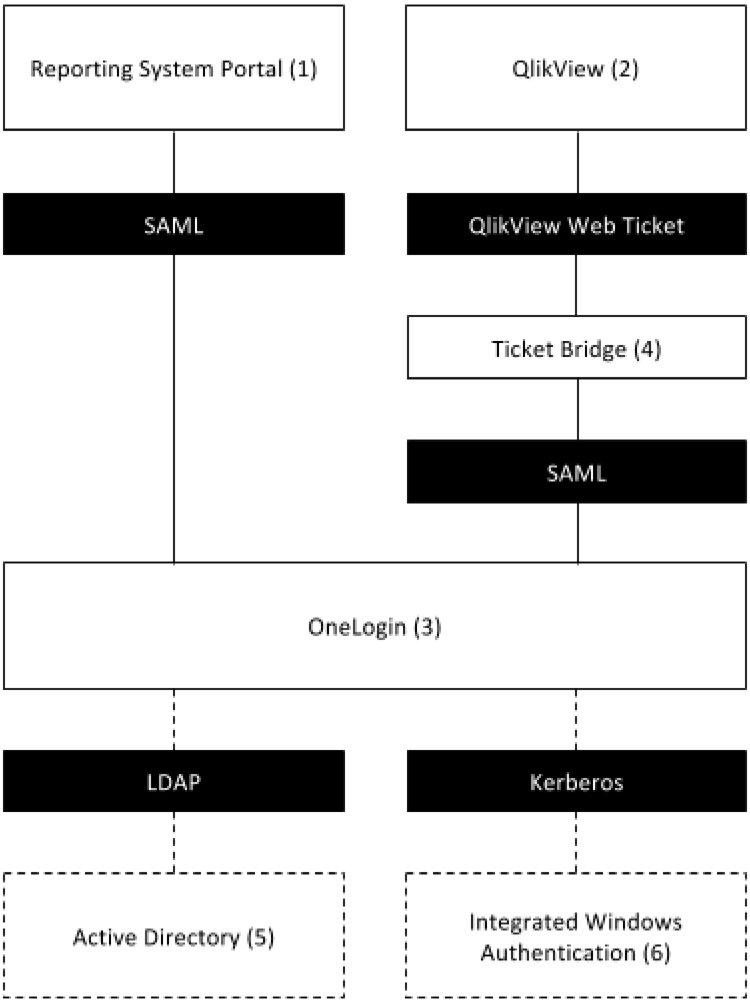
Reporting System Portal
User Authentication & Authorization

Situation and requirements

Akelius uses QlikView for business reports. Authorized users access the reports on a QlikView web server. A separate site, the reporting system portal, will provide information about and links to the reports in QlikView. User shall be able to move between those two sites in either direction without needing to log in a second time.

Information in QlikView has higher security requirements than information in the reporting system portal. Any solution must consider the systems that a hypothetical attacker could compromise to gain access to the QlikView information.

Proposed solution using OneLogin as a 3rd party identity provider



(1) Reporting System Portal

The reporting system portal will be a WordPress site that is initially hosted at Akelius' German datacenter. The web server is being used by Akelius to host several other sites and services, e.g. the public Swedish website.

It would be possible to use the WordPress user database for QlikView authentication. In this scenario, QlikView would redirect unauthenticated users to the WordPress login page. A custom extension to WordPress would issue QlikView Web Tickets to WordPress users so that they can seamlessly switch between WordPress and QlikView. While technically feasible, we do not recommend this solution for security reasons. A hypothetical attacker could try to compromise any website on the server to gain access to QlikView information.

The proposed scenario does not use WordPress authentication but OneLogin as an external identity provider. WordPress works with many external identity providers using many common protocols, e.g. SAML, OpenID, OAuth2. Due to the sizable user base of WordPress, identity providers usually make sure to test the compatibility of their interfaces with WordPress. OneLogin has sponsored development of the WordPress-SAML interface.

(2) QlikView

QlikView supports mainly two methods for third-party authentication and authorization:

1. QlikView Web Tickets: User and group information. This protocol is specific to QlikView and not a general standard.

2. HTTP header: Used with reverse proxies, e.g. CA Single Sign-On. Requires on-premise installation, specific server setup and firewall rules. Cannot transfer group membership information.

We propose using QlikView Web Tickets. Using an authenticating reverse proxy is possible as well, but it would require more coordination with TeleComputing during setup and the end result would be less flexible from both a technical and an organisational perspective.

For security reasons, we recommend issuing web tickets on the same server that hosts QlikView. A single page application is sufficient to do this. In this setup, there is no need to evaluate the security of a separate server that issues tickets.

(3) OneLogin

OneLogin is a 3rd party identity provider. We evaluated Okta and Ping Identity as well. Each of these identity providers has the required features for Akelius' requirements and offers reasonable prices. Each of these companies has been founded in recent years, but each of them has received substantial investments to develop their technology. Choosing OneLogin for this proposal is based on expected ease of implementation.

The proposal uses the following features of OneLogin:

- User authentication (username and password, optionally with multi factor authentication)
- A web interface to maintain the list of users and their groups

- SAML protocol for transferring authentication and authorization data
- Optional integration with Active Directory
- Optional automatic login for users who are signed in using their Akelius Windows account

Other identity providers instead of OneLogin can be used with only minor changes. SAML is a standard protocol that allows integration with e.g. Microsoft Active Directory Federation Services (not as flexible, especially for remote workers and non-Windows clients) or Microsoft Azure Active Directory (requires more initial effort).

(4) Ticket Bridge

The ticket bridge is a small application that is deployed on the same server as QlikView. QlikView redirects unauthenticated users to the ticket bridge. The ticket bridge uses SAML to interface with OneLogin. It redirects users to OneLogin, establishes their identity and group memberships. After successful authentication, a QlikView Web Ticket is issued and the user is redirected to the originally requested QlikView report. The whole process does not require any user interaction if the user is already authenticated at OneLogin, e.g. when arriving via a link from the Reporting System Portal.

A reference implementation has been created by QlikView:
http://community.qlik.com/servlet/JiveServlet/download/575956-117468/Customized%20Authentication%20v2%200.zip (in folder Examples / Webticket / SamlAuthentication)

For further reference, OneLogin provides a SAML Toolkit For C# And ASP.NET:
https://onelogin.zendesk.com/hc/en-us/articles/201175694-SAML-toolkit-for-C-and-ASP-NET

(5) Active Directory

OneLogin can synchronize accounts with Active Directory. To enable this optional functionality, TeleComputing would need to either install the OneLogin Active Directory Connector or allow LDAP access through their firewall.

If Akelius chooses not to synchronize Active Directory accounts, it is possible to maintain the list of authorized users directly using the OneLogin web interface.

(6) Windows Integrated Authentication

Using the OneLogin Active Directory Connector, it is possible to automatically sign in users who are logged into their Akelius Windows desktop, i.e. at the office. This means that those users will have to enter no password at all when accessing the Reporting System Portal or QlikView, since they already entered their password when signing in to Windows.

Comparison with other solutions

1. Users could log in twice
   This might not be as inconvenient for users as it seems: The Reporting System Portal could have long-lived user sessions. Users would authenticate once on each device and remain signed in for months without having to reauthenticate. The security risk might be acceptable, since the portal will not store highly confidential information. If only a few users would access QlikView and the Reporting System Portal, maintaining two separate user directories might be feasible. This solution requires the least implementation effort. It is least maintainable as well.

2. Active Directory and Windows Integrated Authentication
   Using Windows Integrated Authentication requires medium effort and provides optimal maintainability and convenience. There would be no single sign on for users outside the Windows domain, i.e. on tablets or using computers outside the firewall. HeyPragmatic has experience with Kerberos single sign on and even Akelius' Swedish LDAP configuration, since we have developed connectors using both for the Construction Module.

3. Issue QlikView Web Tickets on the Reporting System Portal
   User accounts would be maintained in WordPress. This solution requires medium effort. Security depends on the security of the WordPress installation. If this is acceptable, then we recommend this solution.

4. Reverse Proxy Authentication
   After TeleComputing sets up CA Single Sign-On, IBM Security Access Manager for Web or a similar reverse proxy, this solution requires low effort and is very maintainable. If TeleComputing has experience with such deployments, we recommend this solution.

5. 3rd party identity provider
   Described above. This solution provides good maintainability. It is very flexible and can be used to provide identity to other web applications as well, e.g. the Akelius Construction Module or SaaS services. Recommended if Akelius plans to use additional SaaS (cloud) services or if solutions 3 and 4 are rejected.

Risks and downsides of using a 3rd party identity provider

- Setting up OneLogin means using a big chunk of infrastructure to solve a straightforward problem. The problem may not be worth the effort.

- HeyPragmatic has no direct experience with either OneLogin or QlikView. We have experience designing large scale identity systems. At Akelius, we have implemented Kerberos single sign on and interfaces to Akelius' German and Swedish Active Directory forests via LDAP for the Construction Module.

- Authenticating users via OneLogin means that the security of QlikView information depends on the security of OneLogin. Since security is their business, it seems likely that they will consider security a priority.

- OneLogin is a young company that could encounter operational problems or that might even shut down completely. It has received investments of USD 17.7 million, so it has the resources to continue developing a robust identity provider. If OneLogin would should down, replacing it with a competitor's product would be rather simple, since the interface is implemented using SAML, an open and common standard.

- It might not be feasible to finish setup of OneLogin and the Ticket Bridge in 2014.

Next steps

- Can TeleComputing setup reverse proxy authentication using CA Single Sign-On or a similar product? They might have the infrastructure in place.

- Decide whether to use OneLogin. Can Netlight develop the Ticket Bridge using the reference implementation given above?