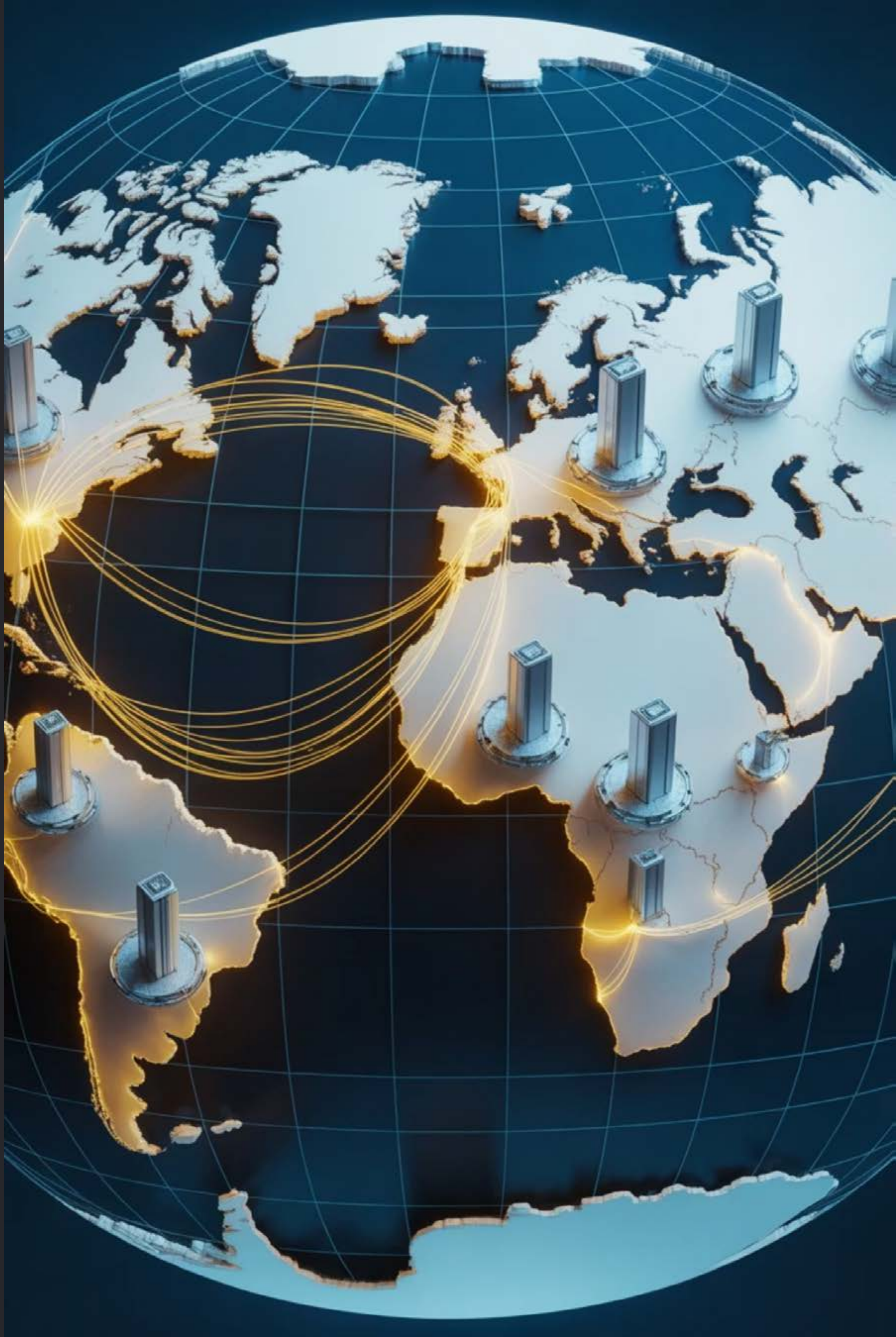
Scaling Identity for Global SASE with Keycloak: The Regional Hub Deployment Model

By Vivek Koodakkara Shanmughan

Aryaka Networks

Conf42.com Kube Native 2025



Agenda

SASE & Identity Challenges

Exploring the evolving landscape of enterprise security and the pivotal role of identity as the new perimeter.

The Regional Hub Model

Understanding its core architecture, key benefits, and critical implementation considerations.

Keycloak: The Identity Solution

Highlighting its capabilities, recommended configurations, and optimal integration patterns.

Implementation & Operations

Practical guidelines, automation best practices, and strategies for performance optimization.

The Evolution of Enterprise Security

Enterprise security is undergoing a fundamental shift. Traditional perimeter-based models are no longer effective in today's distributed enterprise landscape, which is marked by:

- A growing remote workforce.
- Extensive multi-cloud adoption.
- Applications dispersed across data centers, multiple clouds, and edge locations.
- Increasing regulatory compliance requirements across diverse regions.

This fundamental shift necessitates a security paradigm that is inherently **identity-centric and distributed**, moving beyond legacy network-centric and centralized approaches.

Secure Access Service Edge (SASE)

SASE converges networking and security functions into a cloud-delivered service model, with **identity** at its core.

Cloud-Native Architecture

Leverages distributed Points of Presence (PoPs) for global reach and optimized latency.

Zero Trust Model

Enforces continuous verification of identity, context, and policy for every access request.

Identity as the Foundation

Bases authentication and authorization decisions on user and device identity, independent of network location.

Consolidated Management

Provides a single policy framework for consistent security across all access scenarios.

Global SASE Identity Challenges

- Latency Constraints

  Authentication round-trips to distant regions add 200-300ms, significantly degrading user experience.

- Data Sovereignty

  Strict regulations (e.g., GDPR, CCPA) demand careful consideration of identity data processing and storage locations.

- Availability Requirements

  Centralised models risk regional outages or network issues impacting global operations.

- Scale Limitations

  Centralised identity providers struggle to meet the throughput demands of globally distributed traffic.

Traditional centralised IAM architectures create significant operational bottlenecks in global SASE environments.

Regional Hub Deployment Architecture

The Regional Hub Model deploys **autonomous Keycloak clusters in strategic locations** worldwide, creating a distributed but coordinated identity infrastructure.

Strategic Placement

Hubs in major business regions (EMEA, APAC, Americas) aligned with SASE PoPs

Regional Autonomy

Each hub capable of authenticating users independently during normal operations

Global Coordination

Synchronisation mechanisms for consistent policy and user data across regions

Benefits of Regional Hub Architecture

- Reduced Latency

  Bringing identity services closer to users significantly reduces authentication latency, enhancing global user experience and application responsiveness.

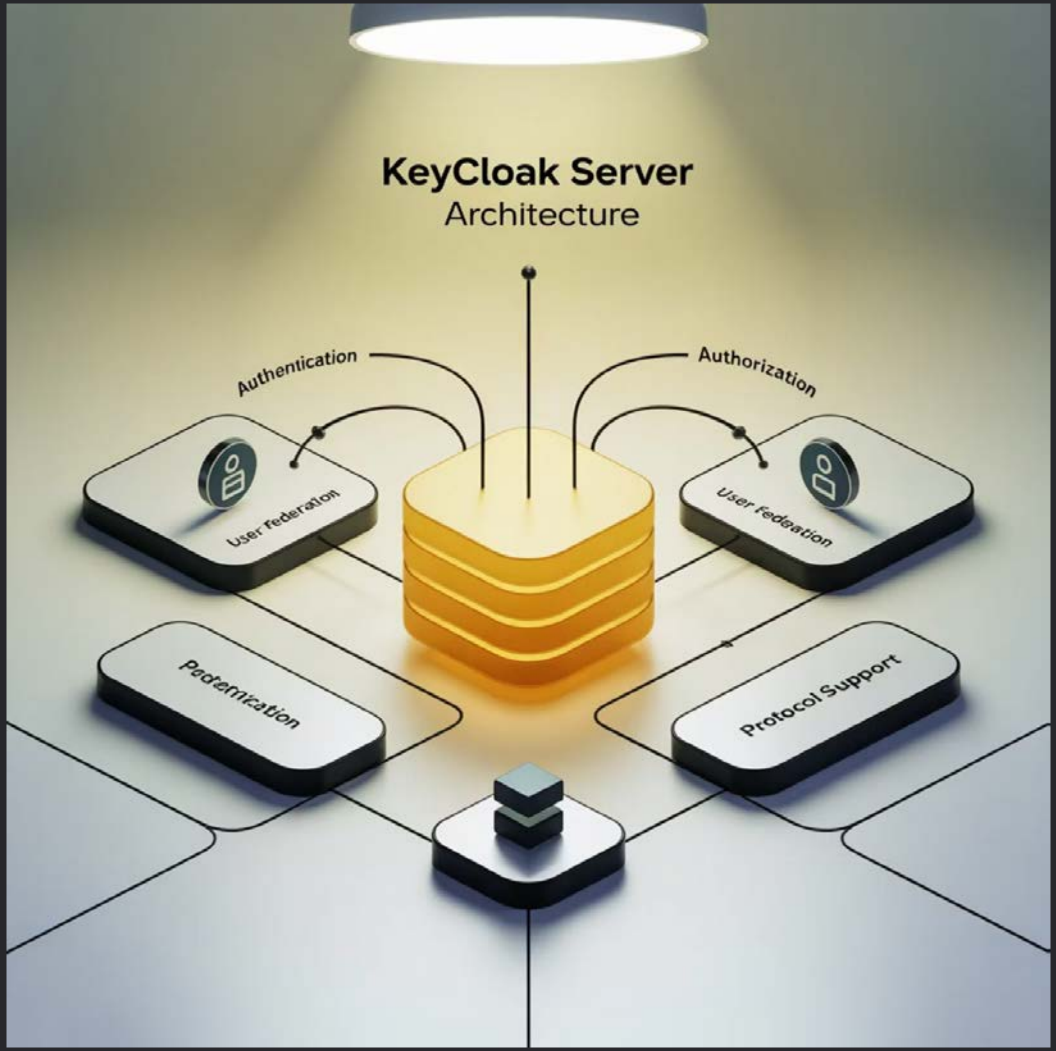
- Enhanced Availability

  Each regional hub operates autonomously, providing high availability and robust disaster recovery. Local outages in one region do not impact global identity services.

- Optimized Cost

  Processing authentication requests locally minimizes cross-region data transfer, leading to substantial reductions in cloud egress and overall infrastructure costs.

Keycloak: The Ideal Identity Platform for Regional Hubs



Keycloak is exceptionally well-suited for distributed SASE environments due to its core capabilities:

- ## Open Source & Kubernetes-Native

  Its containerized deployment, comprehensive Kubernetes operators, and open extensibility model are ideal for modern infrastructure.

- ## Multi-Tenancy via Realms

  Offers isolated security domains (Realms) for distinct business units or customers.

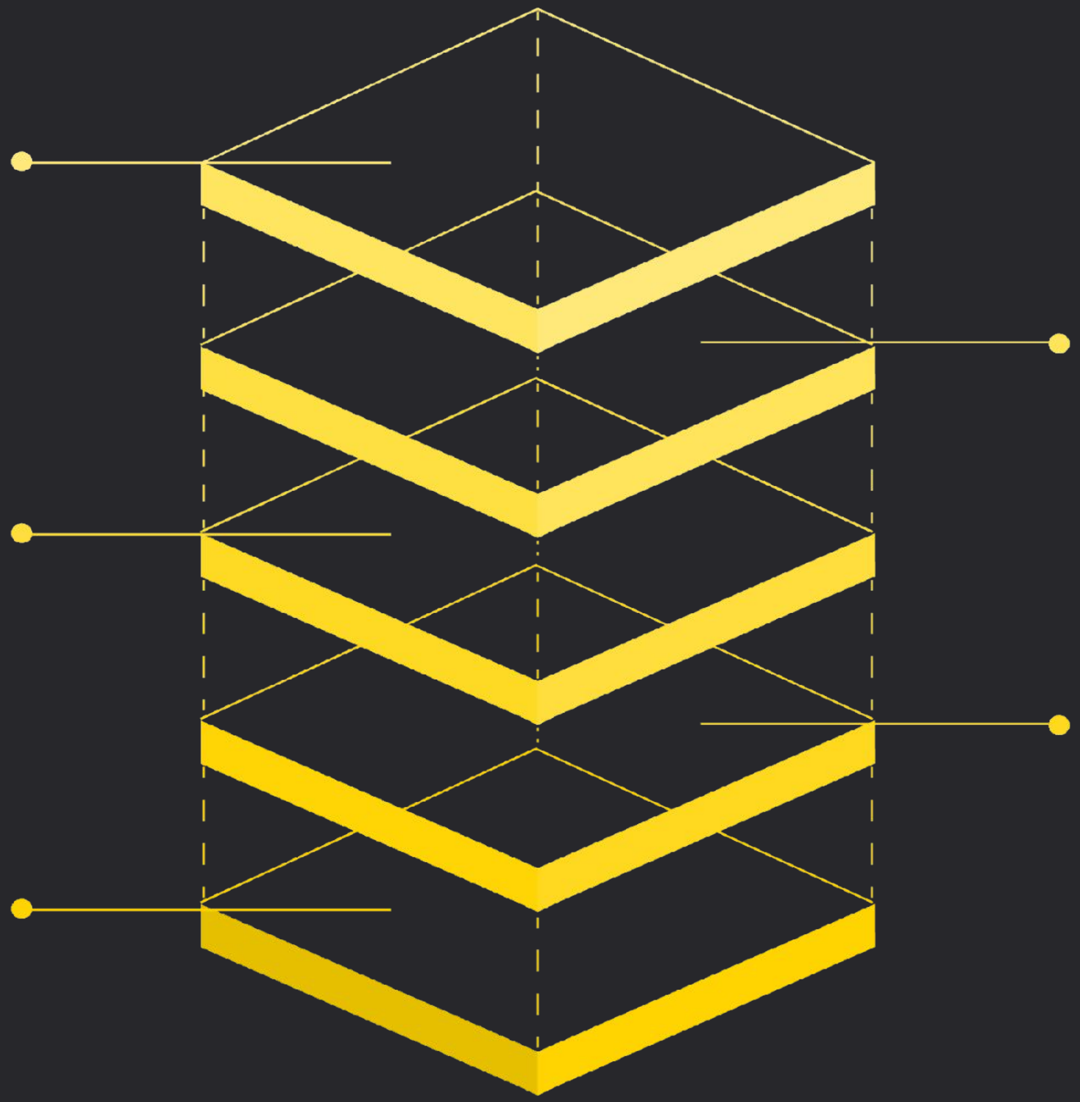
- ## Standards Compliance

  Comprehensive support for industry standards like OIDC, OAuth 2.0, SAML, and WebAuthn ensures seamless integration.

- ## Extensibility

  Enables custom SPIs (Service Provider Interfaces) and event listeners for tailoring to specific SASE security requirements.

Technical Architecture of a Regional Hub



Integration & Monitoring

Integrates with SASE components and provides comprehensive observability.

Global Directory Sync

Synchronizes user identities with global corporate directories.

Load Balancer

Distributes incoming traffic across Keycloak nodes for high availability and scalability.

Database

Stores persistent realm configurations and user identity data.

Keycloak Cluster

Core Identity Provider for regional authentication and Single Sign-On.

Each regional hub adheres to a standardized architecture pattern, yet offers the flexibility for local customization to meet specific regional requirements and regulatory compliance.

Hub Placement Strategy

1. **Analyze Traffic Patterns**

   Identify optimal regional hub locations by meticulously mapping user concentrations and access patterns.

2. **Align with SASE PoPs**

   Strategically position identity hubs in close proximity to existing SASE Points of Presence (PoPs) to optimize traffic flow.

3. **Consider Regulatory Zones**

   Group regions with similar data sovereignty requirements to simplify and ensure compliance.

4. **Evaluate Cloud Provider Capabilities**

   Select regions with robust service offerings from your preferred cloud providers to leverage optimal infrastructure.

5. **Test User Latency**

   Validate real-world performance improvements by conducting latency tests and sample authentication flows from diverse user locations.

A recommended starting point involves deploying **3-4 regional hubs** across major business regions, with future expansion driven by operational metrics and user feedback.

Inter-Cluster Synchronisation Approaches

User & Policy Synchronization

- Utilize shared directory services (AD/LDAP)
- Replicate user profile data via database replication
- Implement GitOps for policy-as-code synchronization

Token & Session Management

- Enable cross-cluster token validation
- Employ distributed session caching (Infinispan)
- Facilitate token exchange between regional hubs

Operational Consistency

- Manage configuration synchronization via CI/CD pipelines
- Stream events for comprehensive audit logging
- Centralize monitoring and metrics collection

Automation & Operational Practices

GitOps Workflow

Manage Keycloak configurations as code in Git for consistent deployment.

Kubernetes Operators

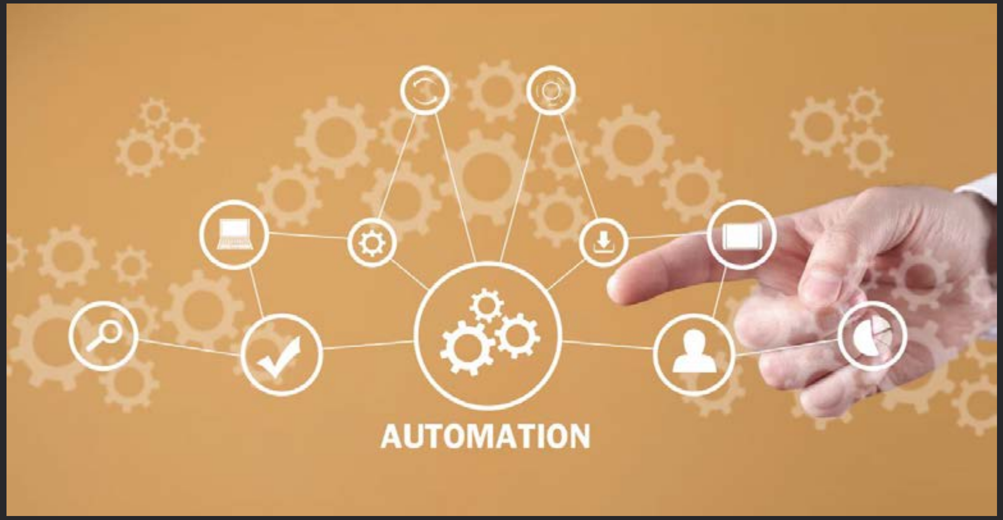
Leverage Keycloak Operator for declarative cluster management.

Canary Deployments

Progressively roll out changes to minimize risk.

Observability Stack

Implement monitoring for cross-region authentication flow tracking.



Automation is critical for ensuring consistency and reliability across regional hubs.

Implementation Challenges & Mitigations

Challenge	Impact	Mitigation Strategy
Data Consistency	Potential for conflicting user data or policies across regions	Establish robust conflict-resolution protocols; designate authoritative data sources
Operational Complexity	Increased management overhead due to distributed deployments	Standardize infrastructure as code; centralize observability and alerting
Failover Coordination	Complex routing decisions during regional outages	Utilize global load balancers with health-aware routing; automate failover testing
Cost Management	Elevated infrastructure costs from multiple deployments	Implement autoscaling based on regional traffic patterns; strategically deploy features
Compliance Validation	Audit complexity stemming from diverse regional requirements	Develop region-specific compliance-as-code checks; automate audit-trail generation

Key Insight: While a regional-hub model introduces complexities, these are significantly outweighed by the long-term operational benefits of enhanced performance, availability, and compliance.

Key Takeaways

- ### Identity Is Critical for SASE

  As the cornerstone of Zero Trust, identity demands a global distribution strategy consistent with other SASE components.

- ### Regional Hubs Solve Real Problems

  Latency, availability, compliance, and scale challenges are effectively addressed by a distributed architecture.

- ### Keycloak Is Well-Suited

  Open-source, Kubernetes-native, and highly extensible, making it ideal for distributed SASE deployments.

Next Steps:

1. Evaluate your current identity architecture against global SASE requirements.
2. Map user concentrations to identify optimal regional hub locations.
3. Pilot a two-region Keycloak deployment to validate performance benefits.
4. Develop automation practices for consistent deployment and management.

Thank You !