

IBM[®] Bluemix[™] Local

IBM

Note

Before you use this information and the product it supports, read the information in Notices (opens a new window).

This PDF was created to supplement the information provided for IBM Bluemix Local. It might not be a complete set of information. For the latest information, see the IBM Bluemix Documentation site at <https://www.ng.bluemix.net/docs/>

© **Copyright IBM Corporation 2015.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Bluemix overview

Last updated: 17 December 2015

IBM® Bluemix™ is the IBM® open cloud platform that provides mobile and web developers access to IBM software for integration, security, transaction, and other key functions, as well as software from business partners.

Built on [Cloud Foundry](#) open source technology, Bluemix makes application development easier with Platform as a Service (PaaS). Bluemix also provides pre-built Mobile Backend as a Service (MBaaS) capabilities. The goal is to simplify the delivery of an app by providing services that are ready for immediate use and hosting capabilities to enable internet scale development.

Bluemix also has cloud deployments that fit your needs. Whether you are a small business that plans to scale, or a large enterprise that requires additional isolation, you can develop in a cloud without borders, where you can connect your dedicated services to the public Bluemix services available from IBM and third-party providers. All service instances are managed by IBM. You'll get one bill for only what you choose to use.

With the broad set of services and runtimes in Bluemix, the developer gains control and flexibility, and has access to various data options, from predictive analytics to big data.

Bluemix provides the following features:

- A range of services that enable you to build and extend web and mobile apps fast.
- Processing power for you to deliver application changes continuously.
- Fit-for-purpose programming models and services.
- Manageability of services and apps.
- Optimized and elastic workloads.
- Continuous availability.

Bluemix abstracts and hides most of the complexities that are associated with hosting and managing cloud-based apps. As an application developer, you can focus on developing your app without having to manage the infrastructure that is required to host it. For both mobile and web apps, you can use the pre-built services that are provided by Bluemix. You can upload your web app to Bluemix and indicate how many instances that you want running. After your apps are deployed, you can easily scale them up or down when the usage or load of the apps change.

You can use Bluemix to quickly develop apps in the most popular programming languages. You can develop mobile apps in iOS, Android, and HTML with JavaScript. For web apps, you can use languages such as Ruby, PHP, Java™, Go, and Python. You can also migrate existing apps to Bluemix and use the runtimes that Bluemix provides to run your apps.

Bluemix also provides middleware services for your apps to use. Bluemix acts on the app's behalf when it provisions new service instances, and then binds those services to the app. Your app can perform its real job, leaving the management of the services to the infrastructure.

In general, you don't have to worry about the operating system and infrastructure layers when running apps on Bluemix. Layers such as root filesystems and middleware components are abstracted so that you can focus on your application code. However, you can learn more about these layers if you need specifics on where your app is running. See [Viewing Bluemix infrastructure layers](#) for details.

Bluemix architecture

With Bluemix, you can access the public Bluemix platform, set up a dedicated Bluemix platform, or use both.

Bluemix Public

At its core, Bluemix is an environment for you to develop apps and use services that provide ready-to-use functions. Bluemix also provides an environment to host application artifacts that run on an application server such as Liberty. By using SoftLayer, Bluemix deploys virtual containers that host each deployed app. In this environment, the app can use pre-built services (including third-party services) to make app assembly easy.

As a developer, you can interact with the Bluemix infrastructure by using a browser-based user interface. You can also use a Cloud Foundry command line interface, called cf, to deploy web apps.

Clients---which can be mobile apps, apps that run externally, apps that are built on Bluemix, or developers that are using browsers---interact with the Bluemix-hosted apps. Clients use REST or HTTP APIs to route requests through Bluemix to one of the app instances or the composite services.

The following figure shows the high-level Bluemix architecture.

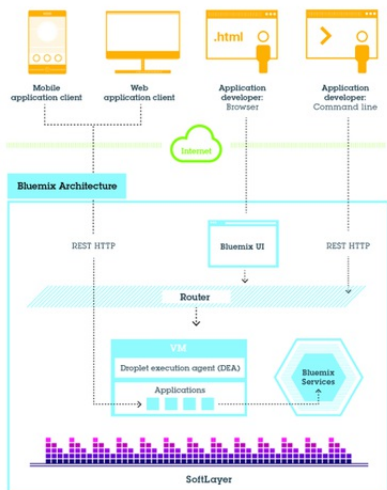


Figure 1. Bluemix architecture

You can deploy your apps to different Bluemix regions, for latency or security considerations. You can choose to deploy either to one region or across multiple regions. For more information, see [Regions](#).

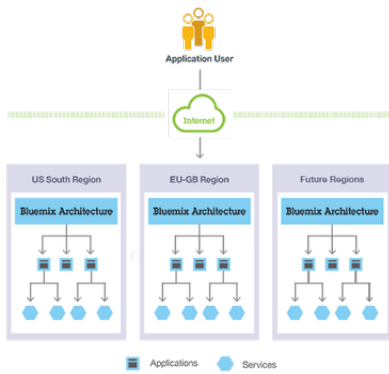


Figure 2. Multi-region application deployment

BlueMix Dedicated

BlueMix Dedicated is your own exclusive SoftLayer environment that's securely connected to both the public BlueMix and your own network. BlueMix Dedicated sits on your network through a VPN or a direct network connection. Your single-tenant hardware can be set up in any SoftLayer data center around the world. IBM manages the dedicated platform and dedicated services, so you can focus on building custom apps. In addition, IBM performs all maintenance to dedicated instances during a maintenance window selected by you.

IBM has several services that are available in your dedicated environment, but you can connect to all public services. All runtimes are available in the dedicated environment. All dedicated deployments of BlueMix include the following benefits and features at no additional cost: VPN, private VLAN, firewall, connectivity with your LDAP, ability to leverage existing on-premises databases and apps, 24/7 on-site security, dedicated hardware, and standard support.

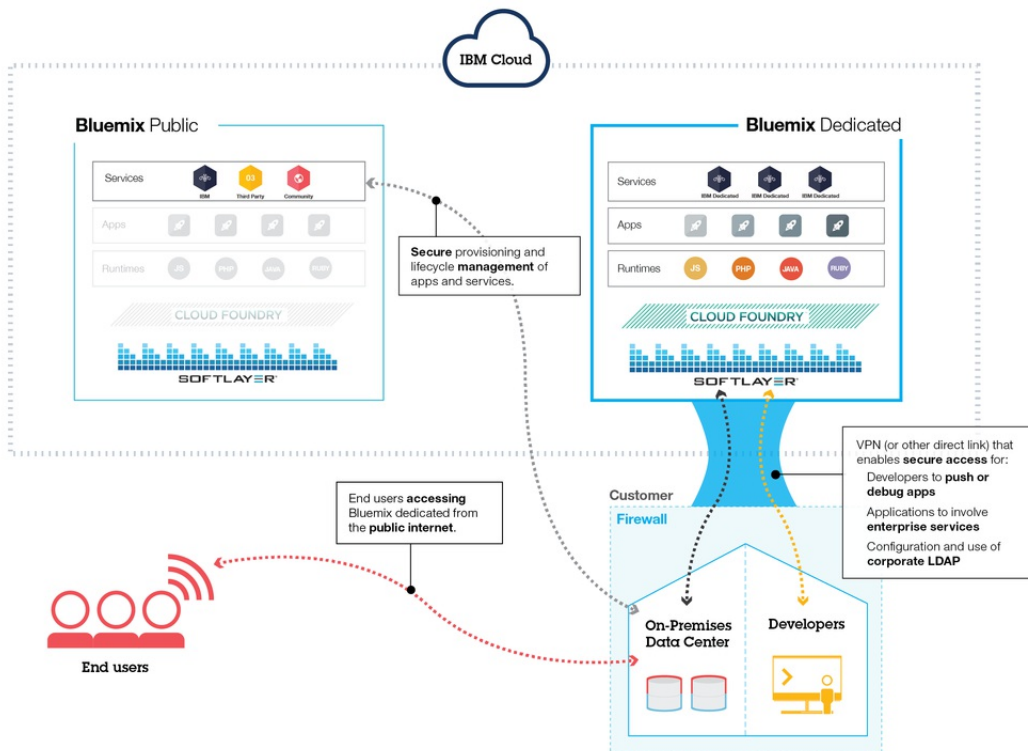


Figure 3. BlueMix Dedicated

BlueMix Local

BlueMix Local is your own BlueMix instance that is deployed in your data center, behind the company firewall. With BlueMix Local, you can stay securely connected and in sync with BlueMix Public.

BlueMix Local includes a private, syndicated catalog that displays the local services that are available exclusively to you. It also includes services that are syndicated from and available for your use from BlueMix Public. All runtimes are available in the local environment. Local deployments of BlueMix include the following benefits and features at no additional cost: relay management technology, connectivity with your LDAP, ability to leverage existing on-premises databases and apps, and standard support.

IBM uses relay technology to securely monitor and maintain your environment, so that you can keep focus on the business. Relay is a delivery capability included with BlueMix Local that enables IBM to automatically and consistently deliver updates, so that you always have an up-to-date, stable, and secure system. Relay achieves connectivity through an open, outbound SSL, VPN tunnel that originates from the inception virtual machine. Through this tunnel, IBM serves and maintains the platform, compute resources, and services for your instance. See [BlueMix Local](#).

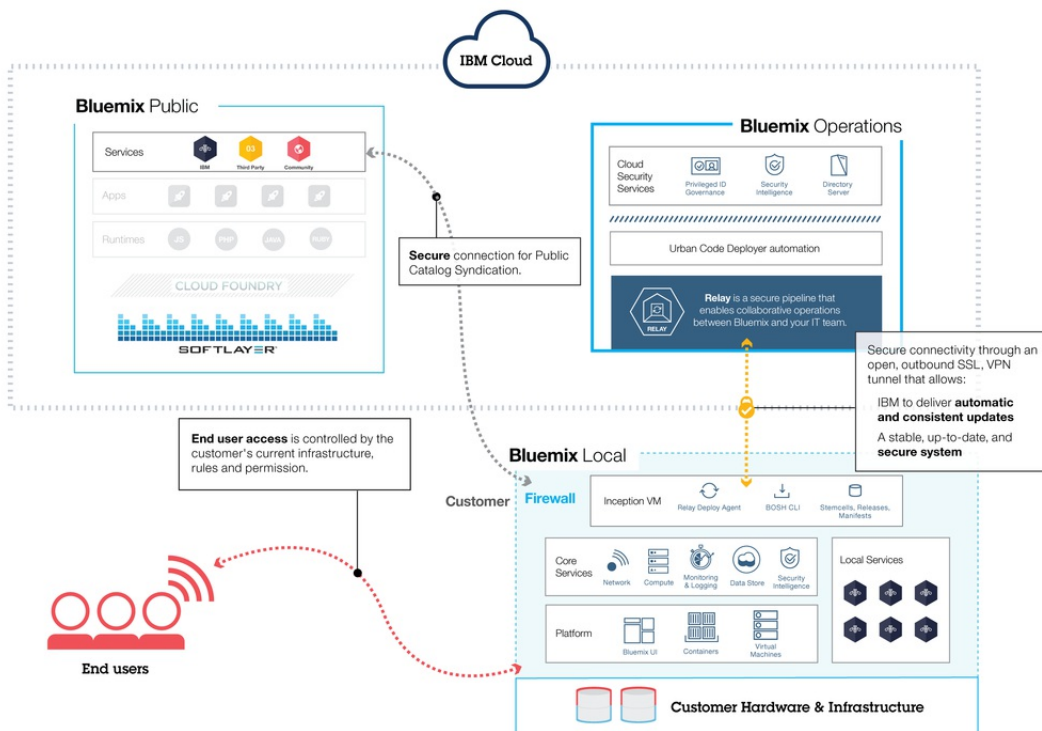


Figure 4. Bluemix Local

How Bluemix works

When you deploy an app to Bluemix, you must configure Bluemix with enough information to support the app.

- For a mobile app, Bluemix contains an artifact that represents the mobile app's back end, such as the services that are used by the mobile app to communicate with a server.
- For a web app, you must ensure that information about the proper runtime and framework is communicated to Bluemix, so that it can set up the proper execution environment to run the app.

Each execution environment, including both mobile and web, is isolated from the execution environment of other apps. The execution environments are isolated even though these apps are on the same physical machine. The following figure shows the basic flow of how Bluemix manages the deployment of apps:

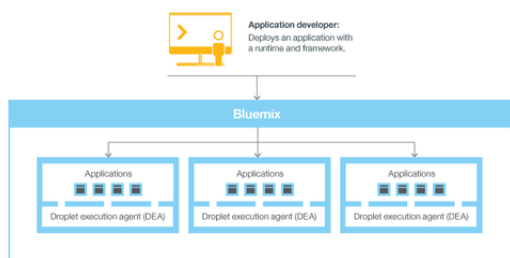


Figure 5. Deploying an app

When you create an app and deploy it to Bluemix, the Bluemix environment determines an appropriate virtual machine (VM) to which the app or artifacts that the app represents is sent. For a mobile app, a mobile back-end projection is created on Bluemix. Any code for the mobile app running in the cloud eventually runs in the Bluemix environment. For a web app, the code running in the cloud is the app itself that the developer deploys to Bluemix. The determination of the VM is based on several factors, including:

- The load already on the machine
- Runtimes or frameworks supported by that VM.

After a VM is chosen, an application manager on each VM installs the proper framework and runtime for the app. Then the app can be deployed into that framework. When the deployment is completed, the application artifacts are started.

The following figure shows the structure of a VM, also known as Droplet execution agent (DEA), that has multiple apps deployed to it:

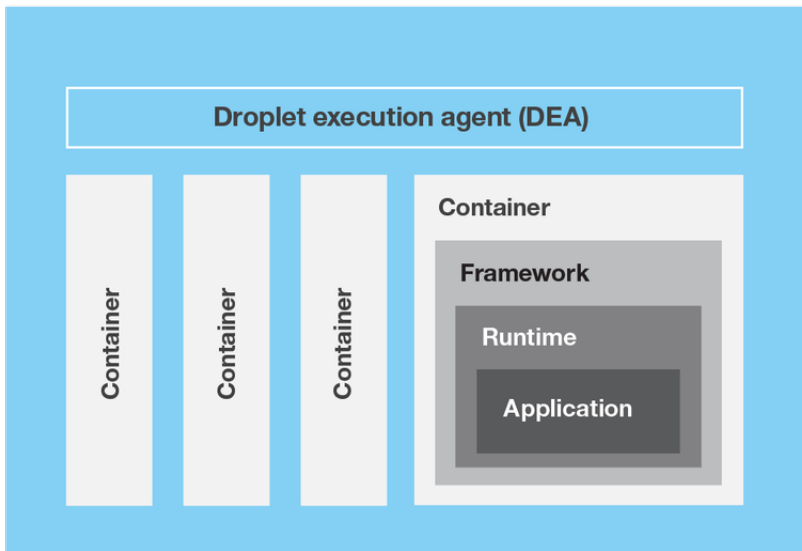


Figure 6. Design of a VM

In each VM, an application manager communicates with the rest of the Bluemix infrastructure, and manages the apps that are deployed to this VM. Each VM has containers to separate and protect apps. In each container, Bluemix installs the appropriate framework and runtime that are required for each app.

When the app is deployed, if it has a web interface (as for a Java web app), or other REST-based services (such as mobile services exposed publicly to the mobile app), users of the app can communicate with it by using normal HTTP requests.

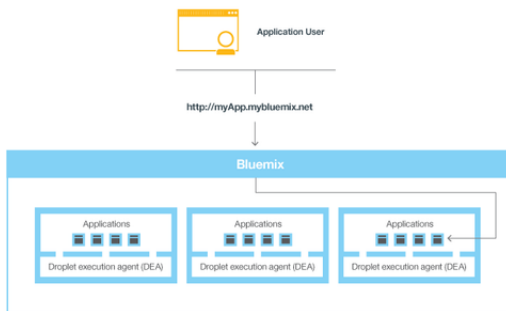


Figure 7. Invoking a Bluemix app

Each app can have one or more URLs associated with it, but all of them must point to the Bluemix endpoint. When a request comes in, Bluemix examines the request, determines which app it is intended for, and then selects one of the instances of the app to receive the request.

Bluemix resiliency

Bluemix is designed to host scalable, resilient apps and application artifacts that can both scale to meet your needs, and remain highly available and quick to recover from problems. Bluemix separates those components that track the state of interactions (stateful) from those that do not (stateless). This separation allows Bluemix to move apps flexibly as needed to achieve scalability and resiliency.

You can have one or more instances running for your app. When you have multiple instances for one app, the app is uploaded only once. However, Bluemix deploys the number of instances of the app requested, and distributes them across as many VMs as possible.

You must save all persistent data in a stateful data store that is outside of your app, such as on one of the data store services that are provided by Bluemix. Because anything cached in memory or on disk might not be available even after a restart, you can use the memory space or filesystem of a single Bluemix instance as a brief, single-transaction cache. With a single instance setup, the request to your app might be interrupted because of the stateless nature of Bluemix. A best practice is to use at least three instances for each app to ensure the availability of your app.

All Bluemix infrastructure, Cloud Foundry components, and IBM-specific management components are highly available. Multiple instances of the infrastructure are used to balance the load.

Bluemix concepts

Bluemix consists of apps, services, buildpacks, and other components. You can deploy apps to different Bluemix regions by using one IBM ID.

Regions

A Bluemix region is a defined geographical territory that you can deploy your apps to. You can create apps and service instances in different regions with the same Bluemix infrastructure for application management and the same usage details view for billing. You can select the region that is nearest to your customers and deploy your apps to this region to get low application latency. You can also select the region where you want to keep the application data to address security issues. When you build apps in multiple regions, if one region goes down, the apps that are in the other regions continue to run. Your resource allowance is the same for each region that you use.

If you are using the Bluemix user interface, you can switch to a different region to work with the spaces in that region.

If you are using the cf command line interface, you must connect to the Bluemix region that you want to work with by using the cf api command and specifying the API endpoint of the region. For example, enter the following command to connect to Bluemix Europe United Kingdom region:

```
cf api https://api.eu-gb.Bluemix.net
```

If you are using the Eclipse tools, you must connect to the Bluemix region that you want to work with by creating a Bluemix server and specifying the API endpoint of the region. For more information about using the Eclipse tools, see [Deploying apps with IBM Eclipse Tools for Bluemix](#).

A unique prefix is assigned to each region. Bluemix provides the following regions and region prefixes.

Region name	Region prefix	cf API endpoint	UI console
US South region	us-south	api.ng.bluemix.net	console.ng.bluemix.net
Europe United Kingdom region	eu-gb	api.eu-gb.bluemix.net	console.eu-gb.bluemix.net
Australia Sydney region	au-syd	api.au-syd.bluemix.net	console.au-syd.bluemix.net

Table 1. Bluemix region list

Infrastructure

Bluemix offers three ways for you to run your code: Cloud Foundry, IBM Containers, and Virtual Machines. The IBM Containers and Virtual Machines are available in only the US South and Europe United Kingdom region. You can pick the right infrastructure for deploying your apps.

Cloud Foundry

Apps running in the Cloud Foundry infrastructure work with existing Cloud Foundry apps and can bind to any of the services available in the Bluemix Catalog. With this infrastructure, you develop and manage your application code and Bluemix takes care of the management and maintenance of the infrastructure that powers those apps.

IBM Containers

With the IBM Containers infrastructure, you can run your web app anywhere that supports container deployment. A *container* is an object that holds everything that is needed for an app to run. This infrastructure includes a private registry for your trusted images, so that you can upload, store, and retrieve them. You can then make those images available in Bluemix and manage your containers in the platform. The IBM Containers infrastructure scales both horizontally and vertically. You can use all of the images that are available in the public Docker Hub and use the docker API and command line interface to manage your containers on Bluemix. IBM also provides some public images in the Containers Registry that you can use and extend. IBM Containers are used to run Docker containers in a hosted cloud environment. Docker adds an engine that deploys an app to the virtual environment that you use for running your containers. Docker also provides an environment that you can use to run your code. When you're ready, it provides the means by which you can transfer the code from your development environment, to your test environment, and then to your production environment. To find out more about IBM Containers, see [IBM Containers](#) in the Creating Web Apps documentation.

Virtual Machines (BETA)

The Bluemix virtual machines infrastructure gives you the ability to create and manage virtual machine groups on the IBM public cloud. You can also create and manage VM groups on your private IBM clouds that you've chosen to make available to Bluemix users. The infrastructure includes a guided experience to connect to your on-premises infrastructure. Support for monitoring and logging is integrated into Bluemix. You can deploy and manage your virtual machines by using either the Bluemix user interface or the cloud's OpenStack APIs. Virtual machines on Bluemix support provisioning of virtual machine groups with auto scaling. Through this support, the number of instances can be automatically increased or decreased, based on CPU load or the failure of an instance. In addition, load balancing is supported, which enables the assignment of virtual IP (floating IP) addresses as needed. To find out more about Bluemix virtual machines, see [Virtual Machines](#) in the Creating Web Apps documentation.

Applications

In Bluemix, an application, or *app*, represents the artifact that a developer is building. The application lifecycle in Bluemix and Cloud Foundry are identical, regardless of how you push the app to the Bluemix. For more information, see [How Applications Are Staged](#).

Mobile apps

Mobile apps run outside of the Bluemix environment and use services that the mobile apps are exposed to. These services typically act in concert, and represent the back-end projection of that app. Bluemix can also host app code that the developer would rather run on a back-end server in a container-based environment.

Web apps

Web apps consist of all the code that is required to be run or referenced at run time. Web apps are uploaded to Bluemix to host the app.

For languages such as Java, where the source code is compiled into runtime binary files, only the binary files are required to be uploaded.

Services

A *service* is a cloud extension that is hosted by Bluemix. The service provides functionality that is ready-for-use by the app's running code. The predefined services that are provided by Bluemix include database, messaging, push notifications for mobile apps, and elastic caching for web apps.

You can create your own services in Bluemix. These services can vary in complexity. They can be simple utilities, such as the functions you might see in a runtime library. Alternatively, they can be complex business logic that you might see in a business process modeling service or a database.

Bluemix simplifies the use of services by provisioning new instances of the service, and binding those service instances to your app. The management of the service is handled automatically by Bluemix. For all available services in Bluemix, see the catalog in the Bluemix user interface.

Starters

A *starter* is a template that includes predefined services and app code that is configured with a particular buildpack. There are two types of starters: boilerplates and runtimes. A starter might be app code that is written in a specific programming language, or a combination of app code and a set of services.

Boilerplates

In Bluemix, a *boilerplate* contains an app and its associated runtime environment and predefined services for a particular domain. You can use a boilerplate to quickly get up and running. For example, you can select the Mobile Cloud boilerplate to host mobile and web apps and accelerate development time of server-side scripts by using the mobile app template and SDK.

Runtimes

A *runtime* is the set of resources that is used to run an app. Bluemix provides runtime environments as containers for different types of apps. The runtime environments are integrated as buildpacks into Bluemix, and are automatically configured for use.

Buildpacks

A buildpack is a collection of scripts that prepare your code for execution on the target PaaS. A buildpack gathers the runtime and framework dependencies of an app. Then, it packages them with the app into a droplet that can be deployed to the cloud.

If you do not specify a buildpack when you deploy your app to Bluemix, built-in buildpacks are used by default.

Built-in IBM buildpacks

The following list is the built-in buildpacks that are created by IBM.

- Liberty for Java
- Node.js

Built-in community buildpacks

In Bluemix, you can also use built-in buildpacks that are provided by the Cloud Foundry community. To list built-in community buildpacks run the `cf buildpacks` command.

External buildpacks

If you cannot find the runtime or framework you want in the built-in buildpacks that are provided by Bluemix, you can bring an external, existing buildpack to use for your app. External buildpacks are provided by the Cloud Foundry community for you to use as your own buildpacks. You specify the buildpack when you deploy your app by using the `cf push` command.

Note: External buildpacks are not supported by IBM; therefore, you might need to contact the Cloud Foundry community for support.

Integration with systems of record

Bluemix can help developers by connecting two broad categories of systems in a cloud environment: systems of record and systems of engagement.

Systems of record include apps and databases that store business records and automate standardized processes. *Systems of engagement* are capabilities that expand the usefulness of systems of record and make them more engaging to users. By integrating a system of record with the app that you create in Bluemix, you can perform the following actions:

- Enable secure communication between the app and the backend database by downloading and installing a secure connector on premise.
- Invoke a database in a secure way.
- Create APIs from integration flows with databases and backend systems, such as customer relationship management system.
- Expose only the schemas and tables that you want to be exposed to the app.
- As a Bluemix organization manager, publish an API as a private service that is visible only to your organization members.

To integrate a system of record with the app that you create in Bluemix, use the Cloud Integration service. By using the Cloud Integration service, you can create a Cloud Integration API and publish the API as a private service for your organization.

Cloud Integration API

A Cloud Integration API provides secured access to the systems of record that reside behind a firewall through web APIs. When you create the Cloud Integration API, you choose the resource that you want to access through the web API, specify the operations that are permitted, and include SDKs and samples to access the API. For more information about how to create a Cloud Integration API, see [Creating Cloud Integration APIs](#).

Private service

A private service consists of a Cloud Integration API, SDKs, and entitlement policies. In addition, the private service might contain documentation or other items from the service provider. Only the organization manager can publish a Cloud Integration API as a private service. To see the private services that are available to you, select the Private checkbox in the Bluemix catalog. You can select and bind a private service to an app without connecting to the Cloud Integration service. You bind private services to your app in the same way as you do for other Bluemix services. For information about how to publish an API as a private service, see [Publishing an API as a private service](#).

Scenario: Creating a rich mobile app to connect with your system of record

Bluemix provides a platform where you can integrate your mobile app, cloud services, and enterprise systems of record to provide an app that interacts with your on-premises data.

For example, you can build a mobile app to interact with your customer relationship management system that resides on-premises behind a firewall. You can invoke the system of record in a secure way and leverage the mobile services in Bluemix so that you can build a rich mobile app.

First, your integration developer creates the mobile back-end app in Bluemix. He uses the Mobile Cloud boilerplate that uses the Node.js runtime that he is most familiar with.

Then, by using the Cloud Integration service in the Bluemix user interface, he exposes an API through a secure connector. Your integration developer downloads the secure connector and installs it on-premises to enable secure communication between his API and the database. After he creates the database endpoint, he can look at all the schemas and extract the tables that he wants to expose as APIs to the app.

Your integration developer adds the Push service to deliver mobile notifications to interested consumers. He also adds a business partner service to tweet when a new customer record is created with a Twitter API.

Next, as the application developer, you can log in to Bluemix, download the Android development toolkit, and develop code that invokes the APIs that your integration developer created. You can develop a mobile app that enables users to enter their information on their mobile device. The mobile app then creates a customer record in the customer management system. When the record is created, the app pushes a notification to a mobile device and initiates a tweet about the new record.

National language support for Bluemix

Bluemix supports national languages other than English. However, not all of the content that is provided with Bluemix is translated. The following table lists the supported national languages and language codes for Bluemix.

National language Language code

Brazilian Portuguese	pt_BR
English	en
French	fr
German	de
Japanese	ja
Korean	ko
Italian	it
Spanish	es
Simplified Chinese	zh_CN
Traditional Chinese	zh_TW

Table 2. Supported national languages and language codes

Bluemix security

Designed with secure engineering practices, the IBM® Bluemix™ platform has layered security controls across network and infrastructure. Bluemix provides a group of security services that can be used by application developers to secure their mobile and web apps. These elements combine to make Bluemix a platform with clear choices for secure application development.

Bluemix ensures security readiness by adhering to security policies that are driven by best practices in IBM for systems, networking, and secure engineering. These policies include practices such as source code scanning, dynamic scanning, threat modeling, and penetration testing. Bluemix follows the IBM Product Security Incident Response Team (PSIRT) process for security incident management. See the [IBM Security Vulnerability Management \(PSIRT\)](#) site for details.

Bluemix Public and Dedicated use IBM SoftLayer Infrastructure-as-a-Service (IaaS) cloud services and takes full advantage of its security architecture. SoftLayer IaaS provides multiple, overlapping tiers of protection for your applications and data. For Bluemix Local, you own the physical security and provide the infrastructure by hosting Bluemix Local in your own data center behind a company firewall. In addition, Bluemix adds security capabilities at the Platform as a Service layer in different categories: platform, data, and application.

Security of the Bluemix platform

Bluemix provides functional, infrastructure, operational, and physical security (through IBM SoftLayer) for the core platform. However, Bluemix Local is unique in that the customer provides the infrastructure and data center, and owns the physical security.

The Bluemix environment on SoftLayer is compliant with the most restrictive IBM information technology (IT) security standards, which meet or exceed the industry standards. These standards include the following: Network, data encryption, and access control

- Application ACLs, permissions, and penetration testing
- Identification, authentication, and authorization
- Information and data protection
- Service integrity and availability
- Vulnerability and fix management
- Denial of service and systematic attacks detection
- Security incident response

Bluemix platform security overview

In Bluemix
On Bluemix

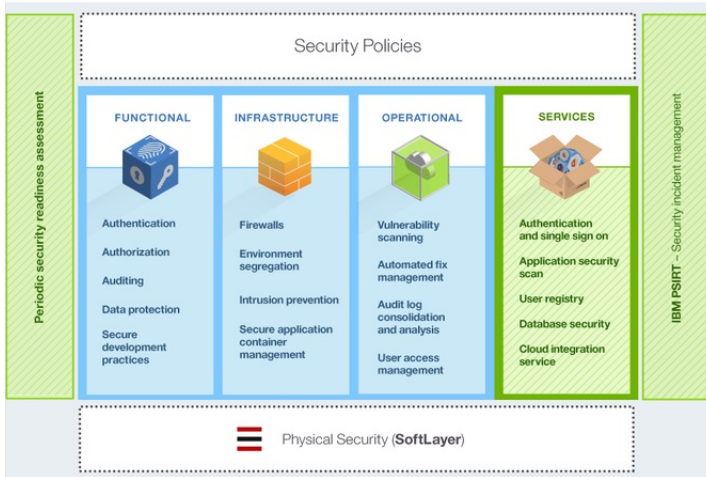


Figure 1. Bluemix platform security overview

With Bluemix Local, you host Bluemix behind your company firewall and in your data center. Therefore, you are responsible for certain aspects of security. The following image details which parts of security are customer-owned and which parts of security are managed and maintained by IBM.

Bluemix Local Security Overview

"In" Bluemix
"In/On" Bluemix
Customer Owned

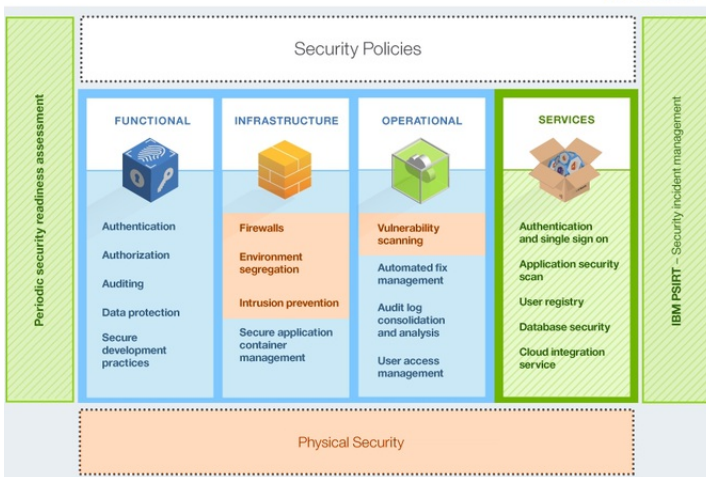


Figure 2. Bluemix Local platform security overview

IBM installs, remotely monitors, and manages Bluemix Local in your data center through Relay, a delivery capability included with Bluemix Local. Relay connects securely with certificates specific to each Bluemix Local instance. For more information about Bluemix Local and Relay, see [Bluemix Local](#).

Functional security

Bluemix provides various functional security capabilities, including user authentication, access authorization, auditing of critical operations, and data protection.

Authentication

Application developers are authenticated to Bluemix by using the IBM web identity. For Bluemix Dedicated and Local, authentication through LDAP is supported by default. On request, authentication through IBM web identity can be set up instead for Bluemix.

Authorization

Bluemix uses Cloud Foundry mechanisms to ensure that each application developer has access only to the applications and service instances that they created. Authorization to Bluemix services is based on OAuth. Access to all Bluemix Platform internal endpoints are restricted to external users.

Auditing

Audit logs are created for all successful and unsuccessful authentication attempts of application developers. Audit logs are created also for privileged access to Linux systems that host the containers where Bluemix applications run.

Data protection

All Bluemix traffic goes through the IBM WebSphere® DataPower® SOA Appliances, which provide reverse proxy, SSL termination, and load balancing functions. The following HTTP methods are allowed: DELETE GET HEAD OPTIONS POST PUT * TRACE HTTP inactivity times out at 2 minutes. The following headers are populated by DataPower:

- \$swis Set to true if client-side connection is secure (HTTPS), set to false otherwise.
- \$swssc Set to one of the following schemes of client connection: https, http, ws, or wss.
- \$swssn Set to host name that is sent by client.
- \$swssp Set to server port that client connects to.
- x-client-ip Set to client IP address.
- x-forwarded-proto Set to one of the following schemes of client connection: https, http, ws, or wss.

Secure development practices

For Bluemix Public and Dedicated, periodic security vulnerability scans are performed on various Bluemix components by using IBM Security AppScan® Dynamic Analyzer and static analyzer offerings. Threat modeling and penetration testing are performed to detect and address any potential vulnerabilities for all types of Bluemix deployments. In addition, application developers can use the AppScan Dynamic Analyzer service to secure their web apps that are deployed on Bluemix.

Infrastructure security

Bluemix builds upon Cloud Foundry to provide a robust foundation for running your applications. Within the architecture, several components are provided for security and isolation. In addition, change management and backup and recovery procedures are implemented to ensure integrity and availability.

Environment segregation

For Bluemix Public, development and production environments are segregated from each other to improve application stability and security.

Firewalls

Firewalls are in place to restrict access to the Bluemix network. For Bluemix Local, your company firewall segregates the rest of your network from your Bluemix instance.

Intrusion protection

Bluemix Public and Dedicated enable intrusion protection to discover threats so that they can be addressed. Intrusion protection policies are enabled on firewalls.

Secure application container management

Each Bluemix application is isolated and runs in its own container that has specific resource limits for processor, memory, and disk.

Operating system security hardening

IBM administrators perform network and operating system hardening regularly by using tools such as IBM Endpoint Manager.

Operational security

Bluemix provides a robust operational security environment with the following controls.

Vulnerability scan

Bluemix uses the Tenable Network Security vulnerability scanning tool, Nessus, to detect any issues with network and host configurations so that the issues can be resolved.

Automated fix management

Bluemix administrators ensure that fixes for operating systems are applied at appropriate frequencies. Automated fixes are enabled by using IBM Endpoint Manager.

Audit log consolidation and analysis

Bluemix uses the IBM Security QRadar® tools to consolidate Linux logs to monitor privileged access on Linux systems. Bluemix also uses IBM QRadar security information and event management (SIEM) to monitor successful and unsuccessful login attempts of application developers.

User access management

Within Bluemix, Separation of Duties guidelines are followed to assign granular access privileges to users, and to ensure that users have only the access that is required to perform their jobs according to the principle of least privilege. Within a Bluemix Dedicated and Local environments, assigned administrators can manage roles and permissions for Bluemix user in their organization by using the Admin Console. See [Managing Bluemix](#) for details.

Physical security

Bluemix Public and Dedicated relies on the network-within-a-network topology of SoftLayer for physical network security. This network-within-a-network architecture ensures that systems are fully accessible only to authorized personnel. For Bluemix Local, you own the physical security for the local instance. Your data center is secured behind your company firewall.

In SoftLayer network-within-a-network, the public network layer handles public traffic to hosted websites or online resources. The private network layer allows for true out-of-band management through a distinct stand-alone third carrier over SSL, PPTP, or IPSec VPN gateways. The data center to data center network layer provides free and secure connectivity between servers that are housed in separate SoftLayer facilities.

Every SoftLayer data center is fully secured with controls that meet SSAE 16 and industry-recognized requirements, without exceptions. For more information, see the SoftLayer Security Compliance page.

Data security

With Bluemix, securing your data against unauthorized access is a joint effort between Bluemix and you.

Data that is associated with a running application can be in one of three states: data-in-transit, data-at-rest, and data-in-use.

Data-in-transit

Data that is being transferred between nodes on a network.

Data-at-rest

Data that is stored.

Data-in-use

Data that is not currently stored, and is being acted upon at an endpoint.

Each type of data needs to be considered when you plan for data security.

The Bluemix platform secures data-in-transit by securing the end-user access to the application by using SSL, through the network until the data reaches IBM DataPower Gateway at the boundary of the Bluemix internal network. IBM DataPower Gateway acts as a reverse proxy and provides SSL termination.

Security for both data-in-use and data-at-rest is your responsibility as you develop your application. You can take advantage of several data-related services available in the Bluemix Catalog to help with these concerns.

Security of Bluemix applications

As an application developer, you must enable the security configurations, including application data protection, for your applications that run on Bluemix.

You can use security capabilities that are provided by several Bluemix services to secure your applications. All Bluemix services that are produced by IBM follow IBM secure engineering development practices.

Note: Some of the services described here might not apply to Bluemix Dedicated or Local instances.

SSO service

IBM Single Sign On for Bluemix is a policy-based authentication service that provides an easy to embed single sign-on capability for Node.js or Liberty for Java®,[®] applications. To enable an application developer to embed single sign-on capability into an application, the administrator creates service instances and adds identity sources.

The Single Sign On service supports several identity sources where your users' credentials are stored:

SAML Enterprise

A user registry with an exchange of SAML tokens that completes the authentication.

Cloud Directory

A user registry that is hosted in IBM Cloud.

Social identity sources

The user registries that are maintained by Google, Facebook, and LinkedIn.

For more information, see [Getting started with Single Sign On](#).

AppScan Mobile Analyzer

This service provides a security analysis of Android mobile applications. To use this service, you must upload a compiled Android app as an APK file. When the security analysis scan is done, you can download a report.

For more information, see [Getting started with AppScan Mobile Analyzer](#).

AppScan Dynamic Analyzer

This service provides a security analysis of web applications with a dynamic analysis tool. The tool works on the deployed web app, not on the app source code, and it can scan any Bluemix web app regardless of its language or technology. You can scan only applications of the organizations that you belong to. To create a scan, you must configure the web app URL and the login credentials if any. When the scan is done, you can download a report.

For more information, see [Getting started with AppScan Dynamic Analyzer](#).

Mobile Analyzer for iOS (Beta)

The Mobile Analyzer for iOS service provides AppScan dynamic security analysis for iOS mobile applications. It helps you identify security issues in your iOS mobile apps.

For more information, see [Getting started with Mobile Analyzer for iOS](#).

Static Analyzer (Beta)

The Static Analyzer service enables static application security testing on the cloud. It helps you find source code vulnerabilities early in the software development lifecycle, so that they can be fixed before deployment.

Static Analyzer enables you to scan Java and Java web content by using a command-line interface (CLI) on your local disk. In addition, you can run a small installer that adds Static Analyzer plug-ins to Eclipse or Maven. You can use the client utility to scan and gather information about your files in an archive file that you then submit to the cloud for scan results.

For more information, see [Getting started with IBM Static Analyzer for Bluemix](#).

IBM UrbanCode plug-in for application security testing

The IBM Application Security Testing for Bluemix plug-in enables you to run security scans on your web or Android apps that are hosted on Bluemix. This plug-in is developed and supported by the IBM UrbanCode, Deploy Community on the IBM Bluemix DevOps Services platform.

For more information, go to [IBM Application Security Testing for Bluemix](#).

SQL Database

The SQL Database service adds a fully provisioned relational database to your app. This service uses IBM Directory Server LDAP for authentication and IBM InfoSphere Guardium Data Activity Monitor to protect the database that is accessed by applications. The connection between applications and the database is protected by the SSL certificate that DigCert signs.

In certain plans with this service, you can use the SQL database console in Bluemix to get reports that contain the following information:

- Sensitive data that might exist in the database that is accessed by applications.
- The application users who accessed the database within a specified period.
- The application users who are accessing sensitive data that is in the database.

To mask data by using SQL, applications can call the masking user-defined functions (UDFs) that are deployed together with the database. For example, you can mask the data that you want to use elsewhere for testing. The UDFs implement the data masking algorithms from IBM InfoSphere Optim.

The premium plan for this service also includes data encryption. For more information about this service, see [Getting started with SQL Database](#).

dashDB

The dashDB service uses an embedded LDAP server for user authentication. The connection between applications and the database is protected by SSL certificates. This service uses the DB2 native encryption capability to automatically encrypt your deployed database and database backups. Master key rotation is automatic and happens every 90 days.

For more information, see [Getting started with dashDB](#).

Cloud Integration

The Cloud Integration service enables you to integrate cloud and on-premises data. You can add a service to interact with backend databases such as DB2, Oracle, and SAP. Next, you can move data or create REST APIs for Bluemix applications to access and use. The service enables secure communication with on-premises secure connectors, and exposes backend systems of record as REST APIs to be used by applications.

For more information, see [Getting started with Cloud Integration](#).

Secure Gateway

The Secure Gateway service enables you to securely connect Bluemix apps to remote locations, either on premises or in the cloud. It provides secure connectivity and establishes a tunnel between your Bluemix organization and the remote location that you want to connect to. You can configure and create a secure gateway by using the Bluemix user interface or an API package.

For more information, see [Getting started with Secure Gateway](#).

Security information and event management

You can use security information and event management (SIEM) tools to analyze security alerts in application logs. One such tool is IBM Security QRadar SIEM, which provides security intelligence in cloud environments. For information, see [IBM QRadar Security Intelligence Platform](#).

Bluemix security deployment

Bluemix security deployment architecture includes different information flows for app users and developers to ensure secure access.

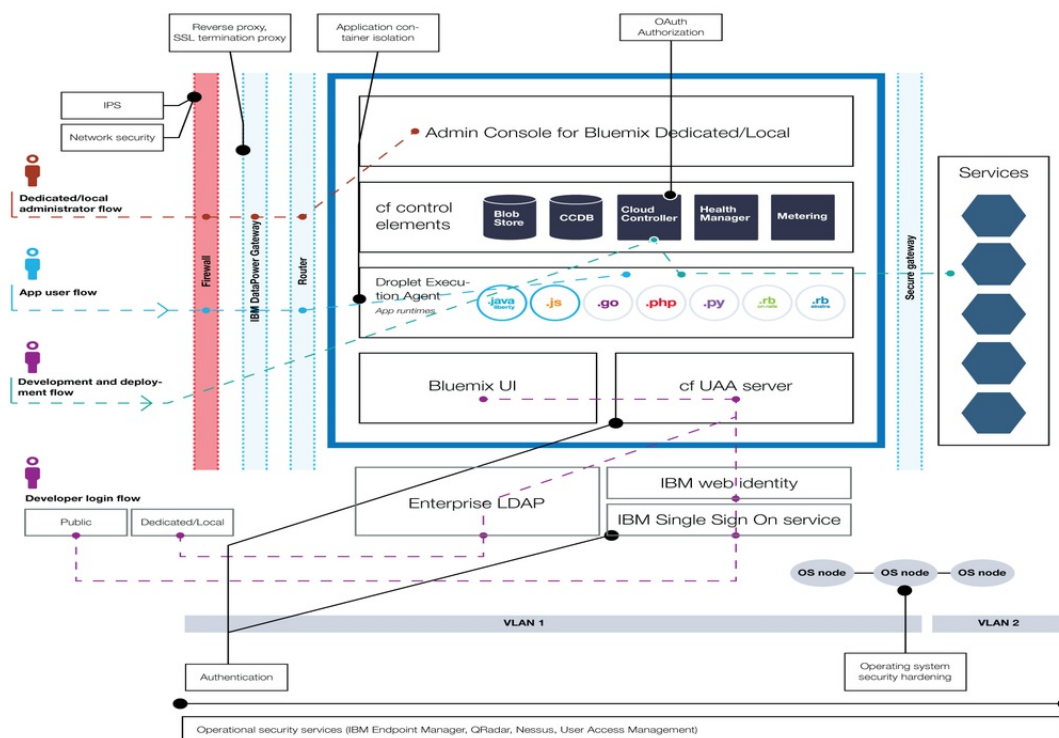


Figure 3. Bluemix security deployment architecture

For Bluemix app users, the **app user flow** is as follows:

1. Through a firewall, with intrusion prevention and network security in place.
2. Through the IBM DataPower Gateway with reverse proxy and SSL termination proxy.
3. Through the network router.
4. Reaches the application runtime in the droplet execution agent (DEA).

The Bluemix developer follows two main flows, for login and for development and deployment.

- The **developer login flow** includes the following:
 - For developers who are logging in to Bluemix Public, the flow is as follows:
 1. Through the IBM Single Sign On service.
 2. Through IBM web identity.
 - For developers who are logging in to Bluemix Dedicated or Local, the flow is through the enterprise LDAP.
- The **development and deployment flow** is as follows:
 1. Through a firewall, with intrusion prevention and network security in place. This applies to Bluemix Dedicated only.
 2. Through the IBM DataPower Gateway with reverse proxy and SSL termination proxy.
 3. Through the network router.
 4. Through authorization by using Cloud Foundry cloud controller, to ensure access to only apps and service instances that are created by the developer.

For Bluemix Dedicated and Bluemix Local *administrators*, the **administrator flow** is as follows:

1. Through a firewall, with intrusion prevention and network security in place.
2. Through the IBM DataPower Gateway with reverse proxy and SSL termination proxy.
3. Through the network router.
4. Reaches the Administration page in the Bluemix user interface.

In addition to users described in these paths, an authorized IBM security operations team performs various operational security tasks, such as the following:

- Vulnerability scans. For Bluemix Local, you own the physical security and any scans within your firewall.
- User access management.
- Operating system hardening by periodically applying fixes with IBM Endpoint Manager.
- Management of risks with intrusion protection.
- Security monitoring with QRadar.
- Security reports available through the Admin Console.

Security reports

With Bluemix Local and Bluemix Dedicated, Bluemix generates various security reports and logs that you can view through the Administration page. For instructions for viewing and using the reports, see [Viewing reports](#).

The following table shows the list of security reports that are generated for Bluemix Local and Bluemix Dedicated.

Category	Report	Description
Firewall	Firewall logins	Events related to administrator login to the Vyatta firewall devices.
Firewall	Firewall denies	Events generated by the Vyatta firewall devices when a request to access is denied according to the firewall rules that are in place.
Bluemix administrator login events	Bluemix administrators login	Events generated by the operating system when an administrator starts an SSH session on every Bluemix system.
Bluemix application developer login events	Bluemix application developers login	Events generated by the Bluemix platform login component when a Bluemix platform user starts a session by using the command line, the REST APIs, or the Bluemix user interface.
Bluemix administrator administrative events	Bluemix administrators operating system administrative events	Events generated by the operating system when an administrator performs action within a current working session.
Bluemix application developer administrative events	Bluemix (Cloud Foundry) administrative events	Events related to operations performed by the Bluemix platform user by using the command line, the REST APIs, or the Bluemix user interface.
Bluemix administrator database administrative events	Database administrative events	Events related to operations performed by a database administrator on the Bluemix internal databases.
Administration events	User management events	Events related to user management actions performed on the Administration page.
Administration events	Catalog	Events related to services Catalog changes.
Administration events	Security reports management events	Events related to security reports management actions performed on the Administration page.
Access reviews	Access reviews report	Reviews for privileged accesses.
Change management	Management of software changes	Change management activity.
Key management	Management of custom SSL certificates	Custom SSL certifications that were uploaded and stored.
Encryption	Data-in-transit encryption	Data-in-transit encryption that is configured.
Anti-virus	Anti-virus scan report	Anti-virus software that is in place.
Software fix management	Patch application report	Software fixes that were applied.
Security incident management	Security incident remediation report	Evidence of security incidents for security incident management.

Table 1. Bluemix Local and Bluemix Dedicated security report list

Bluemix Local

IBM® Bluemix™ Local brings the power and agility of the Bluemix cloud-based platform to your data center. With Bluemix Local, you can protect your most sensitive workloads behind your company firewall, while staying securely connected and in sync with Bluemix Public.

IBM® uses cloud operations as a service to monitor and maintain your environment, so that you can focus on building apps and services that run on top of the environment. IBM also handles platform updates, so that you can focus on the business.

Bluemix Local includes a private, syndicated catalog that displays the local services that are available exclusively to you. It also includes additional services that are syndicated from and available for you to use from Bluemix Public. The syndicated catalog provides the function to create hybrid applications that consist of public and private services. You have the option to decide which public services meet the requirements for your business based on your data privacy and security criteria.

Bluemix Local sits on a virtual machine that is behind your company firewall, so that you have the highest performing and most secure cloud infrastructure available to you. IBM installs, remotely monitors, and manages Bluemix Local in your data center through IBM's relay technology.

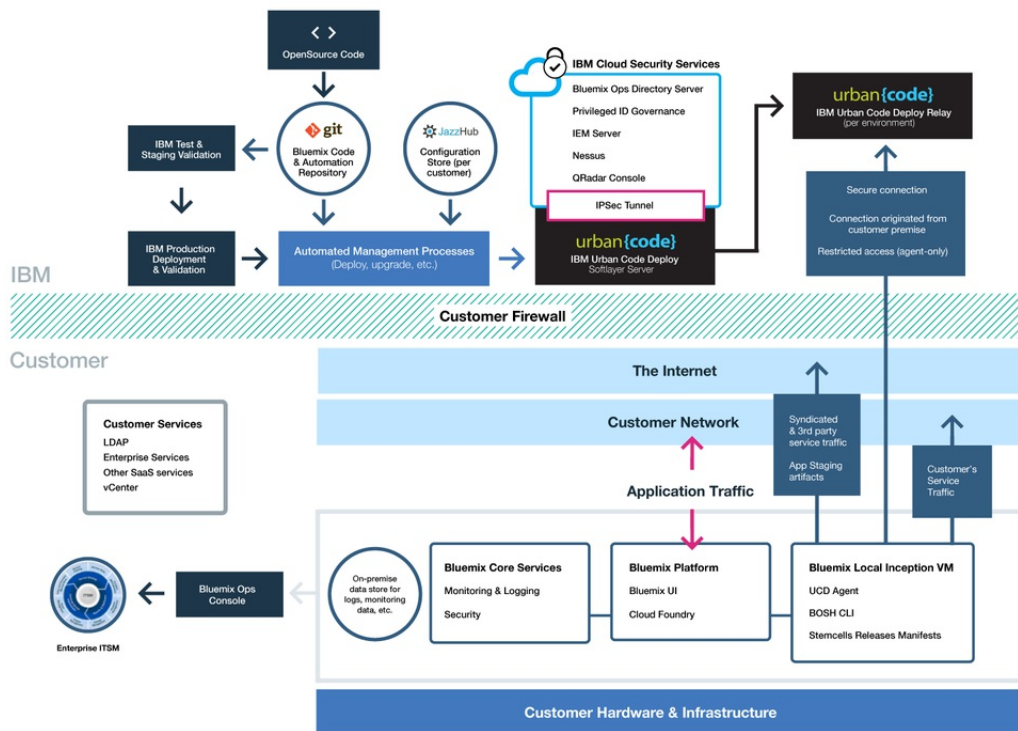


Figure 1. Bluemix Local detailed overview

Bluemix Local environments have the same security standards as the public Bluemix in terms of operational security. You provide the hardware and infrastructure, which gives you control over infrastructure and physical security. Developer access to the local Bluemix is controlled by your LDAP policies, which can be configured by the Bluemix team when they set up your environment. Within the local environment, using the Admin Console, you can manage user roles and permissions.

Bluemix Local comes with all included Bluemix runtimes and 64 GB of compute memory.

In addition, there is a set of services available for Bluemix Local.

Type	Name	Description
Included	Bluemix Runtimes	Use runtimes to get your app up and running quickly, with no need to set up and manage VMs and operating systems. All Bluemix runtimes are available for you to use in your Bluemix Local instance.
Included	Auto-Scaling	Dynamically increase or decrease the compute capacity of your application based on policies. With this service, you have unlimited use in your IBM® Bluemix™ Local environment.
Optional	Data Cache	This service provides an in-memory data grid that supports distributed caching scenarios for your apps. Includes 50 GB of in-memory cache.
Optional	API Management	Use the IBM® API Management for Bluemix™ service to compose, manage, and socialize APIs. You can import APIs with resources by using a proxy URL or by assembling data from HTTP data sources. The benefit of using the API Management service is that you can manage how your APIs are used.

Table 1. Local Services

Relay

Relay is a delivery capability included with Bluemix Local that enables IBM to automatically and consistently deliver the latest updates to all local deployments, so that you always have an up-to-date and secure system. Relay achieves secure connectivity through an open, outbound SSL, VPN tunnel that originates from the inception virtual machine on-premises by using certificates that are specific to each Bluemix Local instance. All initial Bluemix releases are available in the inception virtual machine, which also acts as an automation agent machine for deployments and updates. The SSL connection originates from the inception virtual machine, and once a secure connection is established back to the Bluemix automation server, we can check for the currency and consistency of Bluemix releases, and begin deploying updates.

The traffic on this tunnel is automation for serving and maintaining the platform, compute resources, and services for your instance. The inbound web port 443 is used for this connection. Relay is restricted to automation agent-only access. IBM uses the relay capability to deliver platform updates through a consistent testing and validation process to ensure that all deployments pushed to your local environments are stable and secure.

You have complete visibility of the environment for incident, problem, change, capacity, and security management as an administrator. Administrators access the information about their environment by using the Administration console. Relay technology keeps the Administration console current with the latest data. For more information about user access, security logs, syndicated catalog control, and communication for updates and problem repair, see [Managing Bluemix Local and Bluemix Dedicated](#).

Setting up your Bluemix Local instance

Bluemix Local is designed to provide a private version of the Bluemix Public offering that is hosted on your own hardware, managed by you. You can use Bluemix services and runtimes to support your computing needs in a secure, customer-hosted and managed cloud environment.

IBM provides you access to Bluemix Local by using a password-secured login. You can access the services, runtimes, and associated resources, and deploy and remove Bluemix apps. Review the following steps for working with your IBM representative to set up your local instance of Bluemix.

To set up your private version of Bluemix:

1. Review the [Bluemix Local infrastructure requirements](#) for setting up your local instance.
2. Contact your IBM designated account representative or contact [Bluemix](#) to get started.
3. Establish your Bluemix Local agreement with IBM that includes milestone dates for delivery.
 - a. Work with IBM on your fee for your Bluemix Local instance. The monthly recurring fee is based on the local services that you want to use, plus a subscription to all Bluemix public services. You then receive an invoice for anything that you use beyond that subscription agreement.
 - b. Identify the deadlines for each phase of setting up your Bluemix Local instance.
4. After your platform and account are created, you identify the people in your organization for the roles that are needed to get your local instance up and running. For more information about the roles that you assign, see [Bluemix Local roles and responsibilities](#).
5. You provide the hardware, and IBM helps you define and establish network connectivity between your corporate network and your Bluemix Local instance. For more information about infrastructure requirements, see [Bluemix Local infrastructure requirements](#).
 - a. IBM configures network access and LDAP based on what you provided. Administrative access is given to the contacts that you designate. You must also designate a contact for support and billing.
 - b. IBM sets up a syndicated catalog in your local environment to show your local services and many of the public Bluemix services.
 - c. You validate network and firewall configuration and the LDAP endpoint and access.

You can expect a process similar to the following list for the initial deployment and configuration of your environment. For details about who is responsible for each task, see [Roles and responsibilities](#).

1. You provide the VMware configuration that meets the specifications for compute resources, networking, and storage. For more information about the infrastructure requirements, see [Bluemix Local infrastructure](#)

requirements.

2. You provide the vCenter cluster credentials to be used by the inception virtual machine. You must provide the following information:
 - o Name of the VMware cluster
 - o vCenter cluster credentials including the user ID and password
 - o Datastore name or names (storage LUN name)
 - o VLAN ID/VMware port group
 - o Resource pool name
3. You and IBM work together to validate the credentials that you provided in the previous task.
4. You provide 7 IP addresses on your network. If you have a secured web proxy for allowing outbound access to the Internet for internal Bluemix components, then you must provide the credentials to connect to it.

Note: If your web proxy is not secure, then you do not need to provide the credentials. Also, note that not all Bluemix Local customers use a web proxy.

5. IBM provides a whitelist of URLs that must be allowed through your web proxy before starting the deployment.
6. You specify the domain names for the deployment, and the IDs that you want to use. You get two partially defined domains when you set up your local instance, and you pick the prefix for the two domains. For example, you pick the prefix for *mycompany.bluemix.net* and *mycompany.mybluemix.net*. And, then you can also choose the full domain to create a custom domain.

You can choose as many custom domains as you want. However, you are responsible for the certificates for the custom domains. For information about creating your custom domain, see [Creating and using a custom domain](#).

7. You choose which technology, IPsec or OpenVPN tunnel, to use to configure Relay to connect back to the IBM operations center.
8. IBM installs and starts up the inception virtual machine within the Bluemix cluster. If you provide your own VMware, then an IBM representative helps your customer representative to complete this task.
9. IBM configures the Relay to communicate back to the IBM operations center.
10. The inception virtual machine repository pulls in the updated build artifacts.
11. You provide the credentials for IBM to connect to the corporate LDAP directory instance.
12. IBM uses automation to deploy the core Bluemix platform.
13. IBM deploys the core platform that includes the elastic runtimes, console, administration feature, and monitoring.
14. IBM configures your administrative access to the environment.
15. IBM links your syndicated catalog from your local deployment to a Public Bluemix instance for use of public services. A set of public services are available in your local instance by default. You can use the administration page for catalog management to turn the services on or off for your local instance.
16. You can start using your local instance that is monitored by the IBM operations team in order to respond to alerts.

After your Bluemix instance is set up, you can monitor and manage your Bluemix instance by using the Administration page. For more information, see [Managing Bluemix Local and Dedicated](#). For information about upgrades and maintenance, see [Maintaining your local instance](#).

Roles and responsibilities

If you set up a Bluemix Local account, you identify the people in your organization for the roles that are needed to get your instance up and running.

Roles

The following list shows the customer roles and responsibilities that you assign:

Procurement focal

Works with the IBM representative on establishing your Bluemix Local environment, including identifying the right people in your organization to work on any aspect of the project. The person assigned to this role oversees pattern selection, commercial arrangements, and arrangement of access to customer resources. The procurement focal is the overall contact for setting up the local instance.

Compliance officer

Works with the IBM representative to select a topology and deployment option that meets your security requirements. The person assigned to this role works with the IBM compliance consultant to determine which deployment patterns achieve the compliance goals.

Network specialist

Works with the IBM representative on the network plans for the Bluemix deployment. The person assigned to this role reviews the required networking specifications required by IBM and works together with IBM on an implementation plan. At the end of the installation and verification phase, the person assigned to this role approves that the network configuration is in compliance with corporate standards.

DevOps focal

Works with the IBM representative to plan and apply the maintenance updates that are needed for the Bluemix platform, services, and runtimes. The person assigned to this role also works with the IBM representative on the configuration of your Bluemix Local instance.

IaaS specialist

Works with the IBM representatives on the deployment plan for VMware. Typically, this is someone who is a VMware administrator in the data center. The person assigned to this role reviews the [Bluemix Local infrastructure requirements](#) and works together with IBM on an implementation plan. At the end of deployment, the person assigned to this role approves that the deployment is in compliance with the corporate standards at the IaaS layer.

Your customer representatives work with a dedicated client success manager (CSM) and other IBM specialists that work together to ensure that you always have the support that you need. The CSM is provided for 6 months at no charge. The CSM completes the following tasks:

- Provides technical coordination between you and IBM.
- Coordinates updates, upgrades, expert help from IBM, and initial enablement from a Bluemix support engineer.
- Provides information about the types of support that are available.
- Acts as initial escalation point, if needed.

The Bluemix support and operations team that works with you on your Bluemix instance might access your local environment, but does so only for the following reasons.

- To respond to alerts and perform operational maintenance
- To attempt to reproduce a problem that is reported on a support ticket

Responsibilities

From setting up your environment to continued maintenance, a variety of tasks must be completed by both you and IBM. The following tables outline the required tasks and the owners for completing the task throughout the inception, progression, and completion phases.

The inception phase is used to establish the Bluemix Local environment. At this point, you have already reviewed the [Local infrastructure requirements](#) requirements. The primary goals of this phase include the following:

- Review the financial agreement, and establish the milestone dates for delivery.
- Create the Bluemix platform, and provide access to runtimes and services.
- Define and establish network connectivity between your corporate network and Bluemix operations.
- Identify and assign roles for your administrative team.

Table 1. Inception phase tasks

Task	Task details	Responsible party
Set compliance standards	Identify government, industry, and proprietary corporate standards that are required for the environment.	Customer
Create security and compliance integration plan	Create security and integration plan that includes costs, scheduling, and resources that are required to achieve security compliance.	IBM
Compliance plan approval	Approve the compliance plan.	Customer
Create sizing for environment	Create environment sizing based on predefined choices that take into consideration the high availability and disaster recovery goals, as well as initial DEA and service provisioning that is necessary to support the apps created with the platform. You and IBM work together to define, for example, what databases are needed, what services are offered in the customer's syndicated catalog, and more.	IBM and customer share responsibility
Select architecture	Select architecture based on predefined choices that take into account high availability and disaster recovery requirements.	IBM
Define disaster recovery goals	Define the disaster recovery requirements for the environment.	Customer IBM and
Create disaster recovery plan	Consult and define the disaster recovery plan. IBM creates a disaster recovery model, and consults with you where you provide feedback and approve the plan.	customer share

Task	Task details	Responsible party
Create backup and recovery plan	Create a backup and recovery plan that defines the frequency and the requirements for on-and-off site distribution of the backup. IBM backs up fabric components, IBM services, service metadata including user roles, and more. You back up any application-specific data that you are responsible for.	IBM and customer share responsibility
Identify tools for event detection and problem determination	Identify IBM and third-party tools used for event detection and problem determination at the Bluemix platform level.	IBM
Define escalation plan	Define the escalation plan to triage and resolve events detected from the monitoring components.	IBM
Sign infrastructure, platform, and support agreements	Sign the subscription agreement including the financial terms and conditions for the environment. Sign network and security monitoring agreement. Sign support subscription.	Customer
Procure environment	Procure compute resources, network, and storage. For more information about the infrastructure requirements for the environment, see Local infrastructure requirements .	Customer
Install VPN solution	Install bidirectional VPN solution.	IBM
Install fabric, application, and monitoring and management components	Install, configure, and verify fabric components, such as BOSH Director, Cloud Controller, Health Manager, messaging, routers, DEAs and service providers, and the monitoring components that are defined in the escalation and problem detection plan.	IBM
Install and configure security components	Install and configure security components that are tied into the monitoring and escalation plan including IBM QRadar, credential vault, intrusion prevention system, IBM BigFix, and IBM Security Privileged Identity Management.	IBM
Configure login server	Configure the login server for use with the corporate LDAP.	IBM
Install and configure custom components	Install and configure custom components that reside outside the scope of the Bluemix product and services.	Customer
Connect Bluemix pipeline	Connect Bluemix continuous integration and continuous delivery pipeline with IBM repositories.	IBM
Customize external solution components	Customize load balancers for disaster recovery scenarios.	Customer
Track status for security, compliance, and audit controls	Track status up to the point where all tools and processes are in place to achieve identified compliance.	Customer
Review physical infrastructure	Review physical premises that host the solution components for threats and review of security controls to protect the data center.	Customer
Inspect monitoring software	Inspect monitoring and management components as defined in the escalation and problem determination plan.	Customer
Inspect OS	Inspect to ensure that the operating system image meets compliance standards. IBM provides access to the OS image.	IBM and customer share responsibility

Next is the progression phase. The progression phase describes the on-going, collaborative relationship between you and IBM. The primary goals for this phase include the following:

- Review capacity and coordinate necessary adjustments.
- Review maintenance and platform improvements.
- Coordinate the activities for problem resolution and root cause analysis.

Table 2. Progression phase tasks

Task	Task details	Responsible party
Review weekly capacity reports	Review the weekly capacity reports and take corrective action, if needed.	Customer
Create month-to-month projections	Collect information and create a month-to-month projection of capacity and consumption.	IBM and customer share responsibility
Review capacity projections	Review the capacity projections as they relate to external events that might impact capacity as well as anticipated new deployments of apps. Work with IBM to review the projections and plan accordingly.	IBM and customer share responsibility
Adjust capacity	Add or remove capacity as your needs change.	IBM
Publish upcoming updates and maintenance	Create documentation for the required maintenance of IBM components.	IBM
Perform maintenance	Work with IBM to schedule required maintenance within a 30-day window. You can provide dates that might not work for you in the 30-day window, and IBM works to schedule the maintenance accordingly.	IBM and customer share responsibility
Address provisioning failures	Fix provisioning failures, if they occur, for customer-created services that are deployed to the Catalog.	IBM
Perform network and IP scans	Perform daily and monthly network and IP scans.	IBM and customer share responsibility
Provide access to audit logs	Provide access to all security and administrative audit logs.	IBM and customer share responsibility
Conduct testing	Conduct periodic Key Controls over Operations testing and third-party penetration testing.	IBM and customer share responsibility
Status reporting, audit coordination, and compliance meetings	Complete status reporting, external audit coordination, and representation at compliance review status meetings.	IBM
Employment and business need verification	Complete quarterly employment verification and verification of continued business need for IBM representatives that have access to the customer environment.	IBM
Resolution of security vulnerabilities	Resolve reported security vulnerabilities in the platform.	IBM

The final stage of completion represents the end of the relationship between you and IBM Bluemix. The primary tasks for this phase include the following:

- Ending of the financial agreement
- Removing all network connections
- Recycling infrastructure

Table 3. Completion phase tasks

Task	Task details	Responsible party
End financial agreement	Discuss and agree to an end to the financial agreement contract. IBM and customer share responsibility	IBM and customer share responsibility
Decommission environment	Shut down access to and credentials for the environment.	IBM and customer share responsibility
Shut down Relay	Terminate the Relay connection.	IBM
Recycle infrastructure	Recycle your infrastructure according to company guidelines.	Customer

Bluemix Local infrastructure requirements

For Bluemix Local, you own the physical security and the infrastructure for hosting the local instance. IBM sets the following requirements for setting up Bluemix Local.

Hardware

While there are requirements for the type and size of available hardware, you can choose any combination to meet the set resource total requirements.

VMware ESXi hardware

ESXi is a virtualization layer that runs on physical servers and that abstracts processor, memory, storage, and resources into multiple virtual machines. Choose any combination that meets the following resource totals, on the condition that minimum physical core count per ESXi is eight. The following specifications are for the Bluemix core runtime only.

- 48 Physical cores at 2.0 or more GHz each
- 756 GB of physical RAM
 - Total datastore size of 7.5 TB
 - 7 TB datastore to hold Bluemix

- 500 GB datastore to hold the inception virtual machine

Note: If you use multiple datastores, use the same prefix for each.

High availability

To support a single node failure, you must have $n+1$ ESXi. For example, if two ESXis are used, meaning 16x cores each, then a third is needed.

Note: The customer VMware administrator can decide to enforce strict high availability failover in the cluster to guarantee resources.

Network

Recommended requirements include a customer accessible port group with 7 customer network IP addresses that have outbound internet access in the same subnet. Then, define a second private VLAN between only the ESXis being used for Bluemix Local. This VLAN is shown as a port group in VMware. Bluemix Local uses it for the private subnet, which is more secure and can help avoid routing issues.

Note: If IBM detects a loss of network connection, IBM contacts you and works with your network specialist to resolve the issue.

vCenter server configuration

Review the following version, datacenter, resource pool, and datastore requirements.

Supported VMware versions

vCenter and ESXi 5.1 and 5.5

Supported VMware types

vSphere Enterprise

vSphere Enterprise plus, if you plan to use distributed virtual switches

Datacenter

Create a datacenter, if one does not exist.

Datacenter folder

Create a VM folder with the same name as the cluster, if you do not plan to grant Administrator access that is propagated from the datacenter.

Cluster

Create a cluster specifically for Bluemix Local use. An example for the cluster name is `bluemix`.

Resource pool

Create a resource pool under the Bluemix Local cluster. An example for resource pool name is `local`.

Datastores

Requires 7.5 TB for the initial deployment of Bluemix.

Note: When you use more than one datastore, ensure that each one begins with the same prefix. Examples of multiple datastore names with the same prefix are `bluemix_datastore_01` and `bluemix_datastore_02`.

Network Bandwidth

Recommended throughput is 5 Mbps up and 5 Mbps down, and you can expect a monthly data usage of 10 GB. IBM establishes agreed upon windows when large bundles of data are delivered, which can be as large as 3 GB.

VMware permissions

Set the following roles and permissions. Propagation is set for each permission. If the permission is propagated, the permission gets passed down through the object hierarchy. However, permissions for a child object always override permissions that are propagated from a parent object.

v Center Server

Set the role as read-only and not propagated.

Note: This role is needed to retrieve task status for specific disk operations.

Datacenter

Create the role "Bluemix" and grant permissions for **Datastore** including **Low level file operations** and **Update virtual machine files**.

Note: This role is needed to support file posts to the datastores.

Cluster

Set the role as administrator and propagated.

Datastores

Set the role administrator and propagated for each Bluemix datastore.

Network

Set public and private port groups with the administrator role, not propagated.

Droplet Execution Agent (DEA) pool

Each DEA is configured with:

- 16 - 32 GB of RAM
- 2x - 4x vCPU
- 150 - 300 GB of storage

For example, if the ESXi host size is 256 GB of memory with 16x cores, then eight DEAs are added. If the ESXi host size is 64 GB of memory with 8x cores, then two ESXis and four DEAs are required to be added. An additional 1.5 TB of storage is required for every four DEAs. This example is based on a DEA configured with 32 GB of RAM, 4x vCPU, and 300 GB of storage.

Maintaining your local instance

IBM maintains and installs updates and fixes as IBM deems appropriate to the Bluemix Local platform, runtimes, and services. Services might not be available during maintenance windows.

Important: IBM reserves the right to interrupt services to apply emergency maintenance as needed. IBM might change scheduled maintenance hours, but notifies you of any such changes, as well as any emergency maintenance information.

The following types of maintenance are required for Bluemix Local:

Standard Maintenance Windows

The services utilize pre-defined, standard maintenance windows, which might cause the services to be unavailable. IBM does not require customer approval to perform maintenance, but attempts to minimize impact to your services.

IBM sends broadcast messages of the changes that are planned for each maintenance window, through email, phone, or other methods.

Important: Some service might not be available to you during the maintenance period.

Monthly Change Window

The monthly maintenance window is applied based on coordination between you and IBM within a 21-day window. You can provide IBM with specific dates or times within the 21-day window that might not work for you. IBM attempts to schedule updates around those times. Based on the requests, IBM communicates the scheduled maintenance window to you. Monthly change windows are not expected to impact the running Bluemix Local environment.

Note: If you do not request a specific time for the update, the maintenance is automatically applied at the end of the window.

Go to **ADMINISTRATION > SYSTEM INFORMATION** to view pending updates, set unavailable dates, and approve updates. For more information about notifications and scheduling pending updates, see [Viewing system information](#).

Other

IBM intends to confine all maintenance that might affect your services, in particular the availability of your Bluemix Local environment, runtimes, and services, to the standard and monthly windows. Other change windows might be used on an exception basis for management of the environment. IBM makes reasonable efforts to minimize the impact to you during such change windows and notifies you in advance.

To set up maintenance of your local instance, work with your IBM designated account representative to identify an agreed upon window for the standard maintenance.

If there is a reported issue following a maintenance update, you agree with your IBM representative if it is in your best interest to allow IBM to roll back the update. Upon agreement, IBM rolls back the update to restore the environment to the previous state.

Disaster recovery

Bluemix™ Public provides a continuously available platform for innovation. Multiple fail-safe measures ensure that your orgs, spaces, and apps are always available. Deploying apps to multiple geographic regions enables continuous availability that protects against unplanned, simultaneous loss of multiple hardware or software components, or the loss of an entire data center, so that even in the event of a natural disaster in one geographic location, your distributed Bluemix Public app instances in alternate geographic locations will be available.

Disaster recovery for Bluemix™ Local is made possible through continuous availability for your apps, the inherent high availability of the platform, and the ability to restore your instance in the event of a failure. You are responsible for enabling continuous availability of your apps by deploying to multiple regions. High availability is built in at the platform level through technologies included in Cloud Foundry and other components. And, you can work together with IBM to ensure that your data is properly backed up in the case that you need to restore your instance at any time.

Enabling continuous availability for Bluemix Local

By default, Bluemix Public deploys to multiple geographic locations. However, you must do the following to enable globally distributed Bluemix Local instances:

- Ensure that your developers are deploying apps in more than one region, either through a manual or automated process. Selected regions should be more than 200 km apart from each other to ensure that a natural disaster cannot affect both geographic locations.
- Configure a global load balancer, like Akamai or Dyn, to point to apps in at least two different regions.

Note: Not all Bluemix services support regional distribution. When you construct an app, if you want to achieve geographic distribution, then you must also make sure that the services that are used by that app have data synchronization as a key feature.

Deploying Bluemix Local apps to multiple geographic locations

To deploy into a second location or multiple locations, you must follow a process similar to the one you took to enable your primary geographic location:

1. Enable a new local environment to host additional instances of your applications. To create a new environment, contact your IBM sales team to initiate the process. For more information about setting up a local instance, see [Setting up Bluemix Local](#). You must log in separately to access each environment. Each physical location for the hosted environments should be a minimum of 200 km away from the original location to ensure availability.
2. Obtain the unique domain name where your new deployed app will be hosted. For example, if your original domain is *mycompany.east.bluemix.net*, then you can create a new local environment with a new domain such as *mycompany.west.bluemix.net*, and deploy to the new domain.
3. Deploy to the new location each time you deploy your original app. For more information about deploying, see [Uploading your app](#).

Enabling a global load balancer for Bluemix Local

A global load balancer not only ensures continuous availability and is required for disaster recovery, but it also has several additional benefits:

- Routes users to the closest Bluemix region by default
- Routes based on performance
- Selectively directs a percentage of traffic to a new application version
- Provides site failover based on region health check
- Provides site failover based on application health check
- Uses weighted routing between endpoints

You can choose a global load balancer such as Akamai or Dyn. For more about using Akamai as a global load balancer, see [Global traffic management](#). For more about using Dyn as a global load balancer, see [4 Reasons Businesses Are Taking Global Load Balancing to the Cloud](#).

High availability

In addition to enabling continuous availability, Bluemix also provides high availability across the platform by using technologies built into Cloud Foundry, Docker, and other components.

These technologies include the following:

Scalability in Cloud Foundry

A Cloud Foundry [Droplet Execution Agent \(DEA\)](#) performs health checks on the apps running within it. If there is a problem with the app or the DEA itself, it deploys additional instances of the app to an alternate DEA to address the issue. For more information, see [Configuring CF for High Availability with Redundancy](#).

Metadata backup

Metadata is backed up to a secondary location, typically an on-premises virtual machine. If possible, you should replicate the backup to your own environment at least 200 km away.

Restoring your local instance

Bluemix Local settings, metadata, and configurations are backed up regularly to prepare for any unplanned outages in the environment. Your data that you are responsible for backing up includes application data, cloud database services data, and object stores.

As part of the data backup, which includes system metadata and configurations, IBM completes the following tasks:

- Encrypts all backup copies and manages encryption keys
- Monitors and manages backup activity
- Provides the encrypted backup files
- Restores the requested data
- Manages scheduling conflicts between backup and fix management operations

Because protection of private data is critical, IBM needs your collaboration when dealing with backup file management, so that the files are not moved outside of your data centers. Specifically, IBM asks that you complete the following tasks:

- Move a copy of your encrypted backup data off-site, just as you would for any other backup data that you manage.
- Provide the backup files for the IBM operator in case of any need to restore.

Administering Bluemix

Manage your orgs, spaces, and assigned users by clicking **Account and Support > Manage Organizations**. If you are a Bluemix Local or Bluemix Dedicated user, see [Managing Bluemix Local and Bluemix Dedicated](#) for more information about administering your local or dedicated instance.

Managing your account

In IBM® Bluemix™, you can manage orgs and spaces, including user access all from the dashboard in the user interface. You can also monitor your usage and billing.

Organizations and spaces

As an organization manager or account owner, you can use the Manage Organizations page to view and manage the settings of the organization or space, including user access. To open the Manage Organizations page, on the menu go to *Account and Support > Manage Organizations*.

Organizations

An organization is defined by the following items:

Users

The role with basic permission in organizations and spaces. You must be assigned to an organization before you can be granted other permissions to the spaces within the organization. For detailed information, see [Users and roles](#).

Domains

Provide the route on the internet that is allocated to the organization. A route has a sub-domain and a domain. A sub-domain is typically the application name. A domain might be a system domain, or a custom domain that you registered for your application.

Note: If you add a custom domain, you must configure your DNS server to resolve your custom domain to point to the Bluemix system domain. In this way, when Bluemix receives a request for your custom domain, it can properly route it to your application.

Quota

Represents the resource limits for the organization, including the number of services and the amount of memory that can be allocated for use by the organization. Quotas are assigned when organizations are created. Any application or service in a space of the organization contributes to the usage of the quota. With the Pay as you go or Subscription plans, you can adjust your quota for Cloud Foundry applications and containers as the needs of your organization change.

In Bluemix, you can use organizations to enable collaboration among users, and to facilitate the logical grouping of project resources in the following ways:

- You can group a set of spaces, applications, services, domains, routes, and users together in organizations.
- You can manage the access to the spaces and organizations on a per-user basis.

When you create an organization, the organization name must be unique in Bluemix. After you create the organization, you will be automatically assigned the *Organization Manager* permission, which enables you to edit the organization name, delete the organization, and create spaces in the organization.

When you delete an organization, all the spaces, applications, and services within the organization are deleted.

Bluemix enables collaboration on projects by assigning users within an organization, and within the spaces in the organization. You can use the **Users** tab to display and manage users of the organization. You can also invite users to your organization by clicking the **Invite a New User** link on the **Users** tab. The following permissions can be assigned to users in an organization:

- Organization user
- Organization manager
- Organization billing manager
- Organization auditor

Spaces

Within an organization, you can use spaces to group a set of applications, services, and users.

After you add users to an organization, you can grant them permissions to the spaces within the organization. Similar to organizations, spaces also have a set of permissions that can be assigned to users:

- Space manager
- Space developer
- Space auditor

Note: A user must be assigned at least one of the permissions in the space.

The **Domains** tab for a space is a read-only list of the domains that are assigned to the space. The system domain is always available to a space, and custom domains might also be allocated to the space. Applications that were created in the space might use any of the listed domains for the space.

Users and roles

Account owners perform all operations on organizations and spaces.

User types

You can be either a member or a collaborator of an account.

Member

You are a member of a Bluemix account if you created the account, or you were invited to the account and then you signed up from the invitation, as your first experience with Bluemix.

Collaborator

You are a collaborator of a Bluemix account if you previously used Bluemix with a different account, but then you were invited to this account and you accepted the invitation.

User roles

Users can be assigned the following permissions to take different user roles in an organization or space:

Organization managers

Organization managers have the following permissions:

- Create or delete spaces within the organization.
- Invite users to the organization if you are also a member of the organization or the account owner.
- Manage existing users who are already in the organization.
- Manage domains of the organization.

Note: If you have the user type of collaborator, and previously used Bluemix with a different account, you cannot invite users to the organization even if you are assigned the organization manager role. You must have the user type of member to invite users. See [Unable to add users to an organization](#) for information about how to work around this problem.

Billing managers

Billing managers have permissions to view runtime and service usage information for the organization.

Organization auditors

Organization auditors have permissions to view application and service content in the space.

Space managers

Space managers have the following permissions:

- Add users to the space and manager users.
- Enable features for the space

Space developers

Space developers have the following permissions:

- Create, delete, and manage applications and services within the space.
- Have access to logs within the space

Space auditors

Space auditors have permissions for read-only access to all information about the space, such as information about applications and services, settings, reports, and logs.

Managing your organization

As an organization manager or account owner, you can manage your organizations. Management tasks include creating an organization, renaming an organization, creating a space, inviting users to a space, and deleting an

existing organization.

- **Creating an organization**

Only users with pay accounts can create an organization. With a pay account, you can create an organization by taking the following steps:

1. Go to the Bluemix Dashboard, click the icon in the upper right, and select **Manage Organizations**.
2. Click **Create an Organization** and follow the prompts to create your organization.

- **Renaming an organization**

Take the following steps to rename your organization:

1. Go to the Bluemix Dashboard, click the icon in the upper right, and select **Manage Organizations**.
2. Select the organization that you want to rename.
3. Type a new name in the **Organization** field, and click **Save**.

- **Listing members**

Take the following steps to list the members of your organization or space:

1. Go to the Bluemix Dashboard, click the icon in the upper right, and select **Manage Organizations**. You can see the members of your organization and their roles in the **Users** tab.
2. Click the space name in your organization to see the members of this space and their roles.

- **Creating a space**

You can create spaces in your organization; for example, a *dev* space as a development environment, a *test* space as a testing environment, and a *production* space as a production environment. Then, you can associate your apps with spaces. Take the following steps to create a space:

1. Go to the Bluemix Dashboard, click the icon in the upper right, and select **Manage Organizations**.
2. Click **Create a Space** under your organization name, and follow the prompts to create your space.

- **Inviting users to a space**

You can invite users to your organization as collaborators. You can also add users of your organization to different spaces. The users can access only the space that they were added to. Take the following steps to add a user to a space:

1. Go to the Bluemix Dashboard, click the icon in the upper right, and select **Manage Organizations**. Then, click **Add user** in your organization, and follow the prompts to add the user to your organization.
2. Add the user to a space. Select the space from the left navigation pane, click **Add User**, and follow the prompts to add the user to the space.

- **Deleting an existing organization**

Contact Bluemix registration and ID support to delete your organization.

Note: Deleting operations cannot be reversed. You lose all your applications and services that are associated with the organization.

Managing Bluemix Local and Bluemix Dedicated

Use the Admin Console to manage resources, monitor usage, administer user permissions, and view security reports, logs, status, and upgrade notifications for your IBM® Bluemix™ Local or Dedicated environment.

Accessing the Admin Console

You can access the Admin Console by entering the following URL:

<https://opaconsole.<subdomain>.bluemix.net/>

<subdomain>

This value is the name of your local or dedicated instance. The subdomain name for your IBM® Bluemix™ instance was assigned during onboarding.

Viewing system information

Use the Admin Console to monitor your system information.

To view system information, click **ADMINISTRATION > SYSTEM INFORMATION**.

You can expand and view various sections about pending updates, general system information, and LDAP configuration details.

- In the Updates section, you can view any pending updates that require action on your part. You can also easily track your updates using the calendar link to import your scheduled updates to a calendar app.
 1. To take action for a specific update, complete the following steps:
 - a. Click **Number updates pending** to view all pending updates.
 - b. Select an update to take action or view the details of the update, which include the update window, scheduled date, or disruption status.
 - c. Click **SET UNAVAILABLE DATES** to set specific days in the update window that are not convenient for the update to be applied. If you set unavailable dates, IBM approves and schedules your update based on your selections. You receive a notification when the update is approved and scheduled.
 - d. Click **APPROVE** to approve the update, if you do not have any unavailable dates. If you approve, the update is applied during the scheduled update window. IBM sends a notification when the update deployment starts and ends.
 2. To import your scheduled updates to a calendar app of your choice, complete the following steps:
 - a. Open your calendar app.
 - b. Import the updates calendar by pasting the **Calendar URL** listed on the System Information page in your app. Or, download the calendar file by clicking the Calendar URL, and then import it to your calendar app by using the `.ics` file.
 - c. Enter your credentials.
 - d. View your scheduled updates.
- In the General Information section, you can view the following information:
 - Basic information about the Bluemix build.
 - API information including the version, URL, region, and a link to the CLI documentation.
 - Shared domain information about your system and service.
 - Statistics about the total number of applications, users, and organizations.
- In the LDAP Configuration Details section, you can select the LDAP server, and view information about user and group mappings. If you are using IBM® WebID, it is indicated in the LDAP Configuration Details section.

Viewing usage information

Use the Admin Console to monitor resource and network usage.

To view resource information, click **ADMINISTRATION > USAGE**.

In the Resource Monitoring section, you can view the following information:


- Resource usage information, such as how many GB of memory and how many GB of disk space are used. You can view the CPU usage averaged across all droplet execution agents (DEAs). Click the **CPU** tile, and you can see the CPU usage for each DEA. The DEA with the highest usage is listed first, and each is identified by their job and IP address. The CPU usage is separated into three categories that include amount of CPU spent in system processes, amount of CPU spent in user processes, and amount of CPU spent in waiting processes.
- Network usage information for bandwidth in and bandwidth out, over the past day, week, or month. The data that is displayed is based on the sum of in and out traffic for both public and private networks.
- Average response time for Bluemix over the past 10 minutes, hour, and day.
- Average transactions per second for Bluemix over the past 10 minutes, hour, and day.

Viewing reports

You can view security reports and logs, such as DataPower™, firewall, and login audit, for your Bluemix instance.

To view reports and logs, click **ADMINISTRATION > REPORTS AND LOGS**.

Select from the following options:

- You can select start and end dates from the fields to filter which reports and logs are displayed.
- You can expand and view various reports from the left navigation pane.
- You can search within your collection of reports and logs. The search applies to report names as well as text content that is contained within the reports and logs. You can also choose to filter your search by **Administration Events, DataPower Reports, Firewall, and Login Audit**.
- When displaying a report or log, you can click the  icon at the upper right of the report to download it.

For more information about the types of security reports, see [Security reports](#).



Viewing status

You can monitor status for your Bluemix instance through the Admin Console. You can also subscribe to an RSS feed for notifications so that you don't have to check for them.

To view status for your Bluemix instance, complete the following steps:

1. In the Admin Console in the upper-right corner, click the **Profile Settings** icon.
2. Then, click **Status**.

The System Status page displays. The left pane displays the status of your runtimes and services across regions and your Bluemix instance. The right pane shows notifications.

1. If you configured your browser for RSS feeds, you can subscribe to an RSS feed of the notifications. Locate the  icon to the right of **UPDATES** at the top left of the notifications list, and select one of the following actions:
 2. Drag the  icon into your RSS reader.
 3. Right-click the RSS icon, select **Copy link address**, and paste the URL into your RSS reader.
 4. Filter which notifications are displayed. Click **FILTER** at the top right of the notifications list. Then, you can search and narrow the list of notifications by typing a word that you would expect to find in a notification, for example "maintenance". Or, you can click to select which notifications to display by **Type, Region, Category, Start date, or End date**.

Managing your Catalog

You can manage which Bluemix services and starters are visible to users in the Bluemix Catalog.

To use the Admin Console to manage the Catalog, click **ADMINISTRATION > CATALOG MANAGEMENT**.

Select a service or starter tile to edit the service or starter plan visibility. To edit the visibility, select from the following options:

- To show the hidden service or starter so that it is visible to your users in the Catalog, select **ENABLE ALL PLANS**.
- To hide the service or starter from your users in the Bluemix Catalog, select **DISABLE ALL PLANS**.
- To control the visibility of an individual plan, select the plan name, and then use the drop-down menu to select **Enable for all organizations, Disable for all organizations, or Enable plan for specific organizations**.

Administering organizations

You can manage your organizations by creating and deleting organizations, adding managers to organizations, and monitoring quota usage.

To use the Admin Console to manage your organizations, click **ADMINISTRATION > ORGANIZATION ADMINISTRATION**.

You can expand and view various sections. You can also review and manage the quota plans for your organizations.

- To create a new organization and add managers, click **CREATE ORGANIZATION**. Enter a name for the organization, and then enter the name or email of the person that you want to add as a manager. You can add more than one manager by entering and selecting multiple names. Click **CREATE ORGANIZATION** to save your changes and create the org.
- In the Quota Monitoring section, you can expand the section and view the following information:
 - Environment memory usage. This section details the memory usage for the full system environment. The chart provides information that includes used system memory, total system memory, quota that is used, and the total quota allocated. The following list of terms defines the types of memory usage that are displayed in the chart.

Used system memory

The physical memory that is used by your environment.

Total system memory

The total physical memory that is available to your environment.

Quota deployed

The sum of memory that is allocated for all deployed apps, across all organizations. The sum of the quota deployed can exceed the physical total system memory for your environment. For example, if you have a total system memory of 16 GB, and you allocate 4 GB of memory each for a total of five different organizations, the total quota exceeds the total system memory that has been allocated to you for all organizations. However, in many cases, the organizations might not use the total quota that is allocated individually to each organization. In addition, all organizations might not use their total quota allocation of memory all at the same time.

Total quota

The total memory that is allocated across all organizations.


- Organization memory usage. This section details the memory usage at an organization level. You can view the total quota allowance and the quota that is deployed for each organization. The chart provides information that is listed by highest memory usage per organization, and the organization that uses the largest amount of memory, by default, is listed first. You can sort by **Highest Memory Usage** and **Excess Memory Allocation**.

Highest Memory Usage

Use this option to identify the org using the greatest amount of memory. Sort by highest memory usage to identify the organizations that are using the most amount of memory. The list is sorted by quota deployed.

Excess Memory Allocation

Use this option to identify organizations that have a quota plan that is larger than needed. Sort by excess memory usage to identify organizations that are using the lowest amount of memory for the quota that has been allocated for the org.

- To change the quota plan for an organization, click the bar in the chart for the organization that you want to edit in the Organization memory usage section, or select the name of the org from the Organization List section. On the Edit Organization page, you can change the quota plan, change the name of the org, and add or remove managers. If you select a quota plan that is not sufficient for the current usage for the organization, you receive a message. To save any changes that you made on the Edit Organization page, click **SAVE**.
- In the Organization List section, you can view all organizations in the Bluemix environment.
 - To delete the organization, click  in the Actions column.
 - To view and edit the quota plan for an organization, click the name for the organization in the list.
 - To edit the name of the org and add or remove managers, click the name for the organization in the list.



Managing users and permissions

You can add users to your Bluemix instance from your company's user registry through LDAP. You can add users singly or in groups, and view user permissions. If you are assigned `admin` permission, you can also set and manage permissions for other users.

To use the Admin Console to manage users, click **ADMINISTRATION > USER ADMINISTRATION**.

The User Administration page displays all users for the local or dedicated instance. Permissions for each user are displayed. Permissions can be the following: None, Admin, Catalog, Login, Reports, and Users. Permissions can be enabled, or the user can be given `view` or `write` ability for that permission, as represented by icons. See [Permissions](#) for descriptions of each type and explanation of the icons.

Choose from the following options:

- Locate users. You can locate users in the table by using the **Search** field at the top.
- Add users. If you have `admin` permission or `users` permission with `write` ability, you can add users. To add a user or group of users, click **ADD SINGLE USER** or **ADD USER GROUP**. In the **Search** field, type a user name or group name to search, and select the organization to add the user or user group to from the **Org** list. When you find the user or group that you want to add, click the user name, then click **ADD USER** or **ADD USERS** to add. Groups of more than 50 users are added through a background batch job. When the add operation is successful, the user or group is added to the table for you to view and search. When users are added, they have no assigned permissions.
- Edit permissions and organizations. If you have `admin` permission, you can edit permissions and organizations for other users. To edit permissions, locate the user and click the user name. To enable or disable permissions, select from the following options in the window that opens:
 - Select **On** from the list to enable a permission.
 - Select **Read** from the list to allow the user to have `view` (read-only) ability for that permission, or **Write** to allow `write` (edit, or add and remove) ability for that permission.
 - Select **Off** to disable the permission. To edit organizations, select from the following options:
 - Add the user to an organization by using the search field to locate an organization, clicking to select from the options, and clicking **ADD**.
 - Remove a user from an organization by clicking the  icon. When finished, click **SAVE**.
- Remove users. If you have `admin` permission or `users` permission with `write` ability, you can remove users. To remove a user, locate the user and click the  icon and then **Remove**.




Permissions

Users can be assigned the following permissions:

User permission	Description
Admin	Users with <code>admin</code> permission are allowed to edit permissions for other users.
Catalog	Users with <code>catalog</code> permission can be assigned the ability to <code>view</code> or <code>write</code> (modify) which services are available in the local or dedicated instance.
Login	Users with <code>login</code> permission are allowed to log in to the Admin Console. Without this permission, users can't log in.
Reports	Users with <code>reports</code> permission can be assigned the ability to <code>view</code> or <code>write</code> (modify) security reports.
Users	Users with <code>users</code> permission can be assigned the ability to <code>view</code> the list of users or <code>write</code> (add or remove) users. This permission doesn't allow you to set permissions for other users.

Table 1. Permissions

Permissions can be enabled, or the user can be given `view` or `write` ability for that permission, as represented by the following icons:

- The  icon beside a permission means that it is enabled.
- The  icon means that the user has `view` (read-only) ability for that permission.
- The  icon means that the user has `write` (edit, add, or remove) ability for that permission.

Managing users with the Admin REST API

You can use the Admin REST API to add and remove users for your Bluemix instance. The Admin REST API endpoints and JSON responses are provided on an experimental basis to enable basic operations from a command line. The endpoints and URLs in the examples in this information might change or might be discontinued at short notice.

The following tools are prerequisites for using the examples that follow. You can choose to use other tools as well.

- cURL, to enter REST API requests as commands. cURL is a free utility that you can use to send HTTP requests to a server and receive the server responses through a command-line interface. You can download cURL from the [cURL Download site](#).
- Python, to use the Python pretty-print JSON tool. This optional tool takes the JSON text as input and provides easy-to-read output. You can download Python from the [Python Downloads site](#).

Logging in to the Admin Console

Before you can run any Admin API requests, you must log in to the Admin Console. If you have `admin` permission or `users` permission with `write` ability, you can add or remove users. You must have `admin` permission to edit other users' permissions.

To log in to the Admin Console, you can use basic access authentication on the `https://<your_host>.ibm.com/login` endpoint. The server returns a cookie with your session. You use that cookie for all operations with the Admin Console.

Note: The session becomes invalid if not used for a few hours.

To log in to the Admin Console, run the following command:

```
curl --user <user_id>:<password> -c ./cookies.txt --header "Accept: application/json" https://<your_host>.ibm.com/login | python -m json.tool
```

--user *user_id:password*

Accepts the user ID and password and sends a Basic Authorization header.

-c *filename*

Stores the specified user ID and password as a cookie in the specified file.

--header

Sends an Accept header.

The following example shows output from this command:

```
{
  "message": "Logged in",
  "name": {
    "familyName": "**last_name**",
    "givenName": "**first_name**"
  }
}
```

Listing organizations

When you add a user, you must specify an organization. You can use the Admin REST API to list all organizations. You must have `users` permission with `read` ability to list organizations. To list all organizations, run the following command:

```
curl -b ./cookies.txt https://<your_host>.ibm.com/codi/v1/organizations | python -m json.tool
```

-b *filename*

Passes the user ID and password that was previously stored with the `-c` option in the file to the HTTP server as a cookie.

For each organization, the results include the following information:

- "guid", GUID of the organization
- "name", name of the organization

The following example shows output from this command:

```
{
  "resources": [
    {
      "guid": "05af098d-d476-4fb0-8b87-a84350e72af3",

```

```

    "name": "org-1"
  },
  {
    "guid": "5129a5a8-37c2-4ee4-a9b2-bebae3531db5",
    "name": "org-2"
  },
  ....
],
"total_results": 284
}

```

Listing users

You can determine whether a user was already added to your Bluemix environment by using the Admin REST API to list registered users. You must have `users` permission with `read` ability to list registered users. To list all users, run the following command:

```
curl -b ./cookies.txt https://<your_host>.ibm.com/codi/v1/users | python -m json.tool
```

-b filename

Passes the user ID and password that was previously stored with the `-c` option in the file to the HTTP server as a cookie.

For each registered user, the results include the following information:

- `"first_name"` (given name) and `"last_name"` (surname)
- `"user_id"`, user ID and email address
- `"guid"`, GUID of the organization.
- `"permissions"` that are assigned to the user for the Admin Console.

The following example shows output from this command:

```

{
  "next_url": "/codi/v1/users?results_per_page=100&page=2",
  "prev_url": "",
  "resources": [
    {
      "active": true,
      "created_at": "2015-04-08T17:38:51.788Z",
      "created_by": "",
      "first_name": "some first name",
      "guid": "5d5268cf-39c0-48d3-96ae-7afe928e5dd7",
      "last_name": "some last name",
      "permissions": [
        {
          "display": "ops.admin"
        },
        {
          "display": "ops.catalog.write"
        },
        {
          "display": "ops.reports.write"
        },
        {
          "display": "ops.catalog.read"
        },
        {
          "display": "ops.users.write"
        },
        {
          "display": "ops.reports.read"
        },
        {
          "display": "ops.login"
        },
        {
          "display": "ops.users.read"
        }
      ],
      "user_id": "someid@us.ibm.com"
    },
    ...
  ]
},
"total_pages": 395,
"total_results": 39421
}

```

Adding a user

You can use the Admin REST API to add users to the Bluemix instance. You must have `users` permission with `write` ability to add users.

You can add one user or a list of users. You can add users to a single organization, or to multiple organizations.-->To add a user, you must provide the following information:

- First name (given name) and last name (surname) of the user. Provide the `"first_name"` and `"last_name"` from [Listing users](#).
- Email address and user ID: Provide the `"user_id"` from [Listing users](#) for both the email address and the user ID.
- `"guid"`. Provide the GUID of the organization from [Listing organizations](#).

You provide the information in a JSON file.

```
curl -b ./cookies.txt https://<your_host>.ibm.com/codi/v1/users | python -m json.tool
```

-b filename

Passes the user ID and password that was previously stored with the `-c` option in the file to the HTTP server as a cookie.

1. Create a JSON file that contains the information in a proper JSON format.

For example, create a file that is named `user.json` that has the following content:

```

{
  "members": [
    {
      "emails": [
        "some_user_id@domain.com"
      ],
      "first_name": "Some first name",
      "last_name": "Some last name",
      "user_id": "some_user_id@domain.com"
    }
  ],
  "organization_roles": [
    {
      "id": "7a891f9c-e4e7-46c7-8b4e-dffaa7eb3bcd"
    }
  ]
}

```

```
}
]
}
```

2. Post the content of the JSON file to the user's endpoint by running the following command:

```
curl -v -b ./cookies.txt -X POST -H "Content-Type: application/json" -d @./user.json https://.ibm.com/codi/v1/users
```

-v
Specifies verbose output.

-X POST
Specifies a POST request, overriding the default GET request.

-H "Content-Type: application/json"
Specifies the content-type header, which in this case is JSON.

-d *data*
Specifies the data, in this case the file `user.json`, to be sent in POST request to the HTTP server.

The following example shows output from this command:

```
* Connected to localhost (127.0.0.1) port 3000 (#0)
> POST /codi/v1/users HTTP/1.1
> User-Agent: curl/7.37.1
> Host: localhost:3000
> Accept: */*
> Cookie: opsConsole.sid=s%3AHLcWkGumyEb3IxREmikDOG3ATKD5xYMe.jfjWAaltJC0rGghpeV8RPHqE2JaFVL4ZFIJbQpSC%2FAI
> Content-Type: application/json
> Content-Length: 333
>
* upload completely sent off: 333 out of 333 bytes
< HTTP/1.1 201 Created
< x-powered-by: Express
< vary: X-HTTP-Method-Override
< content-type: application/json
< date: Wed, 22 Apr 2015 19:32:54 GMT
< connection: close
< transfer-encoding: chunked
< X-Time_Check: Proxy Time: 5612 msec
```

Removing a user

You can use the Admin REST API to remove users from the Bluemix instance. You must have `users` permission with `write` ability to remove users.

To remove a user, you must provide the user ID of the user. Run the following command:

```
curl -v -b ./cookies.txt -X DELETE https://<your_host>.ibm.com/codi/v1/users?user_id=<some_user_id@domain.com>
```

-X DELETE
Specifies a DELETE request.

The following example shows output from this command:

```
* connect to ::1 port 3000 failed: Connection refused
* Trying 127.0.0.1...
* Connected to localhost (127.0.0.1) port 3000 (#0)
> DELETE /codi/v1/users?user_id=exampleuser@domain.com HTTP/1.1
> User-Agent: curl/7.37.1
> Host: localhost:3000
> Accept: */*
> Cookie: opsConsole.sid=s%3AHLcWkGumyEb3IxREmikDOG3ATKD5xYMe.jfjWAaltJC0rGghpeV8RPHqE2JaFVL4ZFIJbQpSC%2FAI
>
< HTTP/1.1 201 Created
< x-powered-by: Express
< content-type: application/json
< date: Wed, 22 Apr 2015 21:01:09 GMT
< connection: close
< transfer-encoding: chunked
< X-Time_Check: Proxy Time: 1922 msec
<
```

Managing users with the cf CLI

You can manage users for your Bluemix environment by using the Cloud Foundry command line interface with the Bluemix Admin CLI plug-in. For example, you can add users from an LDAP registry.

Before you begin, install the cf command line interface. The Bluemix Admin CLI plug-in requires cf version 6.11.2 or later. [Download Cloud Foundry command line interface](#)

Restriction: The Cloud Foundry command line interface is not supported by Cygwin. Use the Cloud Foundry command line interface in a command line window other than the Cygwin command line window.

Adding the Bluemix Admin CLI plug-in

After the cf command line interface is installed, you can add the Bluemix admin CLI plug-in.

Complete the following steps to add the repository and install the plug-in:

1. To add the Bluemix admin plug-in repository, run the following command:

```
cf add-plugin-repo BluemixAdmin https://opsconsole.<subdomain>.bluemix.net/cli
```

<subdomain>
Subdomain of the URL for your Bluemix instance.

2. To install the Bluemix Admin CLI plug-in, run the following command:

```
cf install-plugin bluemix-admin-cli -r BluemixAdmin
```

To see a list of commands, run the following command:

```
cf plugins
```

For additional help for a command, use the `-help` option.

For more information about how to work with the Bluemix Admin CLI plug-in, see [Bluemix admin](#).

Getting customer support


If you experience problems with IBM® Bluemix™, you have several support options, such as getting help through Stack Overflow or opening a support ticket.

Getting help

To get help, you can go to Account and Support, or you can go directly to Stack Overflow, where you can search information or post questions.

Using Account and Support

Account and Support is a feature that enables you to check account information, view status, stay up to date with notifications, select your region, select and manage orgs, and log out. In addition, you can get help and provide feedback.

To open Account and Support, log in to the Bluemix user interface and click the **Account and Support** icon  in the upper right of the Dashboard.

Click **Get help** to find answers to your questions. On the page that is displayed, type your question in the search field. Answers from across Bluemix documentation and Stack Overflow are displayed. The page also provides options to post your question to Stack Overflow, or to open a ticket with by clicking **GET IN TOUCH**.

Asking a question

Whether accessed directly or through Account and Support, Stack Overflow is a website that serves as a platform for users to ask and answer questions. The Bluemix development and support teams are active on Stack Overflow, and follow the questions that are tagged with **bluemix**.

To ask a question in Stack Overflow, choose from the following options:

- From Account and Support, click **Get help**. On the page that is displayed, type your question in the search field to find answers. If the expected answer is not returned, you can click **POST TO STACKOVERFLOW** to post your question.
- Or, go directly to [Stack Overflow](#).

When you create a question in Stack Overflow, add a **bluemix** tag to your question to ensure that it is seen by the Bluemix development and support teams.

Viewing Bluemix status

The Bluemix Status page is the central place to find notifications and announcements about key events that are affecting the Bluemix platform and the major services in Bluemix.

On the Status page, you can find the following information:

- Current status of services and components in all Bluemix regions.
- A list of announcements, in chronological order, for maintenance and incidents. You can filter the list or open an individual announcement for more details.
- Planned maintenance windows, which are posted at least 24 hours in advance, except in extreme circumstances.
- Unplanned incidents or outages, which are posted as soon as the Bluemix team becomes aware of them. Incident notifications are regularly updated until they are resolved.
- Security bulletins.
- Other platform-wide announcements of general interest to you.
- An RSS feed to subscribe to.


You can find the Status page by choosing either of the following options:

- From Account and Support: log in to the Bluemix user interface and click the **Account and Support** icon  in the upper right of the Dashboard, then click **Status**.
- Accessing it directly at [IBM Bluemix - System Status](#).

Subscribing to an RSS feed

You can also be alerted of any notifications by subscribing to the RSS feed for the Bluemix Status page. This provides a way for you to get updates without having to regularly consult the status page.

To subscribe, follow these steps:

1. Download and install an RSS reader.
2. Use your reader to subscribe to the feed with one of the following methods:
 - Drag the  icon into your RSS reader.
 - Right-click the RSS icon, select **Copy link address**, and paste the URL into your RSS reader.

See your reader's **Help** section for more information.

Other methods of reading RSS feeds are also available through web browser plug-ins such as [RSS Feed Reader](#) for Chrome or [Brief](#) add-on for Firefox, or with other news sources like [Feedly](#) or [G2reader](#).

You can also use a third-party service to automatically send an email for each RSS update. The following are some example third-party services:

- www.feedmyinbox.com
- www.rssforward.com
- www.feedrabbit.com
- www.mailchimp.com
- www.feedmaier.com
- www.ifit.com

Bluemix typically has approximately 50 updates per month.

Best practices for monitoring status

- Check for upcoming maintenance windows

Check for upcoming maintenance windows posted on the status page, at least once every 24 hours, by using one of the following options:

- By navigating directly to the [Status](#) page
 - By using the RSS feed or an RSS-to-email forwarder
- Check for current maintenance windows or an incident in progress

If you suspect that Bluemix is not functioning as expected, check the status page for current maintenance windows or an incident in progress. To report an incident that is not already listed on the status page, open a Support ticket through the [Client Success Portal](#) or the [simple form](#).

- Take advantage of multiple Bluemix regions

All users of Bluemix Public automatically have access to the US-SOUTH, EU-GB, and AU-SYD regions:

- US-SOUTH: <https://console.ng.bluemix.net>
- EU-GB: <https://console.eu-gb.bluemix.net>
- AU-SYD: <https://console.au-syd.bluemix.net>

The Bluemix Global Operations team manages all regions to avoid maintenance impacts and minimize the risk of incidents that affect all regions at the same time.

- Prepare for minor interruptions

In most cases, Bluemix can continue to be used normally, even during the maintenance window. However, minor interruptions of a service can't always be avoided. Running applications typically remain available even if the application management functions of Bluemix, such as starting and stopping apps, are temporarily interrupted. To maximize the availability of your running applications, run at least three instances of each application.


Contacting support

You can open support tickets if you have a valid Bluemix account. Bluemix Dedicated or Bluemix Local customers also get an option to purchase additional premium support that enables remote access to a named support lead, who is a Bluemix technical advisor and product specialist. All Bluemix customers can also contact IBM for registration or billing questions.

Contacting support for Bluemix Public

If you were unable to resolve your problem with troubleshooting and help options, you can ask for support.

To open a support ticket, use one of the following methods:

- From Account and Support. Log in to the Bluemix user interface, click the **Account and Support** icon  in the upper right of the Dashboard.
 1. First, ensure that you check Bluemix status by clicking **Status**.
 2. Then, if the problem is not due to an outage, click **Get help**. On the page that is displayed, click **GET IN TOUCH**. Fill in the form to indicate what you need technical support for.
- Use the [Bluemix Support ticket](#) form. For technical questions, ID questions, and billing questions, contact support by opening a new ticket.
- From the [IBM® Client Success Portal](#). Support is available through the IBM Client Success Portal with the following options:
 - Initial 30-day trial subscription (complimentary)
 - Bluemix Dedicated environments (included)
 - Bluemix Local environments (included)
 - Pay As You Go with the Support add-on
 - Subscription with the Support add-on

Log in to the IBM Client Success Portal with your IBM ID and password and click **Open a support ticket**.

When opening a support ticket, ensure that you indicate an appropriate severity for your ticket, because the severity determines how your ticket is handled. See [Support ticket severity](#) for information about the different severities.

Contacting support for Bluemix Dedicated

If you are a Bluemix Dedicated customer, support is provided by the IBM Bluemix support team. However, because you might not have an IBM ID, you have a few different options for getting support.

Contacting support for Bluemix Local

If you are a Bluemix Local customer, support is provided by the IBM Bluemix support team. However, because you might not have an IBM ID, you have a few different options for getting support.

Support ticket severity

The following table lists some common examples of support issues and suggested severity levels. The examples are general guidelines for informational purposes only.

Severity	Examples
Severity 1	<ul style="list-style-type: none">• Your application is not accessible by your clients• Data corruption
Severity 2	<ul style="list-style-type: none">• Application errors that are impacting multiple users• Individual user cannot log in
Severity 3	<ul style="list-style-type: none">• General issues• Application errors or that are impacting individual users
Severity 4	<ul style="list-style-type: none">• Minor application issues• How to questions• Enhancements

Table 1. Severity examples

Severity 1 support tickets are monitored 24 hours a day, 7 days a week. Other tickets are processed during normal business hours, 7:00 am UTC to 1:00 am UTC on weekdays.

Collecting diagnostic information

To diagnose and resolve problems with Bluemix applications and services, the Bluemix Support team might ask you to collect diagnostic information.

Before you collect diagnostic information, complete the following steps:

1. Ensure that you have installed the latest cf command line interface. For more information, see [Installing the cf command line interface](#).
Note: If you do not have the latest cf command line interface installed, after the cf command line is connected to Bluemix, the `cf logs` command might not return output.
2. Ensure that you connected the cf command line interface to where Bluemix is running by using the `cf api` command.
3. Ensure that you meet all prerequisites in [Bluemix Prerequisites](#).

Use the following scripts to collect diagnostic information:

- For Windows operating systems, download the [bmdiag-general.bat](#) file and run it.
- For Linux and Mac operating systems, download the [bmdiag-general.sh](#) file and run it.

The scripts use the cf command line interface to extract the following information from your application environment:

- Application logs
- Application metadata
- Configured routes
- Events
- Provisioned services