COLLEGE CODE: 8107

COURSE: Cloud Application Development - Group 5

PHASE IV: PROJECT SUBMISSION

PROJECT TITLE: Chatbot Deployment with IBM Cloud Watson Assistant

Team Members:

ABINAYA S – 810721243002

abinaya.s1@care.ac.in

DHARSHINI K – 810721243017

dharshini.k@care.ac.in

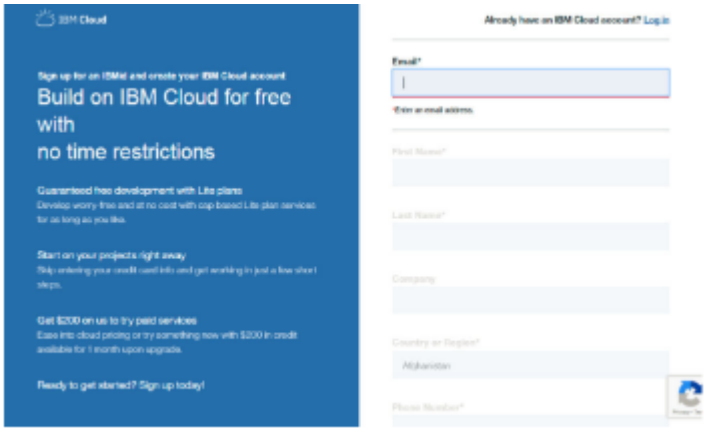
HELAN SUJA R – 810721243021

helansuja.r@care.ac.in

MANIDEEPA – 810721243030
manideepa.m@care.ac.in

MONICA PUSHPA X – 810721243031
monicapushpa.x@care.ac.in

Getting started: Creating an IBM Cloud account



Before you work on any of the exercises in this course, you must sign up for an IBM Cloud account.

You can register for a free IBM Cloud Lite account.

For more information about IBM Cloud Lite account, see the following video:

https://www.youtube.com/watch?v=0rMYXcbpHbI

Getting started: Creating an IBM Cloud account

1. Open the IBM Cloud page: http://bluemix.net

2. Click Create a free account:

If you do not have an IBM ID, complete the personal information to create one.

Creating an IBM Cloud ID automatically creates an IBM ID for you.

There is no charge to create an IBM ID or an IBM Cloud Lite account.

Getting Started: IBM Cloud accounts

IBM Cloud account comparison

	Lite	Pay-As-You-Go	Subscription
Access to free Cloud Foundry memory	256	512	512
Access to Lite service plans	✓	✓	✓
Access to all free plans		✓	✓
Access to the full catalog		✓	✓
No time restrictions	✓	✓	✓
Guaranteed zero cost	✓		
Negotiated pricing			✓
Best for learning or building POCs	✓	✓	
Fit for production use cases		✓	✓

When you sign up for a free IBM Cloud Account, you start with the Lite account. A Lite account includes the following main features:

The account is free (no credit card required).

The account never expires.

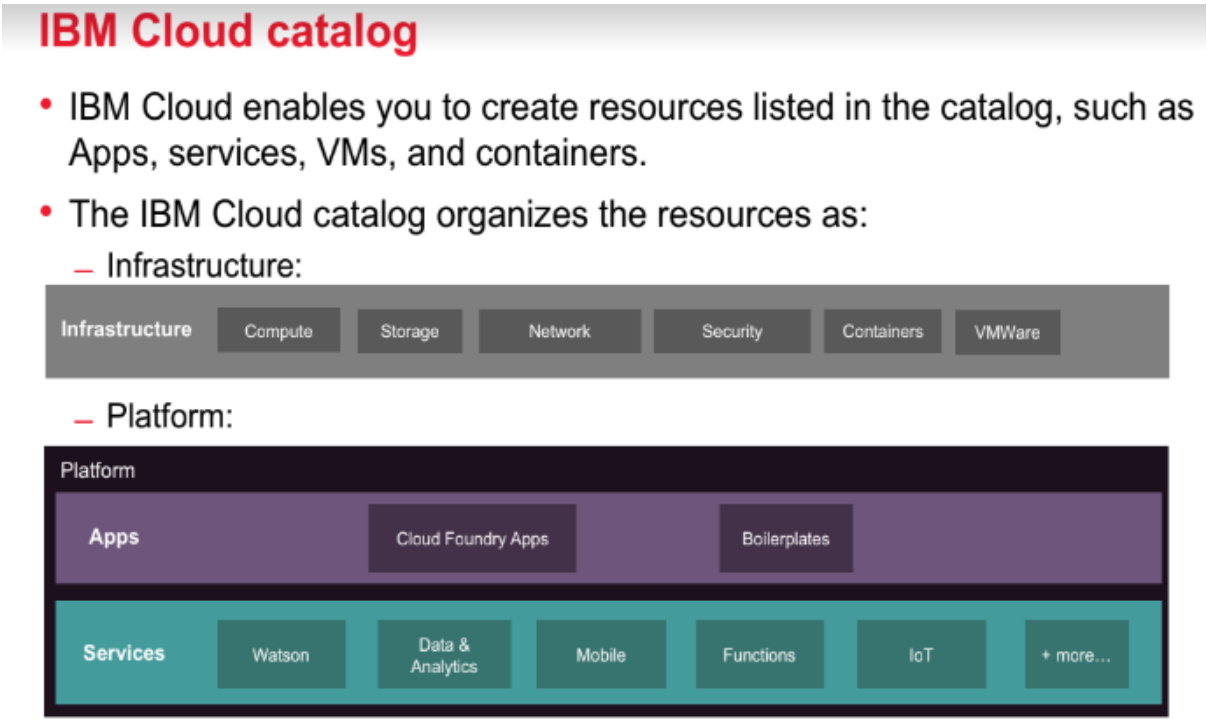
You receive 256 MB of memory for your Cloud Foundry applications.

You have access to a specific services that are tagged as Lite.

A Pay-As-You-Go account requires entering your credit card information. With a Pay-As-You-Go account, you are eligible for free runtime and service allowances. If you use more than the free allowance, you receive a monthly IBM Cloud invoice. This invoice provides 512 MB of free memory for your Cloud Foundry applications. In addition, all of the free services that are in the catalog are available to you. Charges are based on your use of IBM Cloud compute and services.

With a Subscription account, you commit to a minimum spending amount each month and receive a subscription discount that is applied to that minimum charge. You also pay for any usage that exceeds the minimum spending amount.

IBM Cloud catalog



You can create resources in IBM Cloud. Resources are entities in IBM Cloud catalog, such as Cloudant, a Cloud Foundry application, virtual machine, or container.

IBM Cloud catalog features the following categories of resources:

Infrastructure: Resources that provide fine-grained control over the computing infrastructure

Platform: Resources help you rapidly build and deploy your applications. Consider the following points:

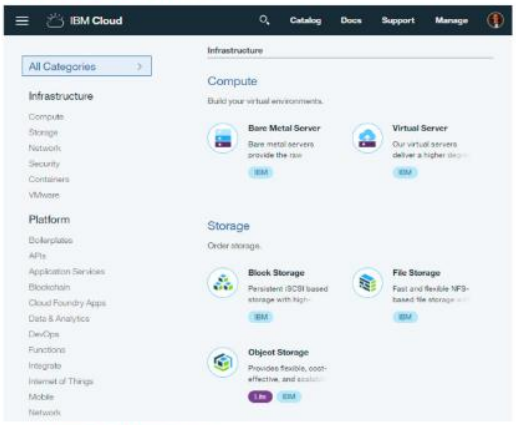
– Applications can be built by using Cloud Foundry Apps or Boilerplates, which provide the runtimes and optionally other services to create your applications.

– Services enable you to easily add relevant functionality to your application.

IBM Cloud: Infrastructure

IBM Cloud catalog: Infrastructure

- Compute
- Storage
- Network
- Security
- Container
- VMWare



Containers and virtual servers share objectives: To isolate an application and its dependencies into a self-contained unit that can run anywhere. They both remove the need for physical hardware, which allows for more efficient use of computing resources.

Virtual servers, or virtual machines (VM), are created by using a hypervisor. The hypervisor virtualizes the physical hardware to create a software-defined computer that runs its own operating system. Unless special software is installed for cloud management, an operating system that is running on a VM is unaware that it is running on VM.

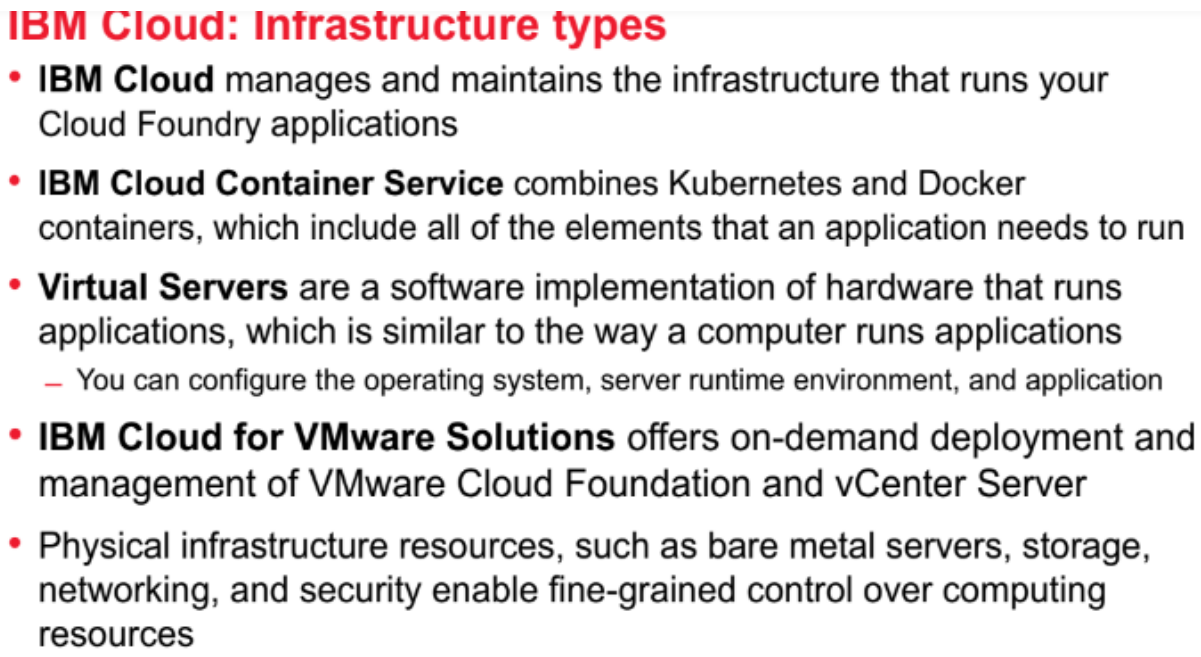
Unlike a VM that provides hardware virtualization, a container provides operating system-level virtualization.

A container library, such as Docker, separates different user spaces for each container. On the surface, these spaces might resemble a VM to a user.

The main difference between containers and VMs is that containers share the operating system kernel with other containers that are running on the machine, which is not the case with VMs. Therefore, you might see a VM running Linux on a Windows server, or Windows on a Linux server.

However, you do not see a container that runs Linux on anything other than a Linux server. The containers on that Linux server are separate user spaces on that Linux server and the hardware is not virtualized.

IBM Cloud: Infrastructure types



IBM Cloud manages and maintains the infrastructure that runs your Cloud Foundry applications.

IBM Cloud supports the following alternative infrastructure types:

IBM Containers provide more control over the computing infrastructure to run the application and services through Docker-like APIs. Docker packages software into standardized units that are called containers. Containers are described later in this unit.

Virtual servers are software implementation of hardware that runs applications, which is similar to the way a computer runs applications. You can configure the operating system, server runtime environment, and application. If you want to control the infrastructure down to the operating system level, consider the use of virtual servers.

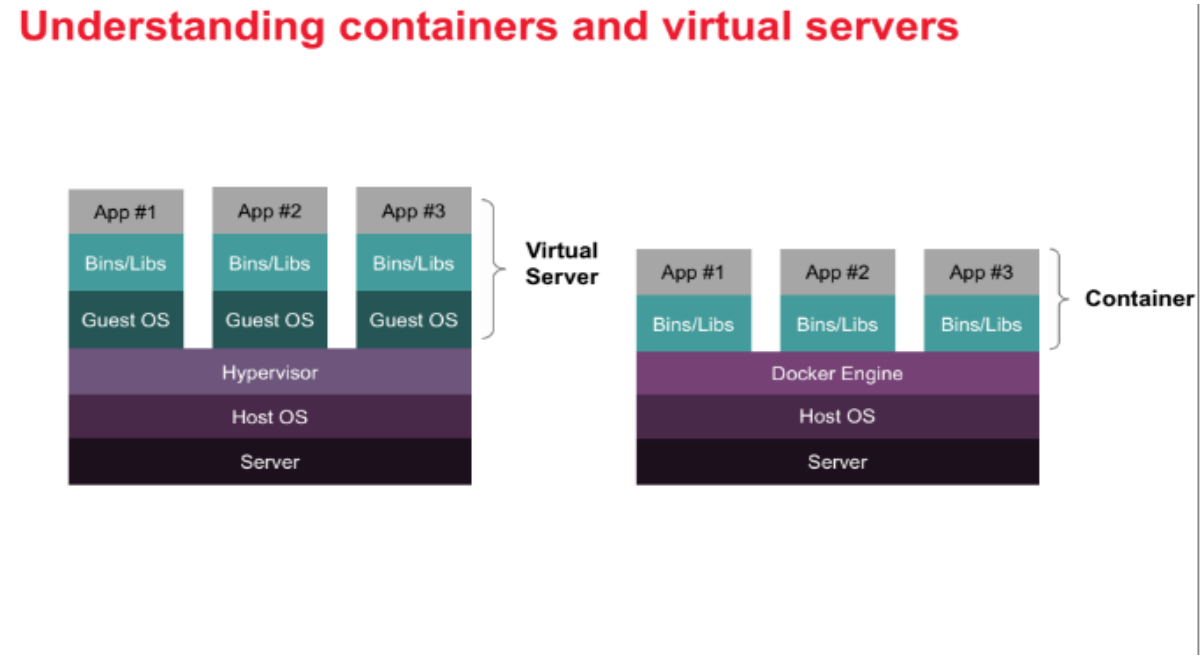
IBM Cloud for VMware Solutions offers on-demand deployment and management of VMware Cloud Foundation and vCenter Server.

You also can deploy and use physical infrastructure resources, such as bare metal servers, storage, networking, and security, for fine-grained control over computing resources.

Most developers in the enterprise likely use some mix of these types of infrastructure. The

exercises in this course introduce you to the Cloud Foundry infrastructure in IBM Cloud. As such, the use of containers, virtual servers, IBM Cloud for VMware Solutions, and physical infrastructure resources are out of scope of this course. This courses focuses on Cloud Foundry applications.

Understanding containers and virtual servers



Containers and virtual servers share objectives: To isolate an application and its dependencies into a self-contained unit that can run anywhere. They both remove the need for physical hardware, which allows for more efficient use of computing resources.

Virtual servers, or virtual machines (VM), are created by using a hypervisor. The hypervisor virtualizes the physical hardware to create a software-defined computer that runs its own operating system. Unless special software is installed for cloud management, an operating system that is running on a VM is unaware that it is running on VM.

Unlike a VM that provides hardware virtualization, a container provides operating system-level virtualization.

A container library, such as Docker, separates different user spaces for each container. On the surface, these spaces might resemble a VM to a user.

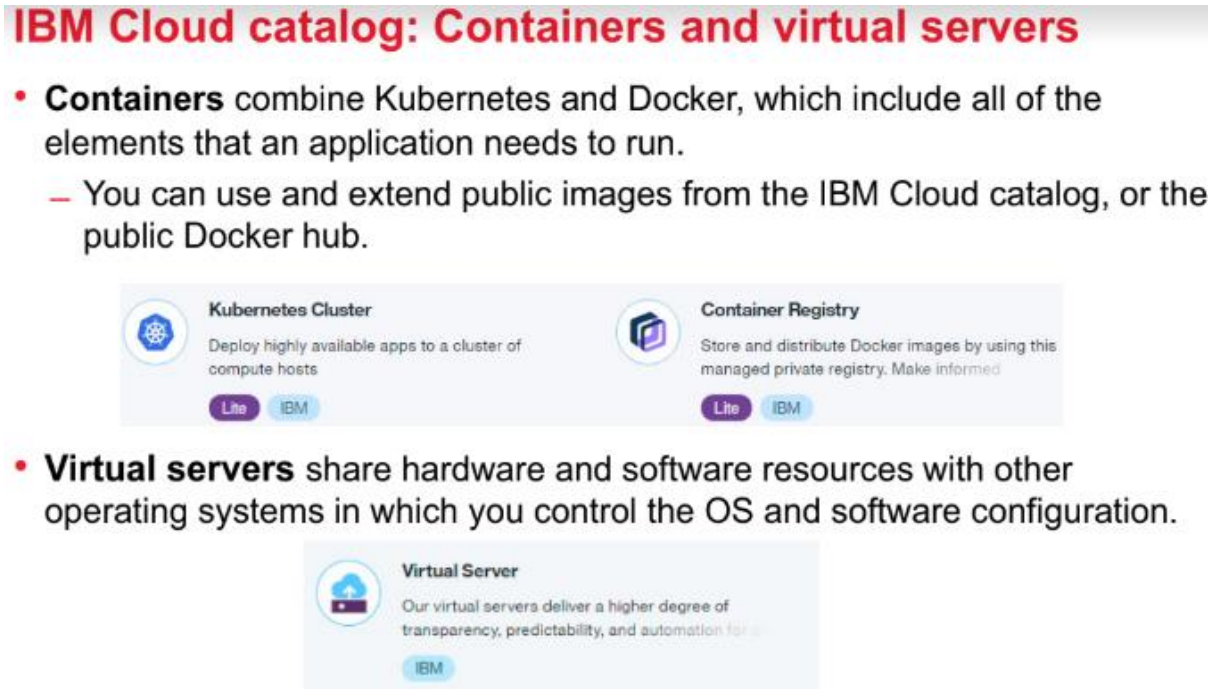
The main difference between containers and VMs is that containers share the operating

system kernel with other containers that are running on the machine, which is not the case with VMs. Therefore, you might see a VM running Linux on a Windows server, or Windows on a Linux server.

However, you do not see a container that runs Linux on anything other than a Linux server. The containers on that Linux server are separate user spaces on that Linux server and the hardware is not virtualized.

Data storage also is managed differently in containers. In VMs, virtual disks are created and are similar to physical disks in that after you write something to the disk, it stays there until you delete it. With containers, you can make changes to the disk and then delete your changes when you are done.

IBM Cloud catalog: Containers and virtual servers



IBM Cloud supports the following alternative infrastructure types:

Containers provide more control over the computing infrastructure to run the application and services through Docker-like APIs. Docker packages software into standardized units that are called containers. Containers include all of the elements that an application needs

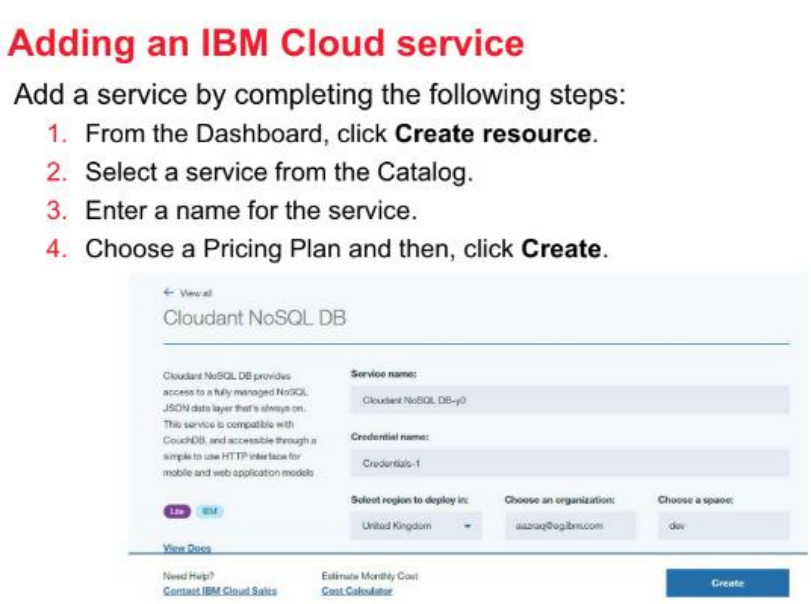
to run. IBM Cloud container service (Kubernetes cluster) combines Docker and Kubernetes to deliver powerful tools, an intuitive user experience, built-in security and isolation to automate the deployment, operation, scaling, and monitoring of containerized applications over a cluster. You can create a Kubernetes cluster that consists of one or more VMs that are called worker nodes. Every worker node represents a compute host in which you can deploy, run, and manage containerized applications.

You can use and extend public images, such as the IBM Integration Bus V10 Developer Edition, which you can use to start developing your own integration solution.

Containers give you more control, but still do not require you to manage an operating system or network. IBM containers resemble the popular open source container engine Docker, but have some IBM Cloud specific features, such as their ability to integrate with the Cloud Foundry routers.

Virtual servers are software implementation of hardware that runs applications that is similar to a computer. You can configure the operating system, server runtime environment, and application. If you want to control the infrastructure down to the operating system level, consider the use of Virtual servers.

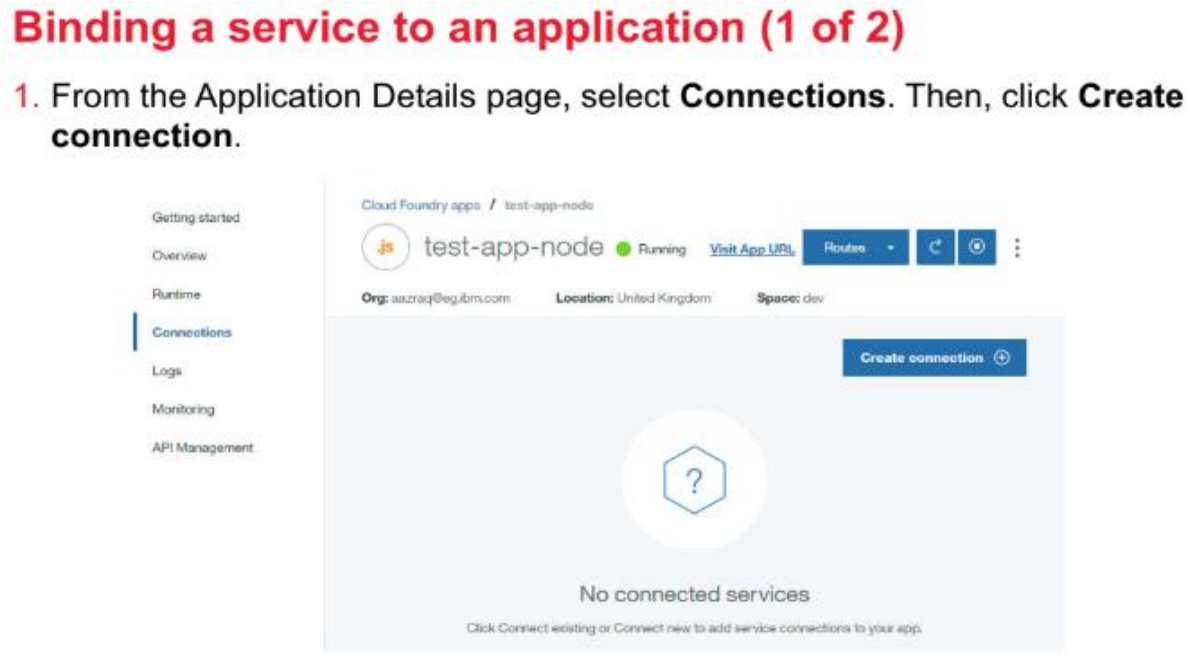
Adding an IBM Cloud service



You can add an IBM Cloud service to your application by clicking Create resource from the application dashboard and then, selecting a service from the IBM Cloud Catalog. You must then enter a name for the service and select a pricing plan for your service. Plans allow you to choose different “sizes” for the service, such as how much power you put behind it. For example, with some services you can choose if you share hardware or use dedicated hardware.

You can bind the service to your application from this page, or leave the service unbound. If you leave the service unbound, IBM Cloud creates and provides credentials for accessing the service, which you can access from within the service dashboard. If you bind the service to an application, the credentials are in the application's environment variables.

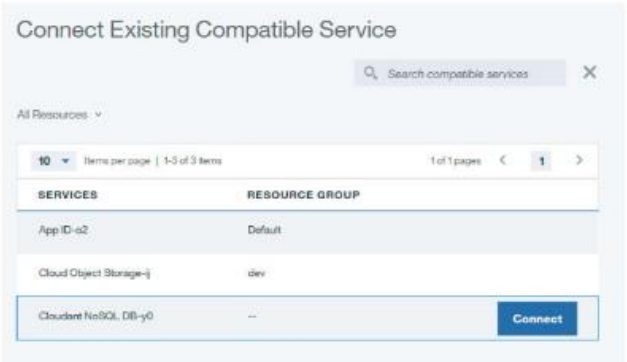
Binding a service to an application



To bind the service to your application, browse to your Application Details page and select the Connections tab on the left navigation bar. Then, click Create connection.

Binding a service to an application (2 of 2)

2. Select the service to bind to your application:
   - IBM Cloud lists the services that are compatible with your application and runtime environment only.
   - You can bind a service to more than one application.



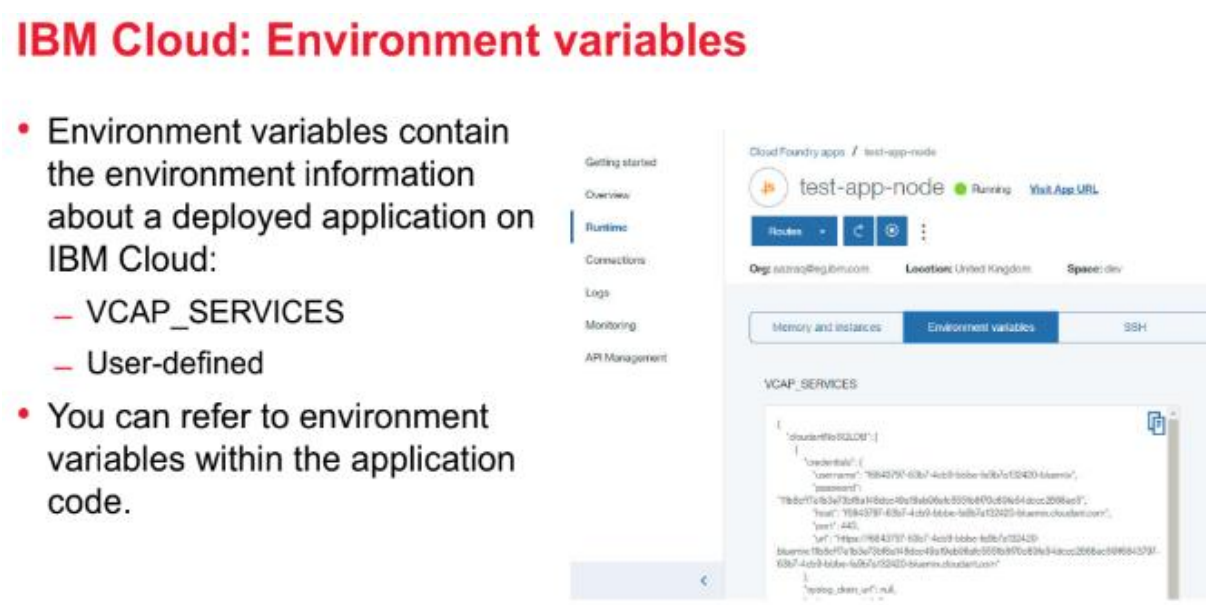
To bind a service to your application, hover over the compatible service and click Connect. A dialog box prompts you to restage the application. Click Restage.

Restaging the application makes the service available for use by your application.

IBM Cloud allows you to choose one of the services that was created earlier to bind it to your application. IBM Cloud lists the services that you created that are compatible with your service and runtime environment. Some services are specific to certain runtimes, such as a Java Runtime monitor, and might not be applicable or indeed usable from your application.

When you bind a service to an application, IBM Cloud creates a set of credentials to access the service and places the connection information for this service in the application environment variable, which is called VCAP_SERVICES.

IBM Cloud: Environment variables



Environment variables contain the environment information of a deployed application on IBM Cloud. IBM Cloud automatically populates the environment variable VCAP_SERVICES with the services that you bind to your IBM Cloud application.

Use the user-defined environment variables for configuration settings, instead of hard-coding the values in your application. For example, you can save the web service endpoint, user name, and password for a cloud-based database as a user-defined environment variable.

You can access the environment variables of the application from the Application Details page by clicking Runtime on the left navigation bar then, clicking the Environment variables tab.

IBM Cloud: Identity and Access Management

Some of the key IBM Cloud Identity and Access Management (Cloud IAM) features are:

Unified user management across IBM Cloud PaaS and IaaS

A unified user management console is used to manage your users across IBM Cloud platform and infrastructure services.

Enterprise federation

A federated ID can be used to sign up for IBM Cloud only if your company worked with IBM to register. Registering a company's domain with IBM enables users to log in to IBM products and services by using their company user credentials. Authentication is then handled by your company's identity provider. When you log in to IBM Cloud with a federated ID, you are prompted to log in through your company's login page.

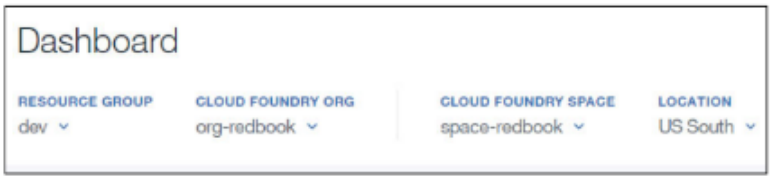
Fine-grained access control

With fine-grained access control, users can be assigned access to only the resources they need.

IBM Cloud: Resources, Users, and Access control

IBM Cloud: Resources, Users, and Access control

- A resource is an entity in your account that you create from the IBM Cloud catalog. You can create multiple resources in an account.
- You can invite multiple users to an account and grant them access to resources.
- If the resources use Cloud IAM for access control, you can grant users access to the resources by using customizable resource groups.
- If the resources do not use Cloud IAM, you can use Cloud Foundry regions, organizations, and spaces for access control.



A resource is an entity in your account that you create from the IBM Cloud catalog, such as a provisioned instance of an IBM Cloud service; for example, Cloudant, a Cloud Foundry application, a virtual machine, or a container. Each account can have multiple resources.

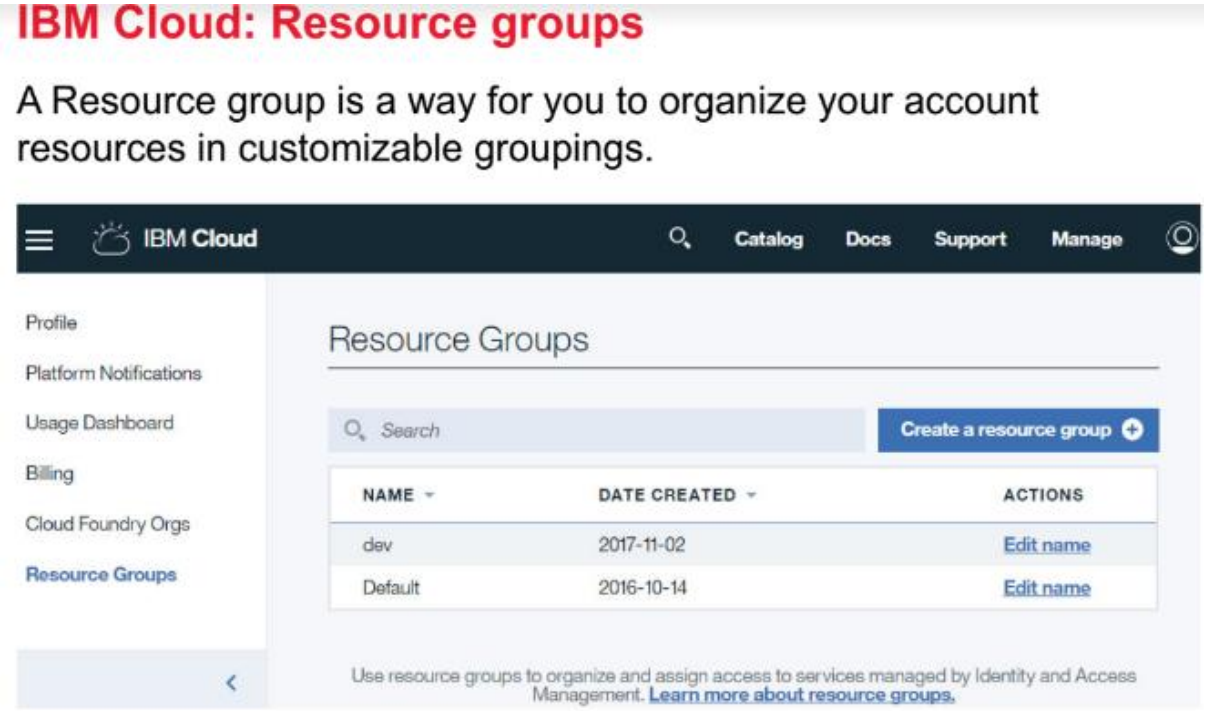
Multiple users (identified by their IBM IDs) can be invited to an account.

Users can be granted access to resources in an account in the following ways:

Organize resources that are enabled to use Cloud IAM into resource groups that you define in your account and assign users access to the resource groups.

Rely on a user's role in a Cloud Foundry region, organization, and space to determine whether a user has permission to access to Cloud Foundry Apps, and services that have not yet enabled the use of Cloud IAM. These resources cannot be added to a resource group.

IBM Cloud: Resource groups



A resource group is a way for you to organize your account resources in customizable groupings so that you can quickly assign users access to more than one resource at a time.

You can use resource groups within your account to group resources that were created from

services that support Cloud IAM for access control. Consider the following points:

Users are granted access to resources in a Resource Group.

Any account resource that is managed by using Cloud IAM access control belongs to a resource group within your account.

Access to resources is not restricted to Cloud Foundry regions, organizations, and spaces.

Complete the following steps to create a Resource Group:

1. Click User Profile.

2. Click Resource Groups.

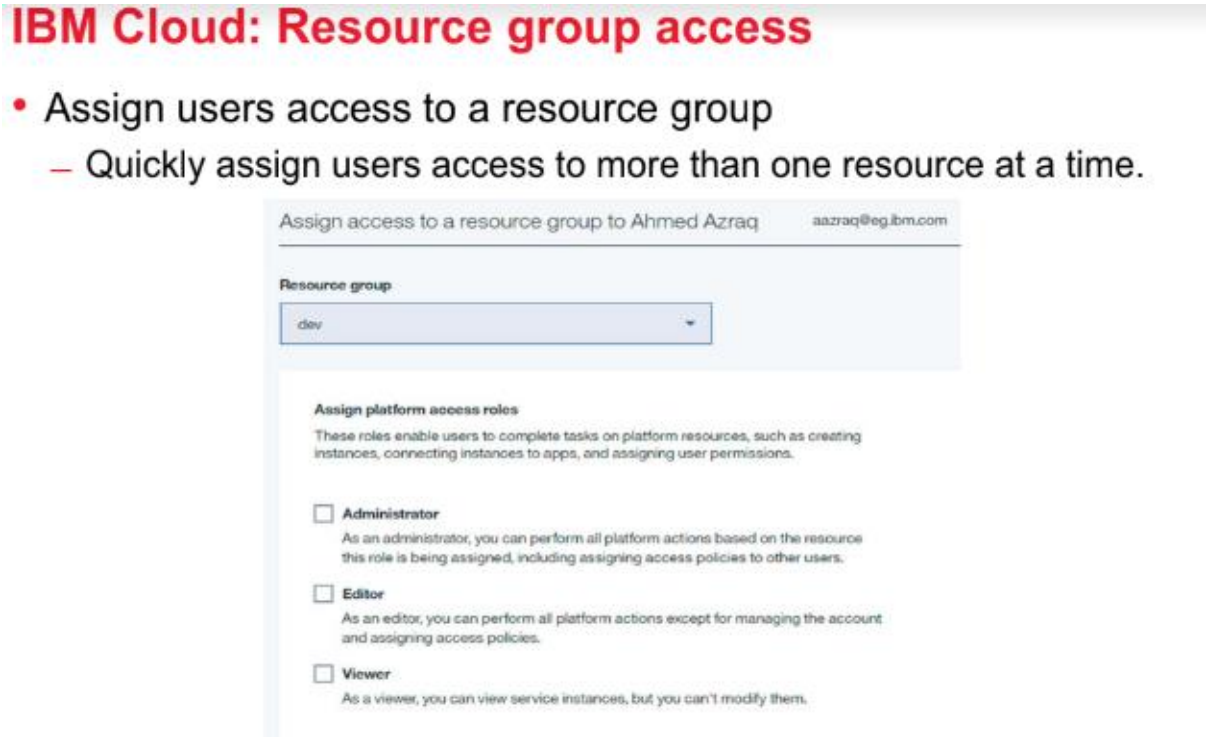
3. Click Create a resource group.

4. Specify the name of the resource group.

5. Click Add.

Resource groups are not restricted by Cloud Foundry regions, organizations, and spaces.

IBM Cloud: Resource group access



Complete the following steps to assign access to users to resource groups:

1. Click Manage in the top toolbar.

2. Click Accounts → Users.

3. Select the user.

4. Click Assign access.

5. Click Assign to a resource group.

6. Select the resource group and the access role, as shown in Figure 2-31.

Resource group access

Assigning a role to a user for accessing a resource group gives the user the ability to manage, edit, or view the resource group with policy access roles Administrator, Editor, and Viewer. This type of access does not give the user access to the resources within a resource group. That access must be assigned separately on the Assign by resource page.

Resource groups and IBM Cloud accounts

If you have a Pay-As-You-Go or Subscription account, you can create multiple resource groups to make managing quota and viewing billing usage for a set of resources easier. You can also group resources to make it easier for you to assign users access to more than one instance at a time.

If you have a Lite account, you cannot create multiple resource groups, but you can rename your default resource group.