ManageEngine
Identity360

Identity360 SOLUTION ARCHITECTURE

www.manageengine.com/identity360

Scope of this document

This document offers an in-depth exploration of the ManageEngine Identity360 architecture and its working. Upon reading this document, you will gain a comprehensive understanding of the necessary components for deploying Identity360, the roles of each component, and their intercommunication to facilitate the diverse functionalities of Identity360. Additionally, the document elucidates the operational aspects of the product.

Identity360 Architecture

ManageEngine Identity360 is a cloud-native solution that helps enterprises address workforce IAM challenges. The application is accessible over the internet without the need for any software installation.

Identity360 is built upon a resilient SaaS framework, embracing best practices to provide a scalable, highly accessible, and secure solution in the cloud.

Components of Identity360

Firewall

The firewall secures all inbound communication to Identity360 service, shielding your applications accessing the Identity360 service from malicious or unnecessary network traffic.

Load Balancer

The Load Balancer serves as a Proxy server, handling SSL offloading and distributing incoming requests evenly across the App server cluster to ensure balanced workloads.

Internal IAM service (Zoho Accounts)

It verifies that all requests originate from a valid, authenticated user; otherwise, it initiates authentication, redirecting to the Identity360 login page.

TaskEngine cluster

The TaskEngine cluster manages backend tasks and serves a crucial role in processing scheduled jobs such as directory sync, bulk operations, etc. without affecting the performance of the main App server cluster.

Web App cluster

The Web app cluster is a collection of application servers which is responsible for handling all incoming requests from an external network. This layer is designed with multiple nodes to handle many requests efficiently and to ensure minimal downtime for individual nodes.

Database cluster and archives

It securely stores Identity360 data and archives database data for disaster recovery as a precaution against potential risks. Three key functions are served:

- Customer data is segregated and isolated from each other using various data partition techniques.
- The database clusters are scaled independently based on the customer count and usage.
- Each Database instance in a cluster has a primary server and two slave servers for High Availability.

Microservices

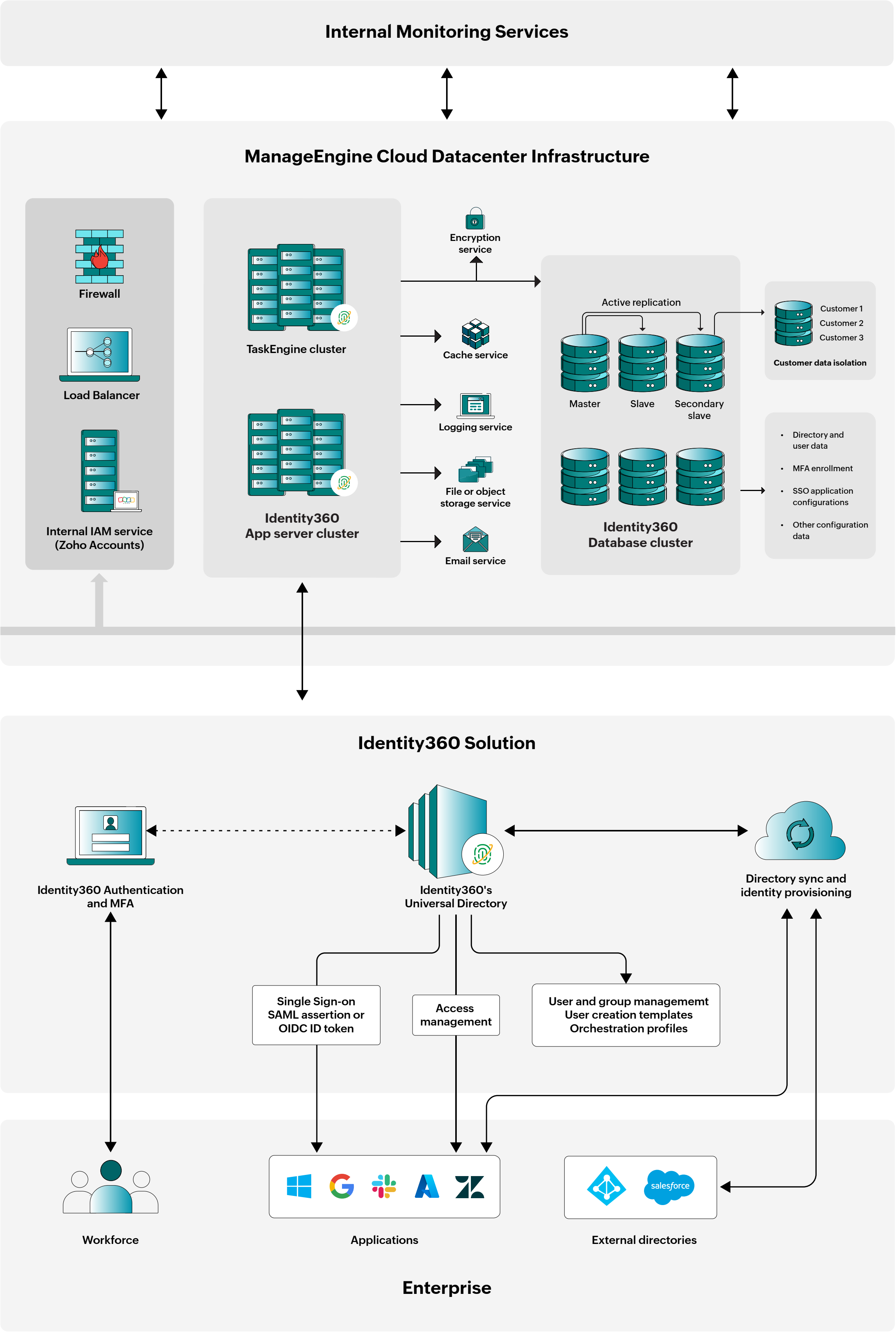
- **Logging service** audits application logs.
- **File service** aids in the storage and retrieval of various data types, including customer logos and temporary processing data.
- **Mailing service** sends one-time passcodes or notifications to email addresses.
- **Cache service** facilitates in-memory storage, where frequently accessed data from the Database cluster is temporarily cached, to reduce database loads and enhance performance.
- **Encryption service** is a centralized service that ensures data protection through strong encryption (AES-256) for all the stored sensitive customer data. Separate encryption keys are used for each registered customer or organization.

How does Identity360 work?

1. All requests from id360.manageengine.com are handled by the Identity360 App server cluster through the firewall, load Balancer, and internal IAM service.

2. To access Identity360, users have to visit and authenticate themselves in the login page followed by an MFA check.

3. After successful login to Identity360, Universal Directory, which is Identity360's directory service, serves the following functionalities:
    a. Identity Life cycle management which can be achieved by-
        i. User creation or modification and
        ii. Syncing existing directories/applications like AzureAD, Salesforce, etc.
    b. Single sign-on to SAML (or) OAuth2 OIDC compliant applications used by the enterprise can be performed.
    c. Access management can be achieved using SCIM-based provisioning. This enables admins to effortlessly manage bulk end-user access to cross-platform enterprise applications.



Internal Monitoring Services

ManageEngine Cloud Datacenter Infrastructure

Firewall

Load Balancer

Internal IAM service (Zoho Accounts)

TaskEngine cluster

Identity360 App server cluster

Encryption service

Cache service

Logging service

File or object storage service

Email service

Active replication

Master

Slave

Secondary slave

Identity360 Database cluster

Customer 1

Customer 2

Customer 3

Customer data isolation

- Directory and user data
- MFA enrollment
- SSO application configurations
- Other configuration data

Identity360 Solution

Identity360 Authentication and MFA

Identity360's Universal Directory

Directory sync and identity provisioning

Single Sign-on SAML assertion or OIDC ID token

Access management

User and group managememt User creation templates Orchestration profiles

Workforce

Applications

External directories

Enterprise

How robust is the security of your data?

Identity360 is securely hosted within data centers, ensuring that communications between the user's web interface and the central server are safeguarded by high-level enterprise encryption protocols. Meticulously engineered to ensure the highest level of security at every phase, Identity360 delivers fortified security for user authentication, data transmission, and access through the entire workflow. All sensitive data is securely stored in an encrypted format within the data centers. Please check this link for more details.

The data centers housing customer data were carefully designed to adhere to security best practices at all levels—physical, technical, people, and processes. Currently, Identity360 is hosted exclusively in US data centers. However, we will consider hosting in other data centers as per requirement. Check out our security page to know more about data centers.

The inherent live replication, scheduled backup, and high availability architecture prevents data loss and ensures business continuity.

How does data segmentation happen?

All customer data is logically partitioned at the software level.
Upon signup, a segmented database is provisioned for your organization by default.

What do you require to access Identity360?

To get started with Identity360, all you need is a standard web browser such as Firefox, Microsoft Edge, or Chrome.

Contact us:
Website: www.manageengine.com/identity360
Support Email: identity360-support@manageengine.com
Toll-free: +1-844-245-1104

Get Quote $

Sign Up ▶