objectstyle

IAM System for Sports League

ObjectStyle creates a company-wide Identity and Access Management (IAM) system for a large sports organization

Industry	year founded	location
Sports & Media	Late 1910's	USA

The client is a major sports league in the U.S. The organization consists of a number of departments that together use around 150 in-house software products.

ObjectStyle has been working with the league since 2002 and currently supports many of its internal business apps and public web properties.

Challenge

When ObjectStyle was commissioned for this task, there were multiple login systems in use at the organization. Some were legacy, and many did not comply with modern security standards.

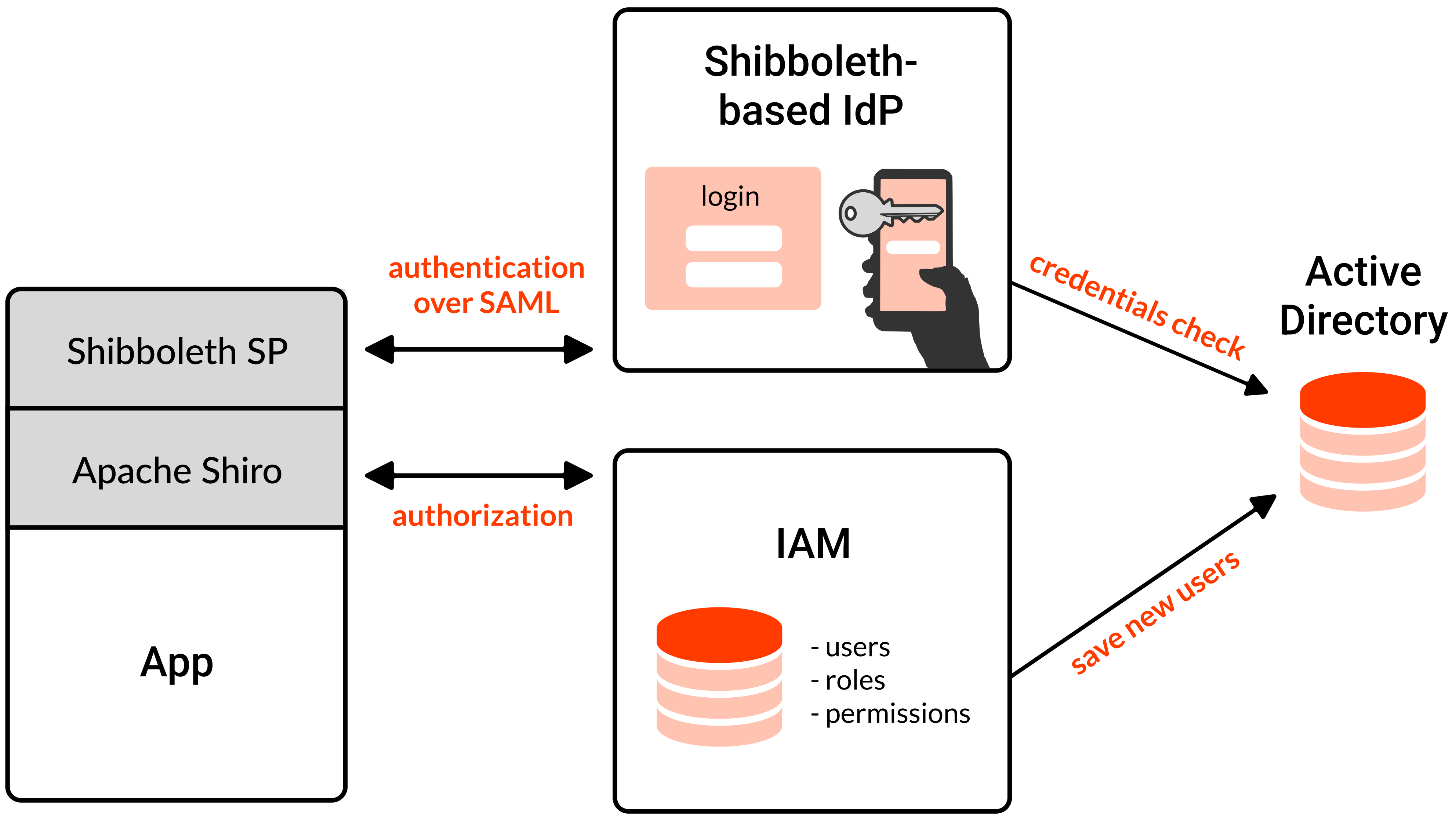
When ObjectStyle began the redesign of the client's old platform as a part of another project, it became obvious that the league needed a more modern, interoperable IAM model. The idea was to make it easier for administrators to manage user access across applications and to tighten security.

Solution

The architectured solution dealt with both authentication (verifying that you are who you say you are in the system) and authorization (verifying that the user is allowed to do what they're trying to do in an application).

ObjectStyle picked Shibboleth, an open-source authentication solution, to handle authentication over the SAML protocol. The apps themselves no longer required access to sensitive user data, which significantly reduced potential *attack surface*. To perform *two-factor authentication*, including *token-based verification*, we integrated a third-party solution that interacts with the system from outside of our client's network.

User data lives in a unified Microsoft Active Directory. The directory supplies data for the IAM and some other services (e.g., a 2-factor authentication provider). The IAM module knows about all users and what they are allowed to do in various applications.



ObjectStyle used the Apache Shiro framework to implement the process of verifying user permissions for a given app. After a user is authenticated, the Shiro layer requests authorization info from the IAM service and grants or forbids the user access to specific features.

Apache Shiro isolates apps from IAM system details. This way, apps work in a security context where they only interact with Shiro and can't see past the Shiro layer.

1. Storing identity profiles.

All employee profiles are now stored in Microsoft Active Directory. The directory is used as a source of user profiles by every other service, like IAM or our client's third-party authentication service. Active Directory is also the only place where user credentials are stored, and every password check in the system occurs over AD.

2. Enabling single sign-on.

Employees now use only one authentication ("login") form to gain access to all apps they are authorized to use. In the apps, they are able to view and use only the features that are made available by the administrator.

3. Roles and permissions.

System administrators can now create roles (e.g., “accountant”) and assign permissions that should be associated with each role (e.g., a permission to view all information within the app pertaining to a single team). In many instances, administrators can go as granular as disabling particular tabs/buttons/features for a role.

4. Inviting people from outside the organization.

The new system allows admins to give third parties (advertising partners, contractors, etc.) access to selected applications. A partner receives an email, clicks the confirmation link, fills in their information, and gets registered in the IAM system.

5. Audit logging.

The system keeps a chronological record of actions performed by system administrators. This is done for security purposes (to tell suspicious behavior from legitimate admin work) as well as in order to evaluate the work of said administrators.

Results

Today, close to a hundred of our client’s apps use the new identity management system. This means that on-boarding new employees and giving them access to the necessary resources has become much simpler. Also, managing the system and its constituent parts has become a lot easier.

Technology stack

- Active Directory
- Shibboleth
- MySQL database
- React JS
- Java
- Agrest.io
- Link Move
- Apache Cayenne

Time Span and Resources

Duration:	N/A – not disclosed
Effort:	N/A – not disclosed

https://www.objectstyle.com/case-studies/sports-identity-and-access-management-system