

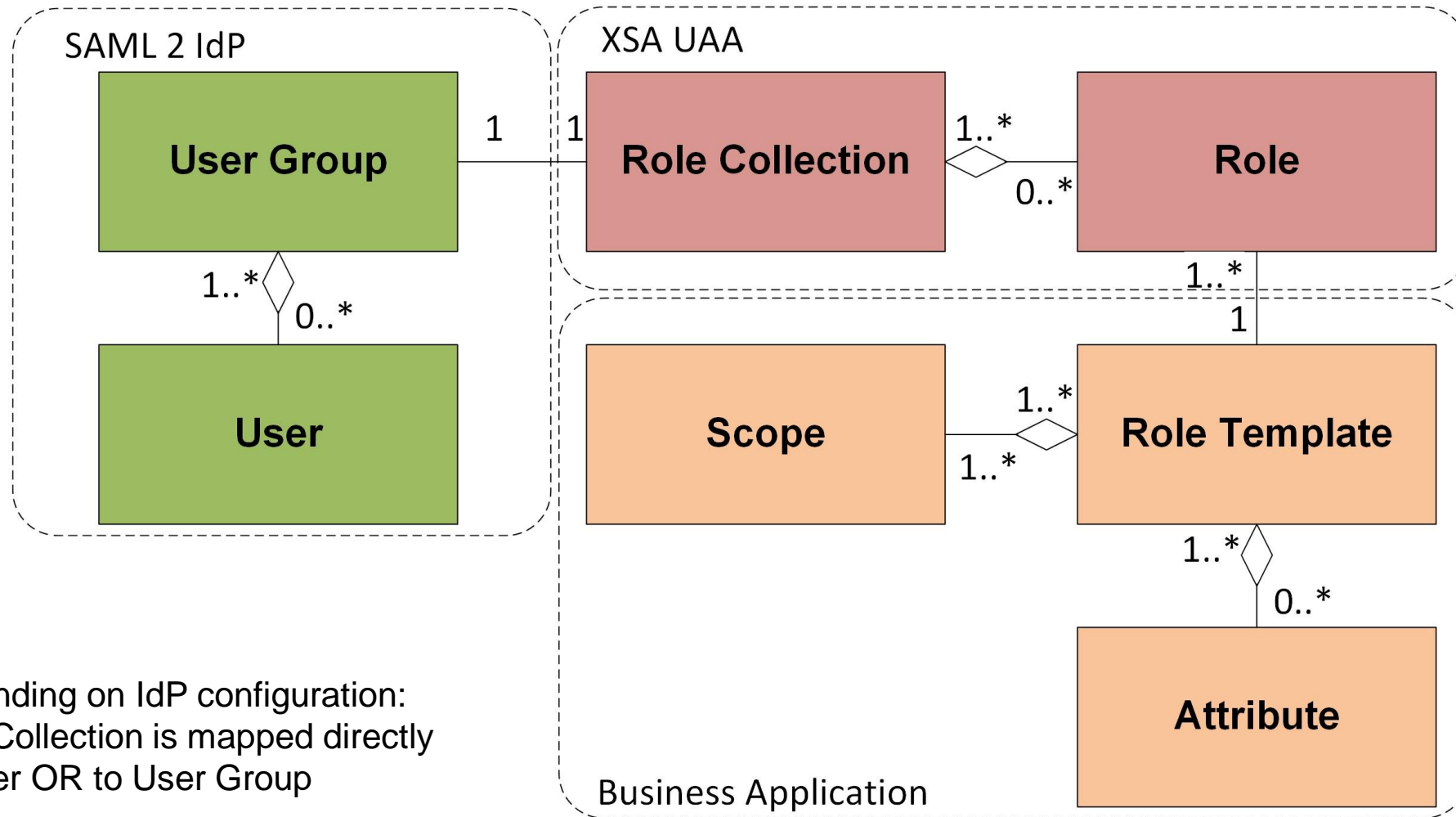


Week 5: Security

Unit 6: Administrating Authorizations

Administering Authorizations

Data model of authentication and authorization



Depending on IdP configuration:
Role Collection is mapped directly
to User OR to User Group

Administering Authorizations

SAP Cloud Platform Cockpit – Security: Create role collection and assign role(s)

The screenshot displays the SAP Cloud Platform Cockpit interface. On the left is a navigation menu with options: Overview, Spaces, Connectivity, Security (expanded), Role Collections, Trust Configuration, Quota Plans, Resource Consumption, Resource Usage Summary, Useful Links, and Legal Information. The main area shows the 'Subaccount: trial - Role Collections' page. A 'New Role Collection' button is highlighted with a red box. Below it is a table with columns: Name, Description, Roles, and Actions. The table contains one entry: 'RC_CC_M2_D' with description 'Role Collection d...' and role 'Advertiser'. A modal dialog titled 'New Role Collection' is open in the foreground. It has two input fields: '*Name:' with the value 'RC_CC_M2_D' (highlighted with a red box) and 'Description:' with the value 'My New Role Collection'. At the bottom of the dialog are 'Save' and 'Cancel' buttons.

Name	Description	Roles	Actions
RC_CC_M2_D	Role Collection d...	Advertiser	

New Role Collection

*Name: RC_CC_M2_D

Description: My New Role Collection

Save Cancel

Note: Roles can be explicitly defined in the context of your application

Administering Authorizations

SAP Cloud Platform Cockpit – Security: Create role collection and assign role(s)

The screenshot displays the SAP Cloud Platform Cockpit interface. The top navigation bar includes a hamburger menu, the title 'SAP Cloud Platform Cockpit', and icons for settings, documents, notifications, user, and power. The breadcrumb trail shows the path: Home > Europe (Frankfurt) - Canary > D [redacted] trial > trial > RC_CC_M2_D [redacted]. The main content area is titled 'Role Collection: RC_CC_M2_D [redacted] - Overview' with a sub-header 'All: 1'. A red box highlights the 'Add Role' button. A search bar is located to the right. Below the header, a table lists the role collection with one entry: 'bulletinboard-[redacted]!t500'. To the right of the table is an 'Actions' column with a trash icon. A modal dialog titled 'Add Role' is open, showing three fields: '*Application Identifier' (bulletinboard-d [redacted]!t500), '*Role Template' (Advertiser), and '*Role' (Advertiser). The '*Role' field has a dropdown menu with 'Advertiser' selected. At the bottom of the dialog, a red box highlights the 'Save' button, with a 'Cancel' button next to it. The left sidebar contains 'Overview', 'Useful Links', and 'Legal Information'.

SAP Cloud Platform Cockpit

Overview

Home / Europe (Frankfurt) - Canary / D [redacted] trial / trial / RC_CC_M2_D [redacted]

Role Collection: RC_CC_M2_D [redacted] - Overview

All: 1

Add Role

Search

Application Identifier	Actions
bulletinboard-[redacted]!t500	

Add Role

*Application Identifier: bulletinboard-d [redacted]!t500

*Role Template: Advertiser

*Role: Advertiser

Advertiser

Save Cancel

Useful Links

Legal Information

Administering Authorizations

SAP Cloud Platform Cockpit – Security: Assign role collection to user

SAP Cloud Platform Cockpit

Role Collection Assignment

Home / Europe (Frankfurt) - Canary / D...trial / trial / SAP ID Service

Trust Configuration: SAP ID Service - Role Collection Assignment

All: 1

Search

User: john.doe@sap.com Show Assignments Add Assignment

Role Collection

RC_CC_M2_D...

Add User Assignment

Assigning a role collection to a user provides the user with all the scopes contained within the role collection.

Role Collection: RC_CC_M2

Actions

Useful Links

Legal Information

Prerequisite: User needs to log on to the subaccount at least once, e.g.

<https://p0123456789trial.authentication.eu10.hana.ondemand.com>

Authorizations assigned to your user? Check via

<https://p0123456789trial.authentication.eu10.hana.ondemand.com/config?action=who>

Administering Authorizations

SAP Cloud Platform Cockpit – Security: Configure trust to IdP

The screenshot displays the SAP Cloud Platform Cockpit interface. The left sidebar contains navigation links: Overview, Spaces, Connectivity, Security, Role Collections, Trust Configuration, Quota Plans, Resource Consumption, Resource Usage Summary, Members, Useful Links, and Legal Information. The main content area shows the 'Subaccount: trial - Trust Configuration' page with a 'New Trust Configuration' button highlighted in red. Below this button, the status is 'Active' and the default is 'Default'. A modal dialog box titled 'New Trust Configuration' is open, showing the following fields:

- *Name: xsuaa-monitoring-idp
- Description: (empty)
- Status: Active (dropdown)
- Show SAML login link on login page: Yes (dropdown)
- Link Text: (empty)
- *Metadata: metadata.xml (text input) with an 'Upload' button next to it.

The metadata field contains the following XML snippet:

```
<?xml version="1.0" encoding="utf-8"?><ns3:EntityDescriptor
xmlns:ns3="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns="http://www.w3.org/2000/09/xmldsig#"
xmlns:ns2="http://www.w3.org/2001/04/xmenc#"
xmlns:ns4="urn:oasis:names:tc:SAML:2.0:assertion" ID="Sb9e38f72-de11-
4b64-9617-24a293be42e8" entityID="xsuaa-monitoring-idp">
<ns3:IDPSSODescriptor WantAuthRequestsSigned="true"
```

The dialog box has 'Parse', 'Save' (highlighted in red), and 'Cancel' buttons at the bottom.

Administering Authorizations

Demo



Administrating Authorizations

Exercise 24 Part 2



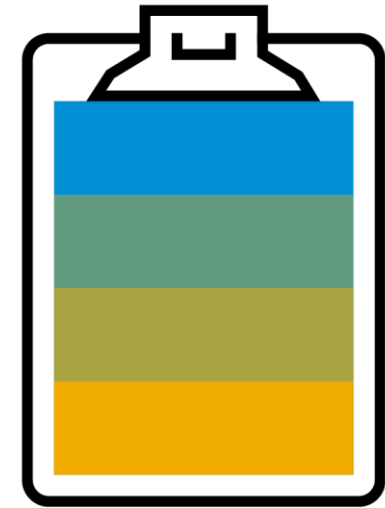
[Exercise 24 Part 2:](#) [Administrate Authorizations](#)



Administrating Authorizations

Recommendations for production applications

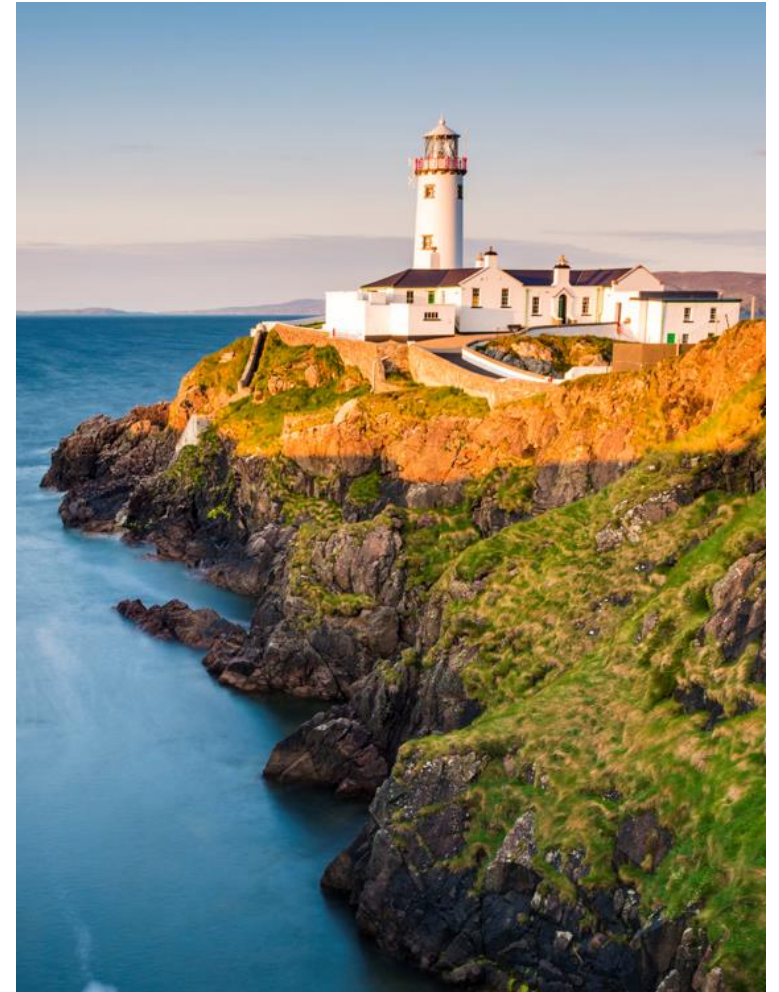
- Ensure that the Java Web Token (JWT) is provided by the request
- Define scopes for generic authorization checks in xs-app.json
- Define scopes for domain authorization checks in xs-security.json
- Support logout functionality in your UIs
- Implement tests that automatically ensure that application endpoints are protected against unauthorized access
- **NEVER** trace Java Web Tokens (JWTs)



Administering Authorizations

What you've learned in this unit

- How the data model of authentication and authorization looks like
- How to use the SAP Cloud Platform cockpit to
 - Create role collections
 - Assign roles to role collections
 - Assign role collections to users
 - Configure trust to an IdP
- What the recommendations for productive applications are



Thank you.

Contact information:

open@sap.com

© 2018 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

The information contained herein may be changed without prior notice. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platform directions and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

See <http://global.sap.com/corporate-en/legal/copyright/index.epx> for additional trademark information and notices.