Sarcouncil Journal of Multidisciplinary

ISSN(Online): 2945-3445

Volume- 05| Issue- 07| 2025

Review Article **Received:** 14-06-2025 | **Accepted:** 08-07-2025 | **Published:** 27-07-2025

Keycloak Implementation for Identity Management in SASE Architectures: A Regional Hub Approach

Vivek Koodakkara Shanmughan
Independent Researcher, USA

Abstract: Implementing Keycloak as an identity management solution within SASE architectures presents a strategic approach to modern security challenges. The Regional Hub Model effectively addresses authentication complexities in distributed SASE environments where continuous identity verification supports Zero Trust principles. SASE architectures struggle with complex challenges stemming from the need to support multiple tenants and connect with various identity systems within organizations. These architectural hurdles demand thoughtful solutions that address both technical and operational needs. Strategically positioning dedicated Keycloak clusters across geographic regions delivers tangible benefits: reduced authentication response times, simplified management overhead, regional capacity scaling based on local demand patterns, and contained failure domains that preserve global service availability. Key implementation factors include careful hub location selection based on user distribution, reliable configuration synchronization between regional deployments, comprehensive performance monitoring frameworks, and robust automation pipelines to maintain consistency across the distributed architecture. This architecture enables effective adoption of Zero Trust security principles within global SASE infrastructure while balancing performance, manageability, and resilience requirements critical to enterprise deployments.

Keywords: SASE, Keycloak, Regional Hub Model, Zero Trust, Identity Management.

INTRODUCTION

In recent years, the technology industry has witnessed the rise of Secure Access Service Edge (SASE), a framework that brings together network and security functions into a single cloud architecture. Remote work expansion and accelerated cloud adoption have driven SASE implementation across sectors, as organizations recognize its capabilities for addressing contemporary security challenges (NordLayer,). At its foundation, SASE depends on sophisticated identity and access management systems that facilitate continuous verification of user identities—a core principle of Zero Trust security models. This verification process establishes the bedrock of SASE's security approach, enforcing appropriate access controls regardless of user location or device characteristics (Zscaler,).

In contrast to conventional perimeter-based security models, SASE environments exist as inherently distributed, multi-tenant systems that must connect with various corporate Identity Providers (IDPs), creating substantial architectural complexities for identity management frameworks. Integration difficulties frequently arise from existing infrastructure constraints and compatibility gaps between established authentication systems and cloud-native SASE components (NordLayer,). Entities deploying SASE platforms regularly face obstacles when integrating pre-existing identity infrastructure with new security architectures, necessitating methodical planning and specialized expertise to navigate these implementation challenges (Zscaler,).

The operational success of SASE deployments fundamentally depends on the authentication infrastructure that effectively balances competing requirements: reduced latency, seamless IDP integration, extensive scalability, and consistent availability. Authentication response time directly affects user satisfaction, especially for delay-sensitive applications requiring immediate access and responsiveness (NordLayer,). These performance demands become particularly acute within global SASE deployments serving users across diverse geographic regions, organizational boundaries, and network environments. Worldwide implementations must address regional network disparities, data sovereignty mandates, and varied compliance frameworks (Zscaler,).

This article examines Keycloak—an open-source identity management solution—as a practical platform for addressing complex authentication requirements inherent to distributed SASE architectures. Keycloak's comprehensive protocol support and adaptable framework make it appropriate for enterprise-grade SASE identity management deployments (Zscaler,). The Regional Hub Model represents an optimal deployment strategy that balances critical technical and operational constraints present in global SASE implementations. This approach resolves key SASE deployment challenges through strategic distribution of authentication services, minimizing

***Corresponding Author:** Vivek Koodakkara Shanmughan

DOI- https://doi.org/10.5281/zenodo.16498126

latency while preserving necessary security controls (NordLayer,). Through careful positioning of identity management infrastructure, organizations can enhance authentication processes while meeting data localization requirements and reducing cross-region network dependencies (Zscaler,).

SASE IDENTITY MANAGEMENT CHALLENGES

High-Volume Authentication

SASE platforms must handle substantial authentication traffic across multiple client organizations. Every interaction between users and SASE security checkpoints may initiate verification processes, creating considerable authentication workloads that grow in direct proportion to user numbers and activity. The transition toward Zero Trust frameworks places greater demands on authentication systems due to persistent verification needs that produce far more authentication events compared to legacy security models (Microsoft Ignite, 2025). This challenge becomes most apparent within large enterprise contexts where simultaneous authentication requests may surge during work hours, necessitating resilient authentication systems capable of expanding dynamically to satisfy demand while preserving performance levels and security standards (Check Point.).

Latency Sensitivity

The operational requirements of SASE services necessitate minimal authentication delays. Prolonged authentication processes negatively affect user satisfaction and application responsiveness, especially for interactive software where users anticipate immediate system feedback. Global user distribution compounds these latency concerns, as network travel times between end-users and authentication servers can markedly reduce service quality. Zero Trust network designs require careful balancing between thorough security verification and performance optimization, since excessive security checks might introduce perceptible delays during application access (Microsoft Ignite, 2025). Distributing authentication capabilities geographically becomes crucial when supporting worldwide users, as regional response time variations may create inconsistent experiences depending on user proximity to authentication infrastructure (Check Point.).

Identity Provider Integration

SASE architectures serve as integration hubs for various organizational identity systems. Such integration demands support for established protocols, including OAuth2/OIDC and SAML, alongside capabilities for attribute mapping and protocol conversion. Varied identity provider implementations across customer environments create notable complexity in maintaining compatible authentication processes. Current Zero Trust architectures must effectively federate identity across organizational limits while ensuring consistent security enforcement (Microsoft Ignite, 2025). Integration challenges extend beyond basic protocol compatibility to encompass policy harmonization, attribute standardization, and certificate management across diverse identity platforms employing different standards (Check Point.).

High Availability Requirements

As critical security enforcement points, authentication systems supporting SASE services require exceptional reliability and fault tolerance. Authentication system outages directly restrict user access to protected assets, potentially causing widespread operational disruptions. Network segmentation within Zero Trust designs demands continuous authentication availability, since security verification occurs during each access attempt (Microsoft Ignite, 2025). Effective SASE implementations incorporate geographic redundancy, automated failover systems, and comprehensive monitoring to maintain operational authentication services despite regional infrastructure problems, thereby preventing authentication components from becoming critical failure points (Check Point.).

Table 1: Authentication Challenges in SASE Environments (Microsoft Ignite, 2025; Check Point.)

Challenge Category	Complexity Level
Authentication Volume	High
Latency Requirements	Critical
IDP Integration	Complex
Availability Needs	Maximum
Operational Overhead	Significant

Publisher: SARC Publisher

KEYCLOAK CAPABILITIES FOR SASE ENVIRONMENTS

Federated Identity Management

The Keycloak codebase contains native implementations for handling SAML assertions, OAuth tokens, and OpenID Connect identity flows. No extra software needed. Most enterprises already use directory services, cloud identity platforms, or workforce authentication systems for managing users. Keycloak connects directly to these systems. This matters for SASE deployments where different company divisions often use different identity systems. In Zero Trust security models, every access request needs verification. Keycloak sits in the middle, handling these constant verification checks between users and protected resources (Solo.io). Through support for multiple federation protocols concurrently, Keycloak allows SASE environments to retain compatibility with established corporate identity systems while delivering consistent security across all application access points. The federated model proves especially beneficial when connecting older systems to modern cloud services, enabling organizations to utilize existing identity assets during migration toward complete SASE frameworks (Jain, P. 2025).

Multi-Tenancy Support

Keycloak uses a realm-based approach that naturally supports multi-tenancy. This lets completely separate authentication spaces coexist in a single installation. Each realm keeps its own users, settings, and identity provider connections, creating strong boundaries between different organizations sharing the SASE system. This design approach corresponds with Zero Trust principles through the establishment of distinct security boundaries between organizational entities while retaining centralized administration (Solo.io). The realm isolation approach prevents security policy crossover between tenants while facilitating efficient resource usage through shared underlying infrastructure. Multi-tenant architecture significantly benefits cloud identity management, allowing service operators to maintain logical separation between customer environments without replicating infrastructure for each client (Jain, P. 2025).

Scalability Architecture

Keycloak supports horizontal scaling through clustering mechanisms where multiple instances share authentication data via distributed caching systems. This architecture facilitates linear capacity growth to handle increasing authentication loads without performance degradation. SASE deployments require identity platforms capable of adjusting dynamically to changing regional authentication demands, precisely what Keycloak's clustering model delivers (Solo.io). Horizontal scaling provides enhanced resilience compared to vertical scaling approaches, as capacity increases occur incrementally without service interruption. Distributed session management within Keycloak maintains authentication state consistency across clusters while reducing inter-node communication overhead, essential for geographically dispersed SASE environments (Jain, P. 2025).

Extensibility Framework

The plugin-based architecture of Keycloak enables customization of authentication processes, identity federation, and attribute mapping. This adaptability proves particularly valuable for SASE environments with unique integration requirements stemming from diverse connected systems and security policies. Zero Trust implementations frequently need context-aware authentication decisions incorporating factors beyond standard credentials, with Keycloak's extension capabilities supporting integration with additional security indicators like device status, network position, and behavior patterns (Solo.io). The modular design allows for specialized authentication flows without core component modifications, preserving upgrade compatibility while meeting specific security needs. This extensibility benefits cloud identity solutions when adjusting to industry compliance requirements or connecting with specialized security tools beyond standard authentication protocols (Jain, P. 2025).

Table 2: Keycloak Capabilities for SASE Environments (Solo.io; Jain, P. 2025)

Capability Category	Implementation Strength
Federation Support	Comprehensive
Multi-Tenancy	Native
Scalability Architecture	Robust
Extensibility Framework	Flexible
Protocol Compatibility	Extensive

Publisher: SARC Publisher

THE REGIONAL HUB MODEL FOR KEYCLOAK DEPLOYMENT

Architectural Overview

The Regional Hub Model employs separate, redundant Keycloak clusters positioned across strategic geographic areas. Authentication requests from SASE enforcement points route to the nearest regional hub, establishing a distributed architecture that mirrors user and service distribution. Modern authentication design principles favor this geographic approach since physical proximity between users and authentication services substantially affects system responsiveness (Singla, D., & Verma, N. 2023). While operating autonomously, these regional installations exchange configuration data and security policies through automated synchronization, maintaining consistent security controls across regions while preserving independent regional operation (Murcia, J. M. B. *et al*., 2025).

Latency Optimization

Directing authentication traffic to regionally proximate hubs markedly decreases authentication response times. Such improvements prove especially valuable for interactive applications where users anticipate immediate system responses and where delays noticeably diminish user experience quality. Research into authentication latency reveals specific thresholds where slower responses begin affecting productivity, particularly within Zero Trust frameworks requiring frequent credential verification (Singla, D., & Verma, N. 2023). Comparative analyses demonstrate that distributed authentication consistently outperforms centralized models regarding response times, with the most dramatic improvements observed for users distant from organizational headquarters or primary infrastructure, where network transmission times would otherwise constitute the majority of authentication delay (Murcia, J. M. B. *et al*., 2025).

Operational Manageability

Regional consolidation enhances management efficiency by limiting the number of distinct Keycloak clusters requiring maintenance. This approach simplifies deployment, updates, monitoring, and identity provider integrations compared to fully distributed models. Analysis of authentication system performance demonstrates that administrative complexity grows disproportionately as independent authentication nodes increase, making regional consolidation advantageous from an operational perspective (Singla, D., & Verma, N. 2023). The hub approach enables standardized configuration and monitoring practices across a limited number of clusters while preserving the latency benefits of geographic distribution, effectively balancing administrative requirements against performance considerations (Murcia, J. M. B. *et al*., 2025).

Scalability Benefits

Distributing authentication processing across regional hubs permits capacity adjustments based on local usage patterns within each region. This approach offers superior resource efficiency compared to global scaling methods since capacity aligns with regional demand rather than worldwide peak requirements. Authentication activity typically follows regional business hours and work patterns, creating natural load distribution across global deployments (Singla, D., & Verma, N. 2023). The regional model leverages these variations through independent scaling decisions for each hub based on local demand characteristics, eliminating unnecessary global infrastructure scaling and optimizing resource utilization (Murcia, J. M. B. *et al*., 2025).

Resilience Characteristics

The Regional Hub Model strengthens system resilience through failure domain separation. Regional hub failures affect only those SASE enforcement points connected to that particular hub, constraining the potential outage scope. This compartmentalization produces better overall system availability compared to centralized authentication approaches. Authentication performance studies consistently highlight geographic redundancy as essential for achieving high availability in global implementations (Singla, D., & Verma, N. 2023). By isolating potential failures within specific regions, this model prevents authentication disruptions from affecting global operations, containing incidents within defined geographic boundaries while preserving service availability in unaffected areas, fundamentally enhancing the reliability profile of the entire authentication architecture (Murcia, J. M. B. *et al*., 2025).

Publisher: SARC Publisher

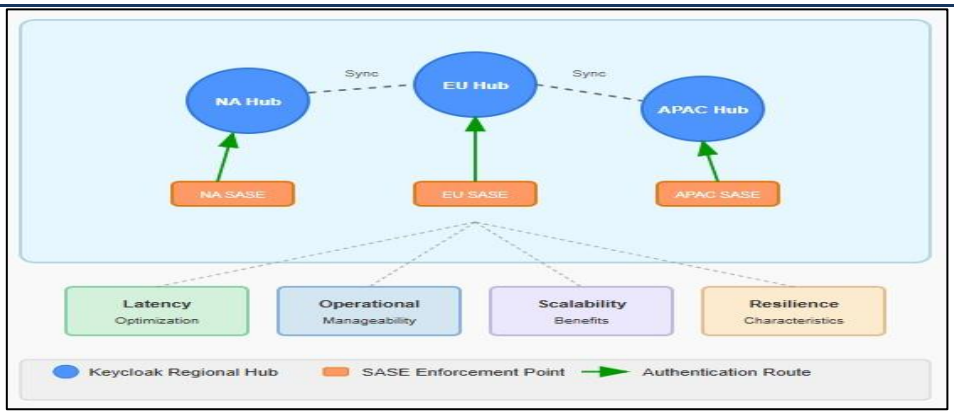

Fig 1: Regional Hub Model: Optimizing Keycloak Deployment for Global SASE Environments (Singla, D., & Verma, N. 2023; Murcia, J. M. B. *et al*., 2025)

IMPLEMENTATION CONSIDERATIONS

Regional Hub Placement Strategy

Effective placement of regional hubs requires balancing several critical factors: user distribution demographics, measured network latency, data sovereignty mandates, and available infrastructure resources. Proper hub positioning reduces average authentication response times while satisfying applicable regulatory frameworks. Regional hub location decisions necessitate evaluation of both physical computing requirements and the logical architecture of Keycloak domain deployments (Younes, S. 2021). Strategic placement must incorporate existing network topologies and connection pathways to minimize authentication delays while ensuring adequate computing capacity within each region to handle anticipated authentication volumes. The complexity increases substantially in multi-cloud scenarios, where varying infrastructure capabilities and differing service agreements between cloud providers must be navigated while maintaining uniform security controls across all environments (Shackleford, D. 2024).

Inter-Cluster Synchronization

Although regional hubs function autonomously, specific configuration components require coordinated synchronization to ensure security policy consistency. These components encompass realm configurations, client registrations, and role definitions. Automated synchronization systems preserve configuration uniformity while maintaining operational independence for each regional hub. Successful Keycloak cluster implementations typically employ domain configuration methodologies wherein shared database infrastructure ensures configuration consistency yet permits independent node operation, enhancing overall system resilience (Younes, S. 2021). Synchronization mechanisms within multi-cloud environments must address potential network reliability variations between regions through appropriate retry procedures and conflict resolution protocols, maintaining policy consistency without introducing centralized failure points within the authentication framework (Shackleford, D. 2024).

Monitoring and Observability

Thorough monitoring of regional Keycloak installations remains fundamental for operational oversight and preemptive problem resolution. Monitoring tools must capture response timing, request volume, and error counts to assess system health. Memory leaks, CPU bottlenecks, and connection pool saturation often precede system failure, making these metrics essential. Identity provider availability and authentication workflow completion rates reveal external integration stability. Rather than isolated regional views, operations benefit from unified dashboards that blend metrics from all geographic hubs. Domain-structured deployments require monitoring at both individual node and cluster levels, with specific attention to node health indicators, database connectivity states, and cache replication performance to verify proper cluster functionality (Younes, S. 2021). Multi-cloud identity implementations particularly benefit from unified monitoring approaches that aggregate authentication statistics across diverse environments, enabling comprehensive visibility despite infrastructure distribution and supporting early detection of regional performance discrepancies or policy inconsistencies (Shackleford, D. 2024).

Automation Requirements

The distributed architecture inherent to the Regional Hub Model demands sophisticated automation for deployment, configuration, and lifecycle management of Keycloak clusters.

Publisher: SARC Publisher

Infrastructure-as-Code methodologies prove essential for maintaining consistency across regional deployments, complemented by automated testing frameworks that validate authentication workflows throughout all regions during implementation changes. Keycloak domain deployments derive substantial benefits from automated provisioning processes, as the intricate interdependencies between cluster components, load distribution systems, and database infrastructure create numerous possibilities for configuration errors when implemented through manual processes (Younes, S. 2021). Automation becomes increasingly vital in multi-cloud environments, where technical teams must orchestrate identity management deployments across heterogeneous infrastructure platforms while preserving consistent security controls and authentication experiences regardless of which regional hub processes any given authentication request (Shackleford, D. 2024).

Table 3: Implementation Considerations for Regional Hub Model (Younes, S. 2021; Shackleford, D. 2024)

Implementation Aspect	Complexity Factor
Hub Placement	Strategic
Synchronization	Critical
Monitoring	Essential
Automation	Fundamental
Multi-Cloud Support	Advanced

CONCLUSION

SASE architectures face substantial identity management hurdles due to distributed services, multi-tenant environments, and diverse corporate IDPs, complicated by needs for low latency, high availability, and extensive scalability. The Regional Hub Model for Keycloak addresses these challenges through strategically placed authentication clusters with operational autonomy. Regional hubs make everything faster, easier to manage, more adaptable to growth, and less prone to widespread outages. Getting this right takes work - choosing hub locations carefully, keeping configurations in sync, watching system health metrics, and automating routine tasks. For global SASE setups, though, the performance benefits make these extra efforts worthwhile. Organizations gain Keycloak's robust capabilities while navigating distributed environment constraints. Identity management increasingly shapes security posture, operational efficiency, and user experience as SASE adoption grows. The Regional Hub Model offers a practical architectural blueprint for Zero Trust implementation across globally distributed SASE frameworks, balancing performance and security requirements. Future implementations will likely refine this model further as SASE technologies mature and enterprise authentication requirements continue to evolve.

REFERENCES

1. NordLayer, "SASE Benefits and Challenges." https://nordlayer.com/learn/sase/benefits-and-challenges/
2. Zscaler, "Understanding the Basics of SASE Implementation." https://www.zscaler.com/zpedia/understanding-basics-sase-implementation
3. Microsoft Ignite, "Secure networks with SASE, Zero Trust, and AI." (2025). https://learn.microsoft.com/en-us/security/zero-trust/deploy/networks
4. Check Point, "Best Practices for Successful SASE Deployment." https://www.checkpoint.com/cyber-hub/network-security/what-is-secure-access-service-edge-sase/best-practices-for-successful-sase-deployment/
5. Solo.io, "Zero Trust Solutions." https://www.solo.io/topics/security-and-compliance/zero-trust-solutions
6. Jain, P. "Identity and Access Management in the Cloud." *International Journal of Scientific Research in Computer Science Engineering and Information Technology* 11.2: (2025) 1528-1535, https://www.researchgate.net/publication/390008967_Identity_and_Access_Management_in_the_Cloud
7. Singla, D., & Verma, N. "Performance analysis of authentication system: A systematic literature review." (2023).
8. Murcia, J. M. B., Cánovas, E., García-Rodríguez, J., Zarca, A. M., & Skarmeta, A. "Decentralised identity management solution for zero-trust multi-domain computing continuum frameworks." *Future Generation Computer Systems* 162 (2025): 107479.

Publisher: SARC Publisher

9. Younes, S. "Installing and Configuring Keycloak - Domain Clustered Deployment." *Medium*, (2021). https://samer-younes.medium.com/installing-and-configuring-keycloak-domain-clustered-deployment-fe941146d3c4
10. Shackleford, D. "Multi-cloud identity management tips and best practices." *TechTarget*, (2024). https://www.techtarget.com/searchsecurity/tip/Multi-cloud-identity-management-tips-and-best-practices

Source of support: Nil; **Conflict of interest:** Nil.

Cite this article as:
Shanmughan, V. K. "Keycloak Implementation for Identity Management in SASE Architectures: A Regional Hub Approach" *Sarcouncil Journal of Multidisciplinary* 5.7 (2025): pp 1001-1007.

Publisher: SARC Publisher