Keystle B2B/B2C

A proposta é mostrar como a Keystle atua como peça central na gestão de identidade e autorização multi-tenant, substituindo ferramentas como o Amazon Cognito e integrando-se de forma transparente com ambientes Kubernetes, sistemas federados e aplicações empresariais.

Visão Funcional

Objetivo da Solução B2B

A Keystle B2B oferece uma solução de **autenticação e autorização centralizada** para ecossistemas com múltiplos tenants (clientes/parceiros), mantendo segurança, flexibilidade e governança.

Principais capacidades:

- Federação de identidade com os IdPs dos clientes (Azure AD, Keycloak, Auth0)
- SSO entre múltiplas aplicações com escopos diferentes
- Suporte nativo a RBAC, ABAC e PBAC
- Delegação de acesso para operadores e times de suporte
- Compatibilidade com ambientes Kubernetes para controle de acesso interno

Casos de Uso Típicos

Cenário: Holding com múltiplas aquisições

Empresa	Integração	Tipo de Login	Observação
Empresa A (matriz)	Nativa na Keystle	SSO interno	Usuários de suporte e administração
Empresa B	Usuários migrados	SSO via Keystle	Centralizado na matriz
Empresa C	Federation via Keycloak	OIDC/SAML	Login corporativo mantido
Empresa D	Federation via Auth0	OIDC	Totalmente federado

Acesso do time de suporte da Empresa A

- Visualiza e gerencia os tenants C e D com escopo de operador
- Recebe token delegado via Keystle com escopo temporário no tenant federado
- Acessa aplicações da C e D como operador, com trilha de auditoria completa

Visão Técnica

Estrutura de Autenticação

- Suporte completo a OpenID Connect, OAuth2, SAML 2.0
- Emissão de tokens JWT com claims customizados
- MFA embutido com fluxo WebAuthn, TOTP, Email ou SMS
- Introspecção de tokens via API
- Refresh Token e revogação de sessão suportados

Federation (modo federado)

- Configuração via painel ou API de Federation:
    - Azure AD
    - Keycloak
    - Auth0
    - Google Workspace, etc.
- Mapeamento de claims → roles, atributos e políticas na Keystle
- Controle por tenant: cada tenant federado possui sua própria federação
- Suporte a fallback login, claims adicionais e override de atributos

Clients B2B

- `web_public_authentication`
- `web_private_authentication`
- `native_authentication`
- `client_credentials`
- `saml_metadata`

Cada aplicação B2B é registrada como client com permissões, redirect URIs, scopes e federation (se necessário).

JWT Server Embutido

- Tokens emitidos pela Keystle contêm:

```
{
  "sub": "user@empresa.com",
  "tenant_id": "empresaC",
  "permissions": ["reports:*:view", "orders:*:manage"],
 "roles": ["role-admin,”role-security”],
 "groups": ["admin", "member"],
  "exp": 1682352342
}
```

- Tokens validados por API Gateway, sidecar, middleware ou webhook OPA

- Validação local ou via introspecção

Integração com Kubernetes

Opções de integração

- Via **sidecar de validação** (ex: Envoy com filtro JWT)
- Via **OPA/Gatekeeper com webhook de política**
- Via **annotations e labels** no manifesto do pod ou namespace

Abordagem recomendada

- Definir as políticas no Golden Source da Keystle (RBAC, ABAC ou PBAC)
- Emissão de JWT para serviços/microsserviços
- Sidecar ou admission controller valida permissões usando claims do JWT

Provisionamento via IaC

- Integração com Terraform (provider da Keystle)
- CRDs customizados opcionais para integração com ArgoCD/Kustomize
- Suporte a CI/CD pipelines para provisionar tenants, clients, roles e federations

Migração do Cognito para Keystle

Componentes substituídos

Cognito	Keystle
JWT Server	Plataforma OIDC/SAML com emissão JWT nativa
Federation SAML	Federation multi-tenant com mapeamento granular
User Pool + App Client	Tenants + Clients com roles, atributos e scopes
RBAC inline no token	PBAC com Resource/Type/Action definidas externamente

Ferramentas de migração

- Scripts de importação de usuários, roles e permissões **Keycloak**
- Suporte a wildcards em resource/action

Benefícios da Gestão de Identidade Centralizada

- Centralização da autenticação e autorização
- Redução da complexidade operacional (sem salto Cognito + JumpCloud)
- Políticas reutilizáveis, versionáveis e auditáveis
- Delegação de acesso com rastreabilidade (operadores e suporte)
- Redução de custos com estrutura federada unificada