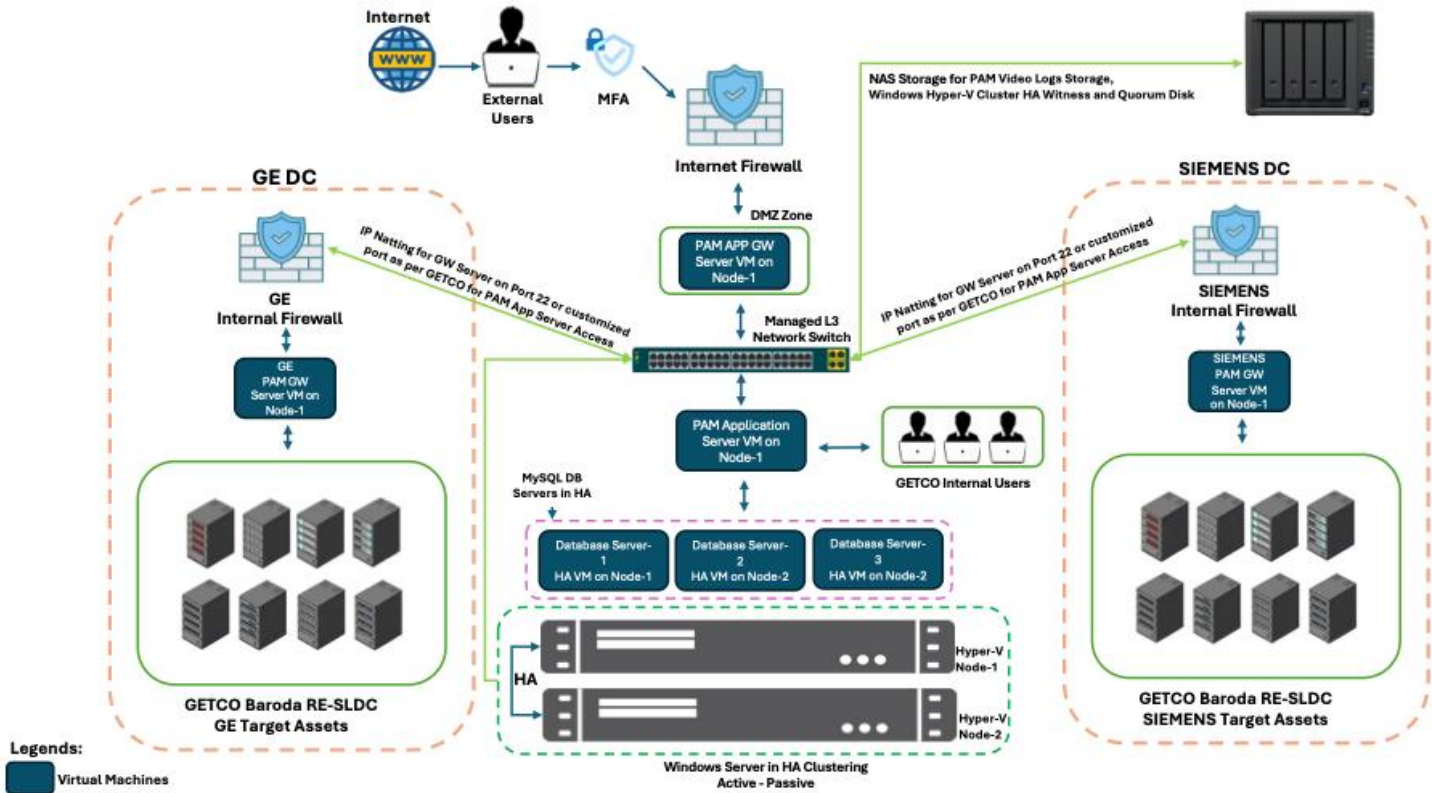


PROPOSED SOLUTION ARCHITECTURE DIAGRAM

PAM Solution Architecture Overview for GETCO



SCOPE OF WORK

4.1 Project Scope Summary

The scope of this engagement shall comprise the design, supply, installation, configuration, testing, and commissioning of the Privileged Access Management (PAM) solution for GETCO in accordance with the technical specifications set out in Technical Annexure hereof.

Scope Parameter	Value
Number of Privileged / Admin Users	40 (Forty)
Target Assets (Managed Devices)	50 (Fifty)
Deployment Type	On-Premises

4.2 Deliverables

System Integrator shall be obligated to deliver the following, subject to the Client fulfilling its obligations set forth hereof:

- PAM software licences and installation media (as applicable) & Solution must be scalable beyond 50 users .
- Installation of PAM components at GETCO for operational users having High-Impact access, Control-room users, Support Engineers, Remote Users and Third-Party/OEM users. Since securing and monitoring third-party/OEM remote maintenance is one of the major objectives of PAM, the bidder's scope should explicitly include the complete OEM remote-access workflow, including MFA, approval, JIT access, session recording, audit trail and automatic access expiry,
- OT: SCADA/EMS-related systems, OT servers, and Critical OT assets. critical applications such as SCADA/EMS, REMC, URTDSM, EASS, WAMS Phase-II and SLDC IT systems
- IT: Servers, Firewalls, Virtual machines, Backup/Storage systems and other critical IT assets.
- Bidder must configure solution for **video/text session recording, playback, audit logs, retention period, storage sizing and monitoring.**
- Configuration of High Availability (HA A-P)
- **Bidder shall showcase HA (HA A-P) configuration failover/failback testing**
- Active Directory / LDAP, SIEM integration and session policy configuration if required
- User Acceptance Testing (UAT) coordination and sign-off

The PAM solution shall initially be implemented in a controlled pilot environment covering selected IT and OT assets to validate functionality, compatibility, performance, and operational impact. Full-scale onboarding of critical OT assets shall be undertaken only after successful pilot validation, resolution of identified issues, and approval by the competent authority.

The implementation shall ensure that deployment of PAM controls does not adversely affect OT availability, reliability, safety, or continuity of critical power-system operations

- Administrator training — two (2) formal sessions with training materials
- Complete as-built documentation and knowledge transfer
- Support for a period of thirty (30) calendar days post-Go-Live

SOLUTION OVERVIEW — PAM

The solution to be implemented is the Privileged Access Management (PAM). PAM is an enterprise-grade, multi-tier solution designed to centrally govern, monitor, and audit all privileged access activities across an organization's IT/OT landscape.

The architectural design of PAM segregates logical software functions into distinct server layers, providing isolation between application logic, data persistence, and session gateway functions. This segregation enables independent scaling and ensures that no single component failure can compromise the integrity of the platform.

PAM Architectural Layers

Component	Technical Function
Application Server	The initial communication point for all privileged users. Hosts the PAM web portal, REST APIs, session management engine, and microservices.
Database Server	Maintains consistent, secure, and redundant storage of session logs, access policies, configuration data, and audit records. Deployed as a MySQL cluster with Cluster Set Replica for DR.
Secure Gateway Server	Creates encrypted, protocol-aware tunnels from end-user machines to target devices.
Application Gateway	Layer-7 HTML5 gateway in the DMZ enabling browser-based, clientless target device access.

PAM DEPLOYMENT ARCHITECTURE

The proposed PAM deployment for GETCO adopts a HA A-P architecture consisting of a Primary Data Centre in Active – Passive configuration.

- (Primary): EPAM Application Servers + Three (3)-node MySQL Cluster + Secure Gateway Servers + Video Log storage
 - Each site shall host the Secure Gateway Servers
 - Application Gateway Servers shall be deployed in the DMZ to serve clientless browser sessions for external and internal users
 - Centralised Active Directory and DNS services, shared between DC shall govern all user authentication
-

HARDWARE SIZING SPECIFICATIONS

The following hardware specifications are mandated by for the deployment of the PAM solution to support the defined scope of 40 Admin Users and 50 Target Assets.

7.1 PAM Application Server

Specification	Minimum Required Configuration Per Server	Qty
Processor Speed	2.5 GHz or Higher	2 Servers (HA A-P)
Processor	Intel Xeon Processor (6 Cores)	—
Memory / RAM	12 GB or higher	—
OS Disk	100 GB dedicated data drive	—
Application Disk	200 GB dedicated data drive	—
Video Log Storage	6 TB minimum (12-months retention)	—
Operating System: Windows Server 2022 Standard		
Framework: Microsoft .NET Core 8.x		
HA Method: Windows Failover Cluster (Active/Passive)		

7.2 PAM Database Server

Specification	Minimum Required Configuration Per Server	Qty — PR + HA
Processor Speed	2.5 GHz or Higher	3 Nodes
Processor	Intel Xeon Processor (4 Cores)	—
Memory / RAM	16 GB or higher	—
OS Disk	100 GB dedicated data drive	—
Database Disk	600 GB dedicated database drive	—
Operating System: RHEL 9.6 / Ubuntu 24.04		
Database Engine: MySQL Enterprise / Community Edition 8.4		
Clustering: MySQL Clustering with Cluster Set Replica for Disaster Recovery		

Database Configuration Requirements:

Database Name	Minimum Size	Growth Configuration
OSDB	1 GB	Unlimited — auto-growth enabled
PRDDB	50 GB	Unlimited — auto-growth enabled

7.3 PAM Secure Gateway Server

Specification	Minimum Required Configuration Per Server	Qty
Processor Speed	2.5 GHz or Higher	2 per Location (HA A-P)
Processor	Intel Xeon Processor (2 Cores)	—
Memory / RAM	6 GB or higher	—
OS Disk	100 GB data drive for OS	—
Storage Class	iSCSI or SATA	—
Operating System: RHEL 9.6 / Ubuntu 24.04		
HA Method: Windows Failover Cluster (Active/Passive)		

7.4 PAM Application Gateway Server

Specification	Minimum Required Configuration Per Server	Qty
Processor Speed	2.5 GHz or Higher	2 Servers (HA A-P)
Processor	Intel Xeon Processor (8 Cores)	—
Memory / RAM	32 GB or higher	—
OS Disk	200 GB data drive for OS	—
Video Log + File Share	500 GB	—
Operating System: RHEL 9.6 / Ubuntu 24.04		
HA Method: Windows Failover Cluster (Active/Passive)		

Note: Each Application Gateway Server handles up to Twenty (20) concurrent user sessions. Resource-intensive thick-client applications (e.g., Toad, SSMS, vSphere Client) will reduce effective session concurrency.