Cloud Services, Virtualization, & Active Directory

Once you complete the items below turn in any documents, spreadsheets, or diagrams used to complete this goal.

Cloud Services

 What are the main cloud types?

• Describe each cloud service and provide the benefits of choosing one cloud service over another.

• List cloud service providers and some of the services each one provides.

Virtualization

 What is virtualization and how can it help an environment or company?

 What are some tools used to manage virtual systems and describe the difference in each one?

• Install a virtual desktop application on your system and setup an operating system inside of the virtual desktop application.

• Take screenshots of the working VM and provide details of the operating system you selected.

Active Directory

 What is Active Directory and how does it help a company?

• Research how to install Active Directory and create a document that shows the process of installing and configuring Active Directory.

• Create a document that shows how to add a computer to the newly created domain.

• List some services that Active Directory provides and how these services help manage an infrastructure.

Systems Administration

Cloud Types

**Public Cloud**

Connecting to a public cloud means using an internet connection to access computing resources hosted on data centers managed by a third-party cloud service provider, rather than owning and maintaining these resources on-premises. A shared public cloud has many organizations (or tenants) sharing the same infrastructure.

The largest cloud service providers with data centers that enable massive scaling are called hyperscalers. The big four hyperscalers, collectively referred to as MAAGs, are: Microsoft (Azure), Amazon (Amazon Web Services or AWS), Alibaba (Alicloud), and Google (Google Cloud). Other cloud providers include IBM and Oracle.

**Private Cloud**

This cloud model is great for organizations concerned about sharing resources on a public cloud. It is implemented on servers owned and maintained by the organization and accessed over the internet or through a private internal network.

A private cloud environment gives you complete control over data and security to meet specific regulatory and other compliance requirements (e.g., HIPAA for healthcare, GDPR, GxP for Pharma, etc.).

**Hybrid Cloud**

Many organizations use a combination of several cloud environments. This is referred to as a hybrid cloud approach. Hybrid cloud often includes a combination of public cloud and private cloud, frequently in combination with some on-premises infrastructure. To create a true hybrid cloud architecture, you must set up communication or orchestration between the various deployments.

Hybrid cloud eliminates reliance on any single cloud provider and allows for additional levels of flexibility in terms of capabilities, security compliance, etc.

In the past, choosing a hyperscaler meant picking public over private. This is no longer the case. To support regulatory, performance, and data gravity requirements, the hyperscalers are now offering private cloud carveouts in public environments. VMware on AWS (VMC), Azure VMware Services (AVS), and Google’s SAP, Oracle and Bare Metal solutions are good examples. Similarly, the hyperscalers have been working on private cloud extensions. This blurring of public and private under a hybrid cloud umbrella is likely to accelerate in the future. Over time, we will no longer see a delineation between "public" and "private" but instead, between "dedicated" and "shared."

**Multi-cloud**

A multi-cloud approach is a particular case of hybrid cloud in which an organization uses services from multiple public cloud providers.

Types of Services

**Software as a Service (SaaS)**

SaaS is the most used cloud application service and is becoming a dominant way for organizations to access software applications.

With SaaS, an organization accesses a specific software application hosted on a remote server and managed by a third-party provider. On a subscription basis, the application is accessed through a web browser, reducing the need for on-device software downloads or updates. Popular SaaS products include Salesforce, Workday, or Microsoft Office 365.

Businesses should use SaaS if they're looking to enable cloud system access quickly and easily with minimal database management, development and/or service provider interaction. SaaS is suitable for applications that require web and mobile access, short-term projects requiring quick collaboration, and startups that need to quickly launch ecommerce websites without server issues or software development.

**Platform as a Service (PaaS)**

PaaS is a popular choice for businesses who want to create unique applications without making major financial investments.

With PaaS, an organization accesses a pre-defined environment for software development that can be used to build, test, and run applications. This means that developers don't need to start from scratch when creating apps. PaaS allows the developer to focus on the creative side of software development, as opposed to tedious tasks such as writing extensive code or managing software updates or security patches. Examples of PaaS products include Google App Engine, web servers, and SQL servers.

**Infrastructure as a Service (IaaS)**

IaaS is the simplest option for businesses. With IaaS, an organization migrates its hardware—renting servers and data storage in the cloud rather than purchasing and maintaining its own infrastructure.

IaaS provides an organization with the same technologies and capabilities as a traditional data center, including full control over server instances. System administrators within the business are responsible for managing aspects such as databases, applications, runtime, security, etc., while the cloud provider manages the servers, hard drives, networking, storage, etc.

Your cloud migration strategy needs to consider the deployment model and service category.

Virtualization

**What is Virtualization**

Software called hypervisors separate the physical resources from the virtual environments—the things that need those resources. A hypervisor is software that creates and runs virtual machines (VMs). A hypervisor, sometimes called a virtual machine monitor (VMM), isolates the hypervisor operating system and resources from the virtual machines and enables the creation and management of those VMs. Hypervisors can sit on top of an operating system (like on a laptop) or be installed directly onto hardware (like a server), which is how most enterprises virtualize. Hypervisors take your physical resources and divide them up so that virtual environments can use them.

virtualization also provides other benefits. It can help with business continuity, improve productivity, lower server infrastructure costs. and complete data protection so companies can achieve continuous application availability and automated disaster recovery across physical sites. With virtualization, businesses can simplify backup and recovery of data and systems and increase responsiveness through improved efficiency and flexibility. These benefits allow IT to become a department that helps drive innovation. Virtualization also helps with disaster recovery by letting businesses repurpose existing servers for disaster recovery rather than needing to buy duplicate servers for rapid recovery

**How virtualization works**

Resources are partitioned as needed from the physical environment to the many virtual environments. Users interact with and run computations within the virtual environment (typically called a guest machine or virtual machine). The virtual machine functions as a single data file. And like any digital file, it can be moved from one computer to another, opened in either one, or be expected to work the same.

When the virtual environment is running and a user or program issues an instruction that requires additional resources from the physical environment, the hypervisor relays the request to the physical system and caches the changes—which all happens at close to native speed (particularly if the request is sent through an open-source hypervisor based on KVM, the Kernel-based Virtual Machine).

VM Manager Tools

**VM Monitor**

SolarWinds has produced a free software application that continuously monitors your virtual machine infrastructure, which includes VMWare vSphere and Microsoft Hyper-V compatibility, allowing you to manage your virtual environment effectively and from one singular location.

Some key features of this application include:

Low system utilization for components such as CPU and memory, network interfaces and VMWare resource usage

Built in thresholds ensure that your environment runs at industry best practice levels

Ensures that performance levels never degrade below acceptable levels

VM details are all easy to access and view, including VM state, name and what the guest OS is that is running on each VM

**SolarWinds Virtualization Manager**

SolarWinds has created an excellent tool that has been designed to optimize performance and reliability in your virtual environment and allows all v-Sphere and Hyper-V issues to be resolved quickly and easily. Some key features of this application include:

Performance recommendations and monitoring

Reduce downtime

Save time by fixing issues more quickly

Reduce resource utilization

Other features include capacity planning, active virtualization alerts, management dashboards, management actions, VM sprawl control, VM right-sizing, application stack integration, cloud infrastructure monitoring, dashboards, high availability and an enterprise command center.

**Site24x7 VMware Monitoring**

Site24x7 Infrastructure is a cloud-based monitoring platform that includes a monitoring and management system for all servers of the services that support user interfaces.

The services covered by Site24x7 Infrastructure include virtualizations implemented by the VMWare and Hyper-V hypervisors. As well as virtualizations, Site24x7 Infrastructure can monitor Docker activity and the Nutanix hyper-converged infrastructure system.

Some of the VM monitoring features of Site24x7 Infrastructure are:

Automatic discovery of virtualizations

Mapping of VMs to servers.

Identification of application dependencies that the VMs support

Tracing of system resources that support the virtualizations

Assistance with capacity planning to size virtualization servers and allocate VMs

Alerts when VM performance deteriorates

Virtual Desktop Application and Setup

**Oracle VM**

Oracle VM is a platform that provides a fully equipped environment with all the latest benefits of virtualization technology. Oracle VM enables you to deploy operating systems and application software within a supported virtualization environment. The following screenshot shows the VirtualBox with an operating system installed inside of the virtual desktop application. I have download the Oracle VM [here](https://www.oracle.com/virtualization/solutions/try-oracle-vm-virtualbox/?source=:ad:pas:go:dg:a_nas:71700000079711823-58700006707759348-p67668617668:RC_WWMK200609P00103C0001:&SC=:ad:pas:go:dg:a_nas::RC_WWMK200609P00103C0001:&gclid=CjwKCAjws8yUBhA1EiwAi_tpEYd5_t7mhP4xGjMb4my2nUgnSqOm7qHmhJ35Ouw59sQ52SNtPQ33yxoC1t4QAvD_BwE&gclsrc=aw.ds) and the operating system Ubuntu [here](https://ubuntu.com/download)

Graphical user interface, text, application

Description automatically generated

**Why Linux**

Computers running on Linux can technically continue to operate without rebooting and without any issues for years.

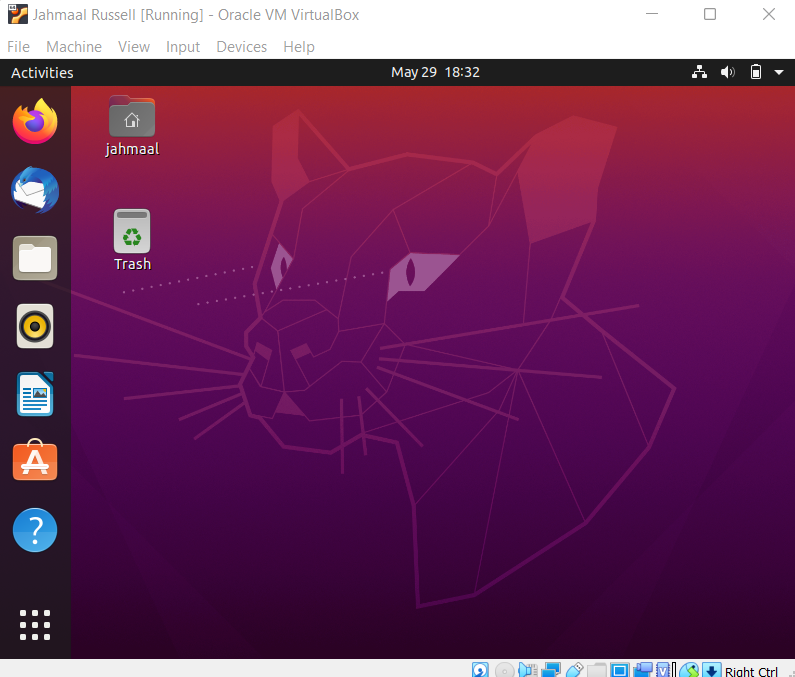
It is rare for a Linux system to freeze or slow down. Whereas with Windows, if you are running too many applications or have too many browsers open at one time, it is more common than not that your computer will freeze.

When it freezes, if you haven’t saved what you have been working on, you will lose it. The only way to unfreeze a system running on Windows is to manually stop the task that is causing the problem.

**Better Security**

Windows is vulnerable to many different types of viruses, malware, and trojans. Users who install Windows know that they also need to purchase and download antivirus programs to protect their computers.

The following screenshot shows what the Ubuntu desktop interface looks like once installed.



Active Directory

**What is Active Directory**

Active Directory (AD) is a database and set of services that connect users with the network resources they need to get their work done.

The database (or directory) contains critical information about your environment, including what users and computers there are and who’s allowed to do what. For example, the database might list 100 user accounts with details like each person’s job title, phone number and password. It will also record their permissions.

The services control much of the activity that goes on in your IT environment. They make sure each person is authenticated by checking the user ID and password they enter and allow them to access only the data they’re authorized to use.

Installing Active Directory

**Windows 10 Version 1809 and Higher**

1. Right-click the Start button and choose “Settings” > “Apps” > “Manage optional features” > “Add feature“.
2. Select “RSAT: Active Directory Domain Services and Lightweight Directory Tools“.
3. Select “Install“, then wait while Windows installs the feature. It should eventually appear as an option under “Start” > “Windows Administrative Tools“

**Windows 8 and Windows 10 Version 1803 or Lower**

1. Download and install one of the following depending on your version of Windows:
   * [Remote Server Administrator Tools For Windows 10](https://www.microsoft.com/en-us/download/confirmation.aspx?id=45520)
   * [Remote Server Administrator Tools For Windows 8](https://www.microsoft.com/en-us/download/details.aspx?id=28972)
   * [Remote Server Administrator Tools For Windows 8.1](https://www.microsoft.com/en-au/download/details.aspx?id=39296)
2. In Windows 8 and older versions of Windows 10, right-click the Start button and choose “Control Panel” > “Programs” > “Programs and Features” > “Turn Windows features on or off“.
3. Scroll down and expand the “Remote Server Administration Tools” section.
4. Expand “Role Administration Tools“.
5. Expand “AD DS and AD LDS Tools“.
6. Ensure that “AD DS Tools” is checked, then select “OK“.
7. You should have an option for “Administrative Tools” on the Start menu. From there, select any of the Active Directory tools. In newer versions of windows 10 (or at least mine), select the “Start” button then type “active directory”, and it should show up.

**To join a computer to a domain**

1. On the Start screen, type Control Panel, and then press ENTER.
2. Navigate to System and Security, and then click System.
3. Under Computer name, domain, and workgroup settings, click Change settings.
4. On the Computer Name tab, click Change.
5. Under Member of, click Domain, type the name of the domain that you wish this computer to join, and then click OK.
6. Click OK, and then restart the computer.

**What Services are Provided in Active Directory Domain Services?**

Here are the services that AD DS provides as the core functionality required by a centralized user management system.

* **Domain Services**: Stores data and manages communications between the users and the DC. This is the primary functionality of AD DS.
* **Certificate Services**: Allows your DC to serve digital certificates, signatures, and public key cryptography.
* **Lightweight Directory Services**: Supports LDAP for cross platform domain services, like any Linux computers in your network.
* **Directory Federation Services**: Provides SSO authentication for multiple applications in the same session, so users don’t have to keep providing the same credentials.
* **Rights Management**: Controls information rights and data access policies. For example, Rights Management determines if you can access a folder or send an email.

Benefits of Active Directory

**A Better Representation of the Network**

The Active Directory structure provides a clear picture of the network. Active Directory allows admins to centrally manage users and authorizations, regardless of the size of the network. A centralized approach to management is one of the most important reasons to implement Active Directory.

**Centralized Policy-Based Management**

Centralized policy-based management is another benefit of Active Directory. This feature helps manage and improve the security settings of workstations from a single point. This means admins can monitor, control, and manage the security settings of all the network resources from a single point.

**Improved Scalability with Organization**

Active Directory uses the concept of organizational units (OUs) to improve scalability in large organizations. An OU can be defined as a collection of users and computers. When companies have large domains, they can be organized into OUs. For example, a company has a huge HR department and there is an admin managing the entire domain. The company can create an OU named HR, and all the user accounts and computers related to HR can be moved to it. The admin who is responsible for this OU can be given certain administrative rights limited to this OU.