SailPoint

< Developer Days2024 >

</title>

Extending Sailpoint Object Model

</title>

Speaker: Kamil Jakubiak;
title: Security Consultant;
company: Ventum Digital Identity Services;

SailPoint CERTIFIED IdentityIQ Architect

SailPoint CERTIFIED IdentityNow Engineer

SailPoint CERTIFIED IdentityIQ Engineer

Agenda

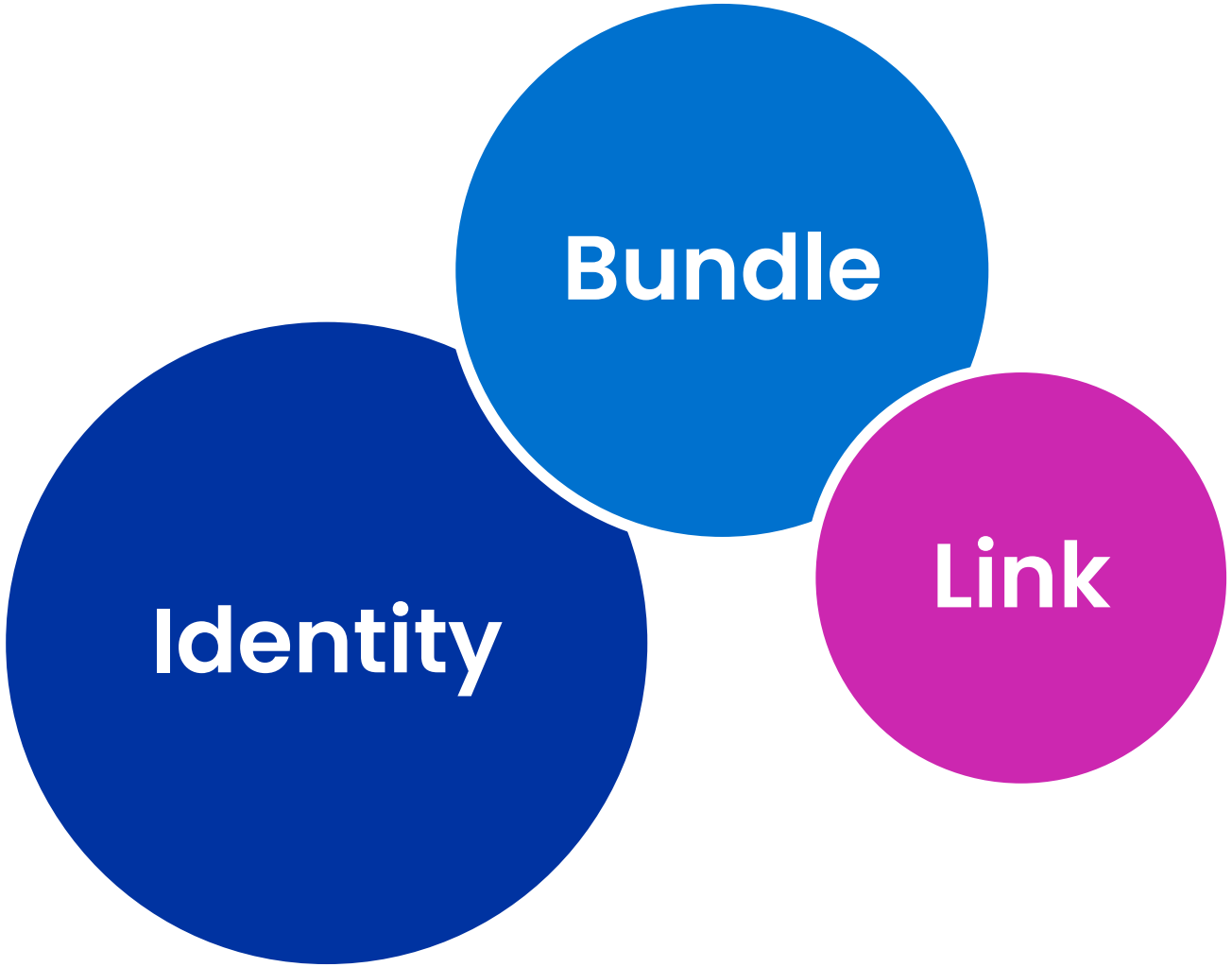
Standard IIQ Objects	What is available in IIQ out of the box?
Business Application	Designing custom Business Application
Why? How? When?	Use case scenarios for extending objects
Risks and benefits	Key risk and benefits considerations
Summary	

Standard IIQ Objects

What is available in IIQ out of the box?

Object-Relational Mapping

HIBERNATE



Types of objects

Do you know how many types of objects is available in IIQ?

Is this number closed?

Identity

Main object used to describe individuals.

Managed Attribute

Atomic permission or entitlement in the target system

Bundle

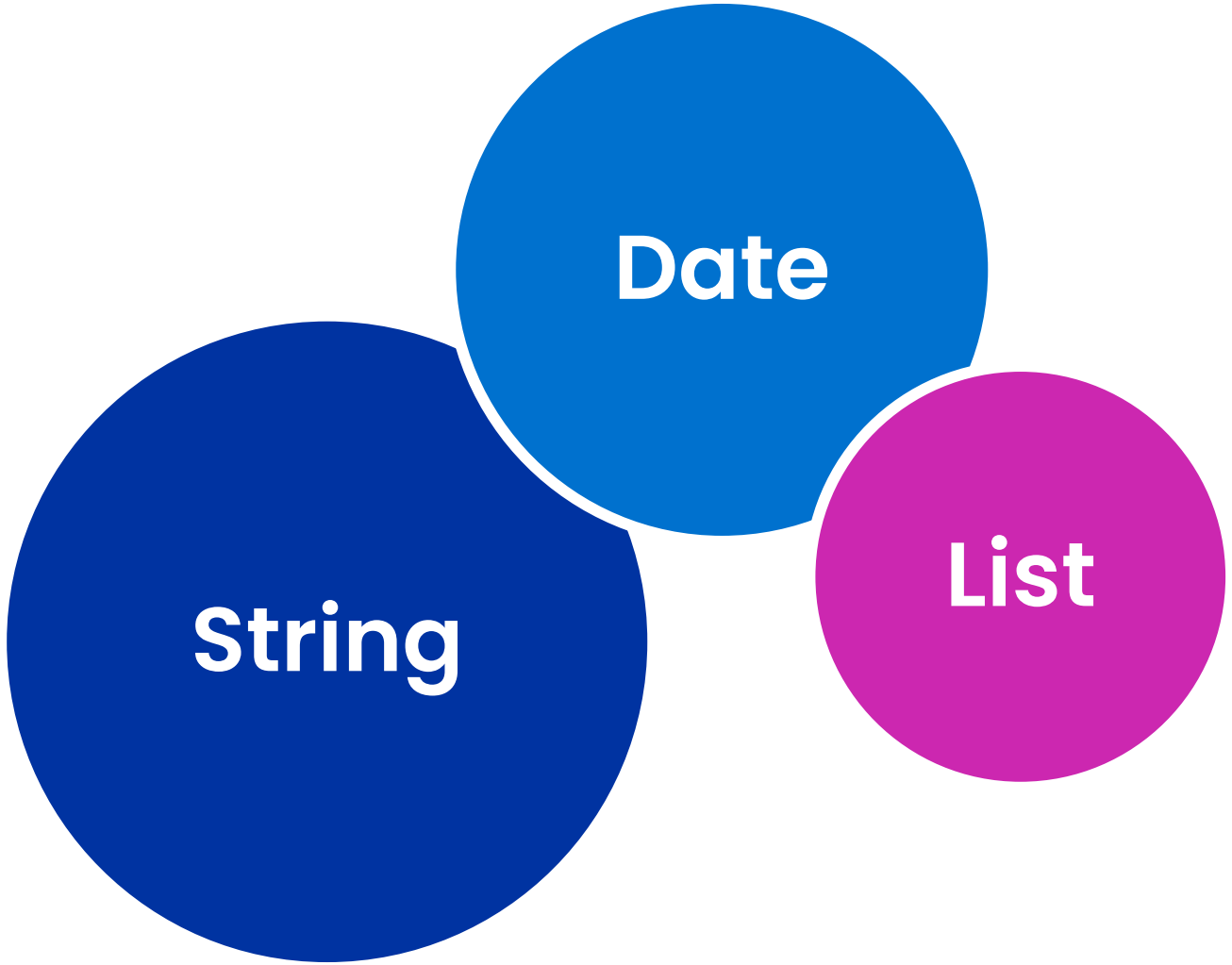
Role – used to aggregate set of permissions

Location

This one does not exist – we will create it

TODAY

OotB Limitations



Business Application

Designing custom Business Application

Business Application

Business software (or a business application) is any software or set of computer programs used by business users to perform various business functions. These business applications are used to increase productivity, measure productivity, and perform other business functions accurately.

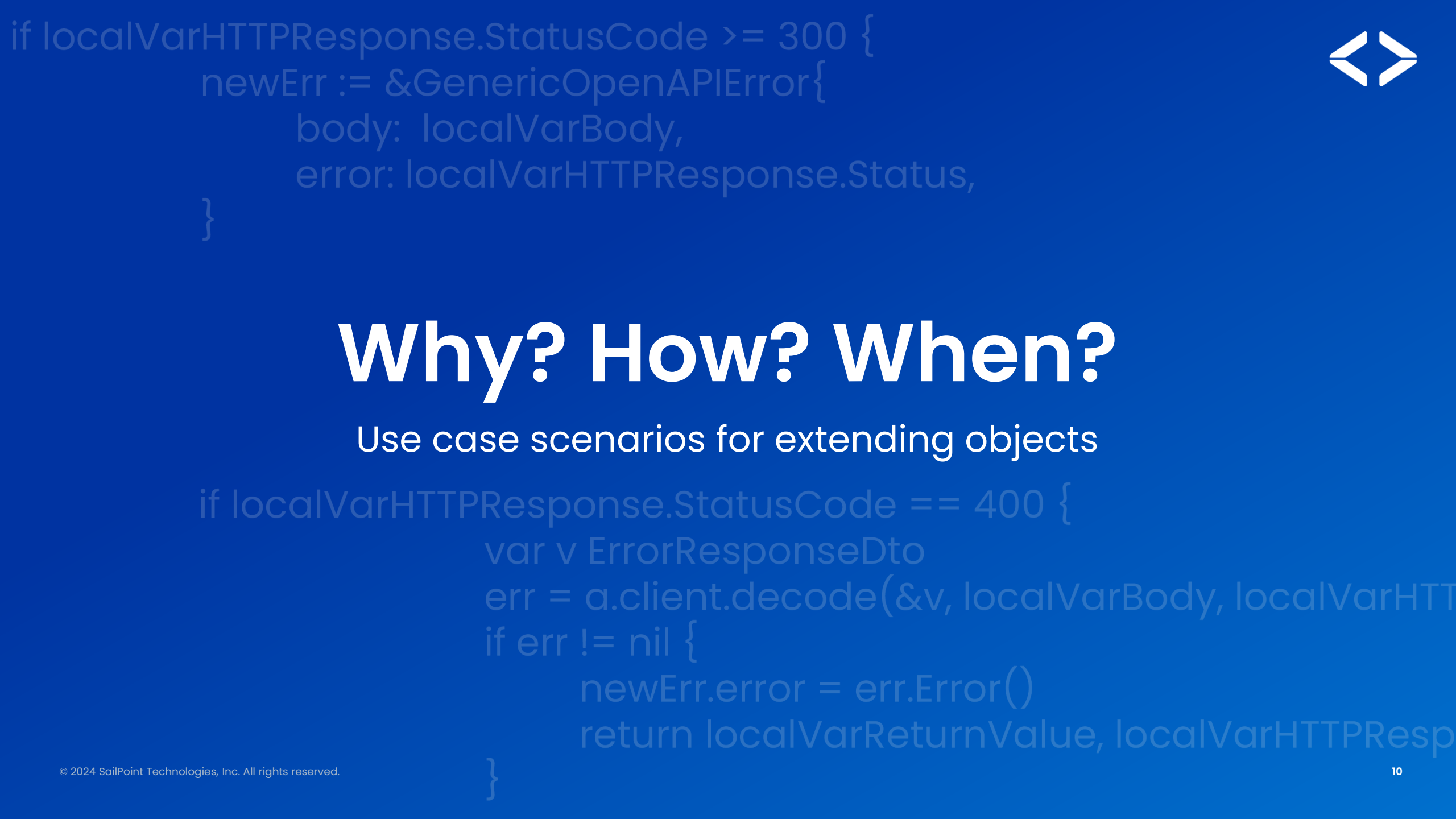
Wikipedia

Our Business Application

- Application Owner
- Application Custodian
- CMDB ID

- Approvers Group
- Approval Mode

- Severity
- Criticality



Why? How? When?

Use case scenarios for extending objects

Step 1 – Prepare Data Model

```java
package developer.days.sailpoint.object;
import sailpoint.object.SailPointObject;
import sailpoint.object.Identity;

public class BusinessApplication extends SailPointObject {

    private static final long serialVersionUID = 1L;
    private Identity custodian;
    private Identity approversWorkgroup;
    private String cmdbId;
    private String approvalMode;
    private String severity;
    private String criticality;

    private String approvalMode;

    public static long getSerialversionuid() {
        return serialVersionUID;
    }
    public Identity getCustodian() {
        return custodian;
    }
    public void setCustodian(Identity custodian) {
        this.custodian = custodian;
    }
    public Identity getApproversWorkgroup() {
        return approversWorkgroup;
    }
    public void setApproversWorkgroup(Identity approversWorkgroup) {
        this.approversWorkgroup = approversWorkgroup;
    }
    public String getCmdbId() {
        return cmdbId;
    }
    public void setCmdbId(String cmdbId) {
        this.cmdbId = cmdbId;
    }
```

/web/WEB-INF/classes/Sailpoint/object/BusinessApplication.hbm.xml

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE hibernate-mapping PUBLIC "-//Hibernate/Hibernate Mapping DTD 3.0//EN"
"http://hibernate.sourceforge.net/hibernate-mapping-3.0.dtd" [
<!ENTITY SailPointObject SYSTEM "classpath://sailpoint/object/SailPointObject.hbm.xml">]>

<hibernate-mapping>
  <class name="developer.days.sailpoint.object.BusinessApplication">
    &SailPointObject;
    <many-to-one name="custodian" class="sailpoint.object.Identity"/>
    <many-to-one name="approversWorkgroup" class="sailpoint.object.Identity"/>
    <property name="cmdbId" type="string" length="128"/>
    <property name="approvalMode" type="string" length="128"/>
    <property name="severity" type="string" length="128"/>
    <property name="criticality" type="string" length="128"/>
  </class>
</hibernate-mapping>
```

/web/WEB-INF/classes/hibernate.cfg.xml

```xml
<mapping resource="sailpoint/object/WorkItemConfig.hbm.xml"/>

<!--  Begin of custom IIQ objects -->
<mapping resource="sailpoint/object/BusinessApplication.hbm.xml"/>
<!--  End of custom IIQ objects -->
```

Step 2 – Generate Database DDLs

Use IIQ Console Schema Generator

```
root:/opt/tomcat/webapps/identityiq/WEB-INF/bin#
cp BusinessApplication.class webapps/identityiq/WEB-INF/classes/developer/days/sailpoint/object/.

root:/opt/tomcat/webapps/identityiq/WEB-INF/bin# ./iiq schema
Home directory: /opt/tomcat/webapps/identityiq
Generating database scripts for mysql
Generating database scripts for postgresql
Generating database scripts for oracle
Generating database scripts for db2
Generating database scripts for sqlserver
```

DDLs Generated

```
create table identityiq.spt_business_application (
   id varchar(32) not null,
    created bigint,
    modified bigint,
    significant_modified bigint,
    owner varchar(32),
    assigned_scope varchar(32),
    assigned_scope_path varchar(450),
    custodian varchar(32),
    approvers_workgroup varchar(32),
    cmdb_id varchar(128),
    approval_mode varchar(128),
    severity varchar(128),
    criticality varchar(128),
    primary key (id)
) engine=InnoDB;

 alter table identityiq.spt_business_application
   add constraint FKnmhoyt3n2i442e6c4cqpv8u9v
   foreign key (owner)
   references identityiq.spt_identity (id);
```

Step 3 – First object creation

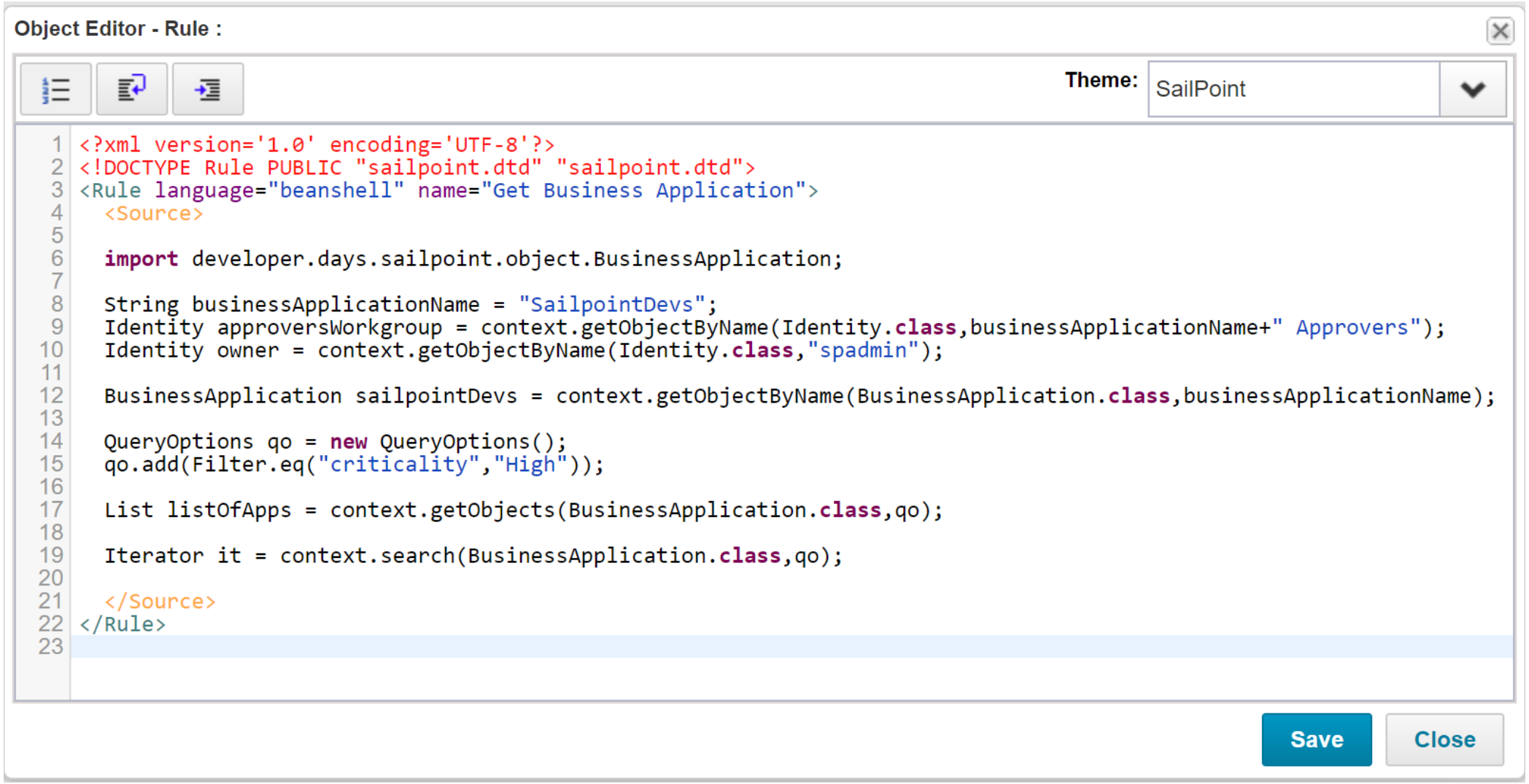
Object Editor - Rule :

Theme: SailPoint

```
<?xml version='1.0' encoding='UTF-8'?>
<!DOCTYPE Rule PUBLIC "sailpoint.dtd" "sailpoint.dtd">
<Rule language="beanshell" name="Create New Business Application">
  <Source>
  <![CDATA[
  import developer.days.sailpoint.object.BusinessApplication;

  String businessApplicationName = "SailpointDevs";
  Identity approversWorkgroup = context.getObjectByName(Identity.class,businessApplicationName+" Approvers");
  Identity owner = context.getObjectByName(Identity.class,"spadmin");

  BusinessApplication bA = new BusinessApplication();
  bA.setName("My new Business Application");
  bA.setOwner(owner);
  bA.setApproversWorkgroup(approversWorkgroup);
  bA.setApprovalMode("Manager, Owner");
  bA.setCmdbId("123456");
  bA.setCriticality("High");

  context.saveObject(bA);

  ]]></Source>
</Rule>
```

Save Close

Step 3 – First object usage



Task for excercise – Create Location Object

Required Attributes:
Street
Country
State
ZIP Code
Janitor

Challenge task*

Create location field in Identity model

Store location assignment in this field

```
if localVarHTTPResponse.StatusCode >= 300 {
        newErr := &GenericOpenAPIError{
                body:  localVarBody,
                error: localVarHTTPResponse.Status,
        }
```

Code Snippets

Link available in the meeting description

```
if localVarHTTPResponse.StatusCode == 400 {
                var v ErrorResponseDto
                err = a.client.decode(&v, localVarBody, localVarHTT
                if err != nil {
                        newErr.error = err.Error()
                        return localVarReturnValue, localVarHTTPResp
                }
```

Risks and benefits

Key risk and benefits considerations

Risk vs. benefit

Upgrades

- Be aware of HBM changes
- Thoroughly test patches and upgrades

Flexibility

- Create any object you need
- Complex structures available
- You can implement any requirement

Maintenance

- Object Management
- Object lifecycle
- Approvals

Real Life Use Case

Business Application based approvals

Differentiate connectors from Business Applications

Drive approval based on role business application

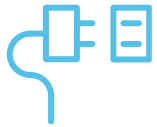
Delegated data owner for approving requests

Data owner vs. Data custodian

Yearly access certification

Summary

Why did I fell in love with IIQ?



Flexibility

- Customization capabilities
- „Open Universe”
- Everything is possible

Flexibility

The impossible I do immediatelly

miracles take a little longer.

[Thank you!]