



Alice

Software as a Service(SaaS) Delivery Platform

Ekartha, Inc.

63 Cutter Mill Road
Great Neck, N.Y. 11021
Tel.: (516) 773-3533

Ekartha India Pvt. Ltd.

814/B Law College Road
Demech House, 4th Floor
Erandwane, Pune, India
Tel.: +91-20-6601-4103

Email: info@ekartha.com

Web: www.ekartha.com

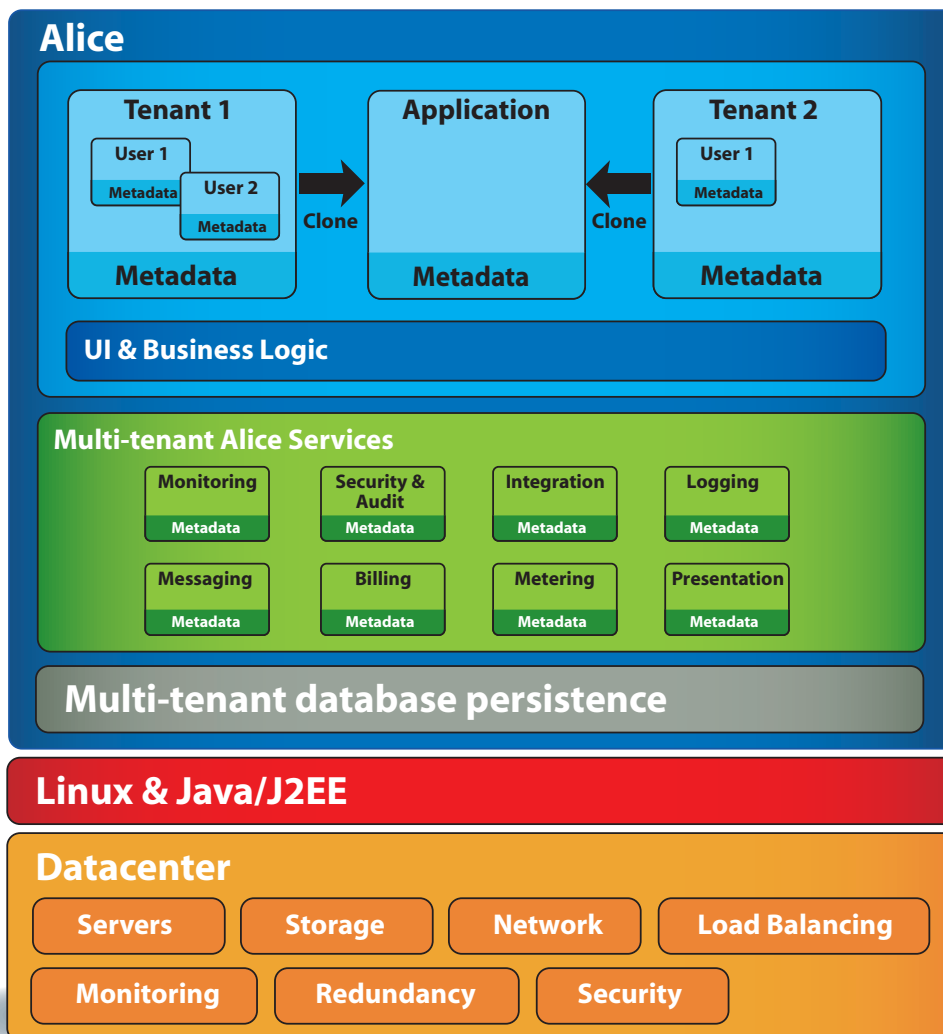
Introduction

Alice is a comprehensive Service Development and Delivery Platform for rapidly building and delivering On Demand/SAAS applications and business services. Alice can help you build your SAAS applications quickly and inexpensively, ensuring that your customers can access your applications in the shortest possible time.

The foundation of a mature SAAS application is based on building a multi-tenanted and scalable architecture. Successful SAAS applications are built as single instance applications that are shared by multiple clients on a common hardware and software infrastructure to achieve economies of scale. Companies can realize large savings in just licensing and infrastructure costs through a well developed multi-tenanted and scalable architecture.

Alice's out of the box architecture allows developers to fully leverage the benefits of multi-tenancy along with a set of essential On Demand Application Services (described below). Alice provides applications with a robust multi-tenant load balanced scale-out architecture that uses standard technologies and infrastructure. This removes tremendous complexity and risks from the SAAS application development process, and has the potential to save companies years of development time, and millions of dollars in development and operational costs.

Alice Architectural Diagram



ALICE SERVICES

Alice Database Persistence Service

Alice multi-tenanted database persistence supports comprehensive database functionality for modern Internet applications. Built over the Oracle relational database, Alice multi-tenant database persistence supports multiple persistence models. These models are:

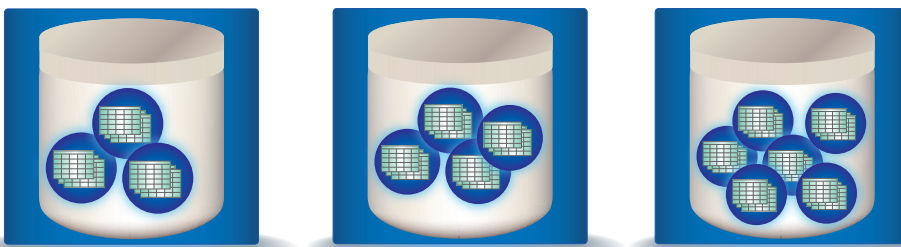
- Separate Database per tenant
- Shared Database, but Separate Schema per tenant
- Shared Database, Shared Schema and Shared Tables for all tenants

Multi-Tenant Database Persistence Models

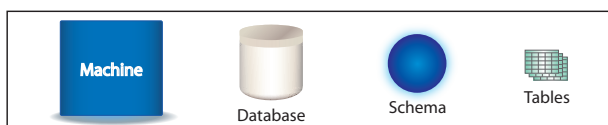
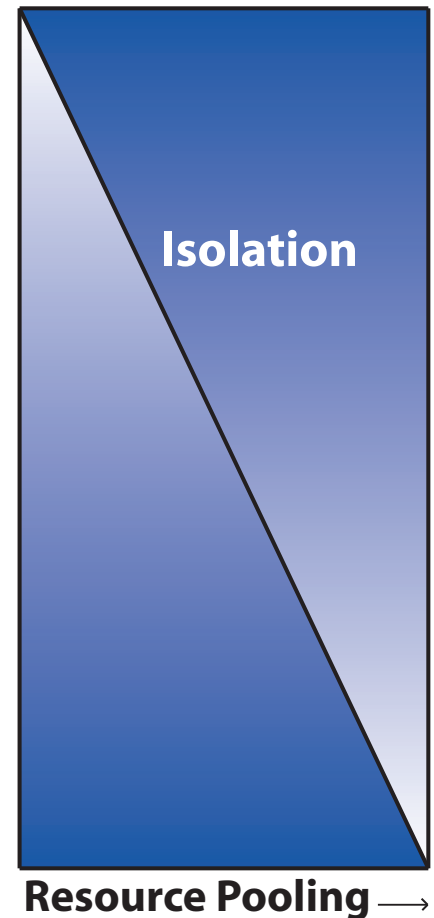
Separate database per tenant



Shared database, but separate schema per tenant



Shared database, shared schema, and shared tables for all tenants



Each of the above models has advantages and disadvantages, and based upon the application and scalability requirements tenants can be assigned any particular model. It is important to note that all three models can be supported with in a single application. This allow companies to judiciously use databases resources based upon the data size, price charged, and other application needs like resource pooling, data isolation, security, and scalability. All three models support unlimited customization across all major concerns of an application like security, workflow, business logic, presentations and more. DML, DDL and upgrades are supported across all tenants and full tenant data migration is supported within and across database clusters.

Security

Security is critical for any organization—failures can have devastating consequences for a company and its customers. As a result, companies spend enormous resources to protect their data and networks. At Ekartha, our security paradigm spans three layers of security:

- Application security (provided through the Alice platform)
- Network security (provided through collaboration with our data center partners)
- Facilities security(provided exclusively through our data center partners)

We use independent security auditors like Cybertrust to validate our security in all three areas on an annual basis. Routine application and network security scans by independent security companies, like Cybertrust, are conducted on a quarterly basis. Our partner data centers use the latest firewall protection, intrusion detection systems, SSL encryption, and proprietary security products that only a world-class security infrastructure can provide.

Protection at the Application Level

The Alice On Demand platform supports comprehensive authentication, authorization, and auditing for all applications built using Alice. Furthermore, the application security module can be extended to meet the specific requirements of an application or a particular business domain. Some of the application security features are:

- Administrators can assign data security rules that determine which users have access to which data based upon Role based Access Control. Application specific sharing models can be defined and data can be accessed based on user defined role hierarchies.
- All data is encrypted during transfer, and all access is governed by strict password security policies. All passwords are stored in MD-5 hash format. Password complexity rules and password expiration dates can be configured.
- Applications are continually monitored for security violation attempts. Policies can be set to define number of invalid login attempts allowed, session timeouts etc.

- All login/logouts are monitored, and applications can have individual password/username reset rules.
- All applications using Alice maintain a complete audit trail of all changes made to application data. For example, in default mode when a user makes a change, the application records the old value, the new value, the user that submitted the change, and a time stamp. All data changes can be reversed and all data and metadata can be restored to old values.

Protection at the Network Level

We select only data center partners that maintain the highest level of network security. All our data center partners use multilevel security products from leading security vendors and proven security practices to ensure network security. Following are some of the network security features provided by our partner data centers:

- To prevent malicious attacks through unmonitored ports, external firewalls allow only http and https traffic on ports 80 and 443.
- Switches ensure that the network complies with the RFC 1918 standard, while address translation technologies further enhance network security.
- IDS sensors protect all network segments.
- Internal software systems are protected by two-factor authentication, along with the extensive use of technology that controls points of entry.
- All networks are certified through third-party vulnerability assessment programs.

Protection at the Facilities Level

The security standards of our partner data centers are on par with the best civilian data centers in the world, including the world's most security-conscious financial institutions.

- Authorized personnel must pass through multiple levels of biometric scanning to reach system cages.
- All buildings hosting server cages are anonymous, with bullet-resistant exterior walls and embassy-grade concrete posts and planters around the perimeter.
- All exterior entrances feature silent alarm systems that notify law enforcement in the event of suspicion or intrusion.

Presentation and User Interface

The Alice multi-tenanted presentation service allows developers to build rich user interfaces using standard technologies like HTML, Flash, JavaScript, JSP and XML. Developers can use Adobe Flex, Google GWT, Openlazo, and other libraries and tools to build re-usable GUI components.

The Alice presentation service uses metadata to weave the GUI components into a complete user interface. This supports non-code based customization of page layouts, page flows, forms, view security, and customization of GUI elements at the portlet and page level. Thus, Alice enables developers to build highly customizable user interfaces that can be customized and configured for the specific needs of each and every tenant and, not just the application.

Furthermore, concerns like security and multi-tenancy are automatically weaved in, thus no security or multi-tenancy code needs to be written or mixed in with GUI code. This allows for clean separation of concerns, and also allows developers to focus on the task at hand.

Messaging

Asynchronous process communication is an important part of many modern internet applications, since many system communications are asynchronous in nature. Alice multi-tenant messaging service enables high performance, scalable, clustered messaging for internet applications.

Alice utilizes the Jboss, Java Message Service (JMS) implementation for asynchronous messaging requirements. Alice messaging supports two main message paradigms:

- Point-to-point (or queue-based) messaging.
- Publish-and-subscribe (or topic-based) messaging.

Furthermore, traditional messaging implementation involves steps like JNDI lookups for the queue connection factory and queue resources, and creating a JMS session before actually sending or receiving a message. Alice simplifies the task of working with the messaging system by hiding the details of a typical messaging implementation so developers can concentrate on the actual task of processing messages instead of worrying about how to create, access, or clean up messaging resources.

Integration

The Alice integration service provides a comprehensive set of technologies that makes it easy for companies to build a comprehensive integration infrastructure for their applications. All application's using Alice automatically have a full featured and straightforward Web services API that can provide programmatic access to almost all of the features and data of the application for each individual tenant.

Furthermore, the Alice integration service supports a wide array of technology options, that allow companies to use the tools and skills of their choice when implementing integrations. Alice Integration Service offers pre-built connectors to standard enterprise applications like SAP (upcoming), and Oracle. The Alice integration service also provides pre-built connectors for many desktop applications like Microsoft Excel, Word (upcoming), Outlook (upcoming). Developers can easily write new connectors for as many applications as they need. All connectors built using Alice automatically support full multi-tenancy including the associated security needs and exception handling mechanisms.

Billing and Metering

The Alice Billing and Metering service, aka Nexus is a highly flexible billing and metering service that allows On Demand companies to develop and bill for simple or complex pricing plans – whether they are based on simple subscription models or complex multi-transaction pricing. The metering systems can be configured to meter all application usage, and companies can monetize any part of the application. Nexus also offers advanced functionality such as: Revenue management, partner revenue sharing, invoicing and bill presentment, integration with multiple payment gateways, and automated payment processing.

Logging and Application Monitoring

Logging and Application monitoring are critical to the successful deployment and management of distributed internet applications. In Alice, all application activities can be monitored and logged. Standard application monitoring includes:

- Feature monitoring to determine usage of specific application features for each tenant.
- Monitoring request/response times to determine application performance for each tenant.
- Security monitoring, like session monitoring, login/logout monitoring etc.
- Database monitoring to determine database resource utilization for each tenant.
- Webservices utilization monitoring for each tenant.

The logging and application monitoring service is also a crucial tool in tracking application bugs in the both the development and production environments. Application logging can be integrated with third party alert generation and management, so that specific alerts can be generated in response to application bugs and exceptions.