ASBP

Entra ID I KeyCloak

Entra ID

- Identity provider
- Cloud based
- Primarily for Microsoft services
- External resources
- Internal resources

Audience

- Admins:
  - control of access
  - Automatizations

- Developers:
  - SSO AAA

- Subscribers:
  - Licence management

What are licences?

- Right to use a product
- Free with any cloud based service
- Can be extended with extra paid features
- Naming is P1, P2, P1 Premium, P2 Premium
- Look it up on https://www.microsoft.com/security/business/identity-access-management/azure-ad-pricing

Additional features

- IdM Governance
- Permission management
- Pay as you go licences

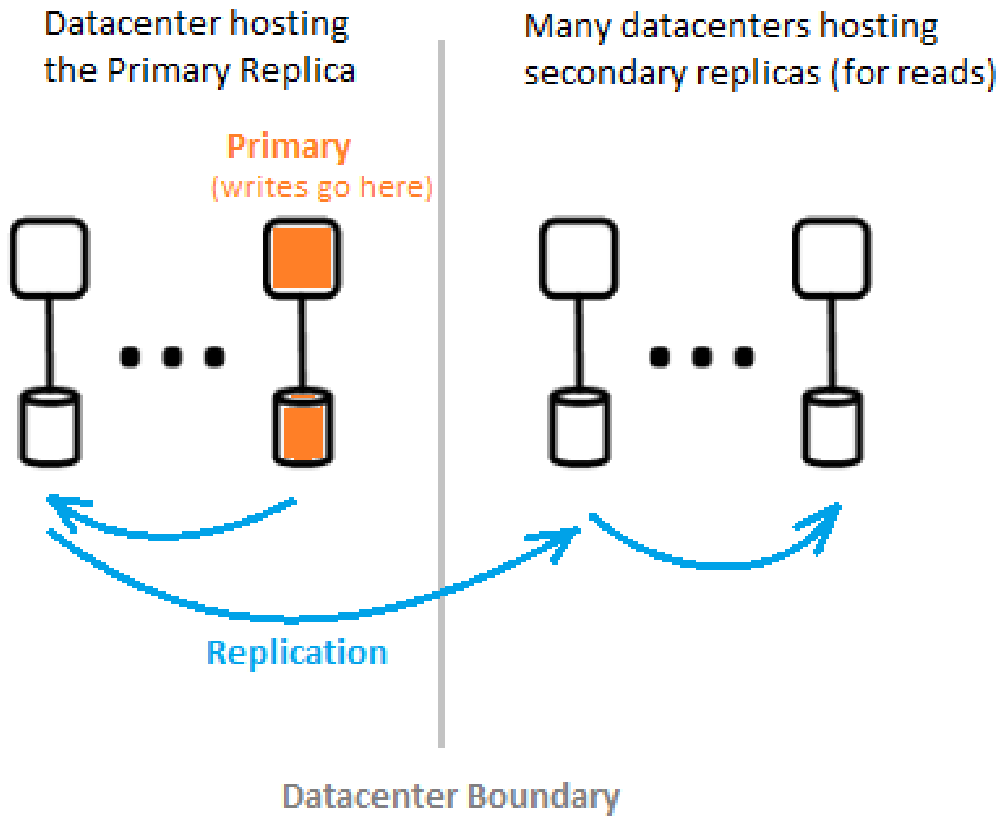
Complete list

- https://learn.microsoft.com/en-us/entra/fundamentals/whatis

Why is IdM important?

- Security
- Compliance

Architecture



- Primary replica (R/W)
- Secondary replicas (R)
- Enables scalability
- Data partitioning to speed writes
- Primary replica is target only for writes
- Single master

Fault tolerance

- Failover from primary to secondary
- Reads are 100% available
- Writes can be affected
- 1-2 minutes
- Enables tolerance to loss of multiple data centers
- https://datacenters.microsoft.com/globe/explore

Data consistency

- Eventually consistent DB
- Any read is targeted to primary and then a sync pull is done to secondaries
- Soft deletes
- Daily backups

- More on all of this:
- https://learn.microsoft.com/en-us/entra/architecture/architecture

Features

- User and Group Management
  - Creating and managing users and groups
  - Assigning roles and permissions
- Authentication Methods
  - Password-based, multi-factor, and passwordless authentication
  - Conditional Access policies
- Application Management
  - Single sign-on (SSO) for SaaS applications
  - Integrating on-premises applications
- Device Management
  - Registering and managing devices
  - Enforcing compliance policies

Integration

- Hybrid Identity with On-Premises Active Directory
    - Synchronization using Microsoft Entra Connect
    - Federation services
- Integration with Microsoft 365 and Azure Services
    - Seamless access to Microsoft services
    - Managing licenses and subscriptions
- Third-Party Application Integration
    - Configuring SSO for external applications
    - Using the application gallery

Monitoring

- Monitoring Tools and Capabilities
  - Microsoft Entra Connect Health
  - Sign-in and audit logs
- Reporting and Analytics
  - Generating security and activity reports
  - Leveraging insights for compliance

Keycloak

- Open-source Identity and Access Management solution
- Supports Single Sign-On (SSO)
- Manages authentication and authorization
- Extensible and customizable platform
- https://www.keycloak.org/

Key features

- SSO across applications
- Identity Brokering and Social Login
- User Federation with LDAP and Active Directory
- Fine-grained Authorization Services

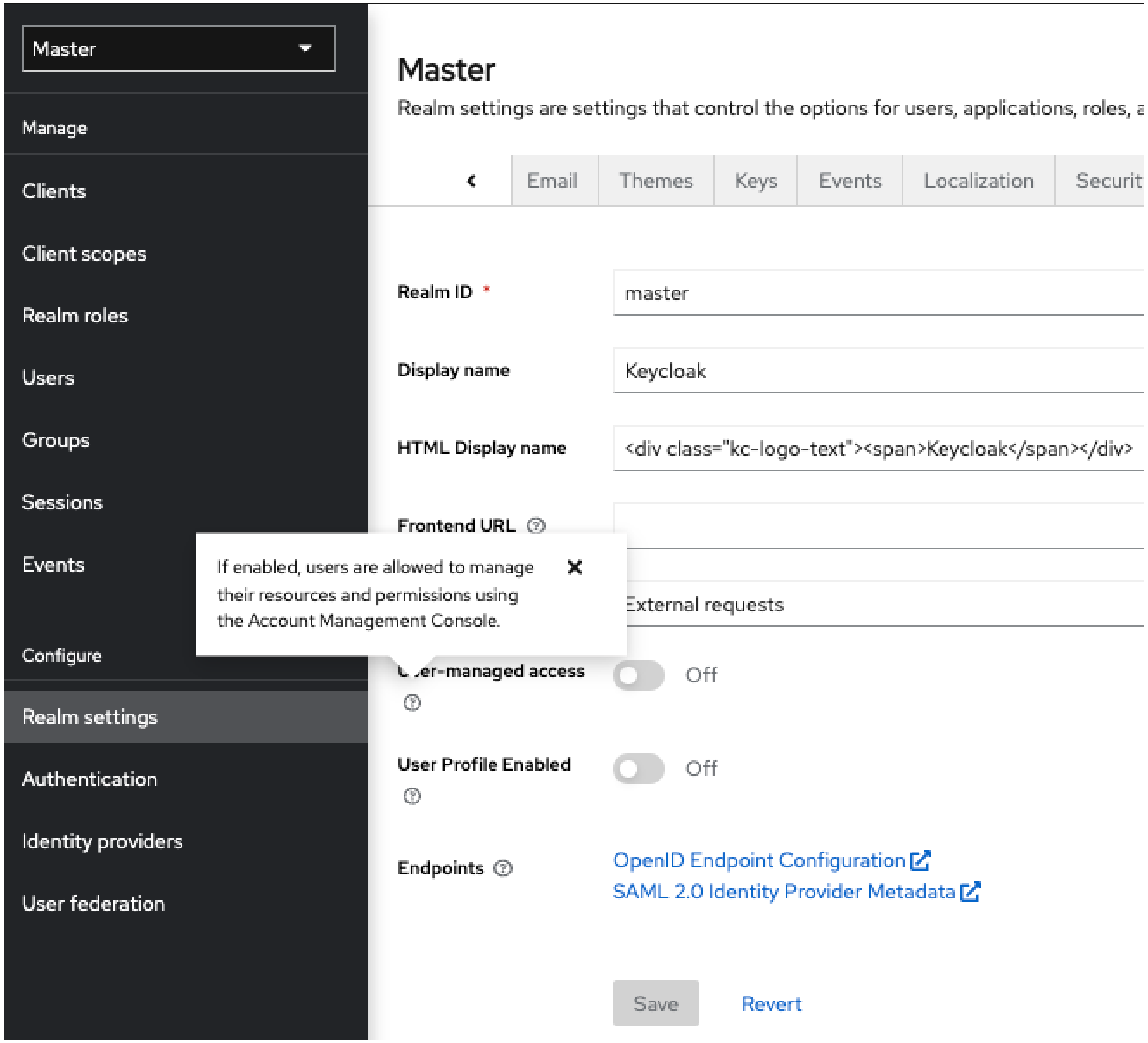
Architecture

- Based on standard protocols: OpenID Connect, OAuth 2.0, SAML
- Components: Server, Adapters, Admin Console
- Supports clustering for scalability
- Extensible through Service Provider Interfaces (SPI)
- https://www.keycloak.org/docs/latest/server_admin/

Installation and Setup

- Available as a standalone server or Docker image
- Requires Java Runtime Environment
- Initial setup via Admin Console
- Supports various databases for persistence

Web based administration



Master

Realm settings are settings that control the options for users, applications, roles, a

Realm ID * master

Display name Keycloak

HTML Display name <div class="kc-logo-text"><span>Keycloak</span></div>

Frontend URL

External requests

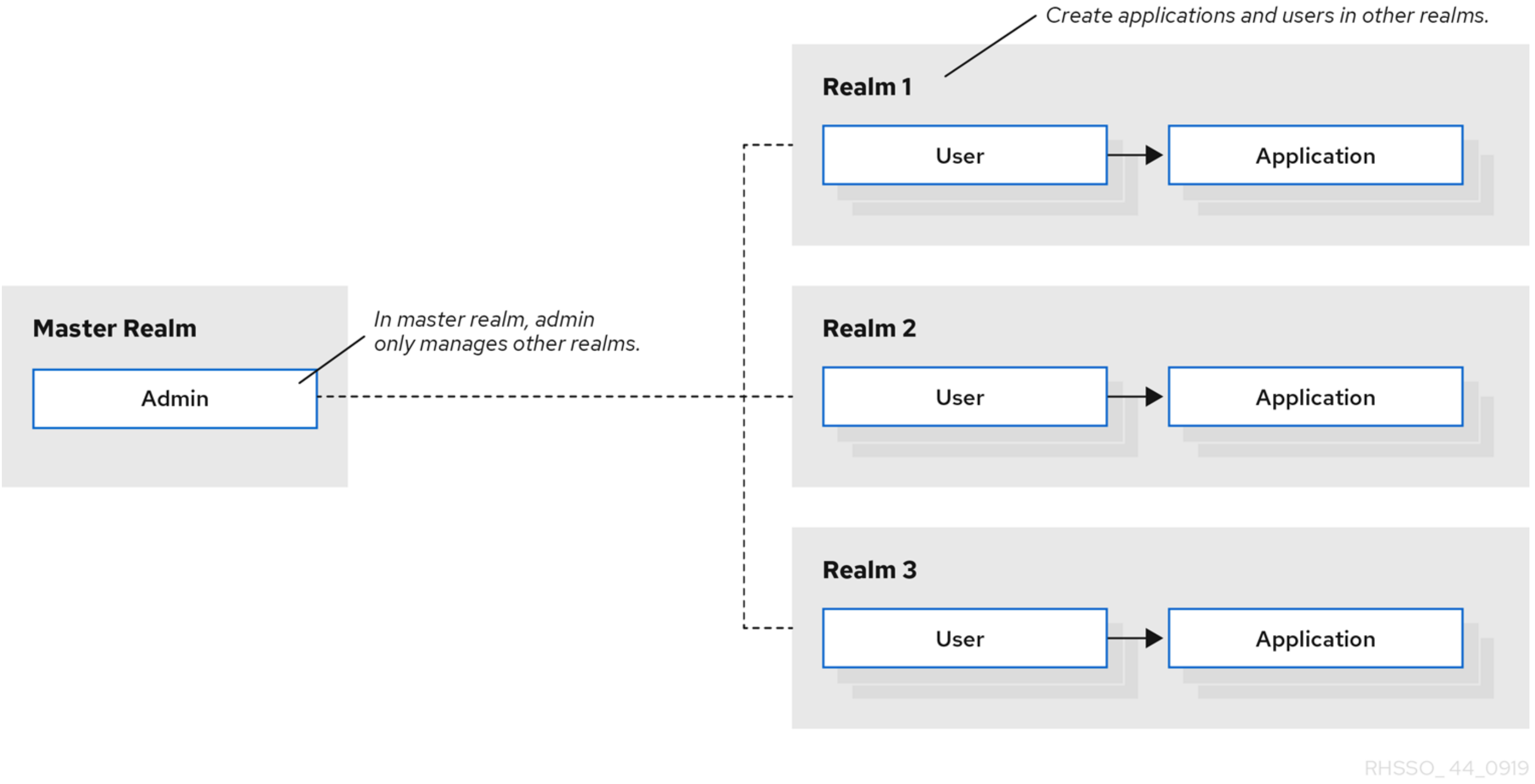
If enabled, users are allowed to manage their resources and permissions using the Account Management Console.

U‸er-managed access Off

User Profile Enabled Off

Endpoints OpenID Endpoint Configuration SAML 2.0 Identity Provider Metadata

Realms


Create applications and users in other realms.
Realm 1
User
Application
Master Realm
Admin
In master realm, admin only manages other realms.
Realm 2
User
Application
Realm 3
User
Application
RHSSO_44_0919

RBAC

- Define roles with specific permissions
- Assign roles to users and groups
- Roles can be composite (contain other roles)
- Simplifies permission management

Identity brokering

- Integrate external identity providers
- Support for social logins (Google, Facebook)
- Configure identity provider mappings
- Seamless user experience across platforms

Federation

- Connect to existing user stores (LDAP, Active Directory)
- Synchronize users and credentials
- Configure mappers for attribute mapping
- Supports read-only and writable federations

Application control

- Fine-grained access control policies
- Define resources, scopes, and permissions
- Support for attribute-based access control
- Centralized policy management

Clustering / HA

- Support for clustering Keycloak servers
- Load balancing and failover capabilities
- Session replication across nodes
- Scalable architecture for large deployments

Hvala na pažnji!