



IBM Cloud

Power Virtual Server for SAP HANA - variation 'SAP ready PowerVS'

Reference architecture

Edition notices

This PDF was created on 2023-09-07 as a supplement to *Power Virtual Server for SAP HANA - variation 'SAP ready PowerVS'* in the IBM Cloud docs. It might not be a complete set of information or the latest version. For the latest information, see the IBM Cloud documentation at <https://cloud.ibm.com/docs?tab=solutions>.

© IBM Corp. 2023

Power Virtual Server for SAP HANA - variation 'SAP ready PowerVS'

The SAP ready PowerVS variation of the Power Virtual Server for SAP HANA creates a basic and expandable SAP system landscape. The variation builds on the foundation of the VPC landing zone and Power Virtual Server with VPC landing zone. PowerVS instances for SAP HANA, SAP NetWeaver, and optionally for shared SAP files are deployed and preconfigured for SAP installation.

Services such as DNS, NTP and NFS running in VPC and provided by Power Virtual Server with VPC landing zone are leveraged.

Redundant IBM Cloud® connections provide the network bridge between the IBM Power infrastructure and the IBM Cloud® VPC and public internet.

The resulting SAP landscape leverages the services such as Activity Tracker, Cloud Object Storage, Key Management from the VPC landing zone and the network connectivity configuration provided by Power Virtual Server with VPC landing zone.

Architecture diagram

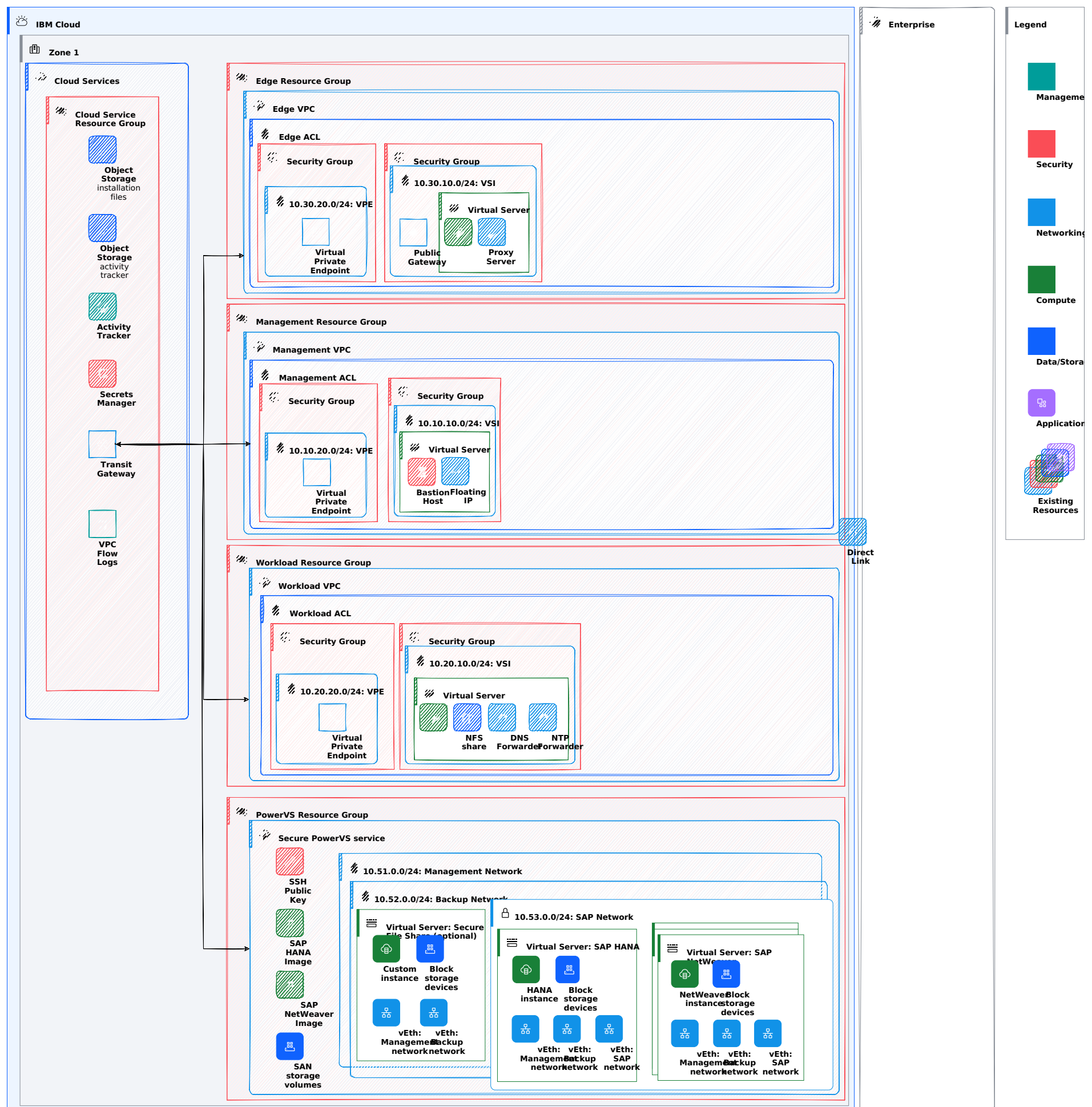


Figure 1. PowerVS instances prepared to run SAP in PowerVS workspace

Design requirements

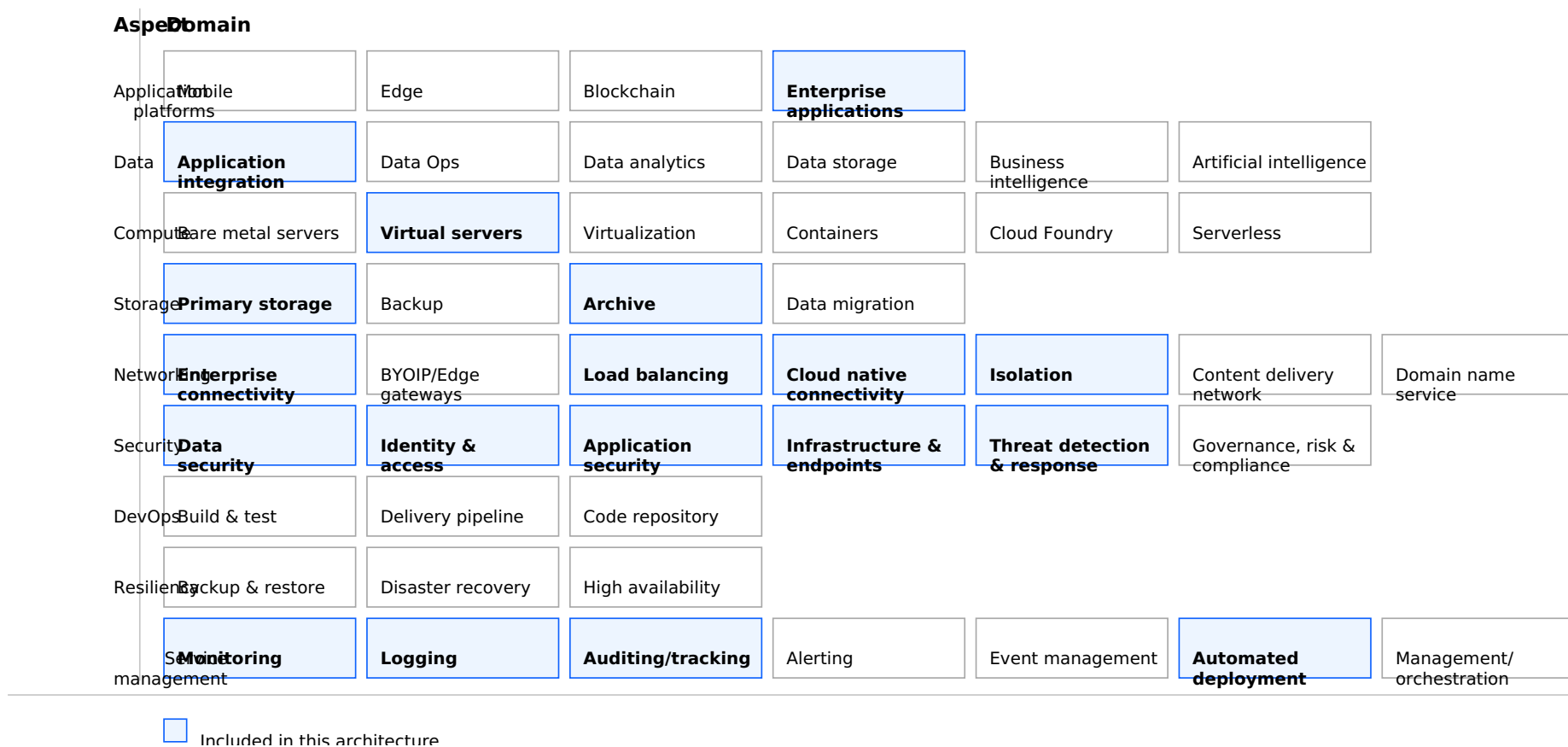


Figure 2. Scope of the solution requirements

IBM Cloud Power Virtual Servers (PowerVS) is a public cloud offering that lets an enterprise establish its own private IBM Power computing environment on shared public cloud infrastructure. Because of scalability and resiliency, PowerVS is the premium platform for SAP workloads in the cloud world. The reference architecture for 'Power Virtual Server for SAP HANA' - variation 'SAP ready PowerVS' is designed to provide PowerVS Linux instances prepared and configured for SAP HANA and SAP NetWeaver workloads according to the best practices and requirements using IBM Cloud® deployable architectures framework.

Components

PowerVS networks for SAP - architecture decisions

Requirement	Component	Choice	Alternative choice
<ul style="list-style-type: none"> Provide reliable network for communication between SAP HANA and SAP NetWeaver instances Ensure that SAP network meet SAP requirements related to throughput and latency 	SAP network	Create a separate SAP network for each SAP system. Tune SAP network in operating system according to SAP on Power best practices.	For very large SAP systems more than one SAP network may be needed.
<ul style="list-style-type: none"> Provide network for SAP system backups Ensure that backup network provides enough throughput 	Backup network	Attach backup network that was created with the PowerVS workspace in 'Power infrastructure for deployable architecture'	For large landscapes with several SAP systems more than one backup network may be needed.
Provide network for SAP system management	Management network	Attach management network that was created with the PowerVS workspace in 'Power infrastructure for deployable architecture'	

Table 1. PowerVS networks for SAP - architecture decisions

PowerVS instances for SAP - architecture decisions

Requirement	Component	Choice	Alternative choice
-------------	-----------	--------	--------------------

<ul style="list-style-type: none"> • Deploy PowerVS instance for SAP HANA workload • Use SAP certified configurations regarding CPU and memory combinations (t-shirt sizes) • Prepare operating system for SAP HANA workload 	PowerVS instance	<ul style="list-style-type: none"> • Allow customer to specify certified SAP configuration and calculate all additional parameters automatically • Attach all required storage filesystems based on PowerVS instance memory size • Attach networks for management, backup and for SAP system internal communication • Connect instance with infrastructure management services like DNS, NTP, NFS • Perform OS configuration for SAP HANA 	Allow customer to specify additional parameters, like non-standard file system sizes
<ul style="list-style-type: none"> • Deploy PowerVS instances for SAP NetWeaver workload • Prepare operating system for SAP NetWeaver workload 	PowerVS instance	<ul style="list-style-type: none"> • Allow customer to specify number of instances that must be deployed and CPU and memory for every instance • Attach all required storage filesystems • Attach networks for management, backup and for SAP system internal communication • Connect instance with infrastructure management services like DNS, NTP, NFS • Perform OS configuration for SAP NetWeaver 	Allow customer to specify additional parameters, like non-standard file system sizes
<ul style="list-style-type: none"> • Deploy PowerVS instance for hosting shared SAP system files • Prepare operating system 	PowerVS instance	Host shared SAP system files on one of PowerVS instances for SAP NetWeaver and do not deploy a separate PowerVS instance	<ul style="list-style-type: none"> • Allow customer to deploy PowerVS instance with specified CPU and memory • Attach specified storage filesystems • Attach networks for management, backup and for SAP system internal communication • Connect instance with infrastructure management services like DNS, NTP, NFS • Perform OS configuration • Allow customer to specify additional parameters, like non-standard file system sizes

Table 2. PowerVS workspace architecture decisions

Key and password management architecture decisions

Requirement	Component	Choice	Alternative choice
-------------	-----------	--------	--------------------

- Use public/private SSH key to access virtual server instances by using SSH
- Use SSH proxy to log in to all virtual server instances by using the bastion host
- Do not store private SSH keys on any virtual instances or on the bastion host
- Do not allow any other SSH login methods except the one with specified private and public SSH key pairs

Public SSH key - provided by customer. Private SSH key - provided by customer.

Ask customer to specify the keys. Accept the input as secure parameter or as reference to the key stored in IBM Cloud Secure Storage Manager. Do not print SSH keys in any log files. Do not persist private SSH key.

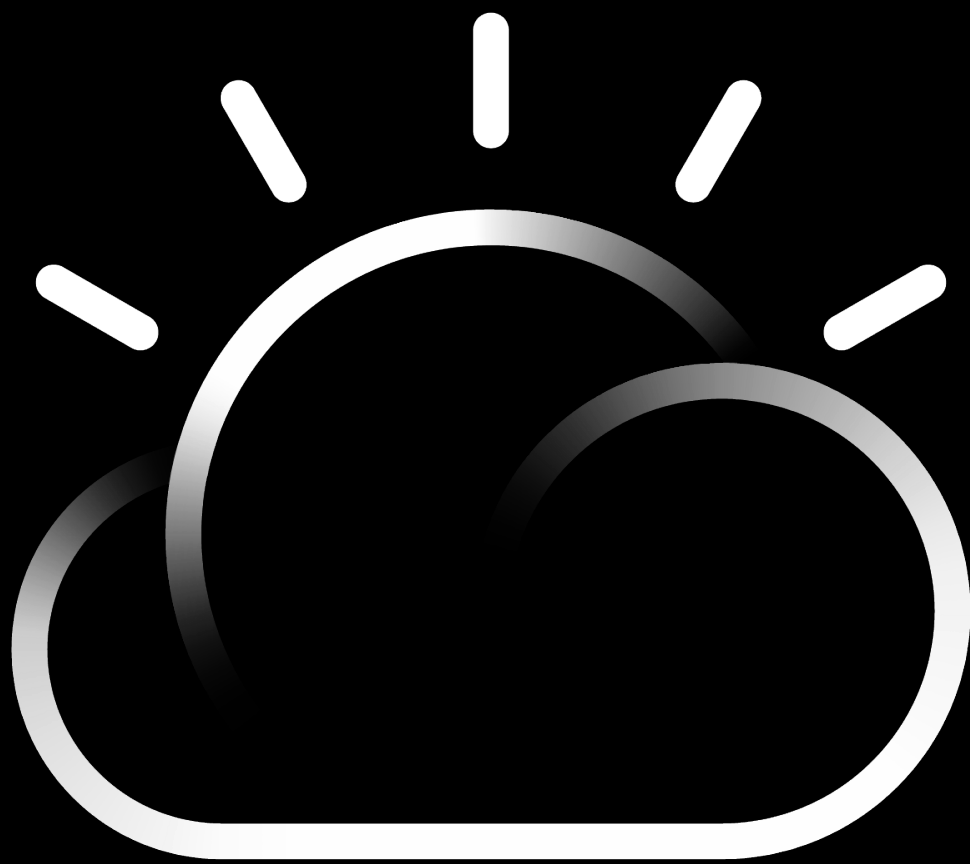
Table 3. Key and passwords management architecture decisions

Compliance

This deployable architecture is certified for SAP deployments.

Next steps

Install the SAP system.



IBM Cloud