

VIRTUALIZATION - DIGITAL ASSIGNMENT 2

QUESTION 1: Identify at least 6 automation tools for datacentre and discuss one elaborately.

Datacentre automation tools are those by which routine workflows and processes of a datacentre such as scheduling, monitoring, maintenance, application delivery, and so on, can be managed and executed without human administration. Datacentre automation increases agility and operational efficiency. It reduces the time IT needs to perform routine tasks and enables them to deliver services on demand in a repeatable, automated manner. These services can then be rapidly consumed by end users.

Need for datacentre automation: The massive growth in data and the speed at which businesses operate today mean that manual monitoring, troubleshooting, and remediation is too slow to be effective and can put businesses at risk. Data centre automation is immensely valuable because it frees up human computational time and is able to:

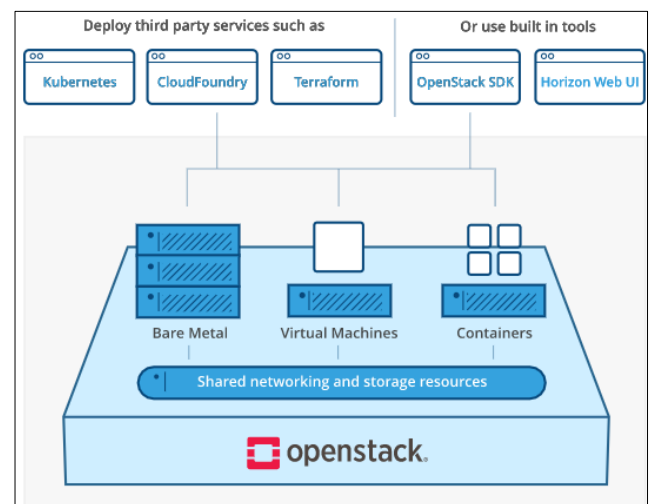
- Deliver insight into server nodes and configurations
- Automate routine procedures like patching, updating, and reporting
- Produce and programs all data centre scheduling and monitoring tasks
- Enforce data centre processes and controls in agreement with standards and policies

The 6 automation tools are as follows:

1. **Red Hat Ansible** - It is an automation platform for Red Hat Linux and more. Ansible Tower is a software framework that supports disciplines ranging from agile development to DevOps to continuous delivery.
2. **Microsoft Azure Automation** - Azure Automation delivers a cloud-based automation and configuration service providing consistent management across Azure and non-Azure environments. It consists of process automation, update management, and configuration features.
3. **Chef** - Chef is a suite of products that is open-source and commercial. Chef is written in Ruby and provides a framework in which users can write recipes. Those recipes can implement processes that span an entire infrastructure or focus on a single component.
4. **Puppet** - Puppet is a framework and language that systems operations professionals use to define operations like software deployment so that they can be automated. IT departments use Puppet to automate intricate processes involving many pieces of hardware and software.
5. **OpenStack** – explained in detail below
6. **IBM UrbanCode** - It enables continuous delivery for any combination of on-premises, cloud and mainframe applications by eliminating manual, error-prone processes. Thus it helps IT teams to maintain control of complex releases, and release software faster without sacrificing quality.

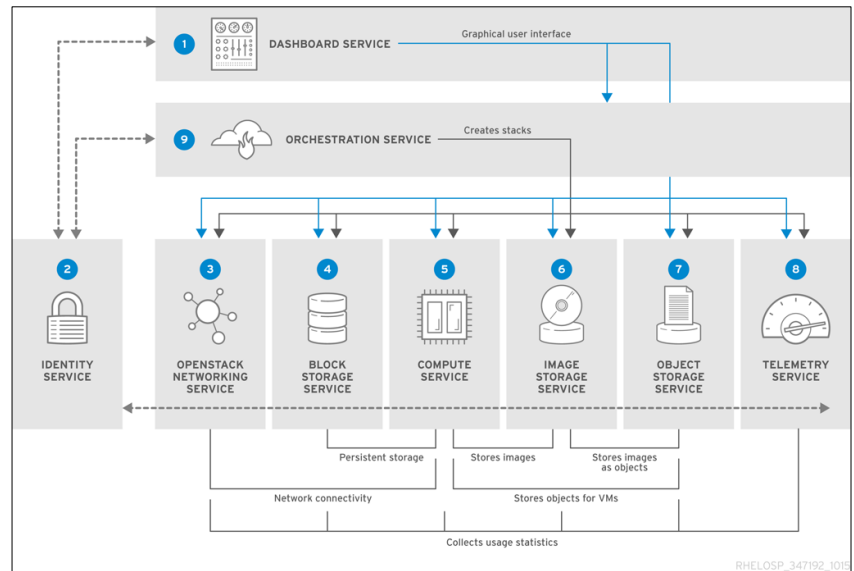
OpenStack – A tool for datacentre automation

OpenStack lets users deploy virtual machines and other instances that handle different tasks for managing a cloud environment on the fly. It makes horizontal scaling easy, which means that tasks that benefit from running concurrently can easily serve more or fewer users on the fly by just spinning up more instances. It controls large pools of compute, storage, and networking resources throughout a data centre, managed through a dashboard or through the OpenStack API. OpenStack is an operating system that helps build a cloud infrastructure or manage local resources as though they were a cloud. This means automating the building, teardown, and management of virtual servers and other virtualized infrastructure. It falls into the category of Infrastructure as a Service (IaaS). Providing infrastructure means that OpenStack makes it easy for users to quickly add new instance, upon which other cloud components can run.



OPENSTACK LOGICAL ARCHITECTURE:

OpenStack has a modular architecture and is made up of many moving parts. There are 9 modules that are a part of the "core" of OpenStack, which are distributed as a part of any OpenStack system and officially maintained by the OpenStack community.



1. **Nova** - primary computing engine behind OpenStack. It is used for deploying and managing large numbers of virtual machines and other instances to handle computing tasks.
2. **Swift** - storage system for objects and files. Rather than the traditional idea of referring to files by their location on a disk drive, developers can instead refer to a unique identifier referring to the file or piece of information and let OpenStack decide where to store this information. This makes scaling easy, as developers don't have the worry about the capacity on a single system behind the software.
3. **Cinder** - a block storage component. This more traditional way of accessing files might be important in scenarios in which data access speed is the most important consideration.
4. **Neutron** - provides the networking capability for OpenStack. It helps to ensure that each of the components of an OpenStack deployment can communicate with one another quickly and efficiently.
5. **Horizon** - dashboard behind OpenStack. Developers can access all of the components of OpenStack individually through an application programming interface (API), but the dashboard provides system administrators a look at what is going on in the cloud, and to manage it as needed.
6. **Keystone** - provides identity services for OpenStack. It is a central list of all users of the OpenStack cloud, mapped against all of the services provided by the cloud, which they have permission to use.
7. **Glance** - provides image services to OpenStack. Here, "images" refer to virtual copies of hard disks. Glance allows these images to be used as templates when deploying new virtual machine instances.
8. **Ceilometer** - provides telemetry services, which allow the cloud to provide billing services to individual users of the cloud.
9. **Heat** - the orchestration component of OpenStack, which allows developers to store the requirements of a cloud application in a file that defines what resources are necessary for that application. In this way, it helps to manage the infrastructure needed for a cloud service to run.

Advantages of using OpenStack

- Enables rapid innovation: Because developers can provision machines rapidly and on-demand, they can significantly reduce development and testing periods and have more freedom to experiment with new ideas.
- Boosts scalability and resource utilization: Although not as scalable as public clouds, OpenStack private clouds still offer a significant degree of scalability. You can still spin up and spin down servers on-demand.
- Eases regulatory compliance: Because OpenStack enables the construction of private, on-premise clouds, it can help in regulatory compliance endeavours. If your cloud is in your own data centre, you'll have more control of access privileges, security measures, and security policies.
- Devoid of vendor lock-in: OpenStack supports a variety of proprietary technologies and can operate in a smorgasbord of hypervisor and bare metal environments. Its ability to work with commodity hardware gives you more flexibility in choosing solutions based on a wider range of costs and competencies.

Disadvantages of using OpenStack

- Scarcity of talent, may take longer to implement: Because OpenStack involves a rather steep learning curve, it might take some time before your staff can fully implement what they learn.

QUESTION 2:

Discuss the need for monitoring in virtualization of Cloud provider's datacentre. Discuss the various tools available in market and its usefulness.

Need for monitoring resources in a Cloud's datacentre

Recent years have witnessed a boom in cloud services utilization. While traditional IT monitoring focused on monitoring servers and infrastructure, more and more organizations now comprehend the value of shifting some, or all of their operations into the cloud. However, there have been issues with cloud services utilization. One of them has been gaining a clear view of performance in cloud environments.

Cloud monitoring

It refers to the use of automated and manual tools to manage, monitoring and evaluating cloud computing architecture, infrastructure, and services. It incorporates an overall cloud management strategy allowing administrators to monitor the status of cloud-based resources. It also helps in identifying emerging defects and troubling patterns so that one can prevent minor issues from turning into major problems.

Tools available in the market

There are many cloud server monitoring services on the market today. Some of them are 'do-it-all' while others are specialized to monitor specific components of your workload at a time. Finding the 'best' or 'perfect fit' of cloud management and monitoring software for your operations among the available options can be a daunting task. With the right understanding of your needs, budget, and applications, you can make the right choice. The tools currently available are as follows:

CLOUD MONITORING TOOL	DESCRIPTION	PROS	CONS
AppDynamics APM	It is an Application Intelligence tool that delivers corporate and operational understanding into application performance and user experience.	<ol style="list-style-type: none"> 1. Gives visibility into application performance 2. Monitor corporate transactions in real time 3. Establish proactive alerting to discover problems 	<ol style="list-style-type: none"> 1. Supports only limited languages 2. Takes more time to set up 3. Training is required to understand the Dashboards
CA UIM	It delivers a single event management solution for IT Operation companies. The solution is seen to be tremendously extendable over scripting, auto workers, and activators.	<ol style="list-style-type: none"> 1. The web interface has great utility and purpose. 2. Distribution of probes and configuration packages uses drag and drop. 3. Easy to use and scalable. 	<ol style="list-style-type: none"> 1. Needs enhancements in inventory management. 2. Node management available is not very effective. 3. Requires more customization.
Amazon CloudWatch	It is a monitoring and management service made for developers, system operators, site reliability engineers, and IT managers.	<ol style="list-style-type: none"> 1. Can be used to set high-resolution alarms, visualize logs and metrics. 2. Can improve applications by troubleshooting issues and automatic activities. 3. Assimilates with AWS products. 	<ol style="list-style-type: none"> 1. Customization of dashboards needs to be enhanced 2. Alerts and alarms are assembled manually 3. Feature allowing transfer of alarms and alerts information is not present
Bitnami Stacksmith	Bitnami cloud tools support a group to accomplish and monitor AWS, Microsoft	<ol style="list-style-type: none"> 1. Gives freedom to install scripts as per requirements. 	<ol style="list-style-type: none"> 1. Pricing isn't very competitive.

	Azure and Google Cloud Platform.	<ol style="list-style-type: none"> Helps in installing several slacks on a single server. Good interface and fast installation. 	<ol style="list-style-type: none"> Non-Root based installations. No real advancement route from one version to the next.
Microsoft Cloud Monitoring (OMS)	These are cloud-based services for handling the on-premises and cloud settings from a single place. OMS components are completely introduced in Azure.	<ol style="list-style-type: none"> Alarms work well, and posts are quickly sent to mobile phones. Security reviewing dashboards are easy to deliver. Supports checking for malware as well Search query is easy, and no different language is required. 	<ol style="list-style-type: none"> Learning is required for beginners. More work is needed on security. Prior knowledge is needed to understand Log Analytics. When compared to other tools, it takes more time to load.
CloudMonix	Its live monitoring dashboard permits Azure Cloud admins to understand the cloud resources, get informed with signals on cautions and exclusions and organize automated restoration activities.	<ol style="list-style-type: none"> Monitors performance & accessibility Admins get notified for production issues Has capability for utomated recovery procedures 	<ol style="list-style-type: none"> Enterprise customers with several Azure Subscriptions, have to create different accounts to use this tool Some user interfaces are difficult to use

Best practices for cloud monitoring

- Decide what metrics are most critical:

There are many customizable cloud monitoring solutions. Take an inventory of the assets currently in use and map out the data that needs to be collected. This helps to make informed decisions about which cloud monitoring software best fits your needs. It also gives you an advantage when moving to implement a monitoring plan. For example, an application developer might want to know which features are used the most, or the least. As they update, they may scrap features that aren't popular in favour of features that are. Or, they may use application performance monitoring to make sure they have a good user experience.

- Automate the monitoring:

One compelling feature is scripting. Monitoring and reporting can be scripted to run automatically. Since cloud functions are virtual, it's easy to implement software monitoring into the fabric of the cloud application. Even logging and red-flag events can be automated to send a notice when problems are detected. For example, an email notification might be sent if unauthorized access is detected or if resource usage exceeds a threshold.

- Consider the security of cloud-based applications:

Many users believe that their data is less secure on a remote cloud server than on a local device. While it is true that data centres present a tempting target for hackers, they also have better resources. Modern data centres invest in top-tier security technology and personnel. This offers a significant advantage over end users. With that said, it's still crucial for cloud users to be mindful of cloud security.

While data centres offer protection for the hardware and infrastructure, it's important to exercise good end-user security habits. Proper data security protocols like two-factor authentication and strong firewalls are a good start. Monitoring can supplement that first line of defence by tracking usage within the virtual space. This helps detect vulnerabilities by reporting habits that might create security gaps. It also helps by recognizing unusual behaviour patterns, which can identify and resolve data breach.