CHAPTER 1

INTRODUCTION:

Setting up a hybrid cloud platform in a small scale will help to manage and compute the data scrapes everywhere. But network security should be managed properly to maintain privacy as cloud computing technology continues to grow at a rapid pace. It introduces even more vulnerabilities. Even in personal and home cloud this will be a much bigger problem without network security. So, we building a data sharing hybrid cloud in a home network. And developing the Azure cloud firewall-based firewall and network managing system. In the realm of modern IT infra-structure, the hybrid cloud model has emerged as a powerful solution, combining the benefits of public and private clouds. However, with this hybrid environment comes the crucial challenge of managing securing network traffic effectively. This is where firewall and network management play pivotal roles. Firewall serves as gatekeepers of networks security, monitoring and controlling incoming and outgoing traffic based on predetermined security rules. In a hybrid cloud setup, firewalls act as the first line of defences, safeguarding the interconnected systems across both onpremises and cloud environments. Network management within a hybrid cloud environment involves overseeing the connectivity, performance, and availability or resources distributed across various cloud and on-premises infrastructure. It entails tasks such as configuring network settings, optimizing traffic flow, and troubleshooting connectivity issues. This introduction sets the stage for exploring the intricate dance between firewall security and network management in the dynamic landscape of hybrid cloud computing, highlighting the critical importance of both elements in ensuring the integrity and resilience of modern IT architecture.

CONCEPT:

As we build a small scale of data sharing cloud platform in home and we using the AZURE to deploying the Arc managed server hybrid cloud to manage files and secure the public cloud side of the hybrid cloud. It should be made up of low cost and it also very scalability device because of its usage may makes portability, deploying a cloud platform on premise by using Hyper-V for object storage. It could be migrating the servers and network between private and public clouds, so it's can make to maintaining the security and firewall management of the hybrid cloud platform. we can configure the firewall with cloud native firewalls in the open cloud on we can implement this SDN. (software defined network) The approach of the firewall management on the home cloud based on SASE, it could provide real time network management. we using Hyper -V for the on-premise object storage, it includes the flexibility and enhance the security, reliability and scalability of the network. However, we can configure firewall in Azure and the same way we can configure VMs in Hyper-V. the newer

Azure firewall implantation provide a much more granular service. It consists of two policies are an inbound policy and an outbound policy. We should provide an easy implementation method of the hybrid cloud structure for the home automation and data centres. This method can be upgrade and utilised as per scale of parameters and hardware. so, this is the focused concept of fire wall and network management in hybrid cloud platform.

APPLICATION:

As we setting up a hybrid cloud platform in a small scale in home, it will help to manage properly to maintain privacy. As cloud computing technology continues to grow at rapid pace, it introduced even more vulnerability. The Azure is the very flexibility to use the computation of the data structure instead the data transmutation on the public cloud to private cloud of the hybrid cloud platform. It is cost effective because other service-based company should provide the high cost and limited resources so, AWS makes different in market to launch service based with quality assurance succeed, it's also scalability and high potential of performance. The Hyper-V for on premise object storage, it is very comfortable with Azure to form a hybrid cloud. It can be performed with more security and flexibility with in house control, it enhances the reliability and scalability of the running software Windows server/pro for on-premise. so, the security of the network can't be attack to hack because it has more data breached to be modified as the network of the firewall managing operator for the home data sharing hybrid cloud.

CHALLENGES:

Managing firewall and network configurations in a hybrid cloud environment presents several challenges.

These include:

- COMPLEXITY:
    - Hybrid clouds involve a mix of on-premises, private cloud, and public cloud environments, leading to complex networking architectures. Coordinating and managing firewall rules across these diverse environments can be challenging.

- CONSISTENCY:
    - Ensuring consistent firewall policies across different cloud environments and on-premises infrastructure is difficult due to differences in tools, APIs, and capabilities.

- VISBILITY:
    - Limited visibility into network traffic and security events across the hybrid environment can make it challenging to detect and respond to threats effectively.
- SCALABILITY:
    - Managing firewall and network configurations at scale in a hybrid environment requires robust automation and orchestration capabilities to handle dynamic workloads and changing traffic patterns.
- COMPLIANCE:
    - Meeting regulatory compliance requirements across multiple cloud environments while maintaining consistent security policies adds complexity to firewall and network management.

INTEGRATION:

Integrating disparate network and security tools across hybrid environments to provide centralized management and monitoring can be challenging due to compatibility issues and differing configurations. Addressing these challenges often requires a combination of advanced automation, centralized management tools, and collaboration between network and security teams to ensure consistent and effective security across the hybrid cloud environment.

PUBLIC CLOUD:

A public cloud is a type of cloud computing service offered by third-party providers over the public internet. It allows users to access computing resources like virtual machines, storage, and applications on a shared infrastructure. Users can scale resource up or down as needed and only pay for what they use. It allows users to access resources such as virtual machines and applications on a pay-as-go basis providing scalability and flexibility without the need of invest in and maintain physical infrastructure public clouds are typically owned and operated by companies like amazon web services (AWS), Microsoft azure, google cloud platform (GCP).

- ACCESSBILITY:

Public cloud services are accessible to anyone with an internet connection. Users can access these services from anywhere in the world, using a variety of devices such as computers, smartphones, or tablets. Shared Infrastructure: In a public cloud, the underlying infrastructure, including servers, storage, and networking components, is shared among multiple users or "tenants." This multi-tenant model allows cloud providers to achieve economies of scale and offer services at lower costs.

- SCALABILTY:

Public clouds offer scalability, allowing users to easily scale their computing resources up or down based on demand. This means users can quickly provision additional resources during peak periods and release them when they are no longer needed, paying only for the resources they consume.

- MANAGED SERVICES:

Public cloud providers offer a wide range of managed services and tools to simplify the deployment, management, and monitoring of applications and infrastructure. These services include compute instances, storage solutions, databases, machine learning, analytics, security, and more. Users can leverage these services to build, deploy, and scale applications without having to manage the underlying infrastructure.

- GLOBAL PRESENCE:

Public cloud providers operate data centres in multiple regions around the world, allowing users to deploy applications and services closer to their end-users for better performance and lower latency. This global presence also enhances the resilience and reliability of cloud services, as data and applications can be replicated across multiple geographic locations.

- SECURITY AND COMPLIANCE:

Public cloud providers implement robust security measures to protect customer data and infrastructure. They offer a range of security features, including encryption, identity and access management, network security, and compliance certifications to meet regulatory requirements in various industries.

- SERVICE-LEVEL AGREEMENTS (SLAs):

Public cloud providers typically offer SLAs that define the level of service, uptime guarantees, and support commitments. These SLAs provide assurance to customers regarding the reliability and availability of cloud services and outline the provider’s responsibilities in

case of service disruptions or outages. Overall, public clouds offer organizations a cost-effective, flexible, and scalable solution for hosting applications, storing data, and running workloads in a highly available and secure environment. They have become increasingly popular for a wide range of use cases, including web hosting, e-commerce, software development, big data analytics, artificial intelligence, and more. And security tools across hybrid environments to provide centralized management and monitoring can be challenging due to compatibility issues and differing configurations. Addressing these challenges often requires a combination of advanced automation, centralized management tools, and collaboration between network and security teams to ensure consistent and effective security across the hybrid cloud environment.

PRIVATE CLOUD:

A private cloud refers to a computing environment dedicated solely to one organization, whether it's a business, government agency, or educational institution. Unlike public clouds, which are shared by multiple organizations, a private cloud is exclusive to the entity that owns it. Here are some key aspects to consider when discussing private clouds:

- INFRASTRUCTURE:

A private cloud can be hosted on-premises, meaning it's built and managed within the organization's own data centres, or it can be hosted off-premises by a third-party provider, often referred to as a managed private cloud. The infrastructure typically includes servers, storage, networking equipment, and virtualization software.

- CONTROL AND CUSTOMIZATION:

One of the primary advantages of a private cloud is the level of control it offers. Organizations have full control over the infrastructure, allowing them to customize it to meet their specific security, compliance, and performance requirements. This control is particularly important for industries with strict regulatory requirements, such as healthcare and finance.

- SECURITY AND COMPLIANCE:

Security is a major concern for organizations when it comes to cloud computing. With a private cloud, organizations can implement their own security measures and policies to protect sensitive data. This level of control is especially important for industries handling sensitive information, such as personal health records or financial data. Additionally, private clouds can help organizations comply with industry regulations and data privacy laws.

- SCALABILITY:

  While private clouds offer scalability similar to public clouds, the process of scaling up or down may be more complex and time-consuming due to the need to provision additional resources within the organization's infrastructure. However, this also means that organizations have more predictable performance and can better anticipate and manage resource demands.

- COST:

  Building and maintaining a private cloud can be expensive, requiring significant upfront investment in infrastructure and ongoing operational costs for maintenance and management. However, for organizations with consistent and predictable workloads or stringent security and compliance requirements, the benefits of a private cloud may outweigh the costs.

HYBRID CLOUD:

A hybrid cloud combines these two models, allowing organization to leverage the benefits of both public and private clouds. This means that certain workloads and data can be stored and processed in the private cloud, while others can utilize the resources of the public cloud. The hybrid approach provides flexibility, scalability and cost effectiveness. Key components of a hybrid cloud environment include:

•ORCHESTRATION AND MANAGEMENT:

To effectively manage resources across both public and private clouds, organizations use orchestration tools and management platforms. These tools automate tasks such as workload deployment, scaling and monitoring.

• CONNECTIVITY:

A robust network infrastructure is essential for seamless communication between the public and private cloud environments. This often involves establishing secure connections, such as VPNs or direct network links, to ensure data can be transferred efficiently and securely.

• DATA INTEGRATION AND INTEROPERABILITY:

Hybrid clouds require effective data integration and interoperability solutions to enable seamless movement of data between public and private cloud environment This may involve using APIs, middleware, or data integration platforms to ensure compatibility and consistency Overall, a hybrid cloud strategy enables organizations to leverage the strengths of both public and private clouds allowing them to achieve their specific business objectives while addressing requirements for security, compliance scalability, and flexibility.

CHAPTER 2

COMPONENTS:

As per the hybrid cloud, the tools and service for software components we use here are Hyper V, the Azure arc, Azure firewall with its virtual networks, windows pro, windows server (Hyper V works only in this platform) and the hardware components are PC with specifications of 16-gb RAM, storage of 60-gb, four core processor. Hybrid cloud requires robust networking solutions to ensure secure communication between on-premises infrastructure and cloud services. These software components are most basic aspect for hybrid cloud, the third-party services such as Azure, where resources are shared among multiple organizations. It provides customizations options. These components are integrated and managed in way that allows data and applications to be shared between them seamlessly, providing the benefits of both private and public clouds. Additionally, hybrid clouds often involve networking, security, and management solutions to ensure smooth operations across the different environments.

2.1 Hyper – V:

Hyper-V is a hypervisor-based virtualization platform developed by Microsoft. It allows you to create and manage virtual machines (VMs) on Windows-based systems. Here's a detailed explanations of its key features and functionality. Hyper-V specifically provides hardware virtualization. That means each virtual machine runs on virtual hardware. Hyper-V lets you create virtual hard drives, virtual switches, and a number of other virtual devices all of which can be added to the virtual machines.

Virtualizations allows you to run software that requires an older version of or non-windows operating systems. Experiments with other operating systems. Hyper-V makes it very easy to create and remove different operating systems. Test software on multiple operating systems using multiple virtual machines. With Hyper-V you can run them all on a single desktop or laptop computer. These virtual machines can be exported and then imported into any other Hyper-V system, including Azure.

2.2 SYSTEM REQUIREMENTS:

Hyper-V is available on 64-bit versions of windows 10 pro, Enterprise, and Education is not available on the home edition upgrade from windows 10 pro by opening settings > Update and security > Activation. Here you can visit the store and purchase an upgrade.

For more information about Hyper-V's system requirements and how to verify that Hyper-V runs on your machine, see the Hyper-V Requirements Reference. Operating systems you can run in a virtual machine. Hyper-V on Windows supports many different operating systems in a virtual

machine including various releases of Linux, FreeBSD, and Windows. As a reminder, you'll need to have a valid license for any operating systems you use in the VMs. For information about which operating systems are supported as guests in Hyper-V on Windows, see Supported Windows Guest

Hyper-V features only available on Windows Server:

- Live migration of virtual machines from one host to another
- Hyper-V Replica
- Virtual Fibber Channel
- SR-IOV networking
- Shared VHDX

Hyper-V features only available on Windows 10:

- Quick Create and the VM Gallery
- Default network (NAT switch)
- The memory management model is different for Hyper-V on Windows.
- On a server, Hyper-V memory is managed with the assumption that only the virtual machines are running on the server. In Hyper-V on Windows, memory is managed with the expectation that most client machines are running software on host in addition to running virtual machines.

Limitations:

Programs that depend on specific hardware will not work well in a virtual machine. For example, games or applications that require processing with GPUs might not work well. Also, applications relying on sub-10ms timers such as live music mixing applications or high precision times could have issues running in a virtual machine. In addition, if you have Hyper-V enabled, those latency-sensitive, high precision applications may also have issues running in the host. This is because with virtualization enabled, the host OS also runs on top of the Hyper-V virtualization layer, just as guest operating systems do. However, unlike guests, the host OS is special in that it has direct access to all the hardware, which means that applications with special hardware requirements can still run without issues in the host OS. Next

let’s see about configurations in Hyper-V:

- Hypervisor
- Virtual machines
- Hardware support
- Scalability

CHAPTER 3

VIRTUAL MACHINES:

A virtual machine, commonly shortened to just VM, is no different than any other physical computer like a laptop, smart phone, or server. It has a CPU, memory, disks to store your files, and can connect to the internet if needed. While the parts that make up your computer (called hardware) are physical and tangible, VMs are often thought of as virtual computers or software-defined computers within physical servers, existing only as code.

3.1 WORKING

Virtualization is the process of creating a software-based, or "virtual" version of a computer, with dedicated amounts of CPU, memory, and storage that are "borrowed" from a physical host computer such as your personal computer and/or a remote server such as a server in a cloud provider's data centre . A virtual machine is a computer file, typically called an image, that behaves like an actual computer. It can run in a window as a separate computing environment, often to run a different operating system or even to function as the user's entire computer experience as is common on many people's work computers. The virtual machine is partitioned from the rest of the system, meaning that the software inside a VM can't interfere with the host computer's primary operating system.

What are VMs used for?

Here are a few ways virtual machines are used:

Building and deploying apps to the cloud. Trying out a new operating system (OS), including beta releases. Spinning up a new environment to make it simpler and quicker for developers to run dev-test scenarios. Backing up your existing OS. Accessing virus-infected data or running an old application by installing an older OS. Running software or apps on operating systems that they weren't originally intended for. What are the benefits of using VMs? While virtual machines run like individual computers with individual operating systems and applications, they have the advantage of remaining completely independent of one another and the physical host machine. A piece of software called a hypervisor, or virtual machine manager, lets you run different operating systems on different virtual machines at the same time. This makes it possible to run Linux VMs, for example, on a Windows OS, or to run an earlier version of Windows on more current Windows OS. And, because VMs are independent of each other, they're also extremely portable. You can move a VM on a hypervisor to another hypervisor on a completely different machine almost instantaneously. Because of their flexibility and portability, virtual machines provide many benefits, such as:

Cost savings running multiple virtual environments from one piece of infrastructure means that you can drastically reduce your physical infrastructure footprint. This boosts your bottom line decreasing the need to maintain nearly as many servers and saving on maintenance costs and

electricity. Agility and speed Spinning up a VM is relatively easy and quick and is much simpler than provisioning an entire new environment for your developers. Virtualization makes the process of running dev-test scenarios a lot quicker. Lowered down time VMs are so portable and easy to move from one hypervisor to another on a different machine this means that they are a great solution for backup, in the event the host goes down unexpectedly. Scalability VMs allow you to more easily scale your apps by adding more physical or virtual servers to distribute the workload across multiple VMs. As a result, you can increase the availability and performance of your apps.

Security benefits Because virtual machines run in multiple operating systems, using a guest operating system on a VM allows you to run apps of questionable security and protects your host operating system. VMs also allow for better security forensics, and are often used to safely study computer viruses, isolating the viruses to avoid risking their host computer.

3.2 HYPERVISOR:

Requests for processing power, memory, storage, and other resources to the host machine in several ways, including API calls. An API is a software communication method that allows different applications to exchange data.

types of hypervisors:

There are two types of hypervisors, each differing in architecture and performance.

a. Type 1 hypervisor:

The type 1 hypervisor sits on top of the metal server and has direct access to the hardware resources. Because of this, the type 1 hypervisor is also known as a bare-metal hypervisor. The host machine does not have an operating system installed in a bare-metal hypervisor setup. Instead, the hypervisor software acts as a lightweight operating system.

Pros and cons:

Due to its architecture, the type 1 hypervisor is very efficient. It can directly manage and allocate resources for multiple virtual machines without going through the host operating system. These types of hypervisors are also more secure, as the absence of a host operating system reduces the risks of instability.

b. Type 2 hypervisor:

The type 2 hypervisor is a hypervisor program installed on a host operating system. It is also known as a hosted or embedded hypervisor. Like other software applications, hosted hypervisors do not have complete control of the computer resources. Instead, the system administrator allocates the resources for the hosted hypervisor, which it distributes to the virtual machines.

Pros and cons:

The presence of the host operating system introduces latency to the virtualized environment. When the virtual machine requests computing resources, the hypervisor cannot directly access the underlying hardware but relays the request to the host operating system. Also, the hypervisor and its hosted virtual machines are dependent on the stability of the host operating system.

C. Type 1 hypervisors compared to type 2 hypervisors:

Despite their differences, both types of hypervisors are helpful in different applications. For example, enterprise cloud data centers use type 1 or bare-metal hypervisors because of their efficiency, scalability, and flexibility when allocating resources to virtual machines. Also, a type 1 hypervisor is generally more secure and stable because it does not run on top of another operating system.

Conversely, administrators use type 2 hypervisors because they are more user-friendly. Type 2 hypervisors are easier to install, configure, and use than bare-metal hypervisors. It is similar to installing and using other desktop applications.

cloud hypervisor:

A cloud hypervisor consists of virtualization technologies that abstract the physical hardware resources of a cloud providers data centre. They allow organizations to run distributed workloads on the cloud architecture. It allows multi-tenant cloud environments, where individual users or businesses can run workloads or store data in a logically independent compartment.

Cloud providers usually use bare-metal hypervisors to allocate virtualized hardware resources to users. For example, Azure allows organizations to scale their cloud computing capacities with Xen-based hypervisors. It provides a cost-effective cloud solution where businesses only pay for the compute resources needed to run their Azure workload.

difference between hypervisors and containers:

A container is a software package that stores all the necessary files and configurations to run an application on any operating system. Developers use containers to reduce software development complexities and improve efficiency when deploying the applications. A containerized application can run on a public, hybrid, or on-premises cloud with consistent performance because it is independent of the underlying operating system.

Both hypervisors and containers provide virtualization but at a different software layer. A hypervisor abstracts the hardware from the software environment. In contrast, a container runs in an environment where a container engine abstracts the operating system.

security considerations for hypervisors:

Software programs on a virtual machine do not interfere with applications on other guest operating systems, which provides a degree of security. However, the virtualized environment relies on the hypervisor for a robust security posture. Any issues affecting the hypervisor will

impact all virtual machines running on top of it. So, its essential to use a hypervisor with built-in safeguard measures to secure the workloads integrity.

3.3 STORAGE ALLOCATION:

Before you can allocate provisioned storage to hosts and cluster, it should be discovered and classified in the VMM fabric:

- Discover and classify storage:

  Add and classify block storage devices. Learn about classification.

  Add file storage. Allocate block storage to host groups. You can allocate an entire storage pool or a specific logical unit (LUN). Ensure that you've completed these steps before you allocate storage to hosts:

- MPIO:

  If you're using fiber channel or iSCSI storage, the Multipath I/O (MPIO) feature must be enabled on each host.

  If MPIO is already enabled before you add the host, VMM will automatically enable it for supported storage arrays using Microsoft DSM. If you've vendor-specific DSMs, these will be used. If you add a host to VMM and enable MPIO later, you need to configure it manually to add the discover device hardware IDs.

- HBA and zoning:

  If you're using Fiber Channel storage array network (SAN), each host must have a host bus adapter (HBA) installed and zoning must be correctly configured.

- iSCSI:

  If you're using an iSCSI SAN, ensure that iSCSI portals have been added, and that the iSCSI initiator is logged into the array. Ensure that the Microsoft iSCSI Initiator Service on each host is started and set to Automatic.

- Storage group:

  Explain to your storage administrator how VMM manages storage. In VMM, a storage group binds together host initiators, target ports, and logical units. A storage group contains one or more host initiator IDs (IQN or WWN) (WWN). A storage group also contains one

or more target ports and one or more logical units. Logical units are exposed to the host initiators through the target ports.

By default, when VMM manages the assignment of logical units, VMM creates one storage group per host, either a standalone host or a host cluster node. For some storage arrays, it's preferable to use one storage group for the entire cluster, where host initiators for all cluster nodes are contained in a single storage group. To do this, you need to set the Create Storage Groups Per Cluster property to $true by using the Set-SC Storage Array cmdlet.

3.4 ALLOCATING:

You can allocate file storage directly to hosts and clusters. You can add LUNs to hosts and clusters. If you already provisioned LUNs on a host group, you can assign these to hosts and clusters. If you provisioned a storage pool on a host group, you can create LUNs during the procedure to add storage to a cluster. If you want to use shared storage that isn't managed by VMM, the storage disks must be available to all hosts or nodes before you can add them. You need to provision one or more LUNs to all hosts you want to cluster, and then mount and format the storage disks on one of the nodes. After adding iSCSI storage to a host, you need to create a new session to the storage. Allocate file storage to a standalone host. You can assign file shares on any host on which you want to create VMs that will use the file share as storage.

Select Fabric > Servers > All Hosts, and select the host or cluster node you want to configure.

Select Host > Properties > Host Access. Specify a Run As account. By default, the Run As account that was used to add the host to VMM is listed. In the Run As account box, configure the account settings. You can't use the account that you use for the VMM service.

Select Fabric > Servers > All Hosts, and select the host or cluster node you want to configure.

Select Host > Properties > Host Access. Specify a Run As account. By default, the Run As account that was used to add the host to VMM is listed. In the Run As account box, configure the account settings. You can't use the account that you use for the VMM service. Select Host Name Properties > Storage > Add File Share.

In File share path, select the required SMB 3.0 file share, and then select OK. To confirm that the host has access, open the Jobs workspace to view the job status. Or, open the host properties again, and then select the Storage tab. Under File Shares, select the SMB 3.0 file share. Verify that a green check mark appears next to Access to file share. Repeat this procedure for any standalone host that you want to access the SMB 3.0 file share or for all nodes in a cluster Assign a logical unit to a standalone host Either assign an existing unit, or create a new one and assign it. In Fabric > Servers > All Hosts, right-click the host that you want to configure > Properties.

If you want to create a new logical unit: On the toolbar, next to Disk, select Add. Next to Logical unit, select Create Logical Unit. In Create Logical Unit > Storage pool, choose the pool from which you want to create the logical unit. Specify a name (alphanumeric only), a description, and the unit size. Select OK to finish. To assign an existing logical unit to the

host, on the toolbar, next to Disk, select Add, and select the logical unit you want to assign. In the Logical unit list, verify that the logical unit that you just created is selected. In Format new disk, if you want to format the disk, select Format this volume as NTFS volume with the following settings, and specify the settings.

not use the Force Format option, the VMM job to assign the logical unit will complete with a warning. VMM assigns the logical unit to the host. You can format the disk later.

In Mount Point, select the mount options. Then select OK to assign the logical unit to the host.

VMM registers the storage logical unit to the host and mounts the storage disk. To view the associated job information, open the Jobs workspace. To verify that the logical unit was assigned, view the information on the Storage tab in the Host Name > Properties dialog. The newly assigned logical unit appears under Disk. Select the new disk to view the disk details. If the Array field is populated in the disk details, this indicates that the storage array is under VMM management.

To configure additional disk settings, open Disk Management on the host. To open Disk Management, select Start, type diskmgmt.msc in the search box, and then press ENTER. The new disk appears in the list of disks as a basic disk. If you chose to format the disk, the disk is already formatted and online. You can right-click the disk to see the available options, such as Format and Change Drive Letter and Paths. Configure storage for a Hyper-V cluster Select Fabric Servers > All Hosts. Rightclick the cluster you want to configure > Properties. In Host Cluster Name > Properties, select a tab:

Available Storage: for adding available storage, converting available storage to shared storage (CSV), or removing available storage.

Shared Volumes: for adding cluster shared volumes (CSVs), converting CSVs to available storage, or removing CSVs. The cluster must run at least Windows Server 2016 to support CSVs.

Configure storage for the host cluster.

If you add available storage for CSVs, use only alphanumeric characters for a LUN. You can't change the partition style of a disk that has already been initialized. If you're converting available storage to CSVs, ensure that there are no VMs on the cluster that have their associated .vhd or .vhdx files located on the storage that you want to convert. Convert volumes one at a time. After conversion, confirm that the logical unit appears on the Shared Volumes tab.

Caution: If you convert shared to available storage and the storage is being used by virtual machines, serious data loss can result. You can only remove storage if there are no VMs in the cluster currently using the storage for their vhds. When you're ready to commit the changes, select OK. Create an iSCSI session. On the target host, in the Services snap-in, ensure that the Microsoft iSCSI Initiator Service is started and set to Automatic. In Fabric > Servers > All Hosts Hosts, right-click the host that you want to configure > Properties.

CHAPTER 4

HYBRID CLOUD INTEGRATION:

Hybrid cloud integration is the process of connecting cloud-based services with on-premises solutions or applications into a larger system1. It allows each solution to function and work together1. Hybrid integration is the ability to connect applications, data, files and business partners across cloud and on-premises systems2. An integrated hybrid cloud platform is a type of cloud-based solution that enables business users to integrate their on-prem legacy system with a hybrid cloud3. Hybrid cloud integration is a strategy to bridge the gap between the existing on-premises systems such as databases, legacy applications and warehouses, and technologies as well as multicloud environments. Organizations are trying to leverage the cloud for operational innovation, revenue model innovation and business model innovation, application modernization, cost-effectiveness, agility, availability, efficiency, rapid scalability and the ability to respond faster. A major portion of processing, systems of engagement, and systems of insight are moving to the cloud. As a result, applications, data, and process integrations should be able to support both cloud-based applications and on-premise systems.

A Cloud-enabled ecosystem and business model not only enables the IT staff but also the LoBs to respond to real business opportunities by forging closer ties with customers and creating innovative customer touch points. Disconnected Silos of Data: Fragmentation of processes and data is caused by the increasing adoption of cloud especially SaaS. Data is scattered across on-premise and cloud. For example, Lines of Business (LOBs), such as marketing, sales, customer support, etc. can consume data from multiple and disparate SaaS applications.

The move towards IoT: Organizations are focused on leveraging IoT as a driver of incremental revenue streams based on new products and services and to improve productivity and save costs, reduce operational overhead, and optimize operational efficiencies. Enormous data that gets generated needs to be integrated and processed to derive appropriate insights to make real-time decisions. For example, the deployment of IoT-based smart energy solutions results in better field communication, reduced cost of maintenance, real-time monitoring, digital oil field infrastructure, reduced power consumption, mining automation, greater safety and security of assets, and thus higher productivity. The move towards APIs and Digitalization: Organizations are crossing over traditional boundaries into new markets and new industries—driving new levels of growth and profitability. As organizations build or partner in industry platforms, new digital ecosystems are growing around them which will become the foundation for the next major stage of technology and economic disruption. To promote their business in a more innovative way, organizations are focusing on innovative digital abilities, such as mobile enablement for employees, location navigation, leveraging new digital channels (omnichannel experience), enhanced customer experience, expansion in online marketing efforts, digital field operations, exposing data as a service, energy consumerization, etc. This has also led data such as sales data and logistics data to be exposed across multiple devices accessible from anywhere. Enterprises need to integrate with third parties, including partners and suppliers, subscribe to data feeds for real-time intelligence, and

the products they build should integrate with other organizations. As the adoption of cloud increases, data that exists outside the organization's firewall needs to be managed and controlled while managing BYOD (Bring Your Own Device) policies, wherein employees want to access the data using any device from anywhere. This has resulted in the need to adopt microservices and API management, which help in providing the required agility and scalability. Integration is the main foundation for enabling organizations to adopt digitalization.

Ability to Support Citizen Integrator Capabilities:

As organizations embrace digitalization, there is a need for agility, dynamic integration, user interface and customer experience capabilities, and velocity. Old integration methodologies will not suffice to meet the scale of connectivity required to support digital business. The result is to enable business users to perform self-service tasks to integrate data and applications with integration tools which provide citizen integrator tools that combine data and application integration that support HIP capabilities. Future Integration Strategy Over time, organizations will have created a scattered landscape with disparate disjointed solutions to cater to the integrating needs like point-to-point connectivity to a SaaS provider, etc. We believe that the majority of large enterprises will continue to use on-premise systems for systems of records but will turn to hybrid integration models that combine on-premise and cloud-hosted systems to handle new integration scenarios. Enterprises should consider hybrid integration for connecting a system of engagements to a system of records, a system of insights, a system of automation and a system of design, which are spread across on-premise and cloud. Hybrid cloud integration defines a holistic integration approach, which utilizes both the traditional investments in the on-premise applications, along with the new and innovative cloud technologies, so the organization can take full advantage of the new and changing enterprise landscape.

The key characteristics of the Hybrid Cloud Integration platform include:

Integrate heterogonous applications and systems to communicate effectively. Provide a comprehensive approach to integrate on-premise and cloud applications. Expose APIs, manage APIs, manage and expose data securely via APIs. Provide velocity to develop and deploy next-gen applications on-premise or to the public cloud. To address the new integration scenarios and patterns, an integration strategy in line with the digital era requirements for agility and adaptability needs to be formulated and renovate the integration platform strategy. Organizations should implement a hybrid integration platform by selecting and aggregating the combination of cloud-native and on-premise integration platforms that best support an organization’s requirements. Enterprises should move towards a new integration strategy which will have consolidated application and data integration capabilities with more hybrid integration capabilities than on-premise or cloud. Key components of integration that should be considered include Application Integration, Data Integration, Process Integration, Cloud Integration, and Infrastructure and Security. The application, data, and process integration strategies complement and enable each other to create a coherent and complete framework, supported by the on-premise and cloud infrastructures, with adequate security considerations.

The integration strategy should include reshaping the organizational model by repositioning the traditional, centralized integration teams from a "software factory" model toward the role of facilitator for HIP-enabled, do-it-yourself integration that is carried out by lines of business (LoBs), subsidiaries, departments, application development (AD) teams, and even business users.

A sound HIP strategy must start with an analysis of:

The integration capabilities already in place in the organization provided by the existing integration platforms. The anticipated short-term, medium-term, and long-term integration needs based on the organization's needs.

4.1 AZURE ARC:

While you are starting out with Azure Arc, you'll likely want to find more information to start evaluating it as a solution for your business. Through search, Azure surface several results. Solution specific views, if you jump in the Arc centre if you're looking for understanding Azure Arc all up or comprehensive views of all Arc resources. The Arc centre helps you find everything Azure Arc-related in one spot, so you can read the latest documentation, stay up to date with new releases, start to bring your hybrid edge or multi-cloud resources into Azure, and even manage them. In the documentation, you can learn more about Azure Arc as well as the use of installation guides. You can look for Azures blue to learn more links to get directed into specific articles or head to the additional resources tab where Azure has compiled useful links. Azure has its documentation hub, Azure's jumpstart repo, relevant training and demos, and hybrid architecture examples. Azure jumpstart repo is a great place to get started with Arc, especially if you are a beginner and do not prefer UI. Updates are where you will be able to keep tabs on our latest new releases. You will be able to learn about new functionality available for Azure Arc technology as soon as they announce it. Cost and pricing are where you find pricing information. You come here to learn how pricing in Azure Arc works and how much you can expect to spend using it. Azure also includes a link to their handy dandy Azure pricing calculator to help with estimations here, especially where other Azure services are involved. Now, head over to overview. Azure infrastructure tab. Within Arc Centre, Azure provides a catalog of the Azure Arc infrastructure offerings that you are able to leverage. You can sign up for some previews to get access to the latest in development before it's released to the public. These items have a preview tag appended to them, and if you are not able to see them. It means you're not signed up for previews yet. Azure has the same catalog view for our data services, so these are all of Azure Arcenabled data services. If you click into servers, you will be taken to a create, which will help to bring on-premises VM into Azure for management. This page takes you through a bunch of prerequisites that you need to make sure you have squared away before proceeding. On this page, you are asked to provide a bit of information. And, you can also optionally use these physical location tags to represent where this resource lives outside of Azure. You basically can download and run this script to complete the connection process connecting on-premises VM to Azure for management. To view the resource, you just created and can head

to Azure Arc resource's view. Here you can sort by type, filter on location. You also have resource-specific views at your disposal. If you head to the servers' view, this shows all of the servers within the subscriptions that you have selected and access to. You can click into a specific one to inspect it and make any modifications or changes that you would like to. Once you get your services set up, you'll probably interact with them directly from the spots that you'd normally expect to in Azure. For example, you'll likely actually manage ARC servers from the ARC servers' page. Arc server. As an example, this is the same ARC serverspecific view that you have just seen within Arc Centre with all the same functionality available, you can add, manage the view, edit the columns, and so on.

In most cases, the location you select when you create the installation script should be the Azure region geographically closest to your machine's location. Data at rest is stored within the Azure geography containing the region you specify, which may also affect your choice of region if you have data residency requirements. If the Azure region your machine connects to has an outage, the connected machine isn't affected, but management operations using Azure may be unable to complete. If there's a regional outage, and if you have multiple locations that support a geographically redundant service, it's best to connect the machines in each location to a different Azure region. SQL Server enabled by Azure Arc migration assessment is a crucial tool for your cloud migration and modernization journey. It simplifies the discovery and readiness assessment for migration by providing:

- Cloud readiness analysis
- Identification of risks and mitigation strategies
- Recommendations for the specific service tier and Azure SQL configuration (SKU size) that best fits the workload needs
- Automatic generation of the assessment
- Continuous running on a default schedule of once per week
- Availability for all SQL Server editions

Migration assessment is for SQL Servers located in various environments, including your data center, edge sites, or any public cloud or hosting provider. It is available for any instance of SQL Server that is enabled by Azure Arc.

SQL BPA uses Azure Monitor Agent (AMA) to collect and analyze data from your SQL servers. If you have AMA installed on your SQL servers before enabling BPA, BPA uses the same AMA agent and proxy settings. You don't need to do anything else. However, if you don't have AMA installed on your SQL servers, BPA installs it for you. BPA will not set up proxy settings for AMA automatically. You need to re-deploy AMA with the proxy settings that you want.. If you use *Configure Arc-enabled Servers with SQL Server extension installed to enable or disable SQL best practices assessment* Azure policy to enable assessment a scale , you need to create an Azure Policy assignment. Your subscription requires the Resource Policy Contributor role assignment for the scope that you're targeting. The scope may be either subscription or resource group. Further, if you are going to create a new user assigned managed identity, you need the User Access Administrator role assignment in the subscription.

CHAPTER 5

NETWORKING:

Networking in Hyper-V is fairly simple and uses two parts - a virtual switch and a virtual networking adapter1. To establish networking for a virtual machine, you'll need at least one of each. The virtual switch connects to any Ethernet-based network1. To connect Hyper-V machines to the internet, run a virtual machine, click File and click Settings, then select Network Adapter from Virtual Machine Settings. From the right side, select the external virtual switch as the virtual switch.

5.1 VIRTUAL NETWORKING:

In general, if we will see a well-established network has become an important part of our lives. Expanding networking helps us to establish relationships with people. Like our social networking in our day-to-day life, computer networking is also important in this digital world where everything is connected to each other. Computer networking helps us to enhance seamless communication, cohesive functioning, and resource sharing. The Internet is an example of a computer network. When we will start thinking that how important is computer networking we can understand the importance of computer networking. With the advancement of technology Virtual networking introduced, now let's understand what is this virtual networking and what are the benefits of it.

- Virtual Networks:

Virtual networking is a technology that facilitates the control of one or more remotely located computers or servers over the Internet. Here data communication occurs between two or more virtual machines. It is similar to traditional networking but interconnection occurs through virtual computing environment means in virtual networking all devices, servers, virtual machines are connected through software and wireless technology. It is based on physical networking principle but its functions are mostly software-driven. In virtual networking devices across many locations connects with each other and function with the same capabilities as a traditional physical network. Virtual networking reduces the cost and complexity of operating and maintaining hardware. Virtual networking software are installed on remote computers or servers to avail of the virtual networking facility.

- Working of virtual networking:

Virtual networking interconnects remote devices and machines from any location using the software. Some vendors offer comprehensive virtual networking software and services. Modern technology is used to create an extended network that works wirelessly.

Virtual networking includes the following parameter:

- VSwitch Software – A software application called vSwitch or Virtual Switch on the host server allows us to set up and configure a virtual network means it controls and directs communication between the existing physical network and virtual parts of the network.
- Virtual Network Adapter – It creates a gateway between networks means it allows computers and virtual machines to connect to a network. It makes it possible for all the computers in a Local Area Network (LAN) to connect to a larger network.
- Physical network – It is required as a host for the virtual network infrastructure. Virtual machines and devices –These are the machines or devices that connect to the network and allow various functionality.
- Servers – It is part of the network host infrastructure.
- Firewalls and security – It is designed for monitoring and preventing security threats in the virtual network.

It is easy to access any parts remotely by virtual networking as it provides more centralized management and simplified network management. Virtual networking is the foundation for Virtualization In Cloud Computing.

Three classes of Virtual Networking:

1. Virtual Private Network – A Virtual Private Network in short called as VPN. VPN uses the internet to connect two or more existing networks. It is an internet-based virtual networking technology that allows to access any physical networks that are connected. It allows connecting any private network through the internet securely and privately. It is just like a private point to point connection between two devices or networks.

2. Virtual Local Area Network –Virtual Local Area Network in short called VLAN. VLAN subdivides the LAN logically into different broadcast domains means it uses partitions to group devices on a LANnetwork into domains with resources and configurations. It allows better security, monitoring, and management of the devices and servers within a specific domain. Each VLANs act as a separate LAN. Data transmission becomes much easier and with VLAN the increasing transmission demand is fulfilled.

3. Virtual Extensible Local Area Network –Virtual Extensible Local Area Network in short called VXLAN. It is a network virtualization technology that stretches layer 2 connections over layer 3 network by encapsulating Ethernet frames in a VXLAN packet which includes IP addresses to address the scalability problem in a more extensible manner.

Benefits of virtual networking:

- Flexibility and scalability.
- Digital security.
- Low networking hardware investment.

- Less overall traffic.
- Centralized network management.
- Easy address to issues.
- Cost savings.
- Remote work capabilities.
- Productivity.

5.2 CLOUD NATIVE FIREWALL:

The definition for the cloud can seem murky, but essentially, it's a term used to describe a global network of servers, each with a unique function. The cloud is not a physical entity, but instead is a vast network of remote servers around the globe which are hooked together and meant to operate as a single ecosystem. These servers are designed to either store and manage data, run applications, or deliver content or a service such as streaming videos, web mail, office productivity software, or social media. Instead of accessing files and data from a local or personal computer, you are accessing them online from any Internet-capable device—the information will be available anywhere you go and anytime you need it. Businesses use four different methods to deploy cloud resources. There is a public cloud that shares resources and offers services to the public over the Internet, a private cloud that isn't shared and offers services over a private internal network typically hosted on-premises, a hybrid cloud that shares services between public and private clouds depending on their purpose, and a community cloud that shares resources only between organizations, such as with government institutions. Most organizations now run more than half of their workloads on public clouds, leveraging the agility and scalability of the cloud to meet rapidly evolving business demands. However, as workloads move to the cloud, networks become more decentralized— and more difficult to secure. Ensuring consistent protection of your cloud resources significantly benefits from a cloud-native solution. A cloud native firewall (CNF) is a managed cloud network security solution delivered as a service that scales to demand, is highly available within cloud regions and across availability zones, and does not require maintenance by customers. A cloud native firewall allows you to define and assign policies that protect selected networks and cloud compute resources without having to configure, provision, or maintain any firewall software infrastructure.

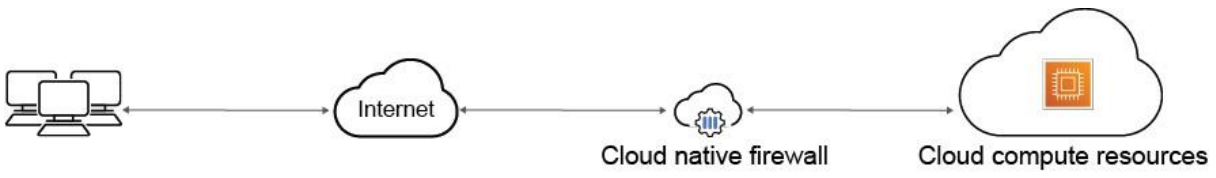

Fig 5.1: Azure cloud-native firewall

Benefits:

- Scalability
  - Cloud-native firewalls like FortiGate CNF can scale up or down quickly to accommodate changing workload demands.
- Flexibility:
  - Cloud-native firewalls are designed to work seamlessly in cloud environments, providing flexibility in terms of deployment and management.
- Security:
  - Cloud-native firewalls provide advanced security capabilities to protect workloads against a wide range of threats and vulnerabilities.
- Egress security:
  - Cloud-native firewalls like FortiGate CNF provide robust egress security capabilities to help prevent data exfiltration and ensure the confidentiality of cloud data.
- Visibility:
  - Cloud-native firewalls provide real-time visibility into cloud network traffic, allowing organizations to identify potential security threats and take proactive measures to mitigate them.
- Compliance:
  - Cloud-native firewalls help organizations meet regulatory compliance requirements by providing advanced security and auditing capabilities.
- Integration:
  - Cloud-native firewalls can integrate with other security solutions and cloud platforms, enabling organizations to create a comprehensive security ecosystem.
- Automation:
  - Cloud-native firewalls like FortiGate CNF can be easily automated, allowing organizations to streamline their security operations and reduce the risk of human error.
- Automation:
  - Cloud-native firewalls like FortiGate CNF can be easily automated, allowing organizations to streamline their security operations and reduce the risk of human error.
- Performance:
  - Cloud-native firewalls are optimized for cloud environments, providing high-performance security and networking capabilities that are essential for modern cloud workloads.

CHAPTER 6

SYSTEM MANAGEMENT:

Azure cloud involves a set of tools, services, and platforms**.** These enable you to configure, run, and optimize your infrastructure, applications, and services on Azure. In addition, other areas of Azure cloud management involve automating processes, monitoring performance, and securing data. Azure has many services and tools that work together to provide complete management. These services aren't only for resources in Azure, but also in other clouds and on-premises. Understanding the different tools and how they work together is the first step in designing a complete management environment.

The following diagram illustrates the different areas of management that are required to maintain any application or resource. These different areas can be thought of as a lifecycle. Each area is required in continuous succession over the lifespan of a resource. This resource lifecycle starts with the initial deployment, through continued operation, and finally when retired.

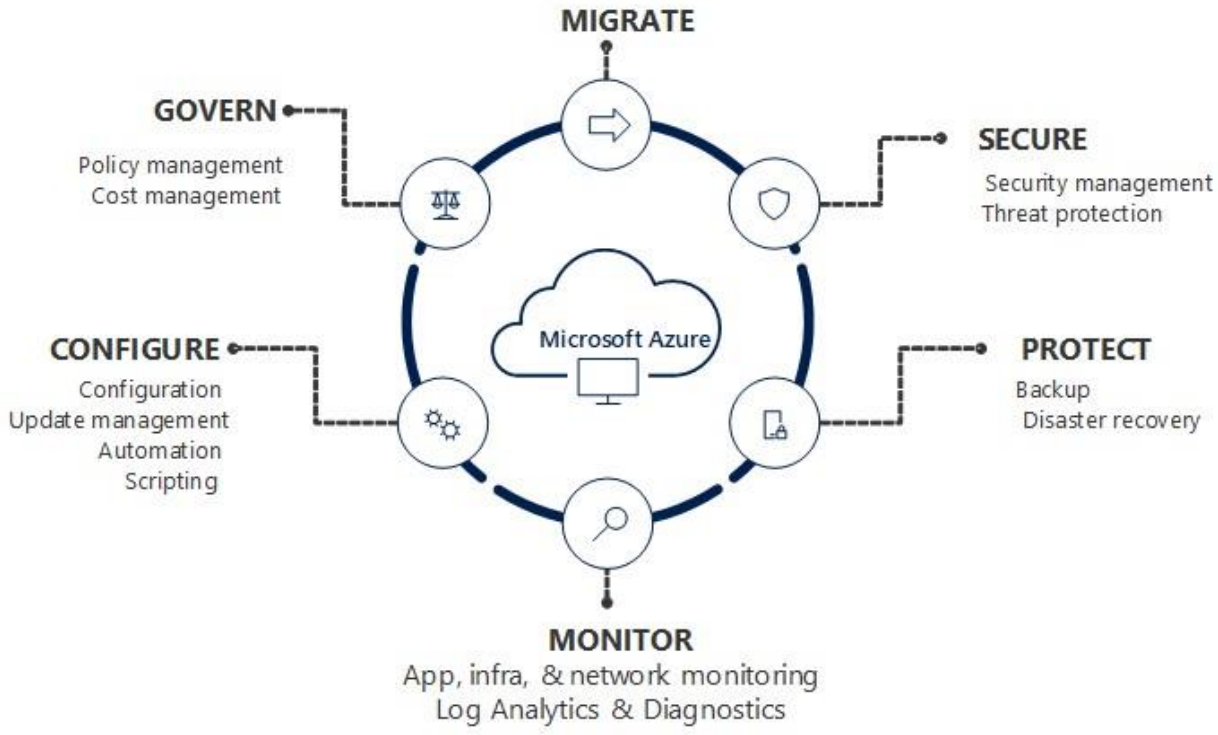

Fig 6.1: Azure wheel of services

wheel of services that support Management and Governance in Azure. Secure has Security management and Threat protection as sub items.
Protect has Backup and Disaster recovery as sub items. Monitor has
App, infrastructure and network monitoring, and Log Analytics and
Diagnostics as sub items. Configure has Configuration, Update
Management, Automation, and Scripting as sub items. And Govern has
Policy management and low-Cost management as sub items. No single Azure service completely fills the requirements of a particular management area. Instead, each is realized by several services working together. Some services, such as Application Insights, provide targeted monitoring functionality for web applications. Others, like Azure Monitor logs, store management data for other services. This feature allows you to analyze data of different types collected by different services.

UPDATE:

Flexible patching options such as automatic virtual machine (VM) guest patching, maintenance schedules, and on-demand updates. Start managing updates for your machines natively in Azure with an intuitive user experience. Use the service globally in all Azure and Azure Arc regions.

Azure Update Management keeps track of each system's status with multiple scans throughout the day, which Azure Log Analytics processes. If a new update is available, each OS retrieves an update from its source, such as Windows Server Update Services (WSUS) for Windows or a local repository for Linux systems.

Provides native experience with zero on-boarding.

- Built as native functionality on Azure compute and the Azure Arc for Servers platform for ease of use.
- No dependency on Log Analytics and Azure Automation.
- Azure Policy support.
- Global availability in all Azure compute and Azure Arc regions

SECURITY UPDATE:

Azure Firewall: a cloud-native, next-generation firewall that protects your Azure Virtual Network resources. Azure DDoS Protection: protects Azure resources from DDoS

attacks with monitoring and automatic network mitigation. Azure Web Application Firewall protects web applications from malicious attacks, bots, and common web vulnerabilities.

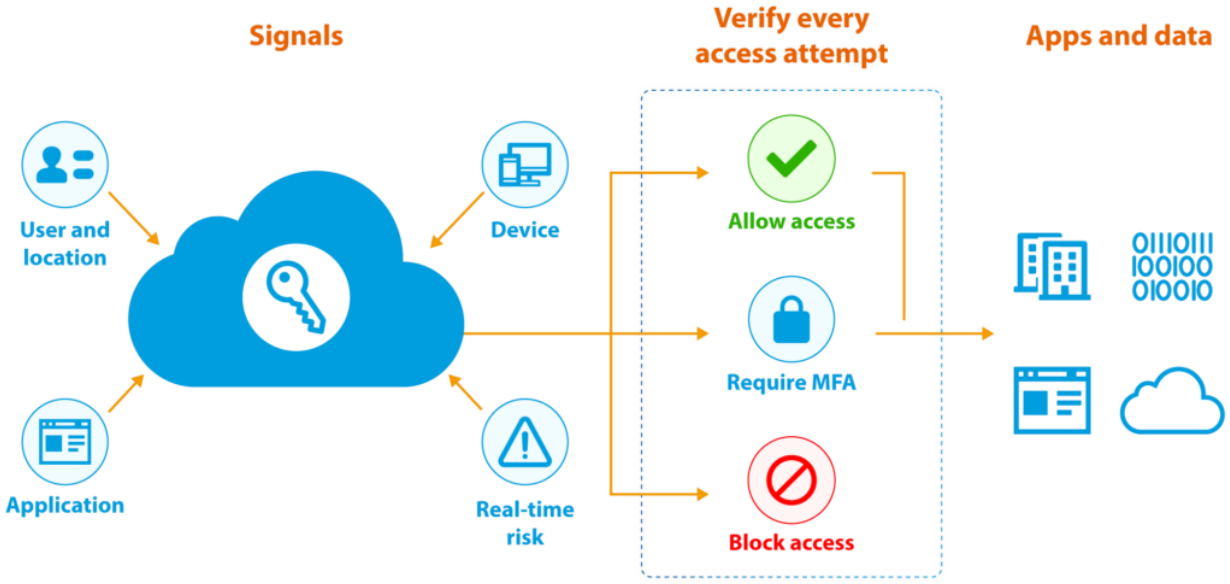

Fig 6.2: Azure security verification

Secure your distributed Windows Server 2012 R2 and SQL Server 2012 resources beyond the end-of-support deadline with flexible pricing options. View compliance status for each individual machine, easily deploy updates, and track results.

SQL SERVER:

Azure SQL is a family of managed, secure, and intelligent products that use the SQL Server database engine in the Azure cloud. Azure SQL is built upon the familiar SQL Server engine, so you can migrate applications with ease and continue to use the tools, languages, and resources.

- AZURE SQL DATABASE:
    - Support modern cloud applications on an intelligent, managed database service that includes serverless compute.
- AZURE SQL MANAGED INSTANCE:
    - Modernize your existing SQL Server applications at scale with an intelligent fully managed instance as a service, with almost 100% feature parity with the SQL Server database engine. Best for most migrations to the cloud.

- SQL SERVER ON VMs:
    - Lift-and-shift your SQL Server workloads with ease and maintain 100% SQL Server compatibility and operating system-level access

In today's data-driven world, driving digital transformation increasingly depends on our ability to manage massive amounts of data and harness its potential. But today's data estates are increasingly complex, with data hosted on-premises, in the cloud, or at the edge of the network. Developers who are building intelligent and immersive applications can find themselves constrained by limitations that can ultimately impact their experience. Limitations arising from incompatible platforms, inadequate data security, insufficient resources and price-performance barriers create complexity that can inhibit app modernization and development.

One of the first things to understand in any discussion of Azure versus on-premises SQL Server databases is that you can use it all. Microsoft's data platform leverages SQL Server technology and makes it available across physical on-premises machines, private cloud environments, third-party hosted private cloud environments, and the public cloud.

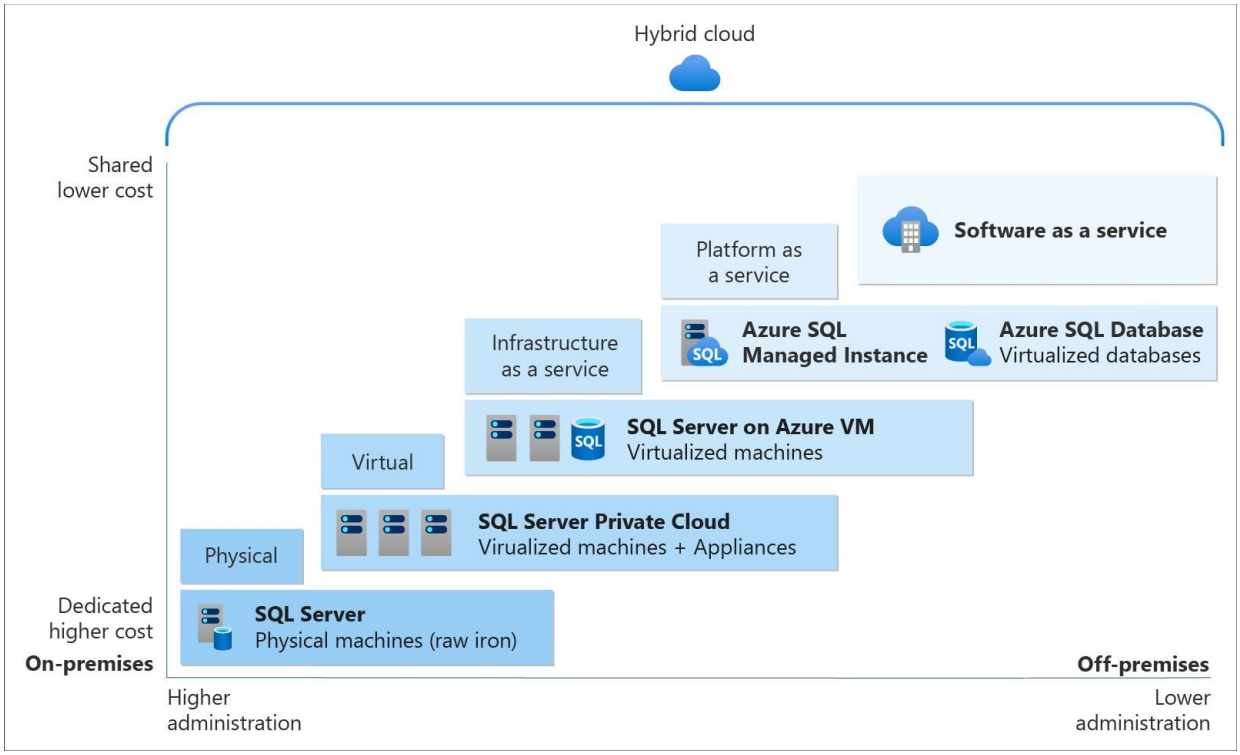

Fig 6.3: Azure SQL server architecture

As seen in the diagram, each service offering can be characterized by the level of administration you have over the infrastructure, and by the degree of cost efficiency. In Azure, you can have your SQL Server workloads running as a hosted service (PaaS), or a hosted infrastructure (IaaS) supporting the software layer, such as Software-as-a-Service (SaaS) or an application. Within PaaS, you have multiple product options, and service tiers within each option.

EXTENSIONS:

Azure virtual machine (VM) extensions are small applications that provide post-deployment configuration and automation tasks on Azure VMs. For example, if a virtual machine requires software installation, antivirus protection, or the ability to run a script inside of the VM, you can use a VM extension. You can run Azure VM extensions by using the Azure CLI, PowerShell, Azure Resource Manager (ARM) templates, and the Azure portal. You can bundle extensions with a new VM deployment or run them against any existing system. This article provides an overview of Azure VM extensions, including prerequisites and guidance on how to detect, manage, and remove extensions. This article provides generalized information because many VM extensions are available. Each extension has a potentially unique configuration and its own documentation.

1. AZURE VM AGENT

To handle extensions on the VM, you need the azure virtual machine agent for windows installed. This agent is also referred to as the Azure VM Agent or the Windows Guest Agent. As you prepare to install extensions, keep in mind that some extensions have individual prerequisites, such as access to resources or dependencies. The Azure VM Agent manages interactions between an Azure VM and the Azure fabric controller. The agent is responsible for many functional aspects of deploying and managing Azure VMs, including running VM extensions. The Azure VM Agent is preinstalled on Azure Marketplace images. The agent can also be installed manually on supported operating systems.

2. RUN VM EXTENSIONS

Azure VM extensions run on existing VMs, which is useful when you need to make configuration changes or recover connectivity on an already deployed VM. VM extensions can also be bundled with ARM template deployments. By using extensions with ARM templates, you can deploy and configure Azure VMs without post-deployment intervention.
When an extension update is available and automatic updates are enabled, if a VM model changes, the Azure VM Agent downloads and upgrades the extension. Automatic extension updates are either minor or hotfix. You can opt in or opt out of minor updates when you provision the extension. The following example shows how to automatically upgrade minor versions in an ARM template by using the "autoUpgradeMinorVersion".

CHAPTER 7

SYSTEM MONITORING:

Azure Monitor is a comprehensive monitoring solution for collecting, analysing, and responding to monitoring data from your cloud and on-premises environments. You can use Azure Monitor to maximize the availability and performance of your applications and services. It helps you understand how your applications are performing and allows you to manually and programmatically respond to system events. Azure Monitor collects and aggregates the data from every layer and component of your system across multiple Azure and non-Azure subscriptions and tenants. It stores it in a common data platform for consumption by a common set of tools that can correlate, analyse, visualize, and/or respond to the data. You can also integrate other Microsoft and non-Microsoft tools. Following given diagram is the azure monitoring architecture,

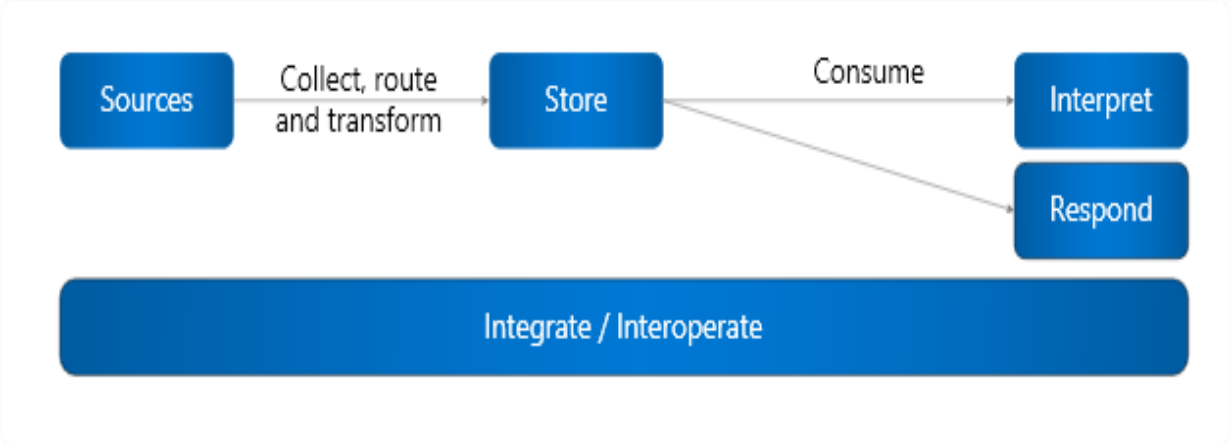

Fig 7.1: azure system monitoring architecture

HIGH LEVEL ARCHITECTURE,

Databases Azure Monitor can monitor these types of resources in Azure, other clouds, or on-premises:

- Applications
- Virtual machines
- Guest operating systems
- Containers including Prometheus metrics
- Security events in combination with Azure Sentinel
- Networking events and health in combination with Network Watcher • Custom sources that use the APIs to get data into Azure Monitor

You can also export monitoring data from Azure Monitor into other systems so you can:

- Integrate with other third-party and open-source monitoring and visualization tools
- Integrate with ticketing and other ITSM systems

Azure Monitor now includes Operations Manager MI is a cloud-hosted version of Operations Manager and allows you to move your on-premises Operations Manager installation to Azure.

7.1 REAL TIME MONITORING:

Azure Arc-enabled servers allow you to manage your Windows and Linux servers and virtual machines that are hosted outside of Azure, on your corporate network, or on a third-party cloud provider. This article will help you operate Azure Arc-enabled servers on Azure enterprise estate, with centralized management and monitoring at the platform level. You will be presented with key recommendations for your operations team, to maintain Azure Arc enabled servers.

7.2 ARCHITECTURE OF AZURE ARC IN MONITORING RTS SERVER:

The following diagram shows conceptual reference architecture that demonstrates how the Azure connected machine agent communicates with the different management and monitoring capabilities in Azure.

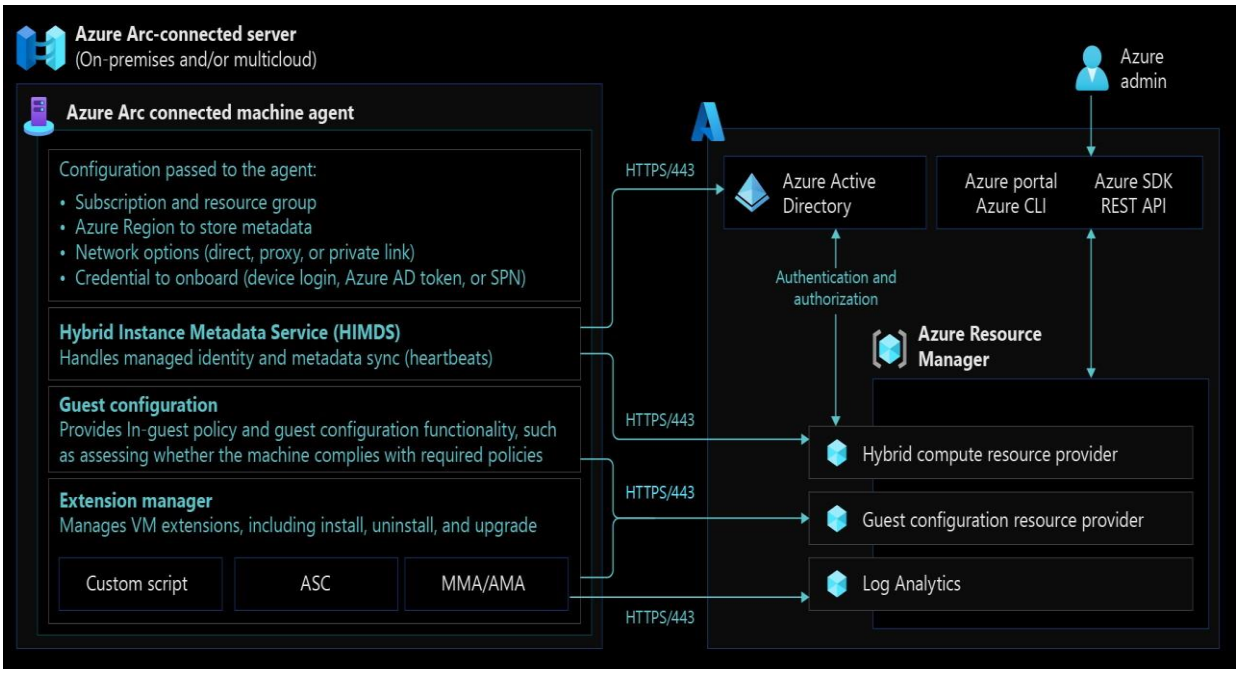

Fig 7.2: azure arc connects server network diagram

7.3 REAL TIME NETWORK MONITORING:

Azure offers a host of solutions to monitor your networking assets. Azure has solutions and utilities to monitor network connectivity, the health of ExpressRoute circuits, and analyse network traffic in the cloud. As of July 1, 2021, you can no longer add new tests in an existing workspace or enable a new workspace in Network Performance Monitor (NPM). You're also no longer able to add new connection monitors in Connection Monitor (Classic). You can continue to use the tests and connection monitors that you've created prior to July 1, 2021.To minimize service disruption to your current workloads, migrate your tests from Network Performance Monitor, or migrate from Connection Monitor (Classic) to the new
Connection Monitor in Azure Network Watcher before February 29, 2024.

7.4 NETWORK PERFORMANCE MONITOR:

Network Performance Monitor is a suite of capabilities that is geared towards monitoring the health of your network. Network Performance Monitor monitors network connectivity to your applications, and provides insights into the performance of your network. Network Performance Monitor is cloud-based and provides a hybrid network monitoring solution that monitors connectivity between:

- Cloud deployments and on-premises locations
- Multiple data centres and branch offices
- Mission critical multi-tier applications/micro-services
- User locations and web-based applications (HTTP/HTTPs)

Performance Monitor, ExpressRoute Monitor, and Service Connectivity Monitor are monitoring capabilities within Network Performance Monitor and are described in the following sections. Network Performance Monitor is a cloud-based hybrid network monitoring solution that helps you monitor network performance between various points in your network infrastructure. It also helps you monitor network connectivity to service and application endpoints and monitor the performance of Azure ExpressRoute. Network Performance Monitor detects network issues like traffic blackholing, routing errors, and issues that conventional network monitoring methods aren't able to detect. The solution generates alerts and notifies you when a threshold is breached for a network link. It also ensures timely detection of network performance issues and localizes the source of the problem to a particular network segment or devices.

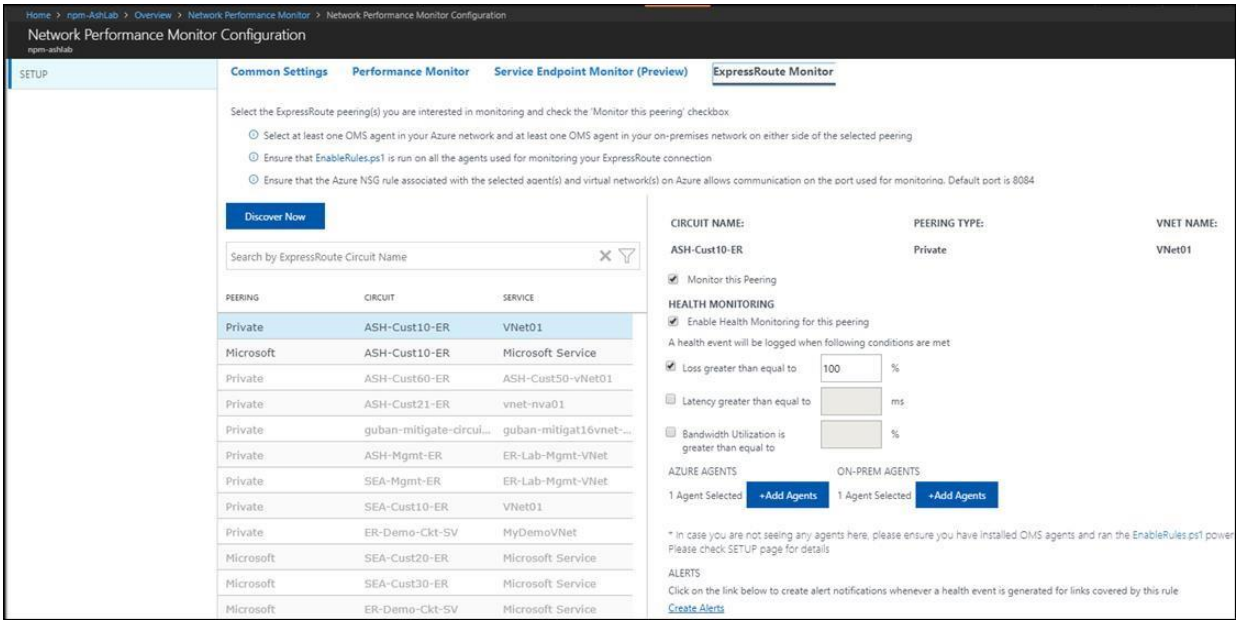

Fig 7.3: Azure network monitoring interface

7.5 THREAT AND FAULT MONITORING:

Azure offers built in threat protection functionality through services such as Microsoft Entrap ID, Azure Monitor logs, and Microsoft Defender for Cloud. This collection of security services and capabilities provides a simple and fast way to understand what is happening within your Azure deployments. Azure provides a wide array of options to configure and customize security to meet the requirements of your app deployments. This article discusses how to meet these requirements.

Azure SQL Database Threat Detection:

Azure SQL database threat detection is a new security intelligence feature built into the Azure SQL Database service. Working around the clock to learn, profile, and detect anomalous database activities, Azure SQL Database Threat Detection identifies potential threats to the database. Security officers or other designated administrators can get an immediate notification about suspicious database activities as they occur.

Each notification provides details of the suspicious activity and recommends how to further investigate and mitigate the threat Currently, Azure SQL Database Threat Detection detects potential vulnerabilities and SQL injection attacks, and anomalous database access patterns. Upon receiving a threat-detection email notification, users are able to navigate and view the relevant audit records through a deep link in the mail. The link opens an audit viewer or a preconfigured auditing Excel template that shows the relevant audit records around the time of the suspicious event, according to the following methodology,

- **Deterministic detection**: Detects suspicious patterns (rules based) in the SQL client queries that match known attacks. This methodology has high detection and low false positive, but limited coverage because it falls within the category of "atomic detections."
- **Behavioural detection**: Detects anomalous activity, which is abnormal behaviour in the database that wasn't seen during the most recent 30 days. Examples of SQL client anomalous activity can be a spike of failed logins or queries, a high volume of data being extracted, unusual canonical queries, or unfamiliar IP addresses used to access the database. **ApplicationGatewayWebApplicationFirewall:**

  Web application firewall (WAF) is a feature of Application Gateway that provides protection to web applications that use an application gateway for standard application delivery control functions. Web Application Firewall does this by protecting them against most of the Open Web Application Security Project (OWASP) top 10 common web vulnerabilities.

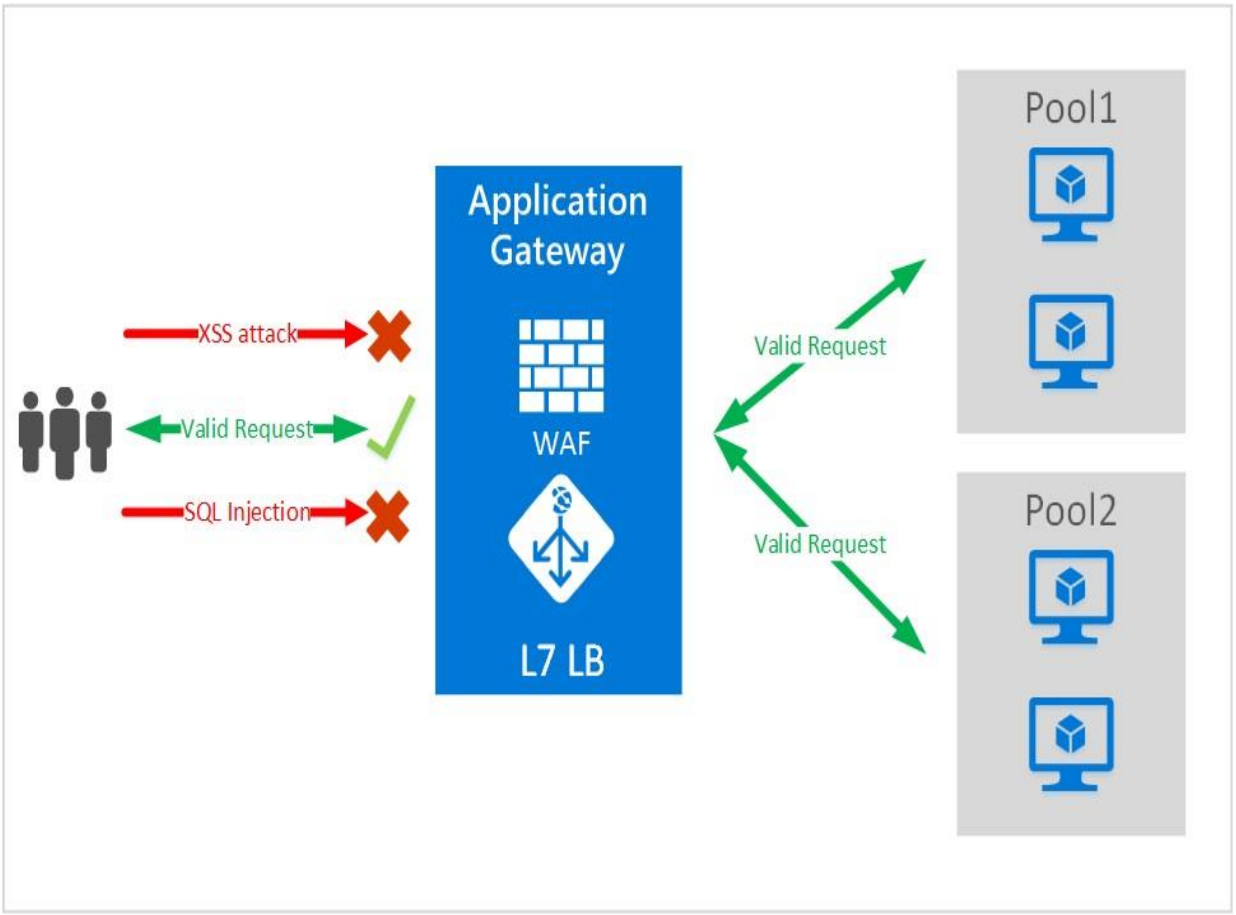

Fig 7.4: Azure application gateway

PROTECTION INCLUDE,

- SQL injection protection and Cross site scripting protection.
- Common Web Attacks Protection, such as command injection, HTTP request smuggling, HTTP response splitting, and remote file inclusion attack.
- Protection against HTTP protocol violations.
- Protection against HTTP protocol anomalies, such as missing host user-agent and accept headers.
- Prevention against bots, crawlers, and scanners.

hardware maintenance and repairs; you can focus your time on your business applications. Azure continuously monitors for hardware that shows signs of degradation or potential failure. When these conditions are detected, Azure will attempt to live migrate your virtual machines (VMs). If live migration isn't possible, Azure will automatically redeploy VMs to a healthy machine. If you have a disaster recovery setup, which is highly recommended, the impact of this redeployment will be minimal. However, a redeployment to a healthy machine may be problematic for some applications that can't tolerate disruption. We've received feedback that in this situation, when possible, customers prefer to control the time the redeployment to a healthy machine will occur.

CHAPTER 8

MIGRATION:

Hybrid cloud migration involves moving your organization's digital assets, workloads, and applications between a mix of on-premises, private cloud, and public cloud environments. This strategy allows you to balance the need for control, compliance, and agility by leveraging the strengths of both on-premises and cloud-based solutions. For example, you can still keep sensitive data on-premises for security reasons while utilizing the Cloud's scalability for customer facing applications. This type of cloud migration enables you to optimize your IT infrastructure for cost, performance, and security, making it a flexible and efficient approach to digital transformation.

Benefits of Hybrid Cloud Migration

1. If done correctly, hybrid cloud migration will enable your apps to pull data from the same databases already running on your customers' sites. So, your customers will be working with the same data and the same trust in that data when using your new cloud-based apps.
2. Data is Stored Securely but Accessible Anywhere Ease of access is both the Cloud's greatest strength and its greatest potential weakness. Many companies, especially those that work with particularly sensitive data (such as confidential customer information or data regulated by HIPAA-like industry standards), are skeptical of storing their data in the Cloud. In the hybrid cloud model, your customers continue to store sensitive data on-site, exposing only nonsensitive material to the Cloud. This allows them to utilize the cheap and flexible cloud infrastructure while preserving data security.
3. Your Existing Software Serves as the Base for Your Cloud Apps This is both the central tenant and the biggest benefit of hybrid cloud implementation.

8.1 AZURE MIGRATE:

Azure Migrate provides a simplified migration, modernization, and optimization service for Azure. All pre-migration steps such as discovery, assessments, and right-sizing of on-premises resources are included for infrastructure, data, and applications. Azure Migrater’s extensible framework allows for integration of third-party tools, thus expanding the scope of supported use-cases. It provides the following:

- Unified migration platform: A single portal to start, run, and track your migration to Azure.
- Range of tools: A range of tools for assessment and migration. Azure Migrate tools include Azure Migrate: Discovery and assessment and Migration and modernization. Azure Migrate also integrates with other Azure services and tools, and with independent software vendor (ISV) offerings.

- Assessment, migration, and modernization: In the Azure Migrate hub, you can assess, migrate, and modernize: ◦Servers, databases and web apps: Assess on-premises servers including web apps and SQL Server instances and migrate them to Azure.
- Databases: Assess on-premises SQL Server instances and databases to migrate them to an SQL Server on an Azure VM or an Azure SQL Managed Instance or to an Azure SQL Database.
- Web applications: Assess on-premises web applications and migrate them to Azure App Service and Azure Kubernetes Service.
- Virtual desktops: Assess your on-premises virtual desktop infrastructure (VDI) and migrate it to Azure Virtual Desktop.
- Data: Migrate large amounts of data to Azure quickly and costeffectively using Azure Data Box products.

Migration and modernization tools:

The Migration and modernization tool helps in migrating servers to Azure:

On-premises VMware VMs -	1. Migrate VMs to Azure using agentless or agent-based migration. 2. For agentless migration, the Migration and modernization tool uses the same appliance that is used by Discovery and assessment tool for discovery and assessment of servers. 3. For agent-based migration, the Migration and modernization tool uses a replication appliance.
On-premises Hyper-V VMs -	1. Migrate VMs to Azure. 2. The Migration and modernization tool uses provider agents installed on Hyper-V host for the migration

On-premises physical servers or servers hosted on other clouds -	1. You can migrate physical servers to Azure. 2. You can also migrate other other public clouds, by treating them as physical servers for the purpose of migration. 3. The Migration and modernization tool uses a replication appliance for the migration.
Web apps hosted on Windows OS in a VMware environment -	1.You can perform agentless migration of ASP.NET web apps at-scale to azure app service using Azure Migrate.

Table 8.2.1: The Migration and modernization

In the Azure Migrate hub, you select the tool you want to use for assessment or migration and add it to a project. If you add an ISV tool or Movere:

- To get started, obtain a license or sign up for a free trial by following the tool instructions. Each ISV or tool specifies tool licensing.
- Each tool has an option to connect to Azure Migrate. Follow the tool instructions to connect.
- Track your migration across all tools from within the project.

- **Current version**: Use this version to create projects, discover on-premises servers, and orchestrate assessments and migrations.

- **Previous version**: The previous version of Azure Migrate, also known as classic Azure Migrate, supports only assessment of on-premises servers running on VMware. Classic Azure Migrate is retiring in Feb 2024. After Feb 2024, classic version of Azure Migrate will no longer be supported and the inventory metadata in classic projects will be deleted. You can't upgrade projects or components in the previous version to the new version.

8.2 AZURE ARC SCVMM:

Azure Arc-enabled System Centre Virtual Machine Manager (SCVMM) empowers System Center customers to connect their VMM environment to Azure and perform VM self-service operations from Azure portal. Azure Arc-enabled SCVMM extends the Azure control plane to SCVMM managed infrastructure, enabling the use of Azure security, governance, and management capabilities consistently across System Center managed estate and Azure.

Azure Arc-enabled System Center Virtual Machine Manager also allows you to manage your hybrid environment consistently and perform selfservice VM operations through Azure portal. For Microsoft Azure Pack customers, this solution is intended as an alternative to perform VM selfservice operations.

Arc-enabled System Centre VMM allows you to:

- Perform various VM lifecycle operations such as start, stop, pause, and delete VMs on SCVMM managed VMs directly from Azure.
- Empower developers and application teams to self-serve VM operations on demand using azure role-based access control (RBAC)
- Browse your VMM resources (VMs, templates, VM networks, and storage) in Azure, providing you with a single pane view for your infrastructure across both environments. • Discover and onboard existing SCVMM managed VMs to Azure.
- Install the Arc-connected machine agents at scale on SCVMM VMs to govern, protect, configure and monitor them.

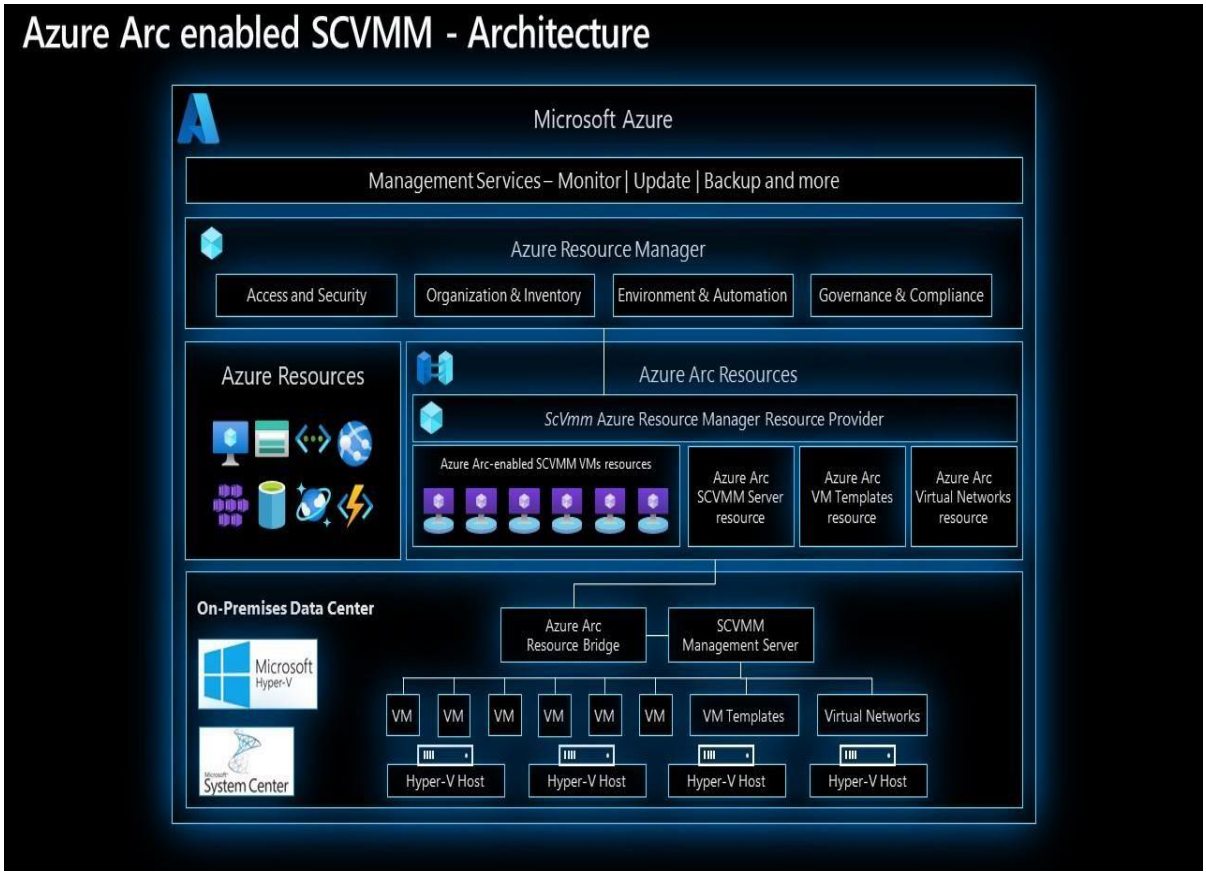

Fig 8.1: Azure arc SCVMM

Azure Arc-enabled servers interact on the guest operating system level, with no awareness of the underlying infrastructure fabric and the virtualization platform that they're running on. Since Arc-enabled servers also support bare-metal machines, there might, in fact, not even be a host hypervisor in some cases.

Azure Arc-enabled SCVMM is a superset of Arc-enabled servers that extends management capabilities beyond the guest operating system to the VM itself. This provides lifecycle management and CRUD (Create, Read, Update, and Delete) operations on an SCVMM VM. These lifecycle management capabilities are exposed in the Azure portal and look and feel just like a regular Azure VM. Azure Arc-enabled SCVMM also provides guest operating system management, in fact, it uses the same components as Azure Arc-enabled servers.

The following scenarios are supported in Azure Arc-enabled SCVMM:

- SCVMM administrators can connect a VMM instance to Azure and browse the SCVMM virtual machine inventory in Azure.

- Administrators can use the Azure portal to browse SCVMM inventory and register SCVMM cloud, virtual machines, VM networks, and VM templates into Azure.
- Administrators can provide app teams/developers fine-grained permissions on those SCVMM resources through Azure RBAC
- App teams can use Azure interfaces (portal, CLI, or REST API) to manage the lifecycle of on-premises VMs they use for deploying their applications (CRUD, Start/Stop/Restart).
- Administrators can install Arc agents on SCVMM VMs at-scale and install corresponding extensions to use Azure management services like Microsoft Defender for Cloud, Azure Update Manager, Azure Monitor.

CONCLUSION:

The hybrid cloud model has emerged as a powerful solution, combining the benefits of public and private clouds. However, with this hybrid environment comes the crucial challenge of managing securing network traffic effectively. Firewalls serve as gatekeepers of networks security, monitoring and controlling incoming and outgoing traffic based on predetermined security rules. Network management within a hybrid cloud environment involves overseeing the connectivity, performance, and availability of resources distributed across various cloud and on-premises infrastructure. This introduction sets the stage for exploring the intricate dance between firewall security and network management in the dynamic landscape of hybrid cloud computing, highlighting the critical importance of both elements in ensuring the integrity and resilience of modern IT architecture. The Azure is the very flexibility to use the computation of the data structure instead the data transmutation on the public cloud to private cloud of the hybrid cloud platform. It is cost effective because other service-based company should provide the high cost and limited resources. The hybrid cloud can be scalable through the requirements of the individual needs and resources. The hybrid cloud has been deployed and managed and the firewall and networks has been configured.

REFRENCES:

- Buchanan, S., Joyner, J. (2022). Azure Arc Servers: Getting Started. In: Azure Arc-Enabled Kubernetes and Servers

  Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-7768-3_4

- Weissman, B., Nocentino, A.E. (2022). Deploying Azure Arc-enabled PostgreSQL Hyperscale. In: Azure Arc-enabled Data Services Revealed.
  Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-8085-0_8

- Maxwell, R. (2024). Monitoring and Process Automation via the Arc Control Plane. In: Azure Arc Systems Management
  .

- https://learn.microsoft.com/en-us/azure/firewall/

- https://learn.microsoft.com/en-us/answers/questions/457732/azure-arc-agent-firewall-port-requirement

- https://learn.microsoft.com/en-us/azure/architecture/hybrid/azure-arc-hybrid-config

- https://learn.microsoft.com/en-us/windows-server/virtualization/hyper-v/hyper-v-technology-overview

- Hybrid Cloud , https://www.redhat.com/en/topics/cloud-computing/what-is-hybrid-cloud , Accessed on 31/07/2020.

- National Institute of standard Technology , https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf , Accessed on October, 2020.

- Hybrid cloud : https://azure.microsoft.com/en-in/overview/what-is-hybrid-cloud-computing/ , Accessed on 9th Oct, 2020

- AI in Hybrid Cloud , https://www.ibm.com/blogs/client-voices/digital-transformation-ai-hybrid-cloud/ , Accessed on October, 2020.

- Pervasive Encryption , https://www.ibm.com/support/z-content-solutions/pervasive-encryption/ , Accessed on 6th December, 2020 .

- Tsai-Wei Wu, Stephen Lien Harrell, Geoffrey Lentner, Alex Younts, Sam Weekly, Zoey Mertes, Amiya Maji, Preston Smith, and Xiao Zhu. 2021. Defining Performance of Scientific Application Workloads on the AMD Milan Platform. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3437359.3465596

- IBM. 2013a. Changing the game: 3 ways IBM cloud is transforming the US open. IBM Case Study. Available at https://www.ibm.com/blogs/cloud-computing/2018/08/20/ibm-cloud-transforming-us-open/ (accessed date October 24, 2016).

- Book: Microsoft Azure Network Security By Nicholas DiCola, Anthony Roman

  https://books.google.co.in/books?hl=en&lr=&id=ktfPEAAAQBAJ&oi=fnd&pg=PP13&dq=azure+firewalls&ots=5pgS-zPysi&sig=1UVLN_FmsnZLr2HdZ5muR2EbYEk&redir_esc=y#v=onepage&q&f=false