



SAP BTP Administration

Administering platform and applications on SAP Cloud



Commencement

Training Agenda

Objective: Understand and appreciate how SAP BTP works and its various components so that it can be used productively in a project.

S. No.	Subject
1	SAP Business Technology Platform (BTP)
2	SAP BTP security basics
3	SAP Identity Authentication Service (IAS)
4	Securing BTP apps
5	On-premise connectivity
6	End to end application demo
7	Conclusion

General guidelines



Identify Take-aways

It is important to understand trainings objective and identify with it.



Ask Questions

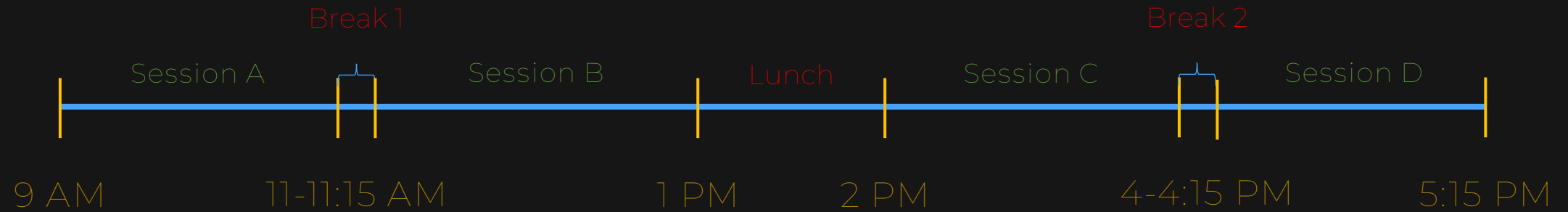
All questions are valid and important. Utilize this opportunity fully and ask as many questions as you can.



Practice → Perfect

Practice makes perfect. Try out the concepts covered in training on your own.

Day planner



Software requirements



JDK (v1.8_192)

Pre-requisite for using SAP Cloud Connector.



SAP Cloud Connector

Required to integrate BTP applications with on-prem resources.



Postman

REST client. Required for testing API end points.



NodeJS (v14)

For local development and testing of the sample application which will be deployed to BTP.



CF CLI (v7)

Required to deploy apps to BTP. Can also be used to manage the cloud foundry environment from CLI.



IDE

Any IDE to see and write code. E.g. Visual Studio Code, Atom.

An aerial view of a city at night, with numerous skyscrapers and a complex highway interchange. Overlaid on the image is a network of glowing yellow lines that arc between various points, suggesting a global or interconnected system. The text is centered over the image.

SAP Business Technology Platform

Fundamentals Walkthrough



What is cloud computing?

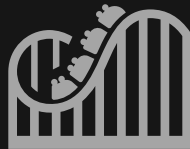
On-demand delivery of resources and services over Internet. Pay only for what you use. No need to buy, own and maintain any physical servers.

Salient benefits



Agility

Quickly access the resources needed. Compute, storage, database, etc



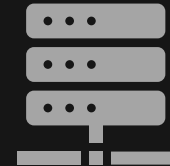
Elasticity

Scale up or down as needed within minutes.



Cost Savings

Trade fixed expenses (CAPEX) with variable expenses (OPEX)

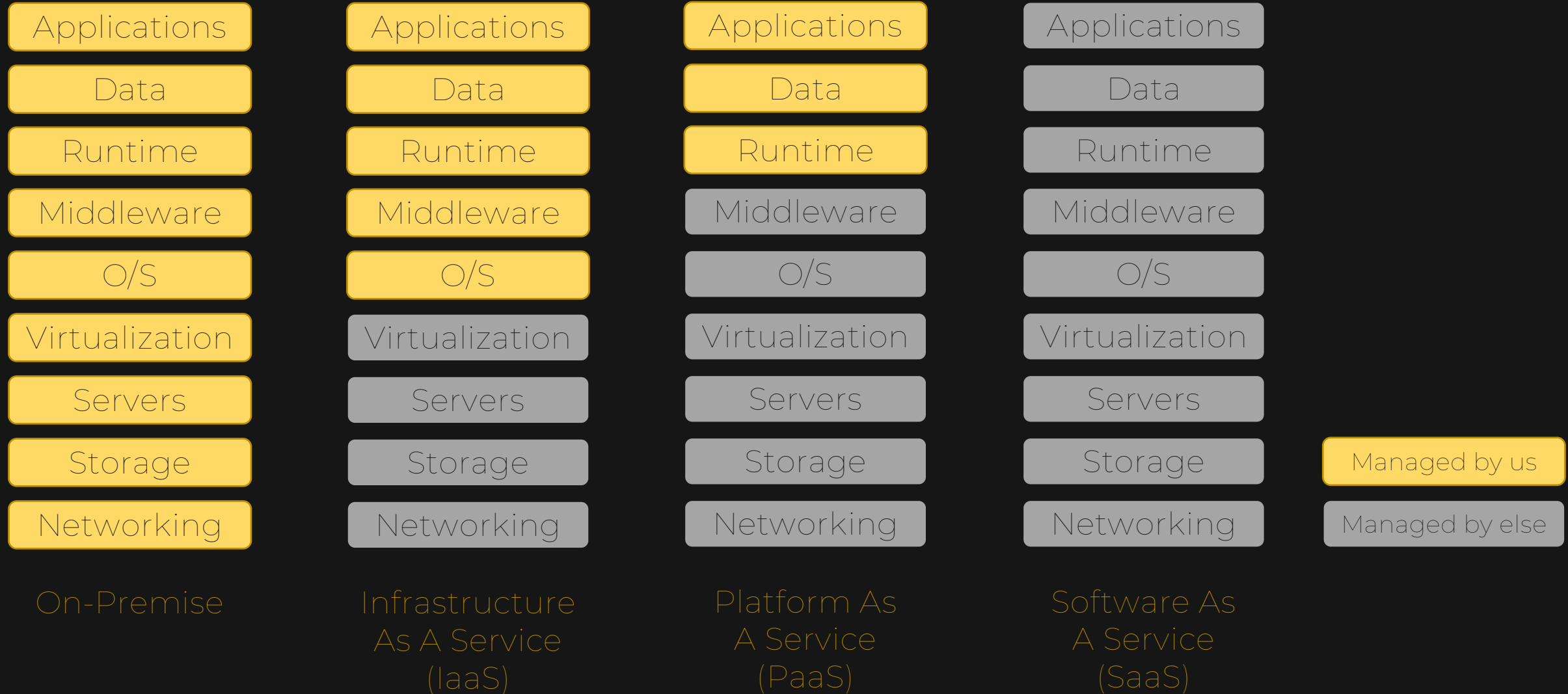


Rapid deployment

Make use of the global cloud infra and tend to global clients in minutes.



SAP BTP – Types of Cloud



2012

2013

2017

2021

SAP BTP – Accounts and Regions



Global Accounts

Entry point into SAP BTP. Based on a commercial model and enables creation of sub-accounts



Environments

Flavours of SAP BTP – Neo, Cloud Foundry, ABAP, Kyma



Sub-Accounts

Regions specific accounts with their own user management, quota of entitlements and environment.



Hyperscalars

IAAS to support various functionalities of SAP BTP



Regions

Various regions spread across the globe to provide low latency to users and cater to data privacy requirements.



Commercial Model

How to pay for the services used?

Personas



Administrators

Platform administration,
security, cost
management, etc.



Developers

Platform users. Application
development, security,
management, etc



End users

Application users, access to
authorized applications
and screens and functions
only.

SAP BTP – Cockpit walkthrough



Account Explorer

Explore and manage the various sub-accounts and directories for the global account.



Usage Analytics

Provides statistics and costs associated with various sub-accounts, directories and services linked to the global account.



Resource Provider

Register and use non-SAP resources to be used with SAP BTP.



Boosters

Meant for developers – provide guided steps to create applications and use various BTP services.



System Landscape

Add various systems in your SAP landscape (such as SuccessFactors, Concur, etc) to enable their APIs' usage within BTP.



Entitlements

Shows the services and features that are allowed to be used in the global account. Administrators can manage the entitlements for sub-accounts.

SAP BTP – Global Account Access



Add Users

Add users to the global account.



Assign Role Collection

Assign relevant role collection to user (admin / viewer).

Role Collection	Roles
Global Account Administrator	Global Account Admin, Global Account Usage Reporting Viewer, System Landscape Administrator, User and Role Administrator
Global Account Viewer	Global Account Usage Reporting Viewer, Global Account Viewer, User and Role Auditor

SAP BTP – Services & Entitlements



Services

Features provided by SAP BTP to use in the applications.



Service Plans

Limits for using that particular service.



Service Assignment

See how much quota each service has for the global account.



Entity Assignment

See what all services and plans are assigned to a particular sub-account.



Service Marketplace

See what all services and plans are assigned to a particular sub-account.



Service Instances

See what all services and plans are assigned to a particular sub-account.



SAP BTP – Trial account

What is a SAP BTP trial account?

SAP BTP trial account enables people who want to understand the usage of SAP BTP. It provides limited access to the BTP features and services to give a sense of what all can be achieved.

What all services are there in trial account?

SAP BTP free tier gives access to 33 services (as of today)

How to create a trial account?

<https://www.sap.com/india/products/business-technology-platform/trial.html>



SAP BTP – Service instances



Assign Entitlements

Assign service entitlements to a sub-account.



Create Spaces

Create spaces in sub-account to create service instances.



Create instances

Create service instances for the services in a space.

An aerial night view of a city skyline with numerous skyscrapers and a complex highway interchange. Overlaid on the image is a network of glowing yellow lines that arc between various points, representing a global or digital connectivity network. The text is centered over the image.

SAP Business Technology Platform

SAP BTP Connectivity and Security Basics

BTP Security – Users & Roles



Platform users

User who need to access the global account or the sub-account. They maintain the accounts, access and applications.



Business users

Users who don't need to access the global account or sub-account. They just need access to the business applications.



Roles

Role contain permissions to do a certain task. SAP provides predefined roles on global and sub-account levels. Developers can define their own roles based on the application requirements.



Role Collections

Collection of different roles. SAP provides predefined role collections on global account and sub-account levels. Administrators (global and sub-account) can define their own role collections based on business requirements.

BTP Security – Segregation of duties



Global Account Admins

- Assign permissions to other global account members.
- Manage global account.



Sub-Account Admins

- Assign permissions to other sub-account members and developers.
- Manage sub-account.
- Create role collections for application roles.



Application Developers

- Develop, deploy and test applications in a space in sub-account.
- Create application level security artifacts.
- Covers both technical and functional roles.



Business Users

- Access applications deployed by Developers.

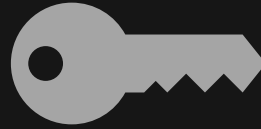


BTP Security – Sub-Account Access



Add Users

Add users to the global account.



Assign Role Collection

Assign relevant role collection to user (admin / viewer).



Provide CF Org access

Assign relevant role collection to user (admin / viewer).



BTP Security – Sub-Account RCs

Just for platform users

Role Collection	Roles
Cloud Connection Administrator	Cloud Connector Administrator
Connectivity and Destination Administrator	Cloud Connector Administrator, Destination Administrator
Destination Administrator	Destination Administrator
Subaccount Administrator	Cloud Connector Administrator, Destination Administrator, Subaccount Admin, Subaccount Service Administrator, User and Role Administrator
Subaccount Service Administrator	Subaccount_Service_Admin
Subaccount Viewer	Cloud Connector Auditor, Destination Viewer, Subaccount Service Auditor, Subaccount Viewer, User and Role Auditor



Installing pre-requisite software



JDK (v1.8_192)



SAP Cloud Connector



Postman



NodeJS (v14)



CF CLI (v7)



Visual Studio Code



Create NodeJS project

1. Make sure Node and NPM are installed on your machine.
2. Create a new folder.
3. Open command prompt at this location.
4. Do "npm init"
5. Install "express" and "body-parser"
6. Create a GET API
7. Test the API from browser.
8. Test the API from Postman.
9. Create a POST API
10. Test the API from Postman.



Deploy NodeJS project to BTP

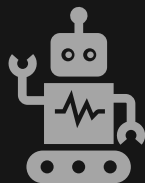
1. Create manifest.yml
2. Create .cfignore (optional)
3. Login to CF CLI
4. Do "cf push"



What is JavaScript Object Notation?



Data Interchange



Machine Readable



Human Readable



Concise Format

XML

```
<concept>
  <title>This is a Content Filtering Example </title>
  <conbody>
    <section>
      <title>This is a section that your customers need to see</title>
      <p>In this section, there is information that your customers needs to
        see. </p>
      <p>No, seriously, they need this.</p>
    </section>
    <section audience="internal">
      <title>This is a section that your internal personnel need to see
        </title>
      <p>Users don't need to see this stuff. In fact, this stuff is likely
        to confuse them.</p>
      <p>Let's make sure the users can't see this section. </p>
    </section>
  </conbody>
</concept>
```

JSON

```
{
  "concept": {
    "title": "This is a Content Filtering Example",
    "conbody": {
      "section": [
        {
          "title": "This is a section that your customers need to see",
          "p": [
            "In this section, there is information that your customers needs to
              see.",
            "No, seriously, they need this."
          ]
        },
        {
          "title": "This is a section that your internal personnel need to see",
          "p": [
            "Users don't need to see this stuff. In fact, this stuff is likely to
              confuse them.",
            "Let's make sure the users can't see this section."
          ]
        }
      ]
    }
  }
}
```

BTP Security – Overview of UAA



CF UAA

- User Account and Authentication.
- Open source implementation provided by Cloud Foundry.
- Enables Single Sign On.
- Acts as a OAuth server.



Platform UAA

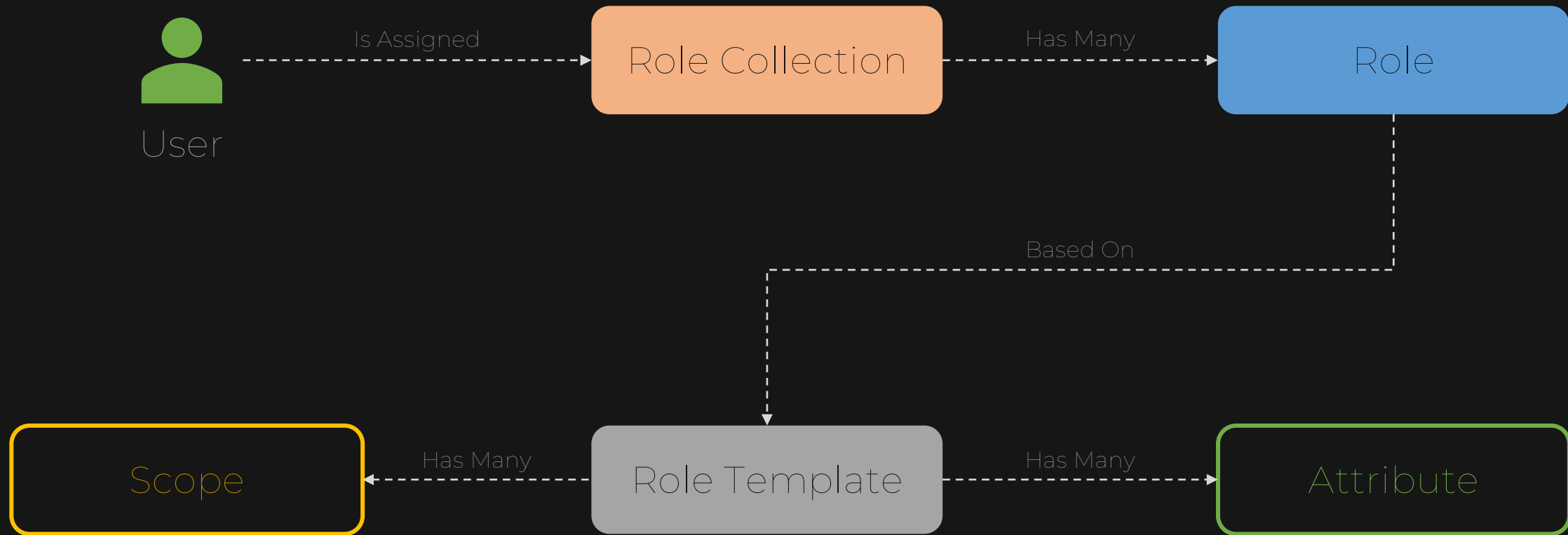
- UAA auth server required to authenticate the platform users.
- Generates OAuth tokens for platform users to administrate platform.
- Isn't a user store.
- Isn't visible to platform or business users.



XSUAA

- SAP's implementation of CF UAA to be used in SAP realm.
- Generates OAuth tokens for business users to use deployed applications.

BTP Security – Security Artifacts

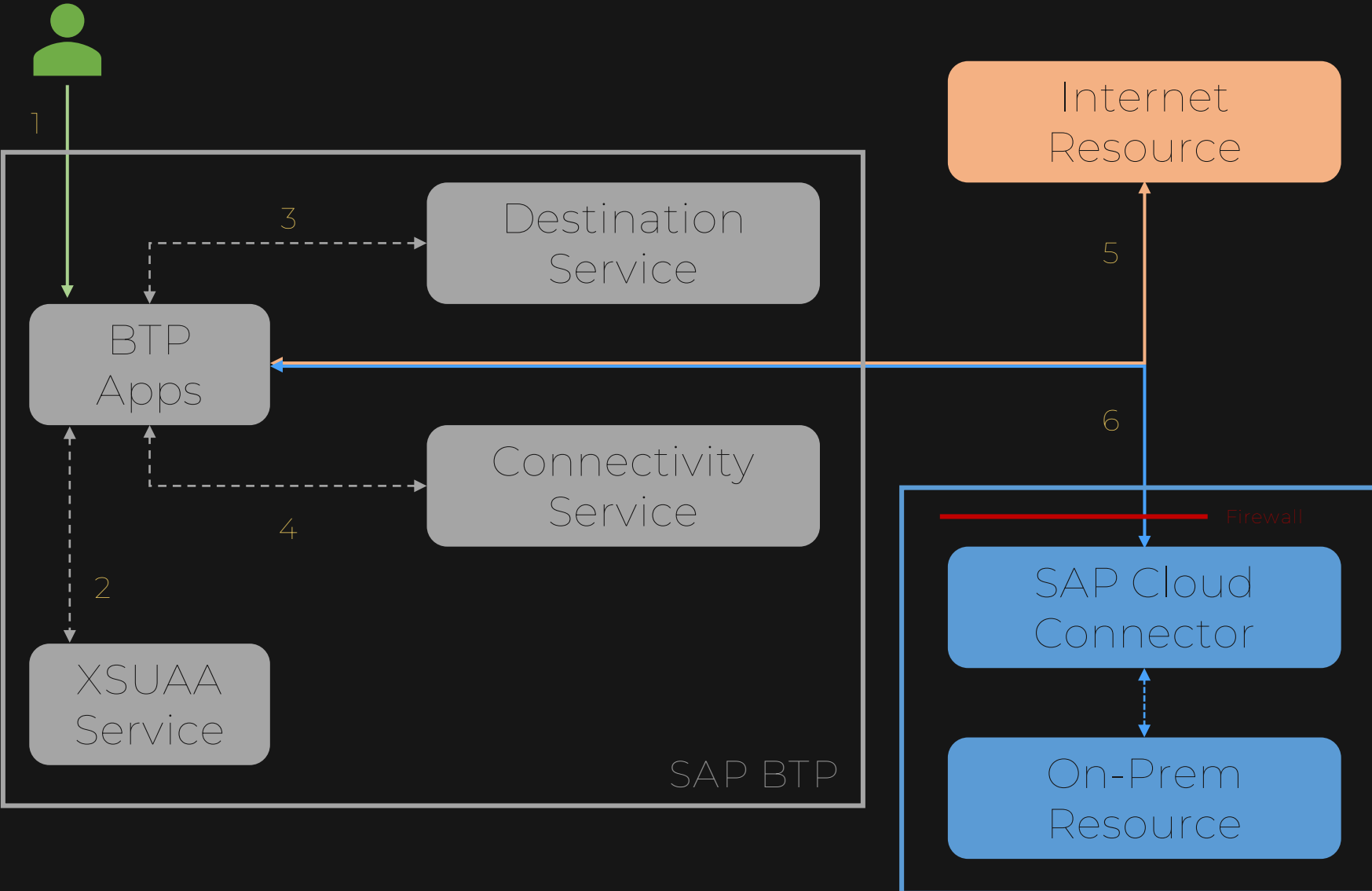


BTP Security – xs-security.json



Sample Security Descriptor

SAP BTP – Connecting other systems



Connection steps

1. User accesses the BTP application.
2. App fetches token from XSUAA service to use Destination and Connectivity services.
3. App fetches destination config – for on-prem and Internet scenarios.
4. App fetches connectivity config – for on-prem scenario.
5. App connects to the Internet resource using HTTP(s).
6. App connects to the on-prem resource through SAP Cloud Connector.



Configure SCC

1. Make sure SCC is installed (or ZIP file extracted in a folder for portable SCC).
2. Make sure JDK is installed and JAVA_HOME is available on PATH.
3. Execute "go.bat" from CMD
4. Wait for the SCC to start and initialize.
5. Open URL <https://localhost:8443> in browser.
6. Initial credentials for SCC are – Administrator / manage
7. Make sure to change the Administrator password upon first login
8. Add the sub-account in SCC (need proper auth).
9. Check in sub-account if SCC is visible.
10. Expose on-prem resources.
11. Check in sub-account if exposed resources are visible.

BTP Security – OAuth overview



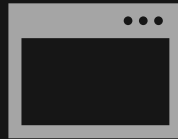
OAuth is an authorization protocol used for allowing an application to access resources on behalf of the user. It can be used with browser based applications, mobile applications, server-to-server communications, IoT devices.

OAuth Roles



Resource Owner

System that owns the protected resources.
E.g. Business user



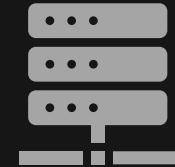
Client

System that requires access to protected resources. Access token is must. E.g. Web browser



Authorization Server

Server which authenticates the request from client and grants access token. E.g. XSUAA



















Resource Server

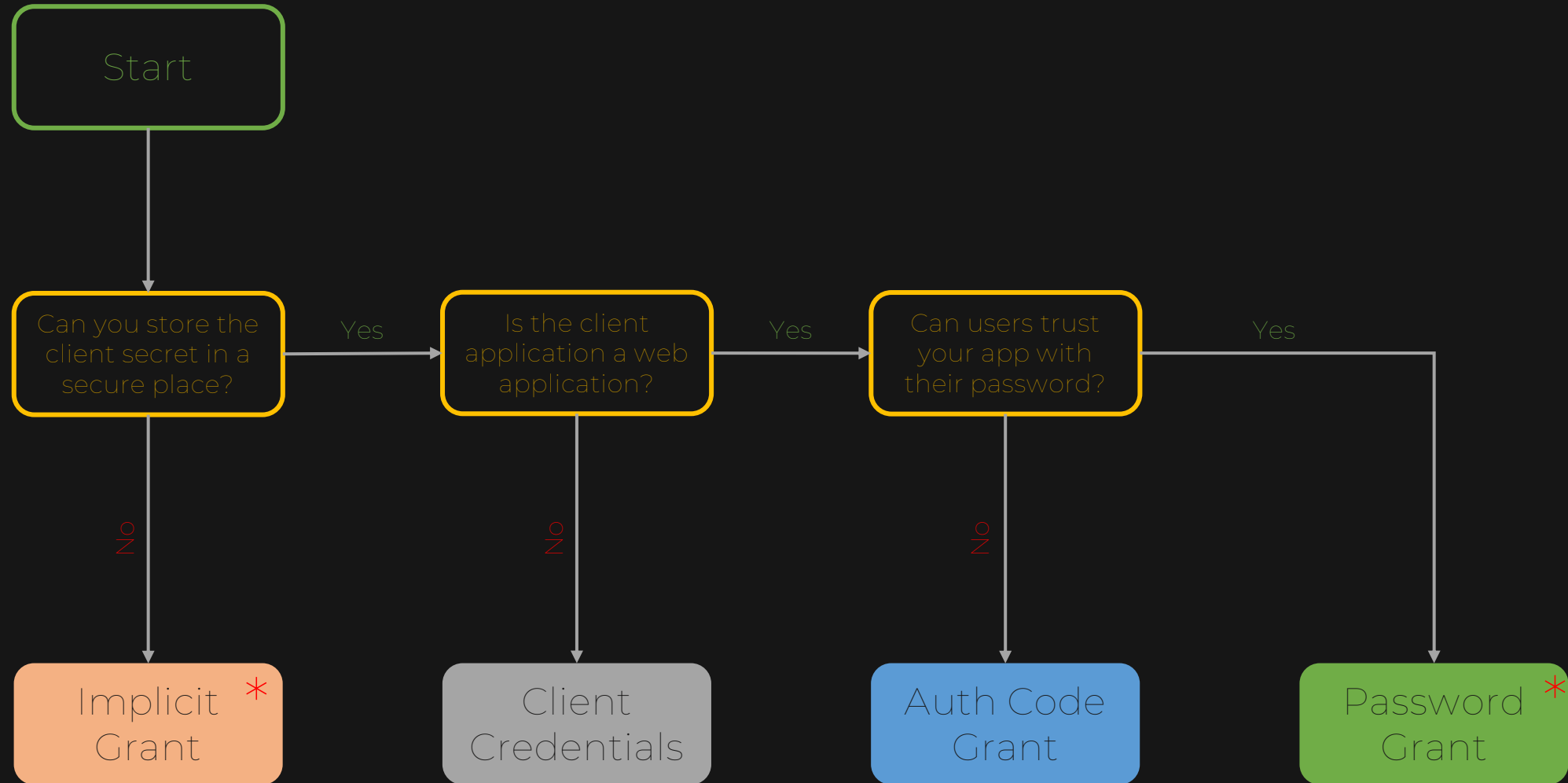
Server that protects the resource in question. E.g. Node application

BTP Security – OAuth flows



OAuth flow	Needs frontend	Needs backend	User interaction	Needs client secret
Authorization Code				
Implicit Grant				
Client Credentials				
Password Grant				

BTP Security – oAuth flows cheat sheet



* - Not recommended



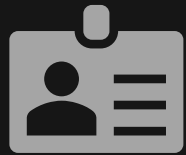
SAP Identity Authentication Service

SAP IAS – Overview



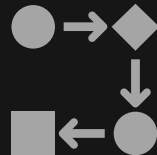
SAP IAS is a SaaS solution provided by SAP to allow controlled access to the cloud based business applications. It enables Single Sign-On (SSO), Risk Based Authentication, Self service as well as SCIM API for management.

Features



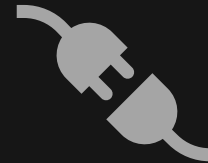
Authentication & SSO

Authentication using Form, Social, Two factor. SSO using SAML.



Risk Based Authentication

2FA based on user groups, user type and other parameters.



Delegate Authentication

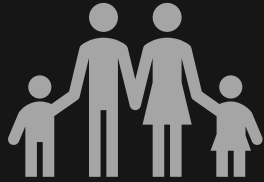
Use a third party Identity Provider as the master user store for authentication



Easy and Versatile Management

Use SCIM API for user and groups management, customize texts and branding.

SAP IAS – Scenarios



B2C

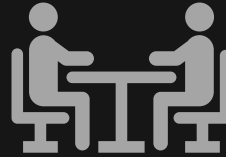
Everyone can access the application, self-registration by new users is allowed.

Administrators

Configure application settings.

Consumer

Self registration before using application.



B2B

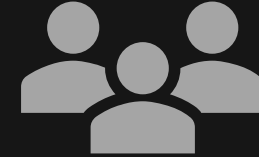
Only specified users can access application post account activation. No self registration.

Administrators

Configure application settings and register users.

Partner

Activates the account and uses application.



B2E

Assign relevant role collection to user (admin / viewer).

Administrators

Configure application and onboard employees.

Employee

Activates the account and uses application.



SAP IAS – Users & Authorization



Add users

Users maintained in the IAS tenant can access the applications linked to the IAS tenant.



Add administrators

Administrators can manage the IAS tenant and the applications and users linked to it.



Add user groups

Users can be grouped together to provide access to various business applications and resources.



SAP IAS – Adding Applications



Add new application



Establishing Trust



Trusted Domains



Risk Based Auth



SAML 2.0 config



Password Recovery



SAP IAS – Tenant Settings



Logo



MFA



Trusted Domains



Risk Based Auth



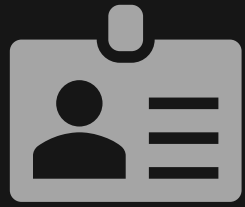
SAML 2.0 config



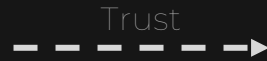
Password Recovery



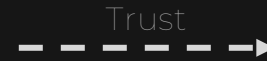
SAP IAS – MS AAD Corporate IdP



MS Azure AD



SAP IAS

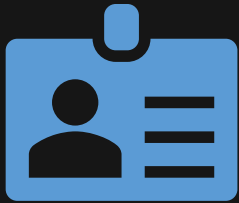


SAP BTP



SAP IAS – SCIM APIs

Within the BTP application configured in IAS tenant go to Trust → Client Authentication



Create a client secret for the client application.



Use client id (username) and client secret (password)



SAP IAS – Two factor authentication

For the IAS Tenant

1. Go to Tenant settings.
2. Go to Multi-Factor Authentication.
3. Turn on Multi-Factor Auth option.

When logging into the IAS tenant,

1. Use SAP Authenticator to link the tenant.
2. Once linked SAP Authenticator will provide TOTP's which will be used as passcode.

For an application

1. Go to the application in question.
2. Go to Authentication and Access.
3. In Risk-Based Authentication either,
 1. Create a new rule for 2FA
 2. Enable 2FA by default

When logging into the application,

1. Use SAP Authenticator to link the tenant.
2. Once linked SAP Authenticator will provide TOTP's which will be used as passcode.

SAP Identity Provisioning Service

SAP IPS – Overview



SAP IPS is a SaaS solution provided by SAP to allow management and automation of lifecycle process of identities.

Features



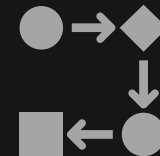
User & Group Provisioning

Provision users and groups between various SAP and Non-SAP systems.



User & Group Filtering

Configure transformations and filtering properties to fine tune provisioning.



Full & Delta Read Mode

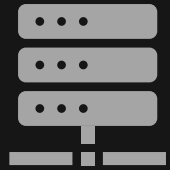
Provisioning job can run in full or delta mode to read all or only the changed identities.



Job Logging & Notifications

View and export job logs. Get notified for status of provisioning jobs.

SAP IPS – Concepts



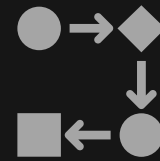
Systems

Source, Target and Proxy systems used for provisioning.



Properties

Properties control the connection to systems and behavior of the provisioning job.



Transformations

Read (source) and write (target) transformations allow conversion of identities from one format to another.



Jobs

Scheduled or ad-hoc on source system provisions identities in all relevant target systems.



SAP IPS – Process overview

Admin



SAP IPS



An aerial view of a city at night, with numerous skyscrapers and a complex network of glowing yellow lines that arc across the sky, connecting various points, symbolizing global connectivity and technology.

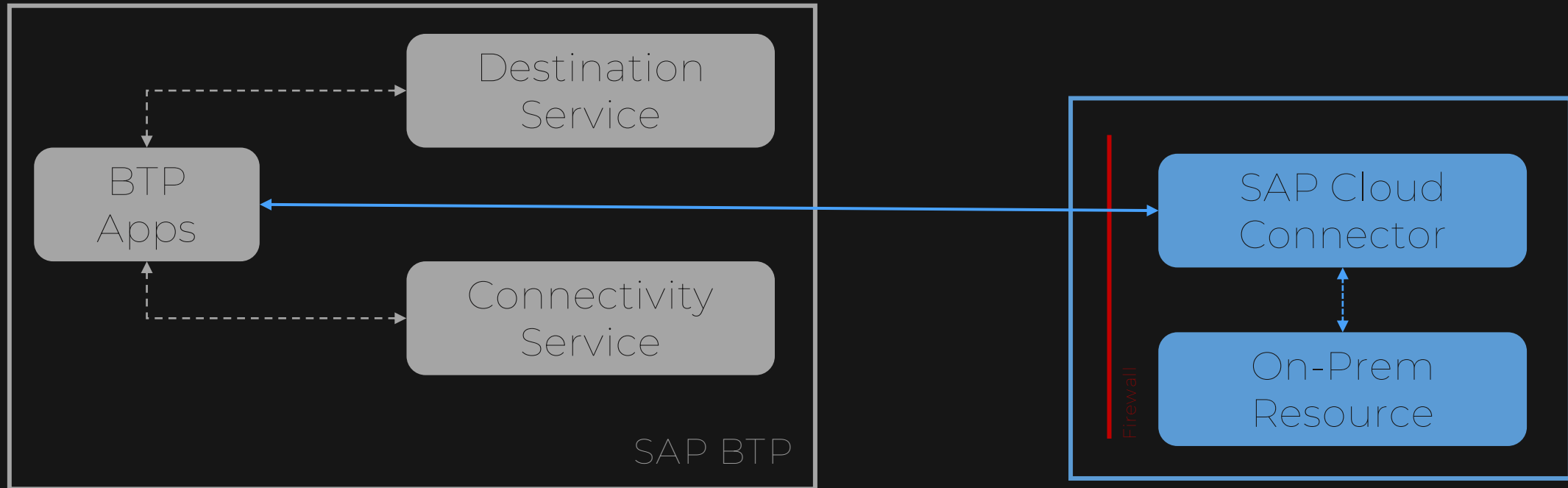
SAP Business Technology Platform

On Premise Connectivity

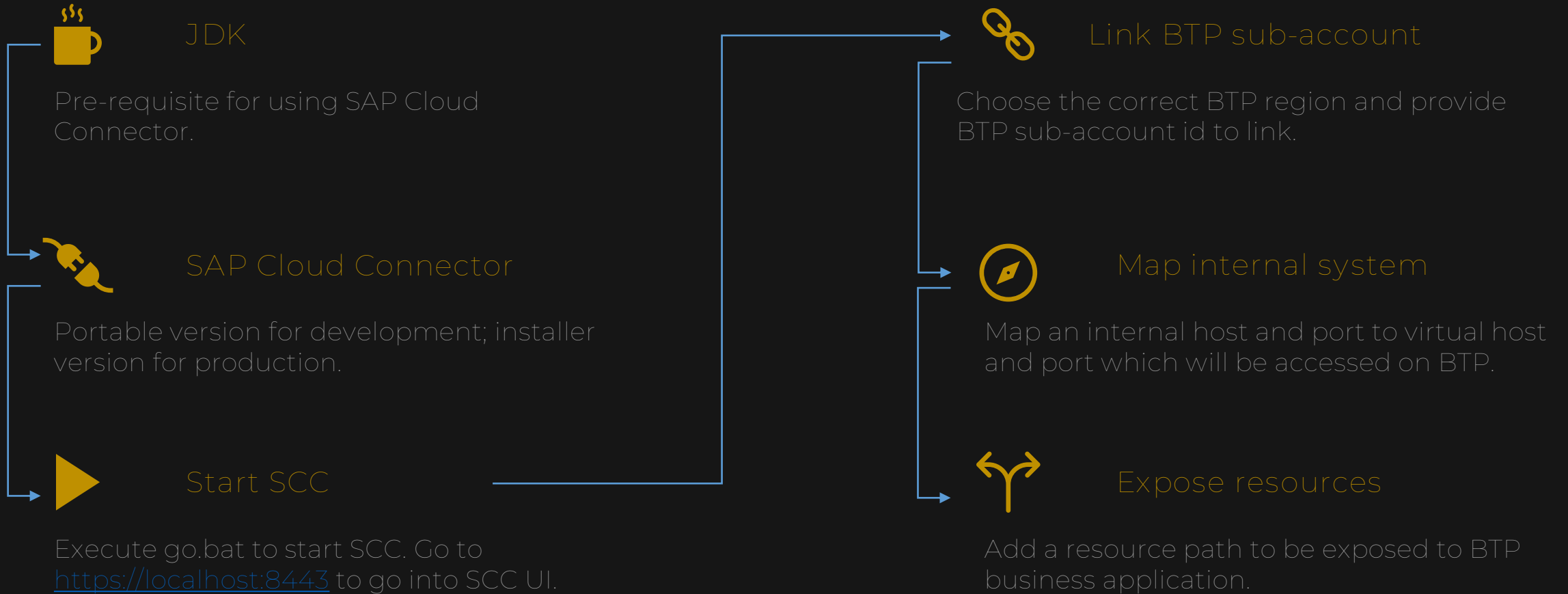


SAP BTP – On-Prem connectivity

In order to connect BTP business applications to an on-prem resource (SAP or Non-SAP) we need SAP Cloud Connector.



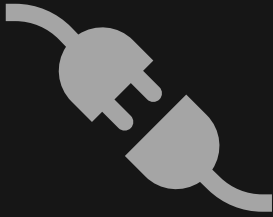
SAP BTP – SCC Setup





SAP BTP – SCC Setup (validation)

1



Cloud Connector should be available (with resources exposed) in BTP sub-account under Connectivity → Cloud Connectors

2



Destination pointing to the cloud connector resource should be able to connect (green tick)

A 3D rendering of a warehouse conveyor belt system. Several cardboard boxes are positioned on the belt, which is flanked by metal guides. Red laser lines are projected onto the floor and the boxes, likely for automated sorting or tracking. The scene is dimly lit, with the primary light source being the red laser lines. The text "Application Walkthrough & Demo" is overlaid in the center in a white, sans-serif font.

Application Walkthrough & Demo

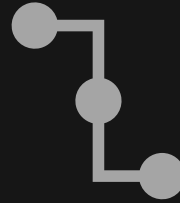


Capstone project – Requirements



Connectivity

Business app should be able to connect to an on-prem server to fetch data and perform operations.



Authentication

Authentication should be enabled on business app so that only the authenticated users are able to access the application.



Authorization

Users should have proper authorization in order to access the application.

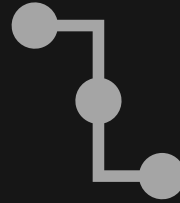


Capstone project – Tech Design



Connectivity

SAP Cloud Connector will be setup and linked to the SAP BTP sub-account to establish on-prem connectivity.



Authentication

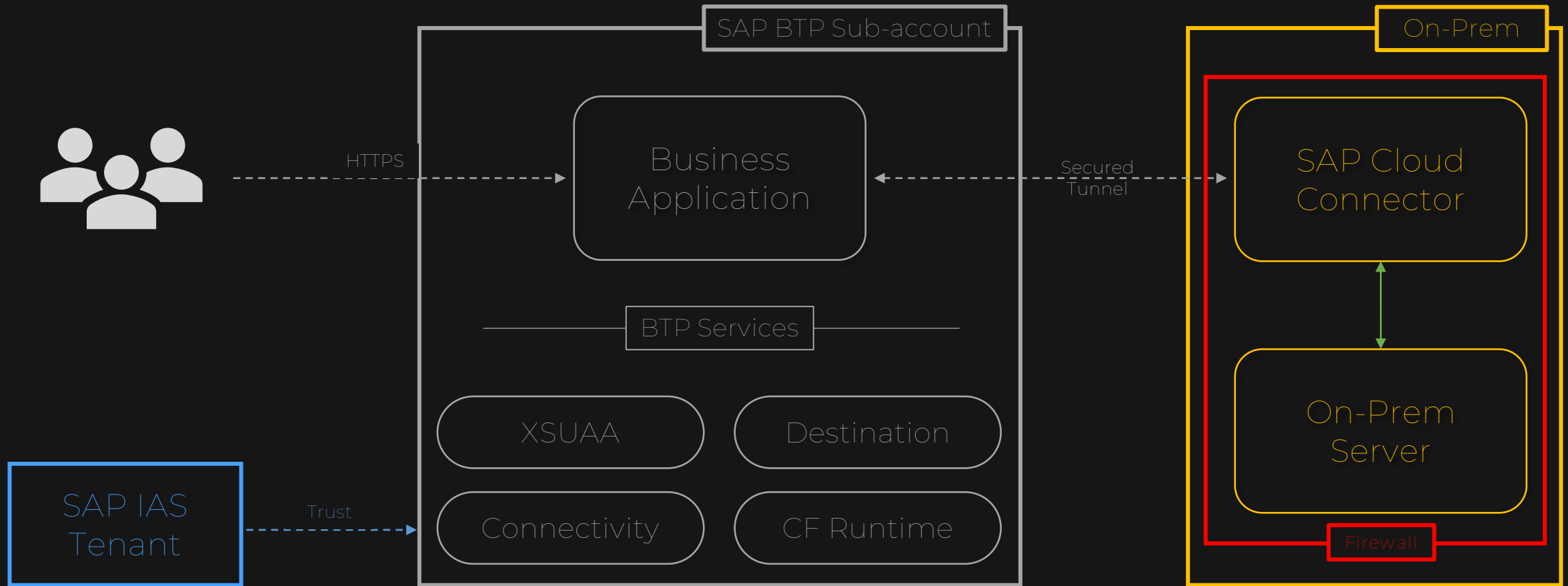
SAP IAS tenant will be setup as the identity provider to supply the users.



Authorization

Application will define role collections and IAS groups will be mapped to those role collections.

Capstone project – Architecture





Capstone project – Steps

On-Prem

1. Install Java (JDK 1.8_192) as a pre-requisite to work with SAP Cloud Connector.
2. Install SAP Cloud Connector.
3. Add the BTP sub-account in SCC.
4. Create a Node application locally.
5. Run the local node server.
6. Expose the local node server resources through SCC.

BTP

1. Validate if cloud connector is linked with the BTP sub-account.
2. Create destination to connect from BTP to the connected cloud connector.
3. Check if destination is working properly (green tick).
4. Deploy an app on BTP (node-btp).
5. Create service instances of XSUAA, Destination and Connectivity services.
6. Bind services instances to the app.
7. Get destination service access token.
8. Get connectivity service access token.
9. Get destination configuration (use the destination access token from step 7).
10. Call the on-prem server from BTP app.
11. Add authentication in BTP app (app-router).
12. Add authorization in BTP app (xs-security.json).
13. Establish trust between BTP and IAS.
14. Create users in IAS.
15. Assign appropriate group in IAS.
16. Map IAS group to BTP role collection.



Capstone project – Hands-on

- 1 On-prem Node server
Clone this git repo - <https://github.com/sagedev2k16/local-node-server.git>
- 2 BTP Node app
Clone this git repo - <https://github.com/sagedev2k16/node-btp.git>
- 3 Setup Cloud Connector
Install, configure and validate SCC configuration on SAP BTP
- 4 Deploy on BTP
Deploy business app on BTP and update XSUAA service instance
- 5 Configure SAP IAS tenant
Establish trust between BTP and IAS, create users and groups in IAS
- 6 IAS groups ↔ BTP role collections
Map IAS groups with BTP role collections.

