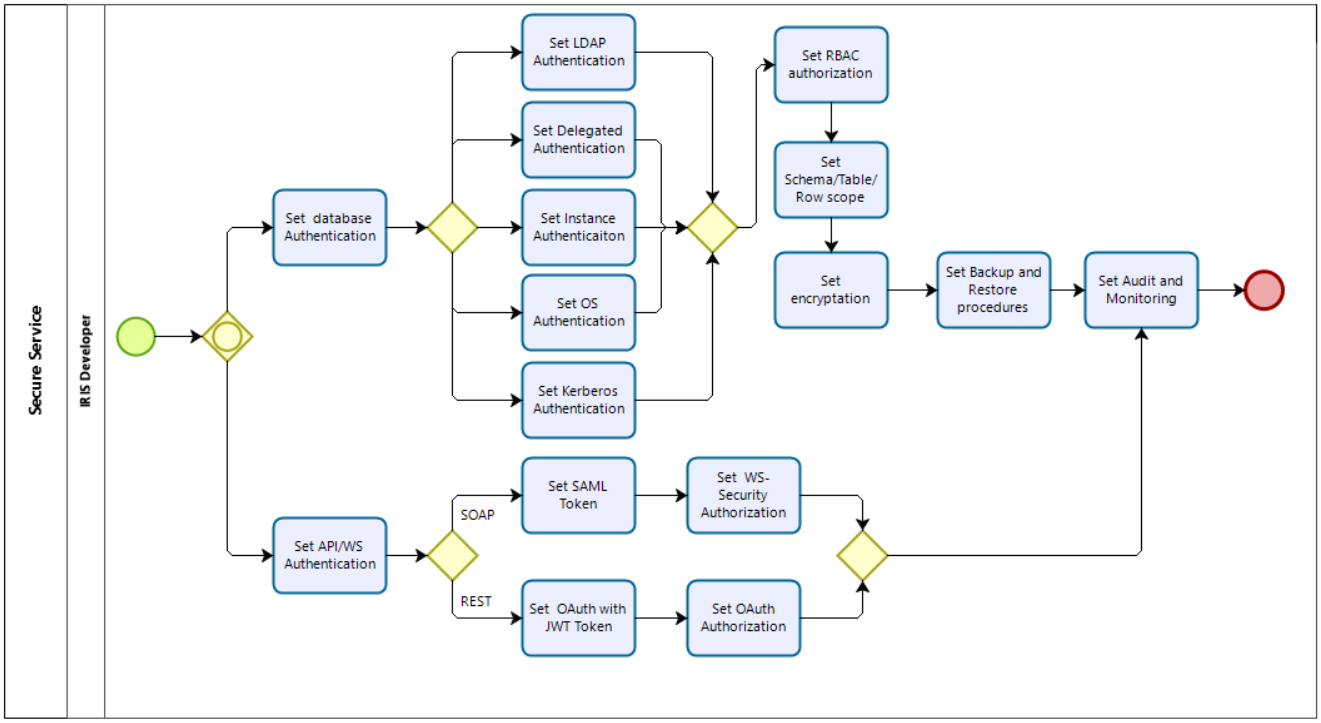
Article
Yuri Marx · Dec 27, 2020 2m read

Secure IRIS Digital Services



The InterSystems IRIS has two major paths to a digital service: API/Web Service into Interoperability module and multimodel Database/Analytics. Each of them has your security configuration.

To do API security you apply an OAuth or JWT plug-in to the API endpoint. So in the Admin Portal, API producer and consumers get the keys to authenticate the API and consume it. The Admin Portal allows you configure RBAC policies too.

To do WS security the best strategy is to use SAML. In the inbound/outbound SOAP message, include X.509 certificate, with a SAML assertion, and include to your WS-Security header.

It is possible encrypt the API and WS messages too.

To the database/analytics services is a good strategy map the database users to your LDAP corporate user repository, to promote SSO (single sign on), but is possible implement a custom class to authenticate, known as delegated authentication. It is possible use IRIS Instance authentication too, managed by IRIS, associated with OS authentication, hash authentication and two factor authentication (Time-based one-time password or SMS). The authentication using OS, can use Kerberos.

Defined the authentication, the authorization can be configured following the RBAC model, with the option to restrict access at Schema, Table and Row (RLS), with the option to configure in the Admin Portal the resources to be protected using RBAC model. Can be implemented fine grained authorization rules, using method classes

callbacks (%SecurityPolice) in the persistent classes.

An additional procedure to the data security is encrypt the database or a data element (custom development).

Another best practice is configure backup/restore procedures. There are four possible strategies, external backup (full copy) and online backup (IRIS.dat files only, with full, cumulative or incremental options), cold backup (external with database in a offline status) and concurrent backup (dirty backup - no interruption based into increment copy to be consolidated).

To complete the security to the IRIS digital services is necessary configure the database audit and monitoring. The audit can be enabled in System Administration > Security > Auditing and capture user, IP, event source, the event and other important information. To the API can be configured an audit plug-in. To Web Services can be used the production trace.

To monitor the API, use IRIS API Admin Portal, to Web Services and Database use the Management Portal.

The InterSystems IRIS has 3 monitors to support audit/monitor: Diagnostic Report, Log Monitor and System Monitor. An excellent tool to complete the toolset is the SAM - System Alerting and Monitoring (SAM). It can monitor and create alerts to your all clusters and is based into excellent monitoring tools (Grafana, AlertManager, Prometheus and NgInx).

#Security #InterSystems IRIS