**­­ Infrastructure Orchestration Assignment 2**

1. Write down the Infrastructure Components in detail.

* **Datacenter:**

To evolve their skill sets for cloud-based infrastructure, IT teams should familiarize themselves with new automation tools, such as Puppet and Chef, and work on their business skills for tasks such as service-level agreement negotiations and the creation of total cost-of-ownership models.

* **Servers and virtualization:**

Some organizations want the benefits of cloud computing, but they're hesitant to move workloads off premises or they want to continue to invest in on-premises hardware. Many times, these organizations turn to private cloud. To prepare for private cloud migration, IT teams first need to ensure their existing virtualized environments are cloud-ready. To do this, check your servers' processor, memory, and network support, and also ensure resiliency.

* **Storage:**

Before a cloud migration,IT teams must ensure existing storage architectures are ready for the move. Storage systems must be able to support elasticity so that cloud users can scale workloads up and down on demand. Teams might also need to assess new storage platforms that will support multi-tenancy, offer programmable APIs and allow for billing and chargeback.

* **Networking:**

An enterprise's network architecture has a major effect on cloud performance, especially in hybrid clouds where workloads must move between private and public cloud platforms. In these instances, organizations need a stable, reliable network. In some cases, it's best to move toward software-defined networking to optimize a cloud deployment. New management tools, including for the network, are a must for successful cloud adoption.

* **Cloud infrastructure management services:**

Admins must effectively monitor performance, security and other aspects of their infrastructure as a service deployment using new management frameworks. For private cloud, teams tend to use the management tools that are a direct extension of their [private cloud platform](https://searchservervirtualization.techtarget.com/tip/Evaluate-private-cloud-service-providers-in-the-market) usually, VMware vCloud or [OpenStack](https://www.techtarget.com/searchcloudcomputing/definition/OpenStack).

* **App dev and management tools:**

Organizations need to decide whether they want a public or private PaaS environment. While the public PaaS option eliminates the need for organizations to manage the underlying infrastructure, it can also create data residency and compliance concerns.

* **User applications and services:**

Cloud computing plays an important role, helping to deliver critical business data and applications to those devices. EFFS services allow users to upload files to the cloud and then share them with team members.

1. What is cloud infrastructure management. List out management services.

**Cloud Infrastructure Management:**

Manage your cloud infrastructure to ensure seamless processes and maintain the utmost security of your system through our infrastructure management services.

Over time, organizations across all major industries have been switching to cloud-based environments. Digitized infrastructures like Amazon Web Services, Microsoft Azure Cloud, and Google Cloud Platform are preferred by companies across the board to undertake their processes and attain their objectives.

**Cloud infrastructure management services:**

* Cloud infrastructure design and development
* Deployment automation
* Support and maintenance
* Infrastructure monitoring
* Security audits (DevSecOps)
* Container orchestration
* Data protection

1. What is deployment automation? Write best practices for deployment automation

Deployment automation refers to a software deployment approach that allows organizations to increase their velocity by automating build processes, testing, and deployment workflows for developers. In other words, it allows organizations to release new features faster and more frequently.

The deployment automation concept focuses on deploying software automatically to different environments, running checks against your software, and pushing the software build to production with limited or no human intervention.

**Three best practices for deployment automation:**

Here’s a shortlist of three essential best practices for deployment automation.

1. Continuous testing

Make sure to include automated testing in your deployment automation pipeline. You want to deliver software as fast as possible to your customers. Therefore, it’s critical to get testing feedback as soon as possible via automated tests.

Types of tests you can include:

* End-to-end (E2E) testing simulates users interacting with your application.
* Performance testing helps you to detect choke points or memory leaks.
* Exploratory testing is a random testing method to find unexpected behavior.

2. Configuration management for environment

It’s important to implement a version control system for storing and making changes against a configuration repository that stores environment-specific configurations letting your deployment automation tool pull in the required configuration per environment.

3. Monitoring and logging

Monitoring and logging tools can reveal a lot of data about your application’s health. A monitoring tool allows you to set alerts to detect issues with your application.

4. Write down Cloud Infrastructure Security audits (DevSecOps)

Cloudsecurity audits on cloud-based applications require a different approach compared to regular audits.

By default, third-party cloud-based infrastructures usually apply measures that cover certain aspects of security.

However, the large number of possible configurations available in the management consoles of these platforms open the door to vulnerabilities that can lead to a major breach of information.

Likewise, these applications are not free from problems related to incorrect programming practices due to business logic, inadequate management of authentication tokens and access policies, and injections that can affect the particularities of the elements that make up their particular architecture.

Concepts like IaaS, SaaS or PaaS are part of the standard language of a generation of applications that benefit from the capacity, power and scalability of third-party services such as AWS or Azure.

5. Write short note on:

1. Container Orchestration

Container orchestration automates the scheduling, deployment, networking, scaling, health monitoring, and management of containers. [Containers](https://www.capitalone.com/tech/cloud/what-is-a-container/) are complete applications; each one packaging the necessary application code, libraries, dependencies, and system tools to run on a variety of platforms and infrastructure

**Container orchestration benefits:**

* Scaling your applications and infrastructure easily
* Service discovery and container networking
* Improved governance and security controls
* Container health monitoring
* Load balancing of containers evenly among hosts

1. Cloud data protection

Cloud data protection is a set of practices that aim to secure data in a cloud environment. These practices apply to data regardless of where it is stored or how it is managed, whether internally or by third parties. Cloud data protection practices have become key aspects of data security as companies increase the amount of data stored in the cloud.

**Data Protection Challenges in the Cloud**

* Integrity—systems need to be designed to ensure that only authorized access is granted. Configurations should also ensure that permissions to modify or delete data are restricted to appropriate users.
* Locality—data regulations are applied by the physical location of data, where it is collected, and where it is used. In a distributed system, this can be difficult to determine and control. Systems should be designed in a way that clearly defines where data is located at all times.
* Confidentiality—data needs to be secured according to its confidentiality level. This requires properly restricting permissions and applying encryptions to restrict readability. Likewise, admin credentials and encryption keys need to be protected to ensure that these restrictions are maintained.
* Storage—cloud infrastructure is entirely controlled by the vendor. This means that companies must rely on vendors to ensure that physical infrastructures, networks, and data centers are secure.

1. Cloud Logging

Cloud logging is a practice that enables you to collect and correlate log data from cloud applications, services, and infrastructure. It is performed to help identify issues, measure performance, and optimize configurations.

Cloud logging relies on the creation of log files, collections of data that document events occurring in your systems. Log files can contain a wide variety of data, including requests, transactions, user information, and timestamps. The specific data that logs collect is dependent on how your components are configured.

When performing cloud logging, there are several types of logs you should collect. These include event logs, transaction logs, message logs, and audit logs. To make the collection and aggregation process easier, you can use log management tools to ingest, process, and correlate data.

1. Cloud Patching

**Patching**

Patches are updates released by software developers (of both operating systems and applications) as well as hardware manufacturers. A patch generally repairs existing bugs, security vulnerabilities, or puts preparations in place to prevent future ones.

A patch can also add new functionality but is often just called a new release or update. which can include bug fixes, changes, and new functionality.

**Cloud Patch Management**

Cloud Patch management is an infrastructure management activity where IT admins or operations managers must identify and prioritize patching needs, obtain and test these patches or fixes, and deploy them to update, improve, or repair existing code.

6. What is cloud asset management? Write down the benefits of the same.

**Cloud Asset Management:**

Cloud asset management provides visibility and control of all assets in the cloud infrastructure. Cloud Asset Management is a better optimized and secured cloud management process. It enables businesses to keep track of cloud assets while keeping cloud infrastructure running smoothly.

Cloud asset management focuses on managing the physical cloud environment such as the product/services that the company offers. It consists of components of cloud applications and manages them all. In this way, it allows businesses to observe all aspects of their cloud assets in areas such as management and compliance.

**Benefits of Cloud Asset Management**

* **Security:** One of the biggest advantages of cloud asset management is that it provides security. Cloud asset management fixes the security issue that may occur by hiding data encoding. Thus, the security of the data is ensured.
* **Time-Saving:** Businesses can easily track their assets thanks to asset management. Thus, companies do not need to spend time finding asset information.
* **Inventory Accuracy:** Another of the cloud asset management benefits is greater visibility into assets in the cloud environment. CAM collects all inventory information and makes conscious decisions about asset management. Inventory accuracy enables businesses to optimize based on secure data. That is why companies make improvements in the right areas. Moreover, CAM also prevents extra expenses thanks to the inventory information it collects. In this way, businesses save both time and cost.
* **Asset Data:** Asset information is important to increase asset efficiency. When businesses acquire asset information, they make transactions easily. In this way, companies track their assets in the cloud environment and make transactions at the right time.

7. What is service catalog management? Write Building a Services Catalog.

**Service Catalog Management:**

An optimum catalog is one that maximizes the alignment of infrastructure capabilities with business requirements while delivering the best value for the end consumer. The service catalog can be used as an effective tool by IT organizations to implement enterprise standards, introduce new technologies, and enforce default regulatory requirements. The enterprise architect is responsible for the service catalog’s alignment with the business architecture, thereby helping to maximize the return on investment in cloud and service catalog development.

**Building a Services Catalog:**

* Step 1: Understand Existing Services Assets

In this step, enterprise IT must list and categorize existing services within enterprise systems. These are typically easy to find since many enterprise systems already expose APIs, which are services. Also, include any data services, or even legacy systems services, that are critical to the enterprise business.

* Step 2: Understand Cloud Services Assets

As in step 1, here you perform the same activities for cloud-based services. This means compiling an inventory of services within private and public cloud resources, including APIs/services that manage storage, compute, resource provisioning, and business services.

* Step 3: Identify Required Types of Automation

The automation is a part of core governance systems that can be put in place to enforce pre-defined policies, or other procedures, in how the services should be provisioned, managed, and utilized, by end users or developers. There are two paths to consider here; first is resource governance, and the second is service governance.

* Step 4: Define Use of Automation

This is the step where you plan to automate the use of cloud services, including binding them into workflows or applications. The use of automation also covers the application of polices that define access to services, as well as track dependencies.

* Step 5: Establish Operations Planning

Operations planning should take the use of services and the services catalog into consideration. This means understanding and dealing with performance and access management issues, as well as having the ability to manage resources using provisioning capabilities to control which resources, including cloud services in the catalog, are provisioned and for what purpose.

* Step 6: Identity Candidate Services

The candidate services are all services identified within the problem domain (a specific area of focus in an enterprise, such as HR systems, inventory, etc.) that have the potential of becoming services. This deliverable is nothing more than a listing of services, and what each does.

* Step 7: Deploy Initial Services

Catalog Creating the initial services catalog means that we list of all the relevant services from the candidate services list and thus selected as services for our problem domain. Moreover, they are decomposed and ordered so all services that are dependent upon other services are understood, from the highest level to the lowest. Again, these services can be private or public cloud, or services found in traditional systems.

* Step 8: Test and Deploy

In this step we test the services catalog, as well as automation and operations, including the invocation of services and their ability to provide the expected behavior and information. We also test the services catalog’s ability to provide the right level of performance, utilization of resources, and its ability to support applied governance and operations polices using the automation capabilities of the catalog.

8. What is cloud Capacity Management? Write capacity management Lifecycle.

**Cloud Capacity Management**

Capacity management has been used for decades to optimize resources on-premises. Now, as cloud environments transform IT, this practice is being extended to enable holistic planning, management, and optimization of all your resources — both cloud and on-premises — in one place and at the same time.

Across both cloud and on-premises resources, capacity management informs forecasting and planning by helping you determine the capacity levels that you’ll notice across your environment, including compute configurations, storage, database, and network bandwidth, as well as the most cost-effective way to provision them.

**The Capacity Management Lifecycle**

**Step 1: Import Data**

Data is power: there’s not much you can do without it. A critical first step in capacity management is to import metrics for performance, capacity, and configuration, as well as business KPIs, for resources including:

* Physical/virtual/cloud infrastructure
* Databases
* Storage
* Networks
* Big data environments
* Facilities

**Step 2: Analyze Data**

Now that you have data, you also need visibility into your assets to understand what is actually going on. This brings us to the second step: data analysis.

Utilization analysis should be performed from several perspectives, as follows.

* **Visibility**: Visibility across your environment is the foundation of any capacity management process. Analyze your discovered data to gain insight into what assets you have, how they are configured, and where they are located.
* **Baselining**: Next, profile normal utilization profiles and baselines (this step requires machine learning). You’ll need to understand usage patterns over time and identify the types of cyclical behavior that exist in the organization and their causes. The longer the period of time you analyze and the more data you collect, the more accurate your baselining and profiling becomes. Ongoing data collection and analysis is the key to proper profiling and baselining.
* **Peak analysis**: Identify periodic behaviors and busiest periods. Understanding when changes in workloads occur is essential to efficient use — especially in the cloud, where you’re paying for resources on a daily, hourly, minute, or second-by-second basis. By understanding these behaviors, you can make better and more informed decisions on how to handle and resource applications to ensure performance without wasting resources.
* **Optimization**: Look for opportunities to optimize your use of resources. This may involve adapting the configuration of computing to changes in workloads such as adding memory or CPU. This requires automation to be done effectively; manual efforts are typically 30 days out of date and can’t hope to keep up with the pace of change in the modern enterprise.

**Step 3: Forecast Data**

Forecasting allows you to anticipate the impact of future configuration changes on utilization levels and flag anticipated saturation points before they impact performance.

To proactively identify storage capacity saturation:

* Identify when storage pools may run out of capacity.
* Quantify the additional capacity required to meet allocation requirements.
* Verify whether there are enough unused disks in your storage systems to extend existing storage pools.

This process makes it possible to avoid under-purchasing and meet both current and future storage requirements so that you can prevent downtime. At the same time, accurate sizing helps you avoid over-purchasing and wasted storage capacity.

**Step 4: Plan With Data**

Now that you understand projected organic growth on existing systems, applications, and business services, you’re ready for Step 4, which centers on planning for new projects, applications, and business services. This is often referred to as demand management or reservation-aware capacity management.

In this step, organizations focus on two questions:

1. Do I have enough capacity for these new projects?
2. How will these new projects affect the other applications and business services currently running?

**Step 5: Report With Data**

After data import, visibility, analysis, forecasting, planning, and modeling, the next step toward capacity management maturity is the ability to automatically generate reports and dashboards that can be distributed to stakeholders. These stakeholders can include personnel responsible only for individual technology silos, the health of the business, specific applications, or a cross-section of all of the above. As a result, it is important to automatically generate a variety of reports and views with different content for each stakeholder on a periodic basis. This can also include generating exception-based reports or showback reports.

9. What are cloud Operations? Write advantages and disadvantages.

**Cloud Operations (CloudOps)**

Known simply as “CloudOps”, Cloud Operations refer to a combination of activities that seek to optimize IT services, tools, workloads, and processes in the cloud. Typical tasks here cover things like device management, performance, security, network, compliance, and software development — for the sake of keeping the underlying [cloud infrastructure](https://www.cloudzero.com/blog/cloud-infrastructure) and its native applications running smoothly.

While the cloud is widely praised for its flexibility, cost-effectiveness, and high accessibility, migrating your applications won’t guarantee you these benefits. Ultimate efficacy here is only achieved when you additionally optimize the cloud-based processes.

Cloud Operations manage the cloud-based data and applications accordingly to keep them performing optimally for increased productivity.

**Benefits And Disadvantages Of CloudOps**

Pros of CloudOps

* **Improves service delivery** - Cloud Operations are great in automating and executing a host of essential system tasks. You can, for example, set the system to generate analytical reports, perform quality assurance tests, create builds, and maintain infrastructure provisioning. Combined, such processes are bound to not only boost IT productivity, but also enhance operational efficiency, as well as improve service delivery.
* **Maintains cloud availability**- By updating cloud applications, [scaling resources in real-time](https://www.cloudzero.com/blog/aws-auto-scaling), monitoring data transfer, automating request handling, and deploying cloud assets when required, CloudOps manages to maintain consistent availability of cloud services. Therefore, organizations should be able to run applications and processes remotely from anywhere at any time, without experiencing downtime or service outage.
* **Strengthens data security**- With data security being one of the core tasks of cloud operations, you get to seal potential vulnerabilities, encrypt data, conduct malware scans, patch applications, set up firewalls, as well as detect possible attacks. Another thing that comes with CloudOps is compliance management, which should help you keep the cloud processes within the confines of the law.
* **Facilitates disaster recovery** - In case you happen to lose data or experience system failure, you can count on CloudOps measures to restore everything. The tools here are automated to back up and recover all types of data from off-site servers, hence guaranteeing business continuity.

Cons of CloudOps

* **Potential budget overruns**- The problem with scaling cloud resources is, you might unknowingly end up overprovisioning yourself with idle assets and underutilized space. This would mean extra charges on your bill, which could add up quite astronomically ovetime.
* **Increased data security risks** - Although cloud platforms are gradually refining their data protection measures, you’ll still be susceptible to breaches and attacks. Cloud systems continue to attract all sorts of cyberattacks because their networks are remotely accessible.

10. Explain in detail the CMDB inventory?

A CMDB is a place to store data regarding your configurable items (CIs), also known as IT assets. But, CMDBs are no ordinary data repositories. They act as a centralised system that encompasses the entire IT environment. Enabling you to monitor, track, and manage your IT estate in one place.

In this guide, you’ll see how CMDBs play a significant role in IT management principles. Particularly your [IT asset management (ITAM)](https://comparesoft.com/it-assets-management-software/) and [IT service management (ITSM)](https://comparesoft.com/help-desk-software/itsm/) processes. As well as how they are designed to help you better understand the ties between your CIs.

A CMDB can play many parts in helping to improve your IT services. For instance, you can be more efficient in troubleshooting a network disruption affecting all workstations. Especially if you knew which routers and servers those machines are connected to. Or you can prevent a potential malware outbreak if you tracked the versions of each desktop’s operating system. In turn, determining which ones needed patching.

**How Does a Configuration Management Database Work?**

All configuration data and asset relationships have to be stored somewhere. In most cases, that ‘somewhere’ would be a CMDB. A CMDB information on:

* Assets, or CIs
* The relationships/dependencies of CIs and other related entities
* Other configuration data

Configurable items include hardware, software, documentation, facilities, and staff and vendors. CI relationships are associated with incidents, issues, changes, and deployments.

Before a CMDB can be of any use, it must be populated with data. This is usually carried out through a combination of manual and automated methods. Although data accuracy can’t be 100%, the aim is to achieve the highest level of accuracy possible. Otherwise, a CMDB’s purpose in life will never be realised.

To make a CMDB reliable, it’s necessary to involve the ‘owners’ of CIs. Both before and during the CMDB population process. These owners should review the data for accuracy, completeness, and consistency.

Once the CMDB has been populated, the challenge shifts into keeping the CMDB updated. Because an IT framework can easily consist of a million moving parts, that won’t be an easy task. This is due to configuration changes, new CIs, deprecated CIs, mergers, and acquisitions. However, it needs to be done for a CMDB to function the way it’s supposed to.