WHITE PAPER

A Guide to WSO2 Identity Server

By WSO2 IAM team

April 2019

Table of Contents

1. Why Identity and Access Management?

Identity and access management (IAM) is the efficient integration and management of identities, giving users access to the right resources at the right time. Identity is no longer a mere security project for enterprises. In the integration and API domain, as businesses continue to increase the number of internal and third-party APIs, it's more important than ever that APIs are integrated and governed securely. In the user domain, with increasing user identity spaces, company-wide policies, complex structure hierarchies and roles, regulatory pressures, and customer-facing applications, security becomes a bigger challenge each day for identity architects and administrators.

WSO2 Identity Server aims to address both API and user domains while providing an enhanced user experience as part of WSO2's open source Integration Agile Platform. It's a highly extensible IAM product, designed to secure APIs and microservices and enable Customer Identity and Access Management (CIAM).

2. Challenges Faced in IAM

In addition to user access management, the application, container, microservices, and integration spaces have grown in complexity and become more decentralized. The challenges for identity management to secure these models have also increased. For example:

- **Complexities created by identity silos:** Heterogeneous and/or distributed applications in an enterprise that use different access mechanisms can create multiple identity silos. This causes secondary complications for IT admins, such as the inability to extend or integrate new applications and users and consistently enforce enterprise-wide security policies.

- **Securing the increasing numbers of APIs and endpoints:** Businesses are increasingly exposing their APIs. As a result, the IAM system in place should be able to effectively integrate and secure these APIs. As new threats and vulnerabilities are created every day, security plays a pivotal role in protecting APIs from attacks. While an API manager can help to a certain extent (e.g., API blacklisting and throttling), an IAM solution is far more instrumental in providing a holistic approach to securing APIs.

- **Difficulties encountered by account management:** With the proliferation of users and distributed workforces, IT security admins find it difficult to manage access controls side-by-side with role changes. It is also difficult to maintain a satisfactory user experience for employees who connect to enterprise applications while balancing security and control.

- **The burden of user password maintenance:** IT admins spend a large amount of time on password and account recovery. Most often, users find it difficult to recall their passwords and manage multiple identities/profiles that are used to access different applications. This leads them to constantly reach out to admins for support, which, in turn, results in operational and time inefficiencies.

- **Varying compliance challenges:** Differing IAM approaches and silos add complexity when trying to comply with regulations such as the General Data Protection Regulation (GDPR), second Payment Services Directive (PSD2), and electronic IDentification, Authentication and trust Services (eIDAS).

- **Burdensome licensing and software costs to implement IAM solutions:** Proprietary software carries heavy licensing costs and start-up burdens. WSO2 Identity Server is designed to solve these challenges through each of its core capabilities. Given its extensible framework and interoperability, the product provides business benefits that include an enhanced customer experience and improved employee productivity in enterprises through agile IAM.

3. Introduction to WSO2 Identity Server

WSO2 Identity Server, a part of the WSO2 Integration Agile Platform, is an open source IAM solution that facilitates single sign-on (SSO) between applications and federates identities between multiple heterogeneous systems. It's optimized for securing APIs, microservices, and customer IAM projects.

It offers enterprise-grade capabilities, such as identity federation, SSO, strong and adaptive authentication, account management, and identity provisioning, to help digital-native organizations become integration agile through CIAM and API security.

WSO2 Identity Server is based on open standards and open source principles, enabling freedom from vendor lock-in and velocity to innovation. The product comes with seamless, easy-to-use integration capabilities that help connect applications, user stores, directories, and identity management systems.

Quick checklist when choosing an IAM vendor

- Provides authentication mechanisms with high usability such as adaptive authentication
- Supports open standards and protocol support such as SAML2, OAuth2, and OIDC
- Integrates and enables bridging with heterogeneous IdPs and systems
- Helps integrate apps in an identity ecosystem
- Accommodates cloud vs. on-premises deployments or interconnectivity
- Supports large-scale deployments
- Enables freedom from platform and vendor lock-in implications
- Governance model of open source business friendliness: Apache 2.0
- Allows ease of extension and customization
- Provides commercial support: Low cost trials, PoCs

4. Capabilities of WSO2 Identity Server

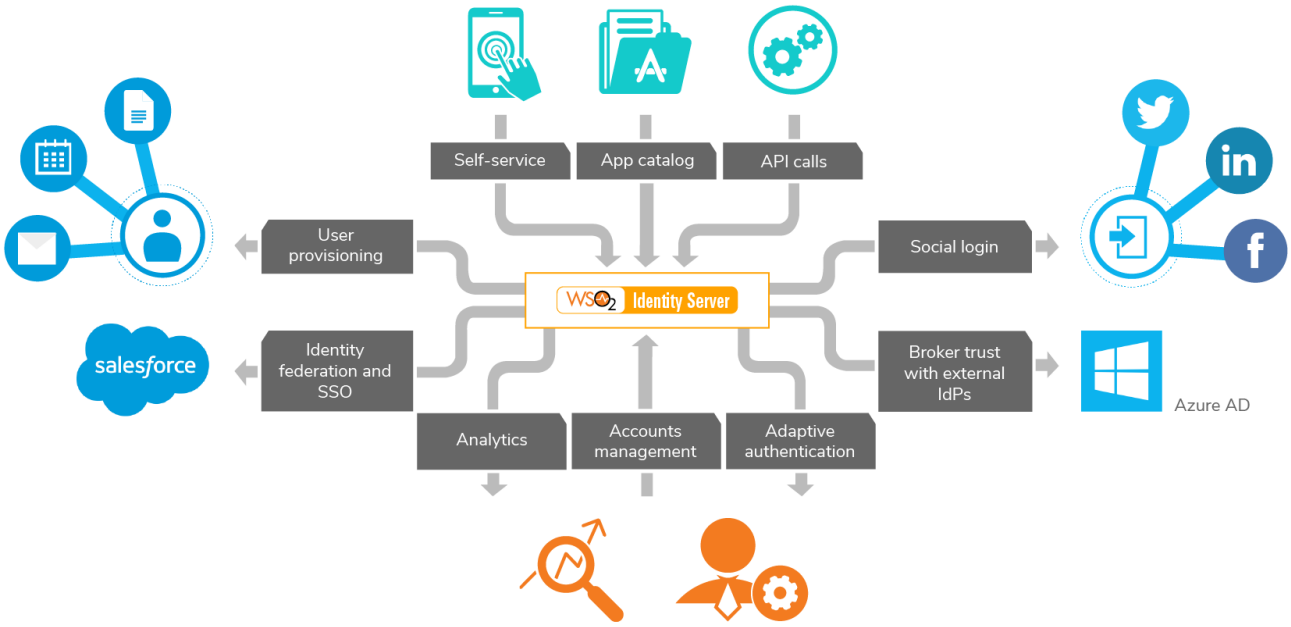

Figure 1 - Block diagram of IAM functionality

Identity Federation and SSO

Business users typically access multiple heterogeneous applications and identity providers (IdPs) that their systems need to integrate with. WSO2 Identity Server alleviates working with identity silos through the ability to connect Java Database Connectivity (JDBC), lightweight directory access protocol (LDAP), or Active Directory (AD) user stores and enforce role- or attribute-based access control with eXtensible Access Control Markup Language (XACML), since user stores alone cannot enable SSO.

Having to fill a form to sign up as a user or having to sign in multiple times creates an unfavorable user experience. Identity federation allows bring your own identity (BYOID) or social logins to access applications and systems. SSO offers the ability to stay signed in to multiple applications. This also includes rule-based authorization support and Google ReCaptcha support for SSO. WSO2 Identity Server offers these capabilities, as well as single logout (SLO) via Security Assertion Markup Language 2.0 (SAML2), OpenID Connect (OIDC) and WS-federation passive, and federated SSO with external providers. With WSO2 Identity Server, you can also integrate with Azure AD, Microsoft 365, and other MS

applications with the use of standards such as OIDC for user provisioning. With Microsoft 365, the product can be used to provide SLO and cloud synchronization.

Strong and Adaptive Authentication

Authentication is the process of validating a user's identity before granting access to a resource. Strong authentication involves multi-step and multi-option with local and federated authenticators such as FIDO, IWA, SAML2, OIDC, MePIN, email/SMS OTP, and Duo security.

Adaptive authentication with WSO2 Identity Server enables authenticating a user by considering the context factors, such as user's risk profile/behavior, identity attributes, environmental attributes, device type, geolocation, machine learning algorithms, and request parameters.

With WSO2 Identity Server, an identity admin is able to use ready-made scripting templates to take complete control of the authentication flow to implement adaptive authentication. This includes enforcing rules, attributing transformations, using provisioning/deprovisioning, communicating with external systems, implementing step-up authentication, and more. Based on a user's context, the authentication sequence changes, providing better usability.

Figure 2

Biometrics are rising in demand as mobile sims can be cloned. WSO2 Identity Server provides federated authentication with biometrics through Veridium, Aware Inc, and other providers.

Identity Bridging

Identity bridging facilitates exchanging identity attributes and authentication decisions between heterogeneous identity systems and protocols in a seamless manner. This includes bridging tokens (OIDC, SAML2, and WS-Federation), service provider claims to IdP claims (email addresses, phone numbers, and names), and identity provisioning requests (from SCIM and SOAP to SCIM, Google apps, and Salesforce).

Account Management and Identity Provisioning

End users can manage their own profiles and set account recovery options in a self-service manner. WSO2 Identity Server supports inbound, outbound, and just-in-time (JIT) user provisioning. These features efficiently, cost-effectively, reliably, and securely help organizations manage user information held on multiple systems and applications.

In terms of managing users and groups, WSO2 Identity Server helps with flexible profile management. This includes the ability to link multiple user accounts belonging to a single user, a self-service user portal for profile management, and password management with Google Recaptcha.

Through account management, WSO2 Identity Server offers support for heterogeneous user stores through a built-in LDAP (powered by ApacheDS), an external LDAP, Microsoft Active Directory, or any JDBC database.

Identity provisioning features can be used to propagate user identities across different software as a service (SaaS) providers. Users and groups can be provisioned to external IdPs using SCIM 2.0, and identities can be created on the fly with JIT provisioning.

Access Control

This controls access to applications in the login flow, with fine-grained access control policies, and acts as a policy decision point for third-party applications. It also helps with managing user entitlements and role-based access control. In this instance, XACML is used as a basis for fine-grained policy-based access control, user-friendly policy administration (PAP), REST profile support, and easy integration with WSO2 Enterprise Integrator.

APIs and Microservices Security

Securing APIs that are being exposed using OAuth2 access tokens and associated grant types including access control APIs. OAuth2 being a key standard, WSO2 Identity Server offers OIDC support, introspection and form post response mode. The product also provides user-managed access and delegated access control using OAuth2.

WSO2 Identity Server easily integrates with WSO2 API Manager for OAuth2 Key Management. WSO2 API Manager, a part of the WSO2 Integration Agile Platform, is an open source solution that addresses full API lifecycle management, monetization, and policy enforcement. WSO2's offering made the company the only open source vendor to be named a leader in The Forrester Wave™: API Management Solutions, Q4 2018 report.

As for microservices, WSO2 Identity Server offers microprofile JWT 1.0 support for role-based access control and SAML2, JWT assertion, and NTLM-IWA grant types.

Privacy Compliance

WSO2 Identity Server is optimized for privacy regulations such as GDPR, including implementing the Kantara consent management specification. This offers consent management for any application without being locked into a vendor. User consent includes self sign-up to provide consent and for SSO/federation to provide users with choice and control over sharing their personally identifiable information (PII). The product also offers a self-service portal to enable users to control their personal data, manage consent declarations, or make any other changes.

The privacy toolkit is instrumental in removing references of user identity as and when required or when requested by a user.

Identity Analytics

The product is equipped with powerful monitoring and analytics tools to keep track of the enterprise IAM system's health when it is deployed in production. The analytics system is capable of generating and analyzing login attempts made via WSO2 Identity Server. In addition, the analytics system is also capable of generating and analyzing information relating to specific sessions that have taken place via WSO2 Identity Server, helping to monitor and prevent fraudulent activity. It can help with manually terminating user sessions and admin-forced password resets.

5. Other Benefits of Using WSO2 Identity Server

Customization to support complex IAM use cases, with an extensible, open source architecture

Each enterprise faces unique identity-related challenges such as integrating user stores, adhering to compliance requirements that come with privacy standards or implementing an authentication system. Whatever the requirement, WSO2 identity Server offers an extensible architecture, with a user store of 40+ connectors, that gives the ability to write custom extensions that enterprises can own. This extensibility also provides authentication and provisioning connectors. Customers such as Nutanix and West Corporation use WSO2's product for the extensibility it offers.

Low-risk scalability to fit any need or use case

Scalability is important to ensure that an IAM product can load balance and accommodate a large number of logins or users. WSO2 Identity Server currently manages 75mn identities and more for enterprises such as Trimble, State of Arizona, Express (retail) and more.

Simplify integrations with a rich connector ecosystem/large identity ecosystem

WSO2 Identity Server also provides a wide array of ready-to-use connectors that can be used to connect with cloud and other third-party systems to build tailor-made solutions. This helps to write custom extensions, based on the third-party application enterprises, and enables quicker integrations, with out-of-the-box compatibility with cloud and on-premises applications, third-party authentication systems, and social IdPs.

Part of a complete integration platform

WSO2 Identity Server is also a part of the WSO2 Integration Platform that includes WSO2 Enterprise Integrator and the WSO2 API Manager. The platform comprises components required for the digital transformation of an enterprise in an API-driven world. Such an example is CIAM, where these components come together to bridge all customer identities and applications to provide an insightful experience.

Deployment options

- On-premises
- Public or private cloud

Deployment infrastructure

- Bare metal hardware
- Virtual machines
- Containers

All these options come with the same seamless developer and IT personnel experience.

6. Customer Case Studies

Nutanix

WSO2 Identity Server is used to provide a seamless experience for different portals and apps via SSO and identity federation to make the user experience simple.

West Corporation

The company built a CIAM platform to connect all solutions, resulting in a “connected customer experience”. This was done by using various capabilities such as SSO and federation supported by SAML2, OAuth2, OpenID, and WS-Federation provided by WSO2 Identity Server. The solution also includes the full WSO2 platform to bring all distributed silos into a unified presentation.

Al Elm

Al Elm implemented SSO with WSO2 Identity Server to streamline administration, improve productivity, and lower costs. The solution currently manages 4 million users in the Unemployment Assistance Program and ensures secure online transactions.

Brigham Young University (BYU)

BYU replaced its API management systems with more modern, standard, and efficient solutions: WSO2 Identity Server and WSO2 API Manager. BYU modernized their API management system using WSO2's API management and identity and access management capabilities. After the introduction of the new solution, BYU experienced higher API consumption. Furthermore, the transition also gave BYU access to monitoring and analytics capabilities.

This helped to improve consumer experiences and minimize the impact on existing development work.

ITDT Services

WSO2 Identity Server was used to achieve GDPR compliance, create identity management infrastructure, and achieve the required level of security in Greek municipalities. Following the success of this project, plans are now in place to expand this identity management platform and deploy it in other municipalities in Crete.

Symcor

After experimenting with several products, Symcor used WSO2 Identity Server to customize its SSO process. The new platform features both WSO2 identity and access management and WSO2 API management technology.

Swiss Alpine Club

The Swiss Alpine Club wanted to provide easy access to all its users. The club wanted to achieve this by providing a single identity login option, SSO, and easy onboarding, and by enabling users to self-manage their profiles. WSO2 Identity Server, along with WSO2 Enterprise Integrator, helped to achieve these goals. This resulted in the ability to de-couple legacy systems and implement both SSO and single identity login, improving the user experience across the platform.

7. Conclusion

WSO2 is the leader in open source IAM that provides advanced capabilities for securing APIs and CIAM. Features also include identity federation, SSO, strong and adaptive authentication, and privacy compliance. While many identity platforms provide multiple products per capability, WSO2 Identity Server is a single solution for common identity requirements. The product's open source nature attracts fortune 500 customers owing to the freedom from vendor lock-in. Read our white paper on the benefits of open source IAM here. WSO2 Identity Server is also extensible as it can be customized as per any unique need. It also helps that WSO2 Identity Server is a part of a larger integration platform, so users can opt for API management or an ESB capabilities that can easily integrate with our identity solution.

If you want to try out WSO2 Identity Server, you can explore our comprehensive documentation and tutorials here and more on IAM design principles here.

8. References

[1] https://wso2.com/library/articles/2017/08/what-is-wso2-identity-server/

[2] https://www.youtube.com/watch?v=ZnWnDZJ_c4o

[3] https://wso2.com/library/articles/2017/02/six-business-benefits-of-identity-and-access-management/

About WSO2

WSO2 is the world's #1 open source integration vendor, and a Leader in the Forrester Research API Management Wave Q4 2018 report. We help digitally driven organizations become integration agile; customers choose us for our integrated platform, our approach to open source, and our agile transformation methodology. Today, 100's of leading brands and 1,000's of global projects execute 5 trillion transactions annually using WSO2 integration technologies. Visit https://wso2.com to learn more.