

Onboarding Applications, Correlation, and Data Transformation

Fundamentals of IdentityIQ
Implementation

IdentityIQ 7.0

Overview

Onboarding Applications, Correlation, and Data Transformation

- Application and connector planning resources
- Defining non-authoritative applications
- Connectors / Application Types
 - Delimited File
 - JDBC
 - LDAP
 - Active Directory
 - Logical and Multiplex

Planning Resources for Onboarding

Planning Resources

Available on Compass

- Application

- *Application Onboarding Questionnaire*
- Helps ensure all information is gathered
 - Identify connectivity plan, data format
 - Identify entitlement data for requests and/or certification
 - Determine application dependencies, aggregation schedules

- Connector

- *SailPoint Functional Requirements* template
 - Gather connection parameters (username, password, host, port, etc.)
 - Collect schema details
 - Identify ownership for approval/certification responsibility

Planning

What information do we need?

- Accounts
 - Represent user identities who may sign into that system
- Attributes
 - Additional information associated with account
- Entitlements
 - Specify what actions a user is authorized to perform in a given application (i.e. access payroll)
- Account Groups
 - Specify set of security rights/permissions (i.e. Administrator)
 - Membership in group provides user with group's access rights

Defining Non-Authoritative Applications

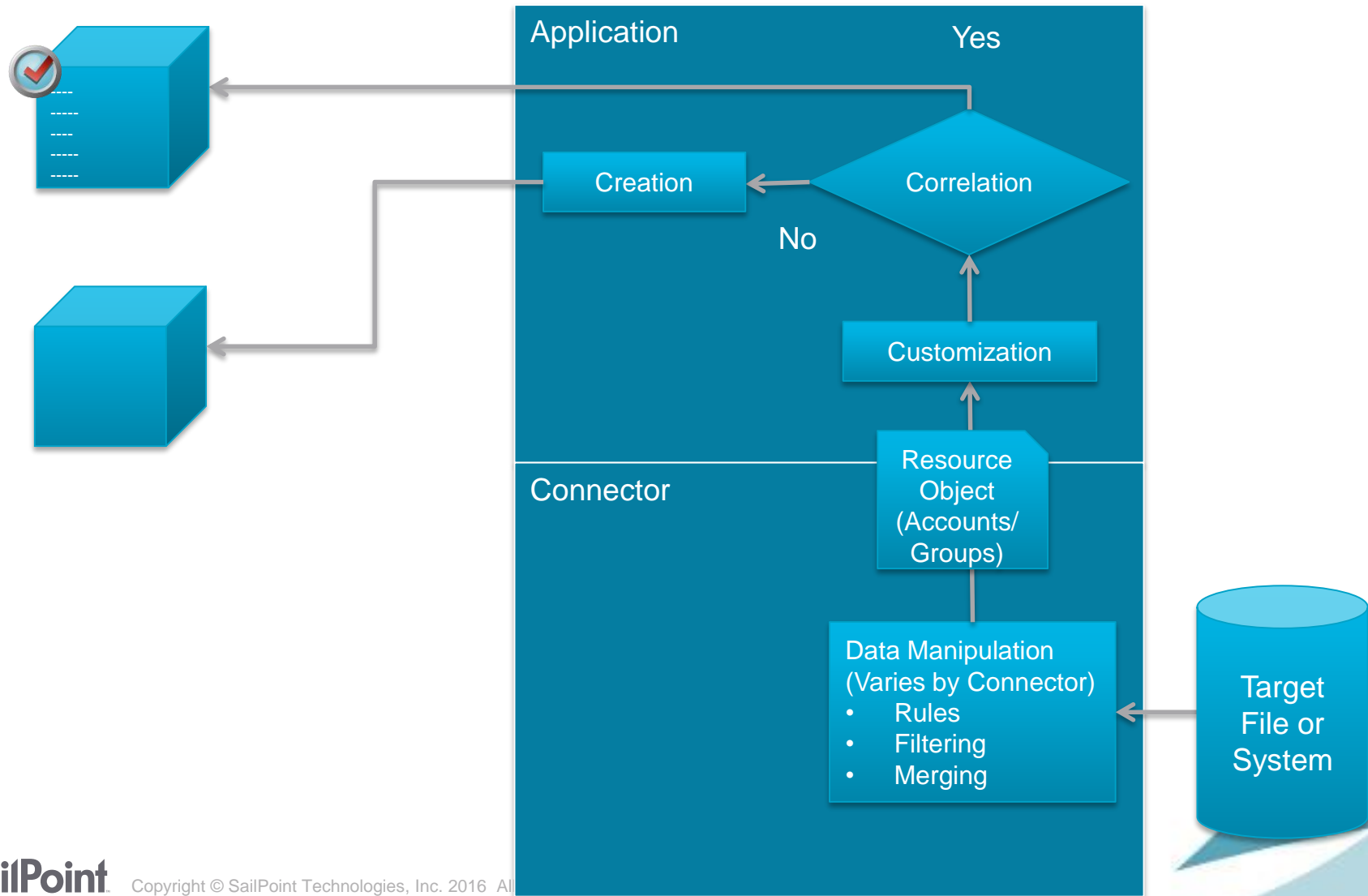
Defining Non-Authoritative Applications

Process Overview

- Define application
- Select connector type
- Define account schema
 - Used to represent individual accounts
- Define group schemas (if needed)
 - Used to represent individual group rights
- Specify account correlation
- Define rules (if needed)
 - Connector Rules
 - Support Data Transformation operations
 - Connector Rules vary based on the connector type
 - Application Rules
 - Act on accounts/account groups (Resource Objects)
 - Available for all connector types
- Define aggregation task and schedule

Application/Connector Processing

Aggregation



Applications – Specifying Connector

- Connectors

- Provide for reading data from
 - Applications
 - Ill-formed text feeds
- Most provide for writing data to applications

- *Application Type* defines connector

- Connectors

- Read Only
 - Delimited File
- Read/Write
 - AD, LDAP, JDBC, etc.
- Rule Based
 - Multiplexed, Logical, Rule Based File Parser

Edit Application

Details

*indicates a required field.

*Name ?

*Owner ?

*Application Type ?

Select One ...

Description ?

B *I* U | [List Icon] [List Icon]

Connector Categories

- **Standard Deployment**
 - Many deployments
 - Independent deployment
- **Assisted Deployment**
 - Few deployments
 - SailPoint provides assistance and guidance during deployment
- **Collaborative Deployment**
 - Few deployments
 - SailPoint provides direct collaboration and oversight of deployment
 - Customer provides access to and expertise about the managed system

For full connector listing and category, refer to *Compass*

Schemas

- Definition of what data to read from the target resource and how to interpret that data
- Schema types
 - Account (required)
 - Represents individual accounts on a target resource (Active Directory or SAP Accounts, for example)
 - Group (optional)
 - Represent native account groups from target resource (LDAP Groups or Active Directory Groups, for example)
 - Certain connectors support multiple group schemas (6.4)
 - JDBC, SQL Loader, Delimited File, and Oracle EBS

Account Schema

Review

- Identify key data to IdentityIQ
 - Identity Attribute
 - Display Attribute
- Specify account attributes to read during aggregation

Settings Schema Provisioning Policies

Object Type: account

Details

Native Object Type
account

Identity Attribute
employeeId

☐ Include Permissions


Display Attribute
fullName

Instance Attribute

Remediation Modifiab
Readonly ▼

Attributes

	Name	Description
<input type="checkbox"/>	login	
<input type="checkbox"/>	description	
<input type="checkbox"/>	first	
<input type="checkbox"/>	last	
<input type="checkbox"/>	groups	
<input type="checkbox"/>	status	







 Copyright © SailPoint Technologies, Inc. 2016 All rights reserved. 12

Account Schema

Entitlement Designations

- Identify attribute that lists user entitlements
 - Entitlement → Identity Cube
 - Include in certifications
 - Include in role mining
 - Managed → Entitlement Catalog
 - Assign ownership, display name, description
 - Request through LCM
 - Use in policy and risk calculations

Attributes

	Name	Description	Type	Properties	
<input type="checkbox"/>	login		string ▼		 Edit
<input type="checkbox"/>	description		string ▼		 Edit
<input type="checkbox"/>	first		string ▼		 Edit
<input type="checkbox"/>	last		string ▼		 Edit
<input type="checkbox"/>	groups		group ▼	Managed, Entitlement, Multi-Valued	 Edit
<input type="checkbox"/>	status		string ▼		 Edit

Entitlement Catalog / Identity Cube

	Name	Description	Type	Properties
<input type="checkbox"/>	id		string	
<input type="checkbox"/>	username		string	
<input type="checkbox"/>	firstname		string	
<input type="checkbox"/>	lastname		string	
<input type="checkbox"/>	email		string	
<input type="checkbox"/>	capability		string	Managed Entitlement Multi-Valued

Entitlement Catalog			
Filter Entitlements		Q	Advanced Search
Application	Attribute	Display Name	Type
TRAKK	capability	super	Entitlement
TRAKK	capability	reject	Entitlement
TRAKK	capability	input	Entitlement
TRAKK	capability	approve	Entitlement
PRISM	groups	User	Group

View Identity Adam.Kennedy

Attributes Entitlements Application Account

Adam.Kennedy was last refreshed on 4/30/15

Roles

Filter by role name



Adv

Name

Description



Page

0

of 0



Entitlements

Filter by attribute



Filter

Attribute

Entitlement

capability

input

groupmbr

PayrollAnalysis

memberOf

Domain Users

memberOf

Domain Admin







Group Schema

- Used to support native account group object model
- Provides framework for defining what group membership really means
 - I am a member of Group 920-100, I can access the financial planning file share
 - I am a member of Active Directory group VPN, I can log in to corporate VPN
- Groups managed in Entitlement Catalog
- Can represent indirect permissions data
 - Permissions are **direct**
 - Group-based permissions are **indirect**

Group Object Reference

Account Schema

- Identifies the attribute that holds user groups
- Used to identify group membership (groupmbr, memberOf)
- Available after Group Object has been defined

Attributes					
	Name	Description	Type	Properties	
<input type="checkbox"/>	login		string ▼		 Edit
<input type="checkbox"/>	description		string ▼		 Edit
<input type="checkbox"/>	first		string ▼		 Edit
<input type="checkbox"/>	last		string ▼		 Edit
<input type="checkbox"/>	groups		group ▼	Managed, Entitlement, Multi-Valued	 Edit
<input type="checkbox"/>	status		string ▼		 Edit

Account Correlation

Non-authoritative Applications

- Matches an account to an authoritative Identity Cube
 - If no correlation, non-authoritative cube is created
- 4 correlation methods
 - Correlation Wizard
 - Correlation Rule
 - Default Logic
 - Manually

The screenshot shows a web interface titled "Account Correlation". Below the title, there is a text instruction: "To Edit the currently assigned configuration click Edit. If you want to create a New Correlation". Below this text is a dropdown menu currently showing "Financial Correlation", followed by "Edit" and "New" buttons. Underneath, there is a section titled "Attribute Based Correlation" which contains a table with two columns: "Application Attribute" and "Identity Attribute". The table has one row with the values "employeeid" and "emplid".

Application Attribute	Identity Attribute
employeeid	emplid

Account Correlation

Correlation Wizard

- Provides a set of ordered correlations
- Result is a reusable correlation configuration
- 2 types of correlations
 - Attribute based
 - Ex: Correlate account attribute **mail** with identity attribute **email**
 - Condition based
 - Ex: Correlate accounts where **app2_service = true** with Admin cube

The screenshot shows a window titled "Correlation Wizard" with a close button in the top right. The main heading is "Define Attribute Based Correlation Assignments". Below this is a section titled "Attribute Based Correlation Assignments". It contains a table with columns for checkboxes, application attributes, operators, and identity attributes. The first row shows an empty checkbox, an empty application attribute field, an empty operator field, and an empty identity attribute field. The second row shows an empty checkbox, up and down arrow buttons, a dropdown menu with "employeeid", the operator "equals", and a dropdown menu with "Employee ID". At the bottom, there are "Delete" and "Add" buttons, followed by a "Select Attribute..." dropdown, the operator "equals", and another "Select Attribute..." dropdown.

<input type="checkbox"/>		Application Attribute		Identity Attribute
<input type="checkbox"/>	^ v	employeeid	equals	Employee ID
<input type="checkbox"/>		Select Attribute...	equals	Select Attribute...

Account Correlation

Manual Correlation

- Manually assign accounts to identities
 - Identities → Identity Correlation
- Correlation permanently retained

Select Uncorrelated Accounts

Financials

Account ID or Name

Included Account Types

<input type="checkbox"/> Account ID	Account Name	Create Date
<input type="checkbox"/> 337	AngieBell	01/02/14 12:45:42 pm
<input type="checkbox"/> 339	FloJohnston	01/02/14 12:45:42 pm
<input type="checkbox"/> 338	JeffMurphy	01/02/14 12:45:42 pm
<input type="checkbox"/> 341	WendyGeorge	01/02/14 12:45:42 pm

Page 1 of 1

Displaying 1 - 4 of 4

Select Target Identity

Filter by Name

Advanced Search

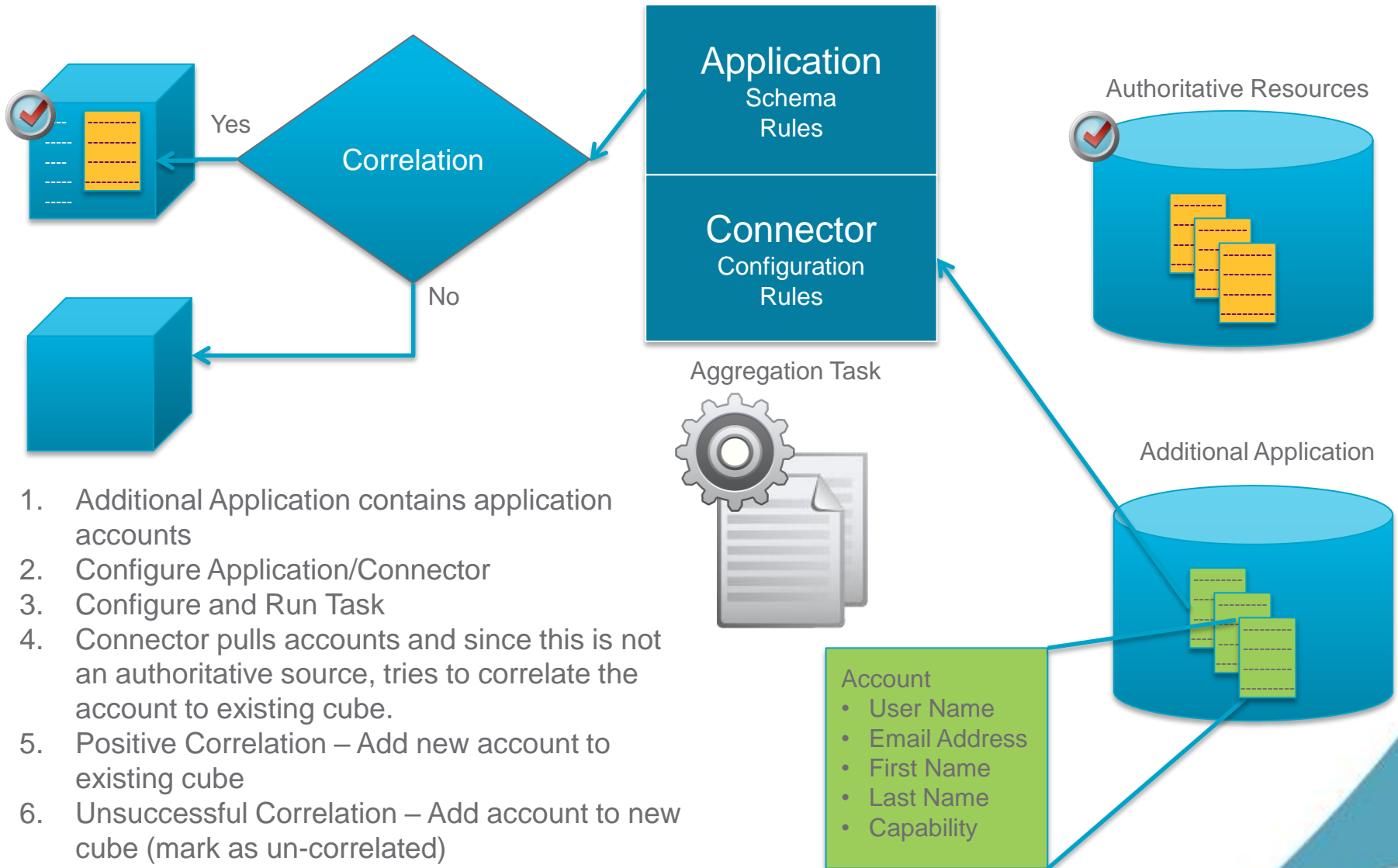
Name	First Name	Last Name	Correlated	Manager	Email
<input type="checkbox"/> Aaron.Nichols	Aaron	Nichols	<input checked="" type="checkbox"/>		Aaron.Nichols@dem

Application Rules

Review

- Correlation Rule (when matching isn't enough)
 - Build and maintain account correlations
- Manager Correlation Rule
 - Build and maintain manager hierarchy
- Creation Rule
 - Perform customizations at cube creation time
Example: *Set default IdentityIQ password*
- Customization Rule
 - Modify/normalize incoming account data prior to saving to an Identity

Aggregation & Correlation



Application Activity Data Sources

Optional

- Utilize externally collected activity tracking and monitoring data
 - Use in Policies and Risk
- Gathering activity data
 - Define how to access the source
 - Define what data to retrieve
 - Define rules for correlation and transformation
 - Enable per user or per role
 - Define Activity Aggregation task
- Standard sources
 - JDBC, Log File, RACF Audit Log Collector, Windows EventLog Collector
- Integration module
 - HP ArcSight

Connectors

Delimited File

Delimited File

File and Transport

The screenshot displays the 'Configuration' tab for a 'Delimited File' object type. The interface includes a top navigation bar with tabs like 'Details', 'Configuration', 'Correlation', 'Accounts', 'Risk', 'Activity Data Sources', 'Rules', and 'Password Policy'. Below this is a sub-navigation bar with 'Settings', 'Schema', and 'Provisioning Policies'. The main configuration area is divided into sections: 'Object Type: account', 'File', 'Filtering', 'Merging', and 'Iteration Partitioning'. The 'File' section contains the following fields:

- * File Path**: A text input field containing the path `/home/spadmin/training/data/AuthEmployees.csv`. A callout box labeled 'File Path' points to this field.
- File Encoding**: A text input field.
- File Transport**: A section with radio buttons for 'Local' (selected), 'FTP', and 'SCP'. A callout box labeled 'File Transport' points to this section.
- Parsing Type**: A section with radio buttons for 'Delimited' (selected) and 'Regular Expression'.
- Delimiter**: A text input field containing a comma (`,`). A callout box labeled 'Delimiter' points to this field.
- Columns**: A large empty text area.
- File has column header on first line**: A checked checkbox. A callout box labeled 'Column Header Present?' points to this checkbox.
- Fail on column length mismatch**: An unchecked checkbox.

Delimited File

Filtering and Merging

Object Type: account

File Filtering Merging Iteration Partitioning

Number of lines to skip ?

Filter Empty ? ☒

Comment Character ?

Filter String ?

Filtering

Object Type: account

File Filtering Merging Iteration Partitioning

Data needs to be merged ? ☒

Index Column ?

Data sorted by the indexColumn(s)? ? ☒

groupmbr

Which Columns should be merged? ?

Merge Config
(Note: sorting
the incoming
data speeds up
the aggregation
when merging)

Merging Example

- Delimited File or JDBC with the following result:

```
username, firstname, lastname, region  
bsmith, Bob, Smith, US  
bsmith, Bob, Smith, EMEA
```

- Set the merging to the following:

- **Data needs to be merged** : true
- **Index Column** : username
- **Which columns should be merged?** : region

- Results

- One Account for Bob Smith (username=bsmith)
- Region attribute set to “US,EMEA”

Delimited File

Connector Rules

Connector Rules

Build Map Rule



-- Select Rule --

PreIterate Rule



-- Select Rule --

PostIterate Rule



-- Select Rule --

Map To ResourceObject Rule



-- Select Rule --

MergeMaps Rule



-- Select Rule --

- Runs for every line in the file
- Converts incoming data into map

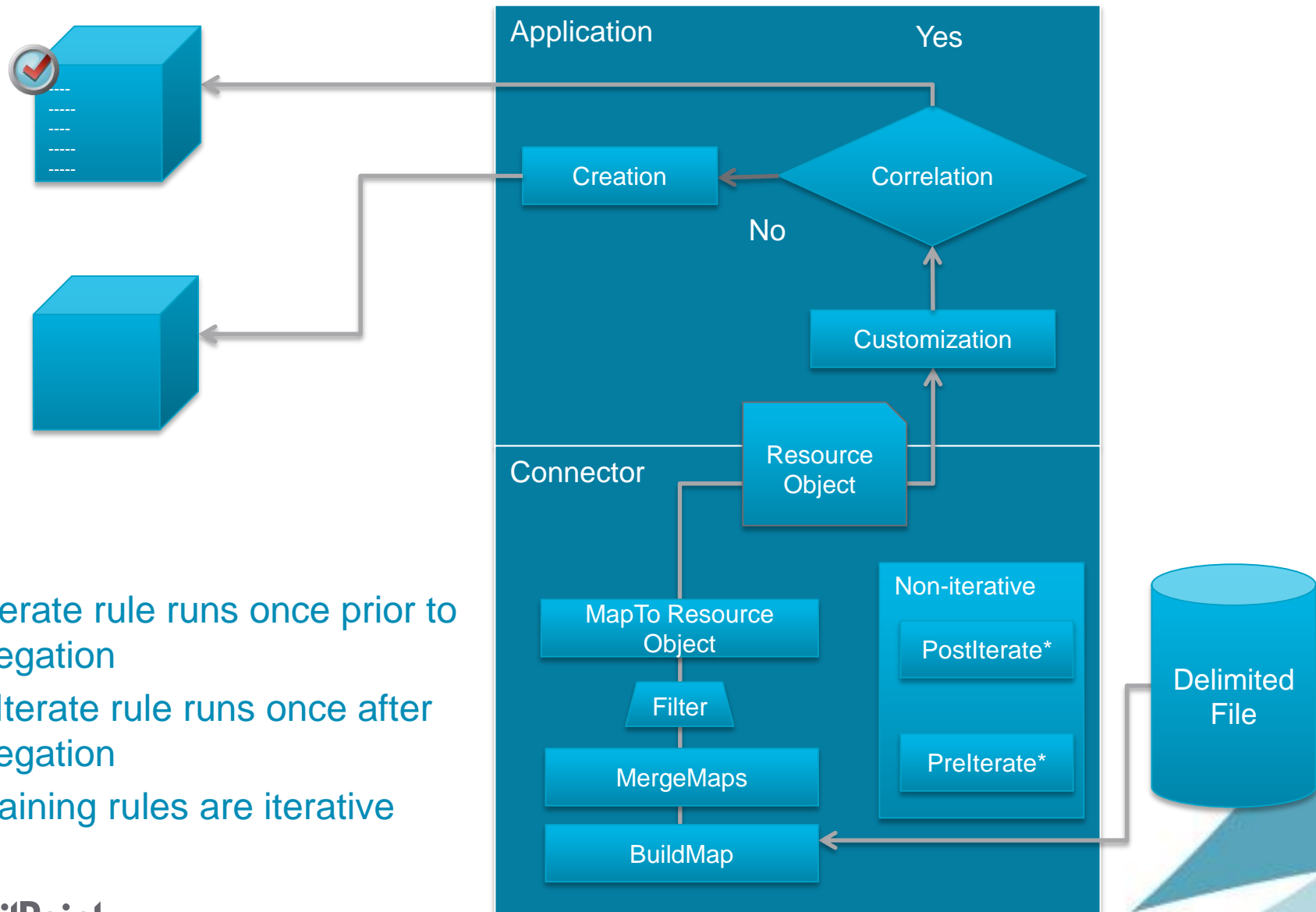
- Runs once for each aggregation
- Can do any pre-processing

- Runs once for each aggregation
- Can do any post-processing

- Performs final conversion to Resource Object
- Runs once for each account or group
- Runs after merging

- Performs merging processing
- If default merge capabilities aren't enough, a rule here can control merging

Delimited File Processing



Notes:

- Prelterate rule runs once prior to aggregation
- PostIterate rule runs once after aggregation
- Remaining rules are iterative

Writing to CSV Files

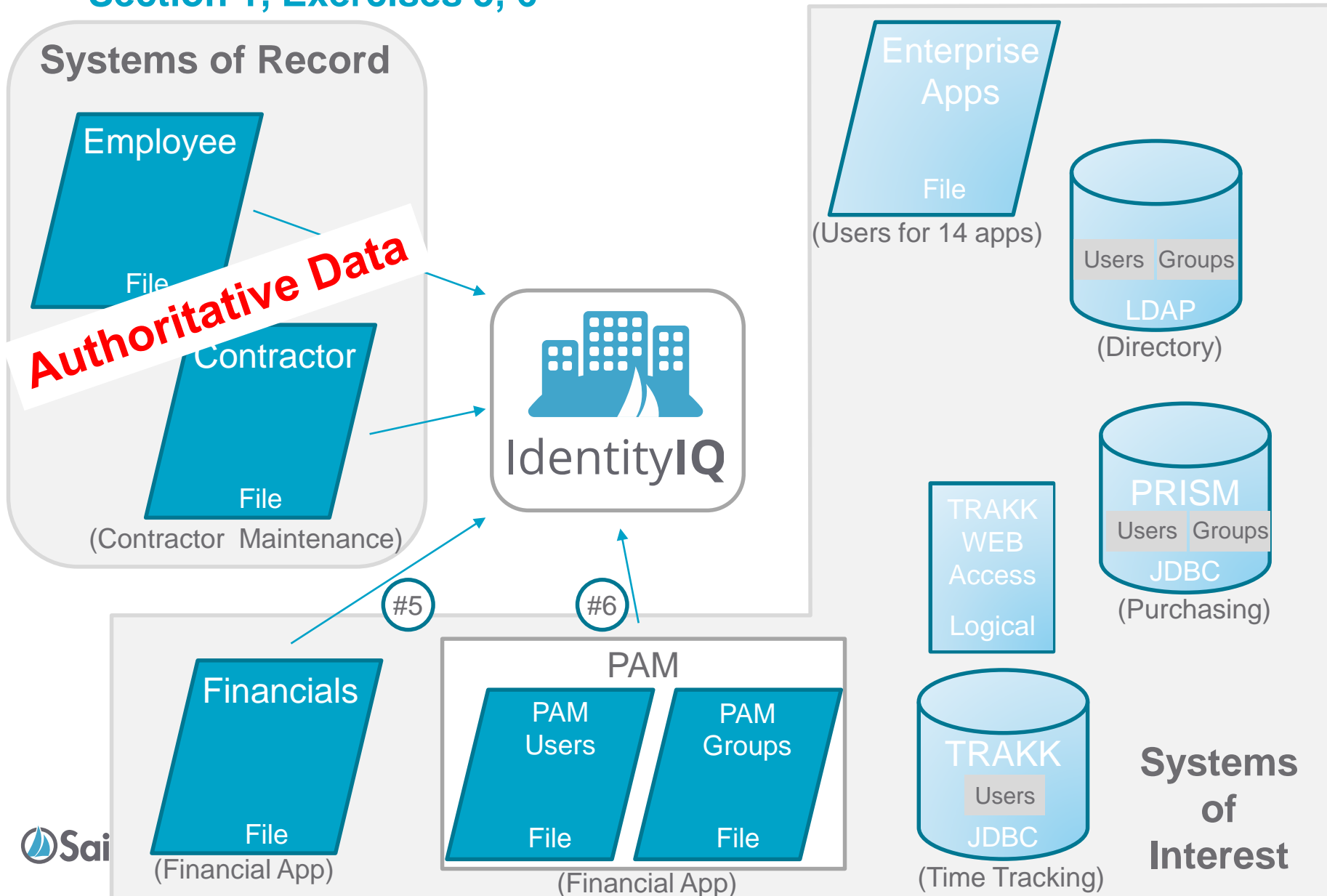
SQL Loader Connector

Overview

- Provides SQL query option to read/write data from CSV/Text files
- Based on JDBC Connector architecture
- Data can be pulled from multiple files
- Support direct Permission functionality

Exercise Preview

Section 1, Exercises 5, 6



JDBC

JDBC Applications

Connection Settings

Object Type: account

Settings Merging Iteration Partitioning Delta Aggregation

JDBC Connection Settings

* Connection User ?

root

Connection Password ?

.....

* Database URL ?

jdbc:mysql://localhost/prism

* JDBC Driver ?

com.mysql.jdbc.Driver

DB user/password

DB URL

JDBC Driver

JDBC Applications

Query Settings

Query Settings

*** SQL Statement** ?

select * from users

getObjectSQL ?

select * from users where login = '\$(identity)'

☐ **useExecuteQuery** ?

☐ **Direct Permission Execute Query** ?

SQL statement for pulling all accounts

SQL statement for pulling single account

Note: Filtering supported by query

JDBC Applications

Merging

Object Type: account

Settings Merging Iteration Partitioning Delta Aggregation

☒ Data needs to be merged ?

Index Column ?

Which Columns should be merged? ?

id

capability

Merge
Configuration

Note: Sorting incoming data speeds up aggregation when merging

JDBC Applications

Connector Rules

Connector Rules

Build Map Rule



PRISM - BuildMap

Map To ResourceObject Rule



-- Select Rule --

MergeMaps Rule



-- Select Rule --

Provision Rule Type



☒ Global Provision Rule

☐ By Operation Rules

Provision Rule



PRISM - Provision

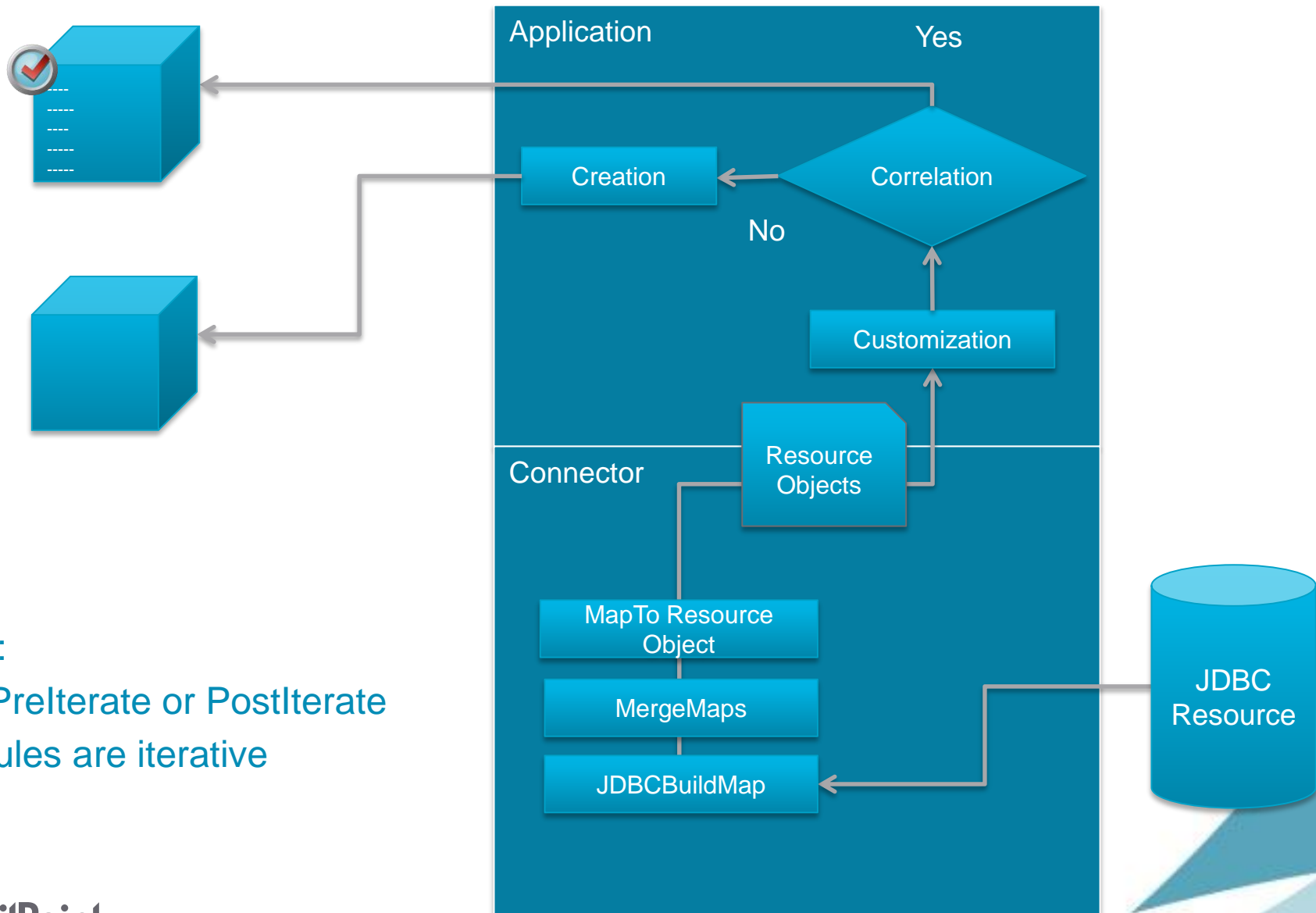
- Runs for every result row
- Converts incoming data into map

- Performs final conversion to Resource Object
- Runs once for each account or group
- Runs after merging

- Performs merging processing
- If default merge capabilities aren't enough, a rule here can control merging

- Handles Provisioning Operations
- All in single rule or per operation
- More on this later

JDBC Processing



Notes:

- No PreIterate or PostIterate
- All rules are iterative

LDAP

LDAP Connector

Connection Information

Use SSL	<input type="checkbox"/>
Authorization Type	Simple
User *	cn=Admin,dc=example,dc=com
Password	●●●●●●●●●●
Host *	host.example.com
Port *	389
Page Size	100
Authentication Search Attributes	cn uid mail

SSL/Auth Type
Credentials

Host/Port

For Pass
Through
Authentication

LDAP Connector

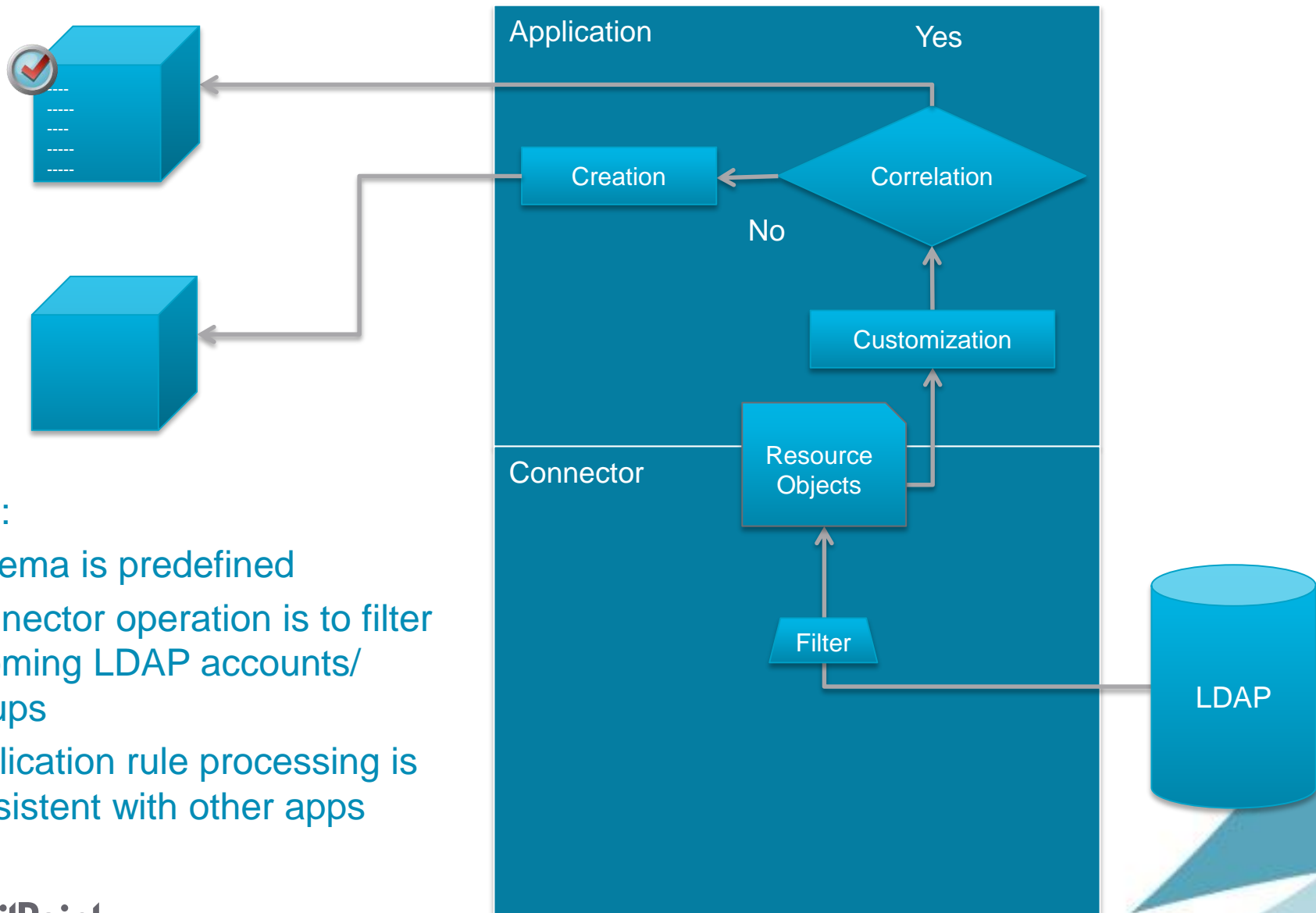
Search DN and Filtering

The screenshot shows the 'Group' tab of the 'Account Settings' configuration page. It contains several input fields for LDAP search parameters. Annotations with blue boxes and arrows highlight specific areas:

- Search Scope:** A dropdown menu is set to 'Subtree'. A blue box labeled 'Search Scope Subtree, Base, OneLevel' points to this dropdown.
- Search DN:** A text field contains 'ou=People,dc=example,dc=com'. A blue box labeled 'Search DNs' points to this field.
- Iterate Search Filter:** An empty text field. A blue box labeled 'Search DNs' also points to this field.
- Group Member Search DN:** A text field contains 'ou=Groups,dc=example,dc=com'. A blue box labeled 'Search DNs' points to this field.
- Group Member Search Filter:** An empty text field.
- Filter String:** An empty text field. A blue box labeled 'Filtering Information' points to this field.

Other visible elements include the 'Account' and 'Group' tabs at the top left, and a 'Search Scope' label next to the dropdown menu.

LDAP Processing



Notes:

- Schema is predefined
- Connector operation is to filter incoming LDAP accounts/groups
- Application rule processing is consistent with other apps

Active Directory

Active Directory Connector

Connection Information

- Auto-discover or manually enter domains
- Specify servers or serverless bind

Domain Configuration* ?

☒ Discover Domains ?

Global Catalog ? 192.168.95.132:3268

Administrator ? SPTRAINING\Administrator

Password ?

Discover

<input type="checkbox"/>	Domain	User	Password	Servers	SSL
<input type="checkbox"/>	DC=training,DC=sailpoint,DC=local	SPTRAINING\Administrator
<input type="checkbox"/>	DC=test,DC=sailpoint,DC=local	SPTEST\Admin
<input type="checkbox"/>					...

Delete

Add

Auth Information
per Domain

Active Directory Connector

Search DN and Filtering

Account **Group**

Account Search Scope* ?

<input type="checkbox"/> Search DN	Iterate Search Filter	Primary Group Search DN	Group Membership Search DN
<input type="checkbox"/> cn=Users,dc=training,dc=sailpoint,dc=local			cn=Users,dc=training,dc=sailpoint,dc=local; ou

Delete Add

DN Information for Searching

Filtering Information

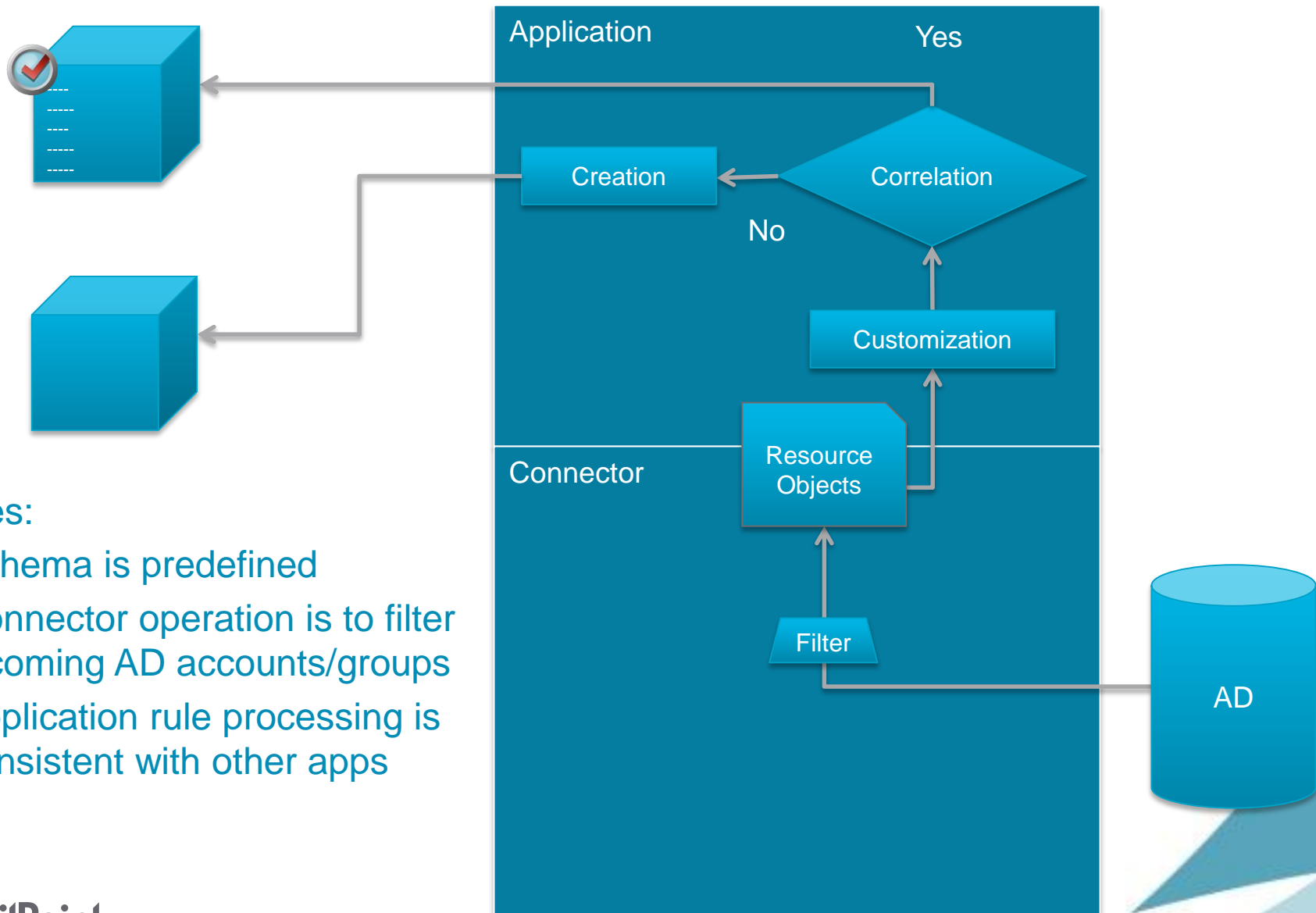
Active Directory Connector

Provisioning and IdentityIQ Authentication

Active Directory - Direct Configuration

IQService Host	<input type="text"/>	Connection Info for IQService for Provisioning
IQService Port	<input type="text"/>	
Page Size	<input type="text" value="100"/>	
Authentication Search Attributes	<input type="text" value="distinguishedName
sAMAccountName
uid
mail"/>	
Exchange Version	<input type="text" value="-"/>	For Pass Through Authentication
Manage Lync	<input type="checkbox"/>	
Delta Aggregation Mode	<input type="text" value="-"/>	

Active Directory Processing



Notes:

- Schema is predefined
- Connector operation is to filter incoming AD accounts/groups
- Application rule processing is consistent with other apps

Other Connectors

- Each connector will vary
 - Connector settings
 - Connector rules
- Each connector is consistent
 - Application Rules
 - How correlation, creation, customization is handled
 - Schema (Account and Group)

Special Case Connectors

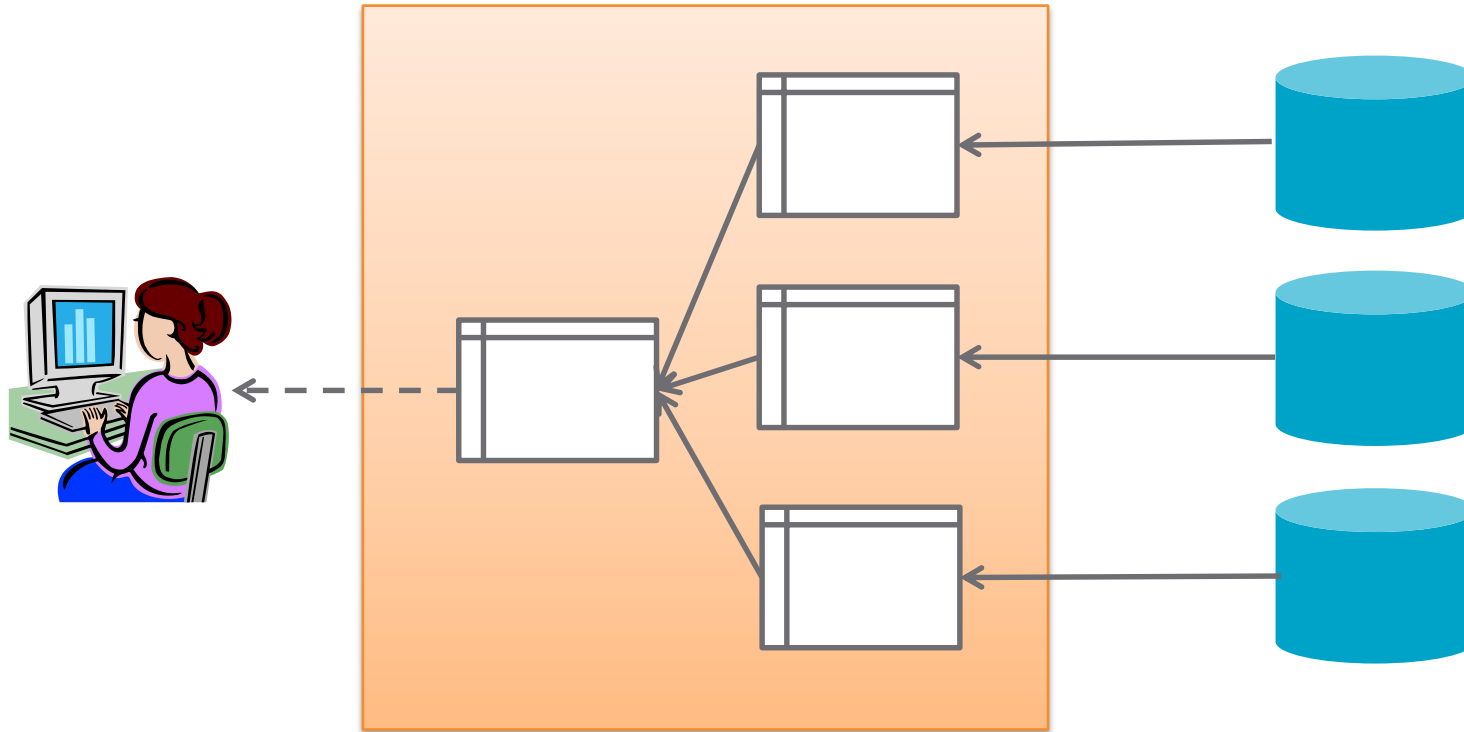
Logical and Multiplex

Logical Application

- Use Cases
 - Multiple separate credentials required for application access
 - Combining/Composite
 - Application access data not recorded in application
 - Usually controlled through group memberships on another application
 - Subdividing
- Simplifies searches, certifications, etc. by treating these special types of applications as a logical entity.

Logical Application

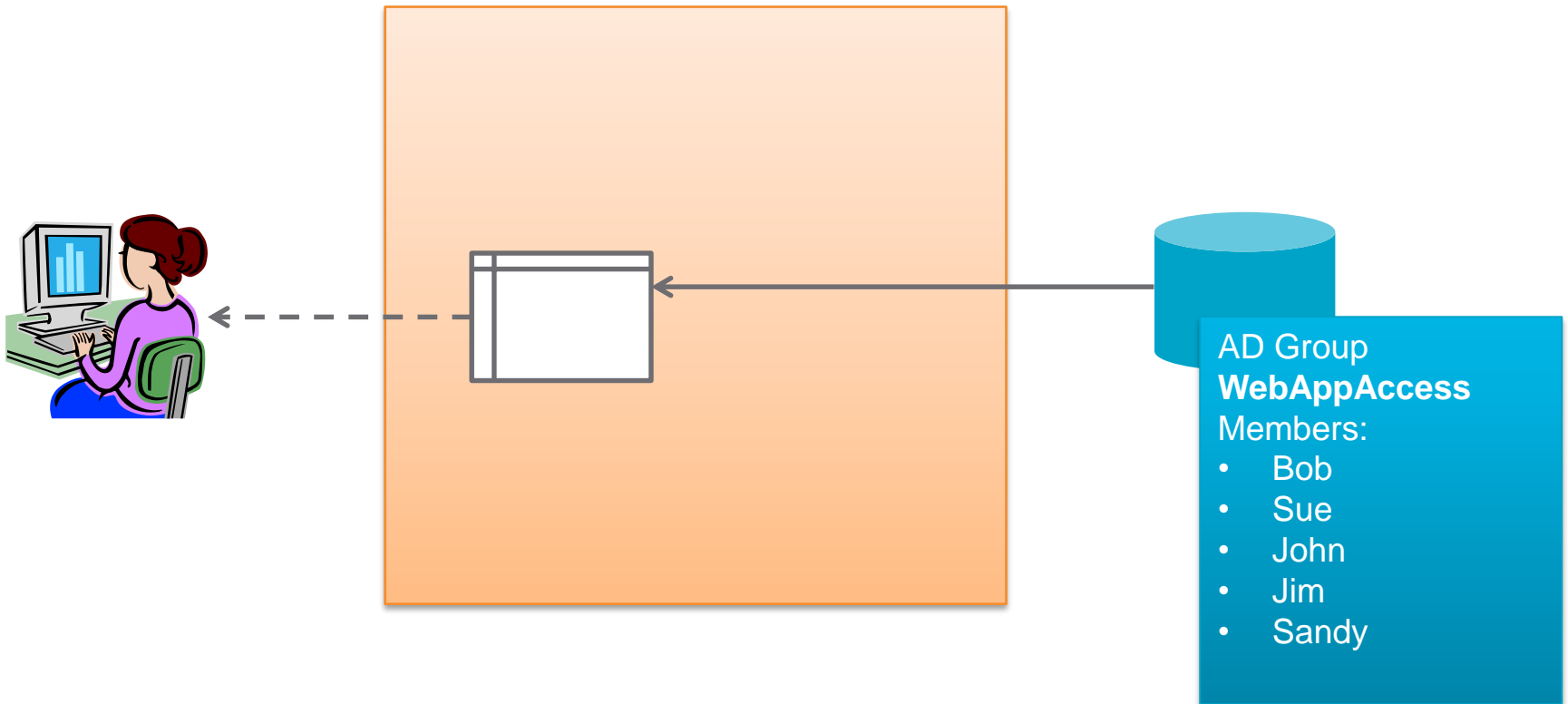
Combining / Composite



Example: Application is defined by Web Application access, Mainframe application access and SQL database access

Logical Application

Subdividing



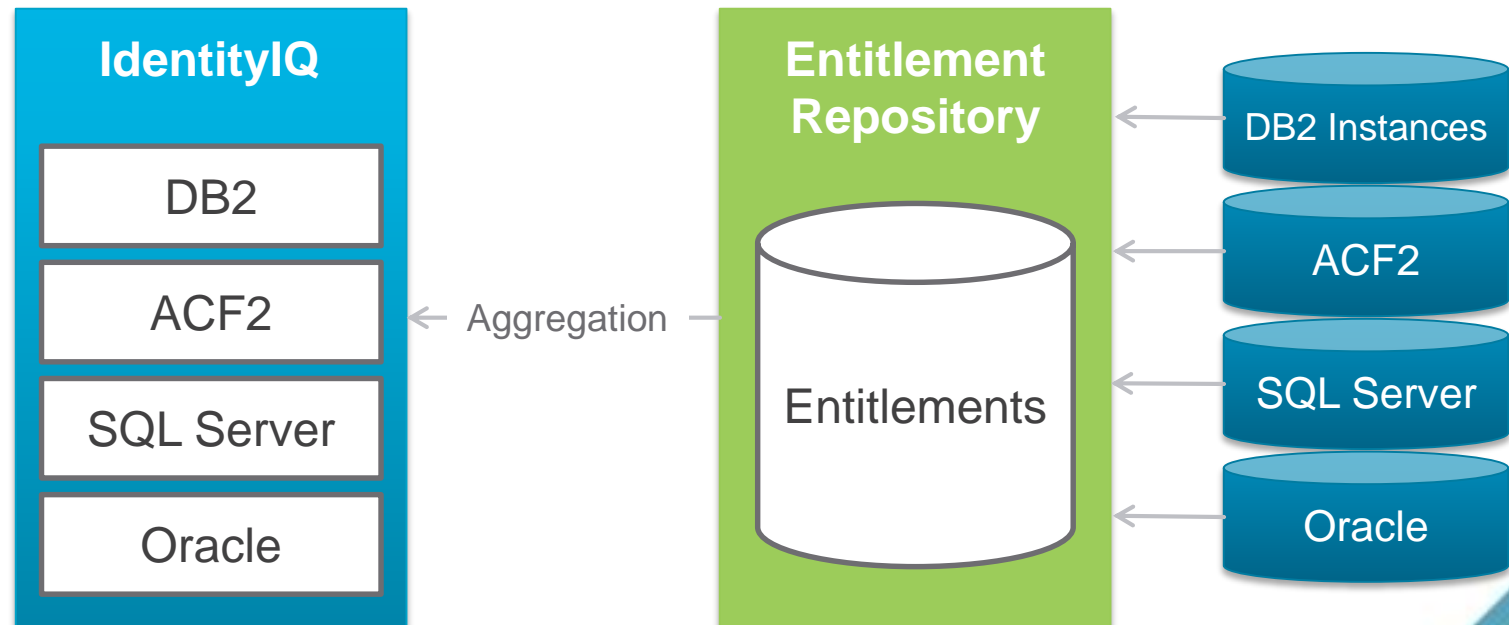
Example: Access to Web application is managed through Active Directory group membership

Logical Application and Roles

- Roles provide an alternative to logical applications
- Roles are more scalable over large volumes
- For provisioning
 - Roles leverage existing connector pathways
 - Logicals supported manually or require writing and maintaining provisioning rules

What is a Multiplex Application?

- Automatically create multiple applications based on a single data feed
- Primarily used with pre-existing entitlement repositories which contain multiple applications

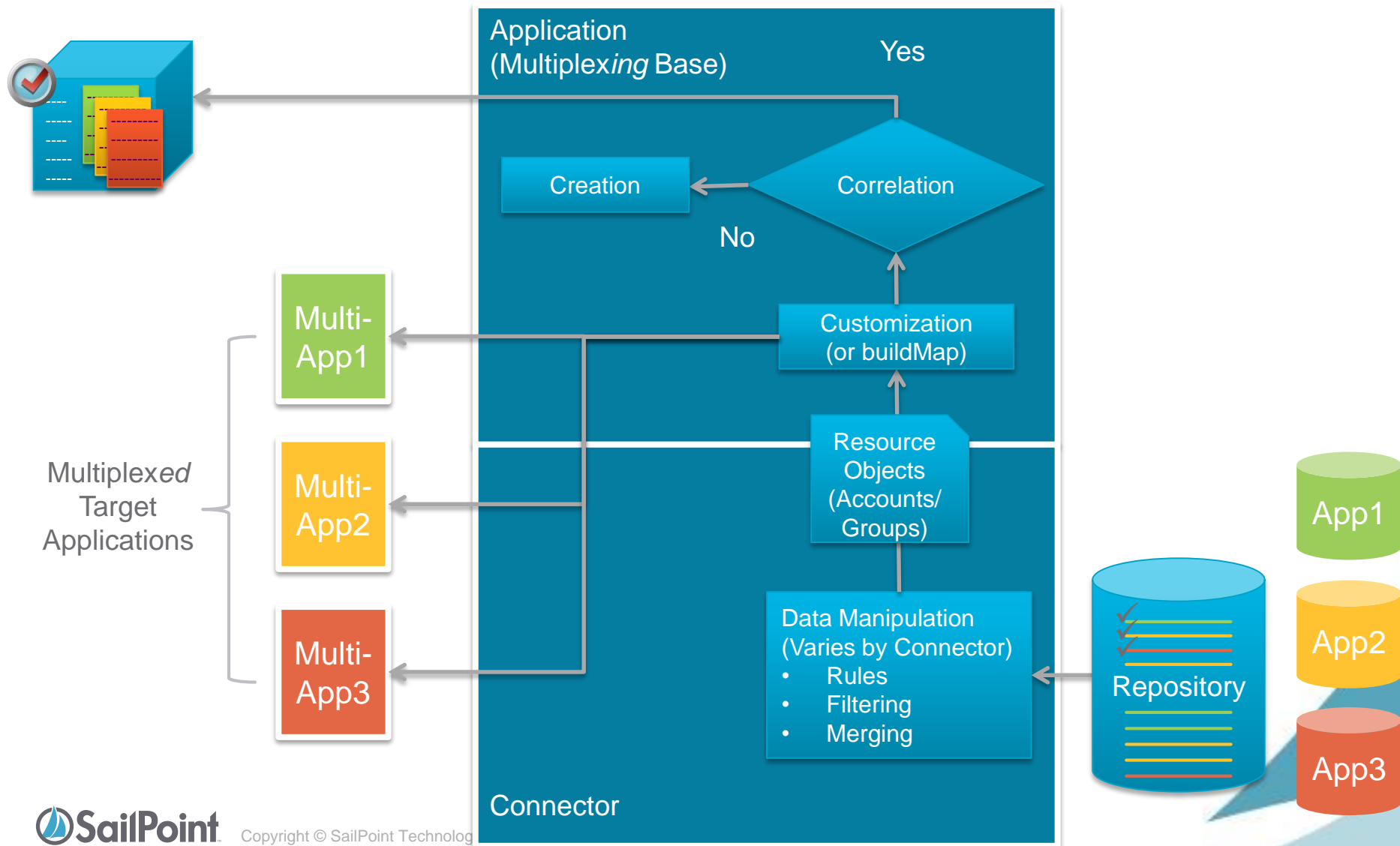


MultiPlex Requirements

- Single data feed containing user entitlements for multiple applications
- Application definition for repository (the base *multiplexing* application)
 - BuildMap or Customization rule sets attribute *IIQSourceApplication*
 - Used to parse records into separate *multiplexed* applications

Multiplex Processing

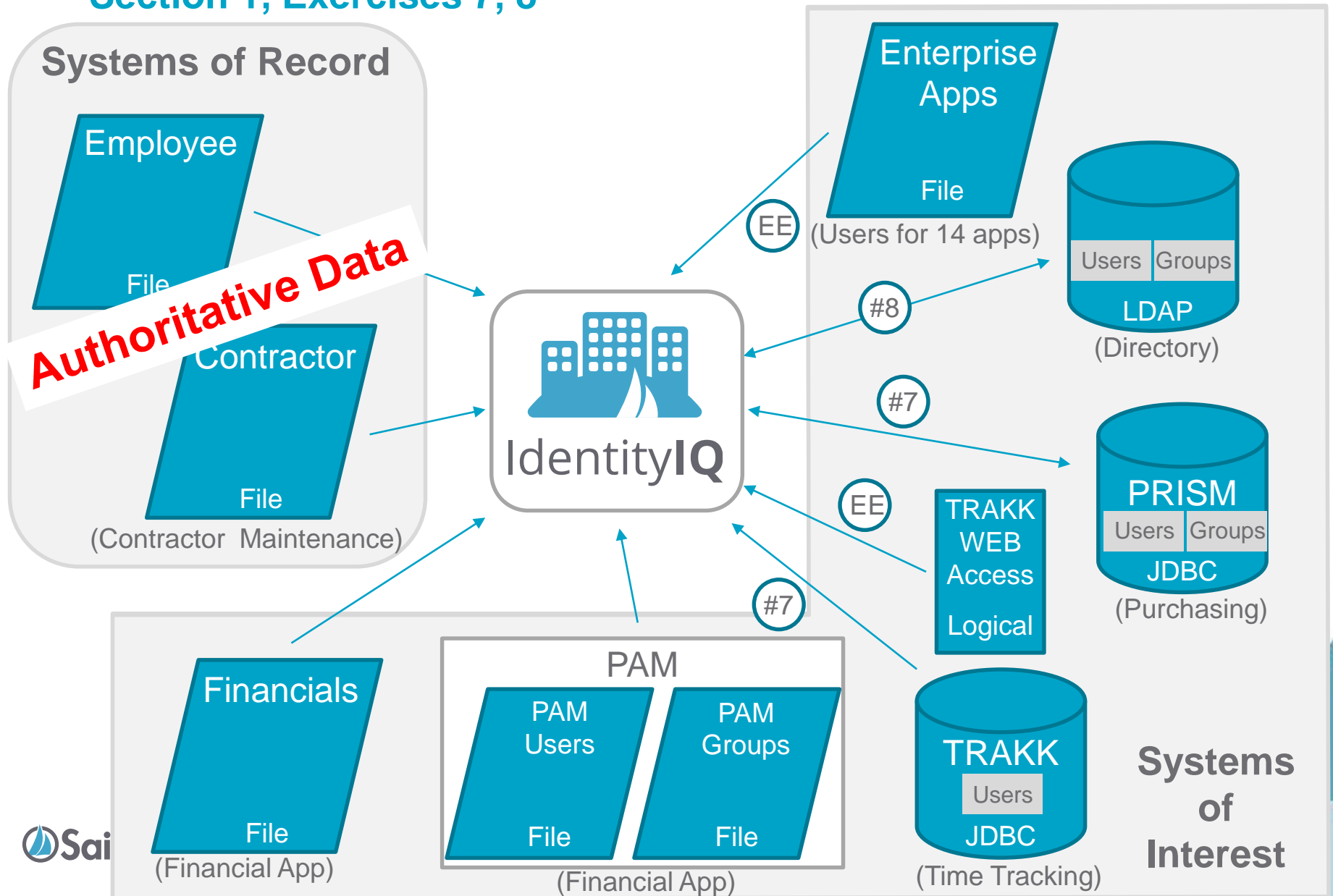
Aggregation



Questions?

Exercise Preview

Section 1, Exercises 7, 8



Exercise Preview

Section 1, Exercises 9

- Exercise #9: Exploring the Identity Refresh Task
- Extension Exercises (optional)
 - Onboarding Logical and Multiplexed Applications