Professional Archibus Cloud Hosting

OVERVIEW

Robotech offers secure, reliable, and professionally managed Archibus cloud hosting services, tailored to meet the needs of organizations seeking high performance and peace of mind. Leveraging the power of Amazon Web Services (AWS) EC2, Robotech delivers a scalable and resilient platform that ensures your Archibus environment is always accessible, protected, and optimized for success.

KEY BENEFITS

- Cost-Effective: Reduces upfront costs and allows businesses to scale their software usage as needed.
- Reduced IT Burden: Robotech manages software upgrades, security updates, and infrastructure maintenance, freeing up your IT teams to focus on other tasks.
- Data Security: Ensures the safety and security of your data by handling all system updates and promptly addressing any discovered vulnerabilities.
- Automatic Updates: Manages software updates and maintenance, ensuring users always have access to the latest features and security patches.
- Faster Time to Market: Hosting solutions are typically ready to use quickly, reducing the time it takes for businesses to implement new software solutions.
- Scalability and Flexibility: Easily adjusts to changing business needs with flexible subscription options.

SECURITY MEASURES

Robotech is committed to maintaining the highest standards of security and reliability. By utilizing AWS, the platform benefits from AWS's robust infrastructure, which is certified under ISO 27001—a globally recognized standard for information security management systems. This certification demonstrates AWS's adherence to stringent security controls, giving you confidence that your data is stored within a secure, compliant environment.

DEDICATED RESOURCES AND DATA SEPARATION

Robotech ensures strict data separation between clients by provisioning dedicated environments for each organization. No shared databases or application resources are used. Each client's instance of Archibus runs in an isolated virtual environment, which eliminates cross-client data exposure and strengthens tenant security. This approach ensures:

- **No shared storage or compute instances** across clients
- **Independent data access control policies** per client
- **Isolated backup and disaster recovery plans**
- **Greater customization flexibility** without compromising another client's environment

This architecture supports both **multi-tenant security expectations** and **enterprise-grade isolation**, giving clients peace of mind and regulatory compliance assurance.

ADDITIONAL SECURITY PRACTICES

- Principle of Least Privilege: User and application permissions are limited to only what is necessary for their tasks. IAM roles and policies are regularly reviewed and updated to reduce exposure.
- Encrypted Volumes: All EBS volumes attached to EC2 instances are encrypted using AWS Key Management Service (KMS) to safeguard data at rest. Snapshots of encrypted EBS volumes are also encrypted, maintaining security throughout the backup process.
- Multi-Factor Authentication (MFA): MFA is required for all users, particularly administrators, to enhance security.

- Single Sign-On (SSO): SSO is implemented for streamlined user access and improved security. Identity Providers (IdP) supporting SAML are used, integrating with third-party solutions like Okta, Ping, or Azure AD for centralized user management.

DATA BACKUP AND RECOVERY

Robotech ensures robust data backup and recovery protocols:

- Automated Snapshots: Regular snapshots of EC2 instances and attached EBS volumes are maintained, storing them in S3 for disaster recovery. AWS Backup is utilized for simplified scheduling.
- Retention Policies:
    - Snapshots: Daily for the previous 14 days, weekly for the previous 4 weeks, and monthly for the previous 6 months.
    - Full Server Backups: Daily for 7 days, weekly for 4 weeks, and monthly for 12 months.
    - Database Backups: In addition to standard server backups, dedicated nightly database backups are retained separately for 90 days to ensure extended data recovery capabilities.

- End-to-End Encryption: All internal communication between components (e.g., load balancers, EC2 instances, and databases) is encrypted. HTTPS with SSL/TLS certificates is enabled to secure communication between clients and servers.

Operations and Customization

- System Updates: All instances of OS and Archibus applications are continuously kept updated with the latest security patches. Automated Patch Management is used.
- Customization: Unlike Archibus SaaS, Robotech offers customization options, allowing businesses to tailor the software to their specific needs. Views, procedures, and the look and feel of the application can be customized to suit your requirements.