



IBM Bluemix Development & Certification

Summary decks for a course that covers the A to Z of IBM Bluemix.

For more information visit:
<http://www.acloudfan.com>

raj@acloudfan.com

1. Security Services
2. Using the SSO Service

PS: Certification practice test questions NOT included in the summary decks

Discounted access to the courses:



<https://www.udemy.com/ibm-bluemix/?couponCode=BLUE100>

Coupon Code = **BLUE100**



<https://www.udemy.com/rest-api/?couponCode=REST100>

Coupon Code = **REST100**

PS:

- For latest coupons & courses please visit: <http://www.acloudfan.com>
- Enter to **WIN Free access** – please visit: <http://www.acloudfan.com/win-free-access>



Static Analyzer



Static Analyzer
IBM

- Static code analysis to identify vulnerabilities (Java)
- Should be leveraged during the software development cycle
 - Identifies unsafe data handling and API calls
- How it is used?
 - Create instance of the service
 - Generate *Intermediate Representation (IRX)* of code & upload to analyzer
 - Address vulnerabilities using the report

Single Sign On Service



Single Sign On
IBM

- Policy based configuration of single sign on (SSO) implementation
 - Applications need not be aware of identity sources
- Identity sources
 - Enterprise LDAP directory – SAML integration
 - Cloud directory. A user registry hosted on IBM Cloud
 - Social identity sources. Facebook, LinkedIn, Google+

AppScan Dynamic Analyzer

- Scans a deployed web application for vulnerabilities



AppScan Dynamic
Analyzer
IBM

Enging scan	Production scan
<ul style="list-style-type: none">Abuse of FunctionalityBuffer OverflowContent SpoofingCredential GuessingCross-site Request ForgeryCross-site ScriptingDenial of ServiceDirectory TraversalFormal StringHTTP Response SplittingInformation LeakageInteger OverflowInsufficient AuthenticationInsufficient AuthorizationInsufficient Session SignatureInsufficient Transport Layer ProtectionInteger OverflowLDAP InjectionSQL Command InjectionMalicious Content TheftNull Byte InjectionOS CommandingPath TraversalPredefined Resource LocationRemote File InclusionServer MisconfigurationSession FixationSQL Audit AbuseSQL InjectionSQL InjectionURL Redirect AbuseXML External EntityXML External Entity	<ul style="list-style-type: none">Abuse of FunctionalityBuffer OverflowContent SpoofingCross-site Request ForgeryCross-site ScriptingDirectory TraversalFormal StringHTTP Response SplittingInformation LeakageInsufficient AuthenticationInsufficient Transport Layer ProtectionLDAP InjectionMalicious Content TheftNull Byte InjectionOS CommandingPath TraversalRemote File InclusionServer MisconfigurationSession FixationSQL InjectionSQL InjectionURL Redirect AbuseXML External EntityXML InjectionXML Injection

raj@acloudfan.com
<http://www.acloudfan.com>



Summary

- Static analyzer service used for detecting vulnerabilities in the code
- AppScan Dynamic analyzer identifies vulnerabilities in the deployed app
- SSO service for implementing SSO for applications
 - Enterprise LDAP directory – SAML integration
 - Cloud directory. A user registry hosted on IBM Cloud
 - Social identity sources. Facebook, LinkedIn, Google+



Using the SSO Service

Steps to integrate with SSO service (Cloud Dir)

1

Create the SSO service Instance

2

Create a new Identity source - cloud directory + add users

3

Integrate the application with the identity source



Step#1 From Bluemix service catalog select the SSO service



Single Sign On

Step#2 Provide a name for the service



Single Sign On

PUBLISH DATE
12/15/2015

AUTHOR
IBM

TYPE
Service

LOCATION
US Northeast

[VIEW DOCS](#)

Implement user authentication for your web and mobile apps quickly, using simple policy-based configurations.

- **Secure apps with confidence, not a lot of coding**

Add user authentication to your apps with policy-based configuration options and an easy to use SDK. Writing Java apps? Take advantage of our zero-coding approach.

- **You choose the identity sources and we do the rest**

Whether you are using an existing enterprise directory with SAML, popular social identity sources like Facebook, LinkedIn, and Google, or you want to create your own cloud directory, it's easy to setup. Even better, apps don't require knowledge about all of the sources that users might authenticate from.



Add Service

Space:

App:

Service name:

Selected plan:

[CREATE](#)

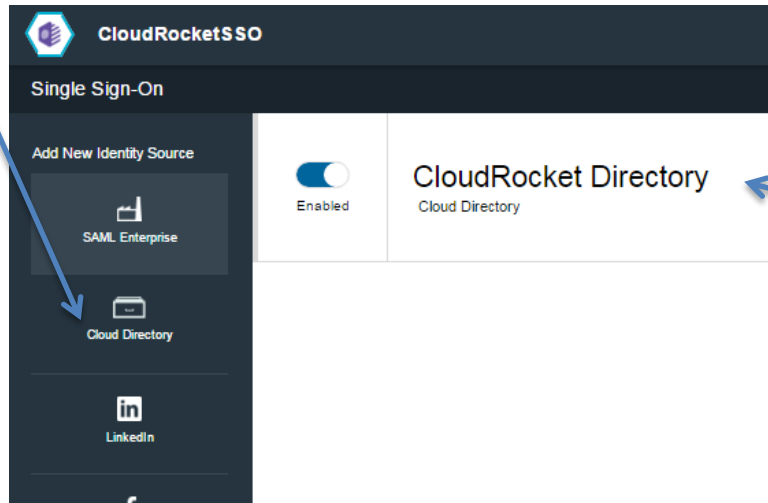
rocketsso

Step#3 Save the service instance



Step#1 Click on manage

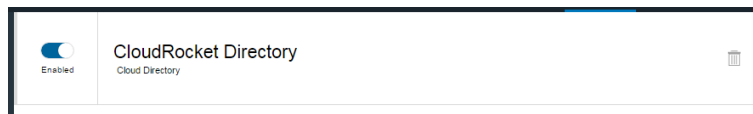
Step#2 Create the provider for Identity Source



Provide the name



Step#1 Click on *Cloud Directory*

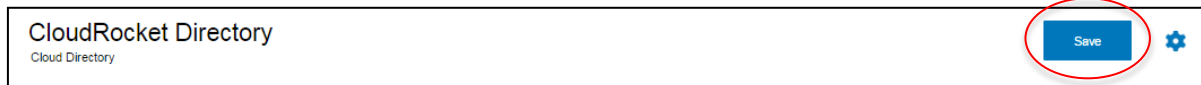


Step#2 Click on  to add the users

Step#3 Provide user information & save

A screenshot of a 'Add User' form. It contains several input fields: 'Username' (with 'acloudfan' entered), 'Password', 'Verify password', 'Given name', 'Surname', and 'Email'. At the bottom of the form are two buttons: 'Cancel' and 'Save'.

Step#4 Save the cloud directory



Here you associate configure the application:

1. Select the Identity source e.g., cloud directory you may have created
2. Set the Return URL – NOT the same as user/password screen URL

