiently handle escalating complexity. In case of the primary node's failure, any sub-node can be upgraded to the role of the primary node. Upon recovery of the primary node, it resumes its function, while the former primary node assumes the role of a sub-node.

Server and Database Behavior - MS SQL | PostgreSQL		
Operations	**Primary Server**	**Secondary Server**
Operates with a dedicated database	No (Database Cluster)	No (Database Cluster)
Server is continuously up and operational	Yes	Yes
Server's database remains synchronized with the primary server's database 24/7	-	Yes
Secondary server takes over response handling in the event of primary server	-	Yes

downtime		
Server's web interface is accessible and fully functional	Yes	Yes
Creation or modification of entities (such as users, resources, accounts, and client organizations) is supported	Yes	Yes
Password retrieval is supported	Yes	Yes
Access control workflow is fully functional	Yes	Yes
Session initiation supported	Yes	Yes
Password reset functionality is available	Yes	Yes
Scheduled task execution supported	Yes	Yes (Only during Primary downtime)
Report generation capabilities are available	Yes	Yes
Personal tab is accessible	Yes	Yes
Password provisioning is supported for the ticketing systems	Yes	Yes
RESTful API responses	Yes	Yes

PAM360 Application Scaling Architecture Diagram



4. Secondary Server Architecture Model

PAM360's secondary server architecture provides a foundational approach to tackle downtime and ensure continual access to privileged accounts. By deploying a PAM360 instance on a secondary server, organizations establish a solution that facilitates smooth transitions in the event of service interruptions on the primary server.

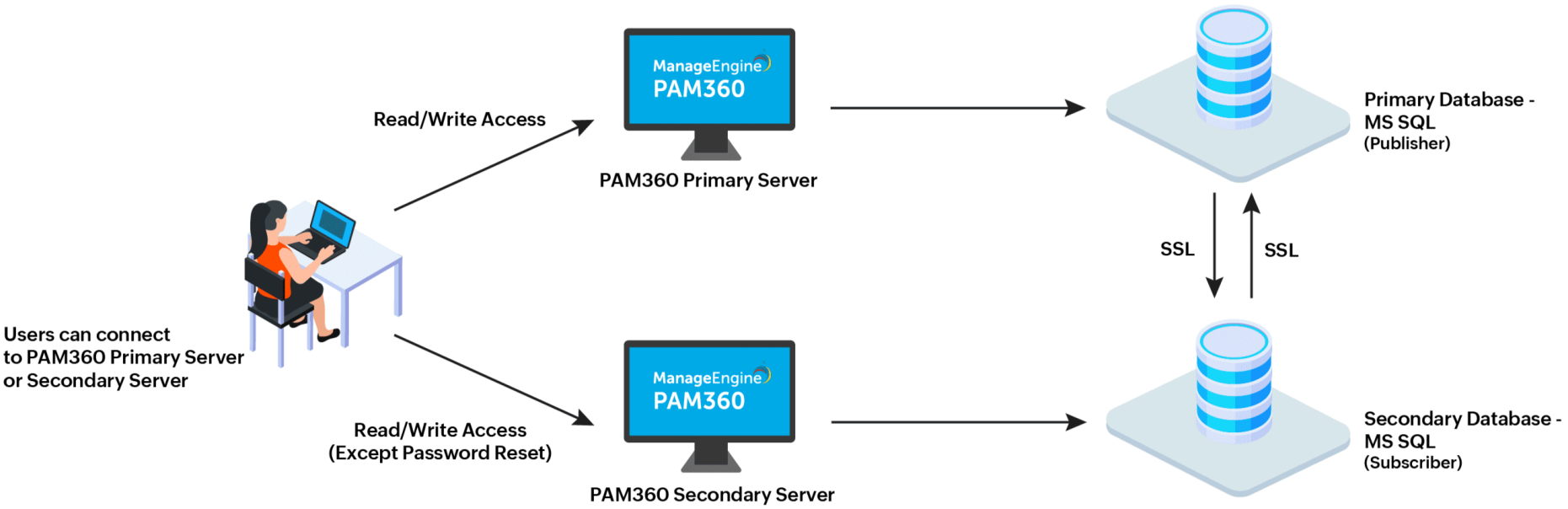
Initially, a PAM360 instance is installed on a server and connected to a primary database, serving as the primary PAM360 server. Subsequently, another instance is established on a separate server, linked to a new secondary database, serving as the secondary server. In the event of the primary server's inactivity, operations are seamlessly transferred to the secondary server. Once the primary server resumes operation, database synchronization occurs using the merge replication methodology, restoring it as the primary server.

Server and Database Behavior - MS SQL		
Operations	**Primary Server**	**Secondary Server**
Operates with a dedicated database	Yes	Yes
Server is continuously up and operational	Yes	Yes
Server's database remains synchronized with the primary server's database 24/7	-	Yes
Secondary server takes over response handling in the event of primary server downtime	-	Yes

Server's web interface is accessible and fully functional	Yes	Yes
Creation or modification of entities (such as users, resources, accounts, and client organizations) is supported	Yes	Yes
Password retrieval is supported	Yes	Yes
Access control workflow is fully functional	Yes	No
Session initiation supported	Yes	Yes
Password reset functionality is available	Yes	No
Scheduled task execution supported	Yes	No
Report generation capabilities are available	Yes	Yes
Personal tab is accessible	Yes	Yes
Password provisioning is supported for the ticketing systems	Yes	Yes
RESTful API responses	Yes	No

Server and Database Behavior - PostgreSQL		
Operations	**Primary Server**	**Secondary Server**
Operates with a dedicated database	Yes	Yes

Server is continuously up and operational	Yes	Yes
Server's database remains synchronized with the primary server's database 24/7	-	Yes
Secondary server takes over response handling in the event of primary server downtime	-	Yes
Server's web interface is accessible and fully functional	Yes	Yes (Only during Primary downtime)
Creation or modification of entities (such as users, resources, accounts, and client organizations) is supported	Yes	Yes
Password retrieval is supported	Yes	Yes
Access control workflow is fully functional	Yes	No
Session initiation supported	Yes	Yes
Password reset functionality is available	Yes	No
Scheduled task execution supported	Yes	No
Report generation capabilities are available	Yes	Yes
Personal tab is accessible	Yes	Yes
Password provisioning is supported for the ticketing systems	Yes	Yes


Read/Write Access
ManageEngine
PAM360
PAM360 Primary Server
Primary Database -
MS SQL
(Publisher)
SSL
SSL
Users can connect
to PAM360 Primary Server
or Secondary Server
Read/Write Access
(Except Password Reset)
ManageEngine
PAM360
PAM360 Secondary Server
Secondary Database -
MS SQL
(Subscriber)

5. Multi-Server Architecture with Concurrent Connections and Database Synchronization

Note: PAM360 currently supports the Multi-Server architecture model in MS SQL database on beta basis.

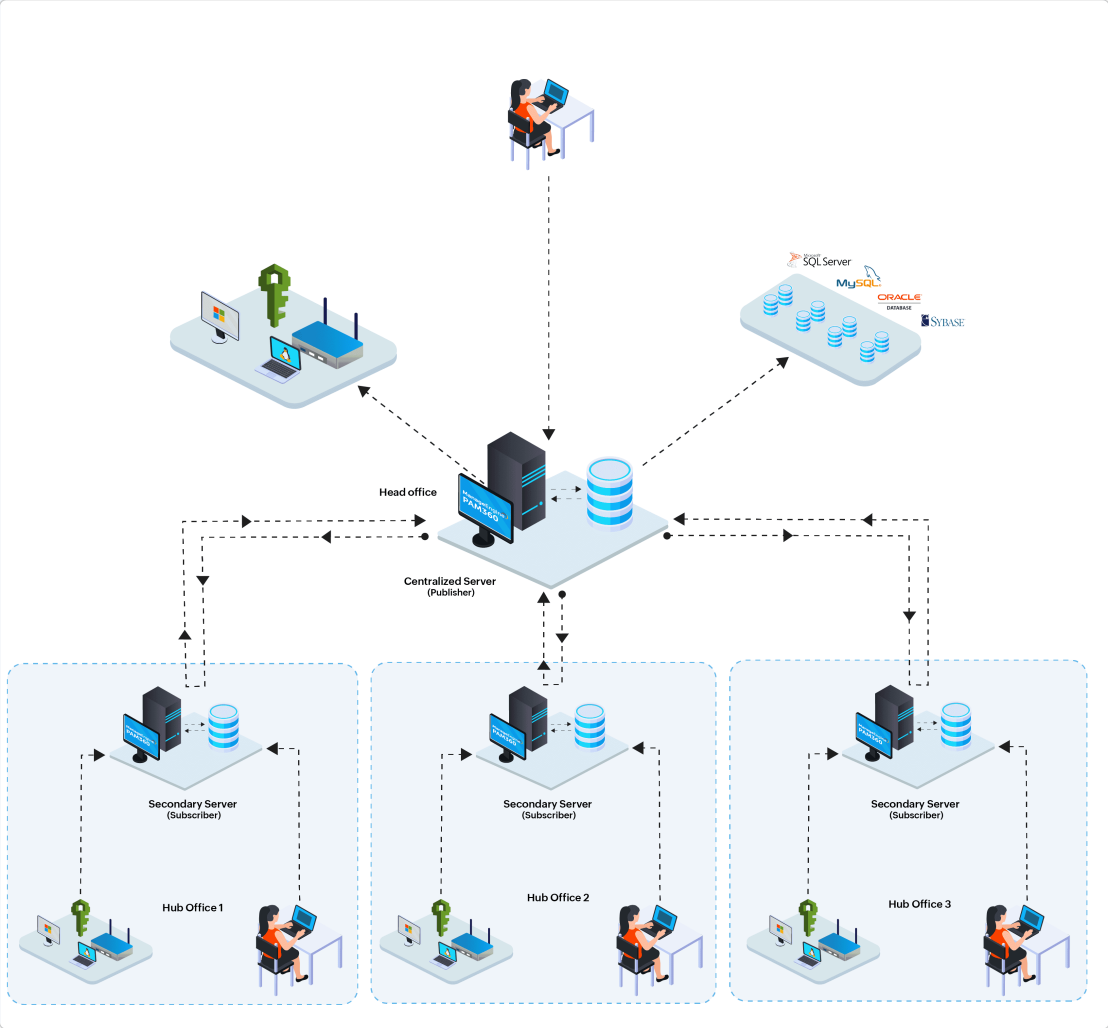
This model mirrors the secondary server architecture but with parallel request handling across multiple secondary databases. In this configuration, all secondary server databases synchronize with a central server database to address data inconsistencies during downtime among secondary server databases located in different geographic regions.

To implement this model, PAM360 instances are initially installed on a server with a dedicated database known as the centralized server. Subsequently, instances are deployed on several servers, each equipped with its dedicated database across various locations. These databases are then linked to the centralized database for data synchronization among secondary servers using the merge replication methodology. Requests from each server are directed to their respective databases, and subsequently, data synchronization occurs across all configured databases via the centralized database. In the event of server inactivity, unaffected servers seamlessly continue operations. Upon resuming, the inactive server's database syncs with all others through the centralized database.

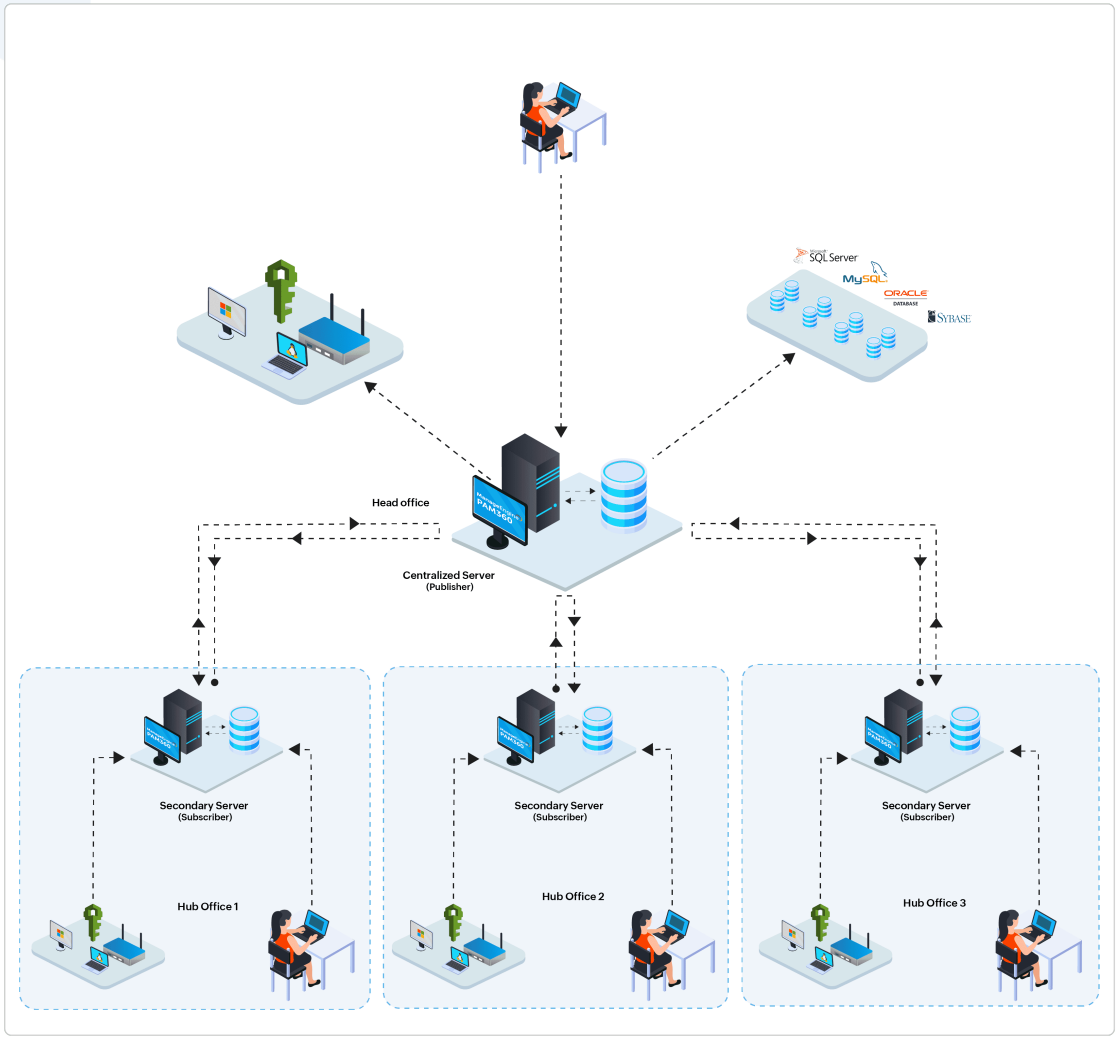
Server and Database Behavior - MS SQL		
Operations	**Primary Server**	**Secondary Server**
Operates with a dedicated database	Yes	Yes

Server is continuously up and operational	Yes	Yes
Server's database remains synchronized with the primary server's database 24/7	-	Yes
Secondary server takes over response handling in the event of primary server downtime	-	Yes
Server's web interface is accessible and fully functional	Yes	Yes
Creation or modification of entities (such as users, resources, accounts, and client organizations) is supported	Yes	Yes
Password retrieval is supported	Yes	Yes
Access control workflow is fully functional	Yes	Yes
Session initiation supported	Yes	Yes
Password reset functionality is available	Yes	Yes
Scheduled task execution supported	Yes	Yes
Report generation capabilities are available	Yes	Yes
Personal tab is accessible	Yes	Yes
Password provisioning is supported for the ticketing systems	Yes	Yes
RESTful API responses	Yes	Yes

Data Synchronization Between the Centralized Server and Secondary Servers' Databases



Data Synchronization Between the Secondary Servers and Centralized Server Databases



6. Instant and Scheduled Database Backups

Data stored in PAM360 is critical for maintaining operational continuity and securing privileged access management. In any production environment, regular and reliable backups are essential to protect against data loss, corruption, or unforeseen disasters. Backups serve as a vital safeguard against hardware failures, cyber-attacks, or accidental data deletion, while also ensuring smooth data recovery and compliance with organizational and regulatory standards.

To meet these demands, PAM360 provides a robust Database Backup feature, allowing users to efficiently manage backups for both reference and disaster recovery purposes. Recognizing the criticality of stored data, PAM360 incorporates live data backup and automated periodic backups through scheduled tasks. These disaster recovery measures provide flexibility for organizations to choose the backup method that aligns with their needs. Emphasizing secure remote locations for backup storage, PAM360 mitigates potential data loss risks in the face of production setup glitches.

7. Data Restoration

In the face of a disaster or unexpected data loss, restoring critical database backup to the PAM360 database becomes essential for ensuring uninterrupted business operations. Recognizing the importance of rapid recovery, PAM360 offers comprehensive data restoration methods designed to minimize downtime and restore access to privileged resources swiftly. With dedicated scripts and step-by-step guidelines, the restoration process is both secure and efficient, ensuring organizations can quickly regain control.

PAM360's robust data restoration process guarantees that all encrypted data - vital to your security infrastructure - is retrieved and seamlessly reloaded into the database. This ensures the integrity and confidentiality of sensitive information, while helping organizations meet compliance requirements and resume normal operations without significant delays.

By leveraging PAM360's disaster recovery capabilities, organizations can mitigate the impact of data loss and safeguard against prolonged disruptions, providing peace of mind and operational continuity in the most critical and disaster scenarios.

280,000 organizations across 190 countries trust ManageEngine to manage their IT

ManageEngine

Nine of every ten Fortune 100 companies trust us to manage their IT.

4141 Hacienda Drive Pleasanton,
CA 94588, USA

US : +1 888 204 3539
UK : +44 (20) 35647890
Australia : +61 2 80662898

ManageEngine
PAM360

pam360-support@manageengine.com

Toll Free : +1 888 720 9500