

APPENDIX C

INFRINGEMENT CHART
U.S. Patent No. 10,810,050

ToutVirtual, Inc. (“ToutVirtual”) provides the following chart pursuant to Patent Local Rule 3-1 regarding Microsoft Corporation’s (“Microsoft”) infringement of U.S. Patent No. 10,810,050 (the “’050 Patent”).

Microsoft infringes the asserted claims (1-3, 5-6, 9-11, and 13-14) of the ’050 Patent through direct infringement and indirect infringement (see Cover Pleading), including inducement of infringement and/or contributory infringement.

The “Accused Instrumentality” is the Azure Cloud System that is operated by Microsoft and includes all necessary hardware, auxiliary hardware, and software used in its operation. As explained below, the Accused Instrumentality provides to its customers (*e.g.*, “tenants” or “users”) various functionalities that meet the elements of the asserted claims identified below. While the provided functionalities are referred to as products and services, they are not separate from each other and operate on the same Azure Cloud System operated by Microsoft.

The Accused Instrumentality includes, but is not limited to, the functionalities listed in the Cover Pleading, including the associated features as indicated throughout the chart below.

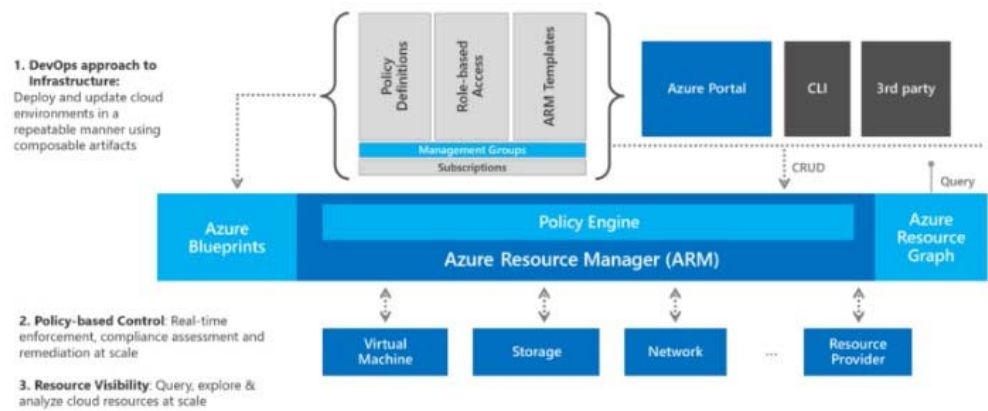
Because certain elements reference previous elements with the same or similar elements, the analysis included for any claim element incorporates all previous analysis related to any referenced elements.

ToutVirtual contends that none of the elements of the asserted claims of the ’050 Patent are governed by 35 U.S.C. § 112(6).

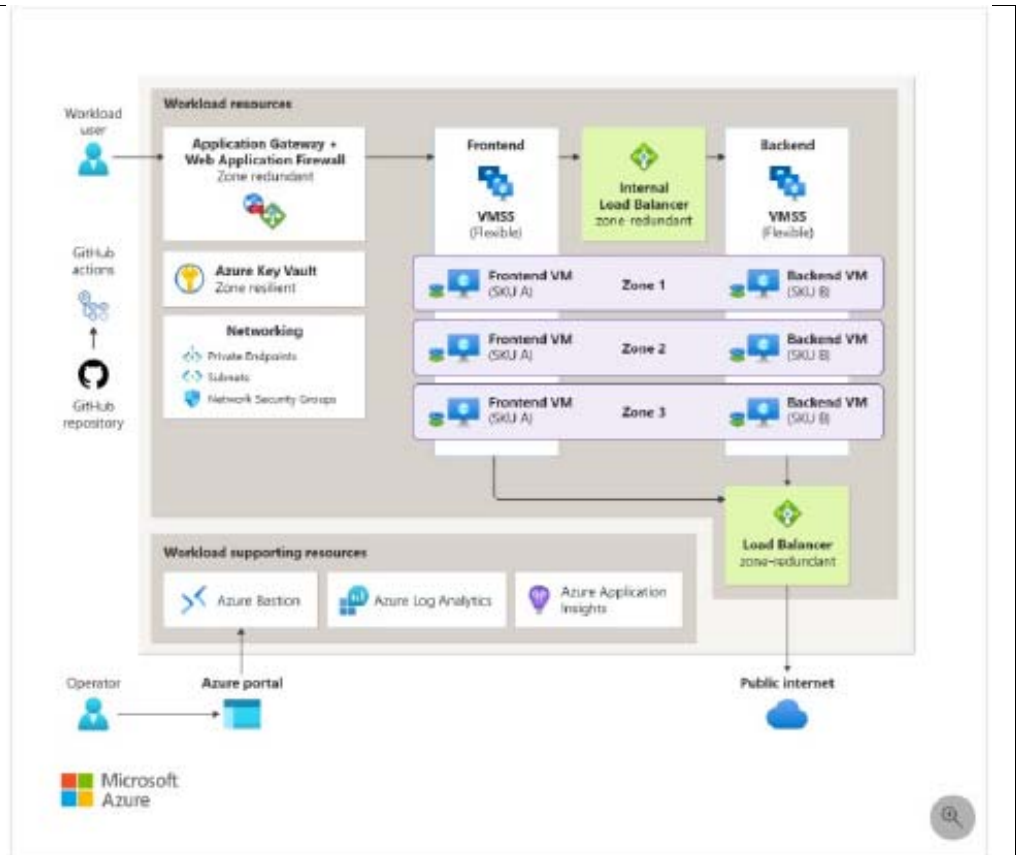
To the extent that it is determined that Microsoft does not make, use, offer for sale, or sell any of the components as described below, Microsoft jointly infringes with its customers or third-party cloud services providers that provide the relevant elements.

Claim 1	
1[pre]. A method for on demand provisioning of virtual asset via a self-service portal in a virtualization system, the method comprising:	The Accused Instrumentality meets the recited claim language because it encompasses every step of the claimed method for on demand provisioning of virtual assets via self-service portal in a virtualization system, as set forth below. The Accused Instrumentality are controlled by hardware owned and controlled by Microsoft, such that all steps are performed by it. The Accused Instrumentality is a cloud-based computing system that generates and automatically manages a distributed virtualization environment in a computer network, enabling users to deploy, configure, and operate virtual machines, containers, and other virtualized resources on demand without managing the underlying physical and software infrastructure. TOUTVIRTUAL 002978-TOUTVIRTUAL 002985;

Azure Governance Architecture



TOUTVIRTUAL 002425-TOUTVIRTUAL 002426;



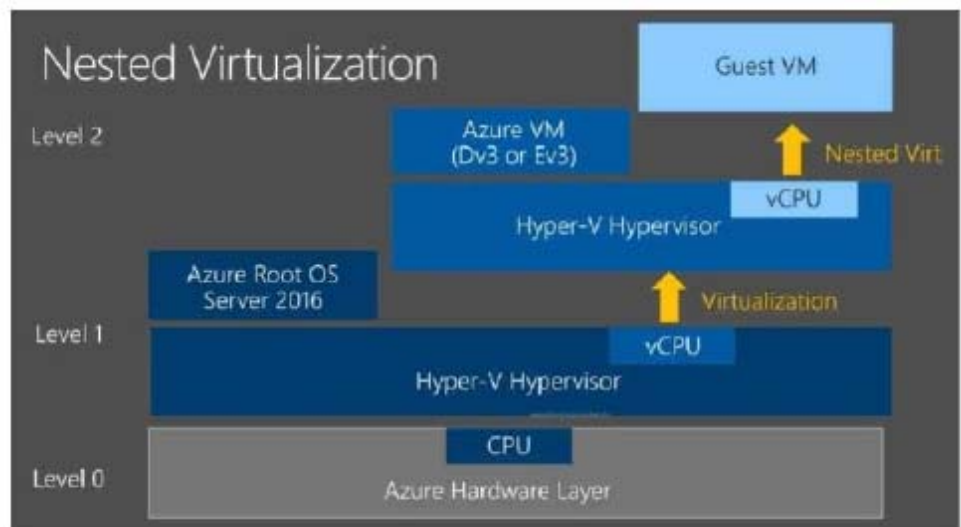
TOUTVIRTUAL 002512-TOUTVIRTUAL 002542.

The Accused Instrumentality collectively encompasses every step of the claimed method, as set forth below.

1[a].
providing a virtualization system that has an inventory that includes physical resources and virtual assets managed by a virtualization layer running on the physical resources; wherein virtual assets are software instantiations of computer systems;

The Accused Instrumentality meets the recited claim language because it includes a technology stack of hardware and software that performs steps of generating and operating a virtualization environment that has a virtualization layer, physical resources, and virtual assets.

The Accused Instrumentality provides a cloud-based environment that operates hypervisor technology (including Azure Hypervisor and/or Hyper-V), which creates the virtualization layer. This virtualization layer is the software that runs in conjunction with the physical servers in the datacenters to virtualize physical resources and virtual assets. The hypervisors used in the Accused Instrumentality are software technology that creates and manages virtual machines by virtualizing and allocating hardware resources like compute, network, and storage. Hypervisors serve as the foundational virtualization layer upon which compute virtualization, network virtualization, application virtualization, and storage virtualization operate within the virtualization environment.



TOUTVIRTUAL 002658-TOUTVIRTUAL 002663; TOUTVIRTUAL 002651-TOUTVIRTUAL 002657; TOUTVIRTUAL 002664-TOUTVIRTUAL 002703.

The Accused Instrumentality provides virtualization systems that have an inventory that includes physical resources including, but are not limited to, processors, storage, and networking

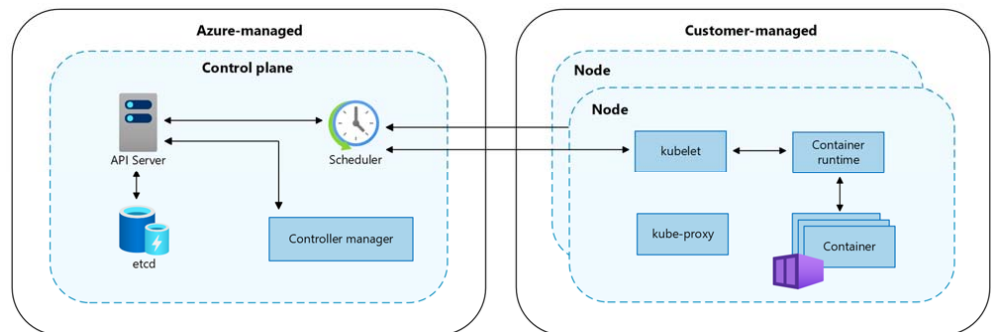
infrastructure components. Physical resources may further include Microsoft datacenters hosting the Accused Instrumentality and Azure Dedicated Hosts. TOUTVIRTUAL 002152-TOUTVIRTUAL 002156; TOUTVIRTUAL 002157-TOUTVIRTUAL 002165; TOUTVIRTUAL 002630-TOUTVIRTUAL 002637. These physical resources are utilized to run the virtualization layer and enable communication, connectivity, security, and management among the virtual assets.

TOUTVIRTUAL 002621-TOUTVIRTUAL 002629.

The Accused Instrumentality provides virtual assets by abstracting hardware components within the virtualization environment that provide compute, network, applications, storage, etc. These virtual assets include, but are not limited to, software-based instantiations of equipment objects such as Azure Virtual Machines (servers) (TOUTVIRTUAL 002238-TOUTVIRTUAL 00224657), Azure Virtual Desktop session hosts (desktops) (TOUTVIRTUAL 002247-TOUTVIRTUAL 002249), Azure Kubernetes Service (“AKS”) nodes and pods (application servers) (TOUTVIRTUAL 002260-

TOUTVIRTUAL 002264), Arc-enabled virtual machines and Kubernetes nodes (on-premises and non-Azure servers) (TOUTVIRTUAL 003217-TOUTVIRTUAL 003219; TOUTVIRTUAL 003220-TOUTVIRTUAL 003224), and storage provided by Azure storage services (storage) (TOUTVIRTUAL 002883-TOUTVIRTUAL 002899). Microsoft Azure's virtualization layer manages these virtual assets which are software instantiations of computer systems by allocating underlying physical resources and controlling execution within the Azure virtualization environment.

The Accused Instrumentality provides a virtualization layer (i.e., Azure Hypervisor and/or Microsoft Hyper-V) on which its Kubernetes-based virtualization services operate, such as AKS, Azure Container Apps, Arc-enabled Kubernetes clusters, and Arc-enabled servers. TOUTVIRTUAL 002986-TOUTVIRTUAL 002988. The Accused Instrumentality implements a virtualization layer on physical servers that abstracts the underlying system and provides a virtualization environment for services and applications, regardless of whether they run in the Azure virtualization environment or on an Arc-enabled infrastructure outside the Azure environment. The Kubernetes-based virtualization services allow for the deployment and management of containerized applications. TOUTVIRTUAL 002260-TOUTVIRTUAL 002264;



TOUTVIRTUAL 002614-TOUTVIRTUAL 002620.

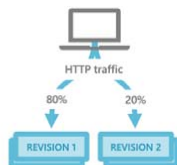
The Accused Instrumentality's virtualization environment provides virtual assets, which include pods, containers, container groups, AKS nodes, Arc-enabled Kubernetes nodes, and deployments. These virtual assets are software instantiations of equipment objects, such as application servers, microservice components, data processing nodes, and workload endpoints. TOUTVIRTUAL

	002260-TOUTVIRTUAL 002264; TOUTVIRTUAL 002614-TOUTVIRTUAL 002620; TOUTVIRTUAL 002649-TOUTVIRTUAL 002650. The Accused Instrumentality’s virtualization environment provides physical resources that support these virtual assets, including Azure Virtual Networks, container network interfaces, AKS networking, ingress controllers, and load balancers that route traffic internally and externally across the virtualization environment. Through Azure Arc, these same network and management capabilities extend to Arc-enabled servers and AKS clusters, allowing Microsoft Azure, including the Accused Instrumentality, to create, configure, monitor, inventory, and control virtualized applications running on non-Azure infrastructure. TOUTVIRTUAL 002134-TOUTVIRTUAL 002137; TOUTVIRTUAL 002138-TOUTVIRTUAL 002142; TOUTVIRTUAL 002646-TOUTVIRTUAL 002648; TOUTVIRTUAL 002649-TOUTVIRTUAL 002650; TOUTVIRTUAL 003205-TOUTVIRTUAL 003208. The Accused Instrumentality provides AKS, which is a Kubernetes management service that allows users to deploy, scale, and manage containerized applications. AKS provides automated upgrades, node health monitoring, workload scheduling, and integration with Azure networking, storage, and security services. AKS relies on Azure virtual machines to serve as Kubernetes worker nodes. TOUTVIRTUAL 002260-TOUTVIRTUAL 002264; TOUTVIRTUAL 002614-TOUTVIRTUAL 002620, TOUTVIRTUAL 002640-TOUTVIRTUAL 002645; TOUTVIRTUAL 002646-TOUTVIRTUAL 002648; TOUTVIRTUAL 002649-TOUTVIRTUAL 002650. The Accused Instrumentality provides Azure Container Apps, which is a container platform that runs microservices, event-driven applications, Application Programming Interfaces (“APIs”), and background jobs without requiring a user to manage the underlying Kubernetes clusters directly. TOUTVIRTUAL 002986-TOUTVIRTUAL 002988. Azure Container Apps leverages Kubernetes, Kubernetes Event-driven Autoscaling (“KEDA”), Distributed Application Runtime (“Dapr”), and Microsoft-managed scale controllers to automatically scale containers based on events, HTTP load, or resource metrics. TOUTVIRTUAL 003095-TOUTVIRTUAL 003103. Container workloads from Azure Container Apps are executed inside managed Kubernetes clusters that run on Azure compute infrastructure. These Azure Container Apps compute hosts are implemented as Azure virtual machines, which run on physical servers controlled by the virtualization layer.
--	--



Azure Container Apps: Example scenarios

PUBLIC API ENDPOINTS



HTTP requests are split between two versions of the container app where the first revision gets 80% of the traffic, while a new revision receives the remaining 20%.

AUTO-SCALE CRITERIA

Scaling is determined by the number of concurrent HTTP requests.

BACKGROUND PROCESSING



A background job that transforms data in a database.

AUTO-SCALE CRITERIA

Triggered by a schedule, on demand, or based on events.

EVENT-DRIVEN PROCESSING

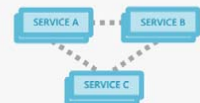


A queue reader application that processes messages as they arrive in a queue.

AUTO-SCALE CRITERIA

Scaling is determined by the number of messages in the queue.

MICROSERVICES



Deploy and manage a microservices architecture with the option to integrate with Dapr.

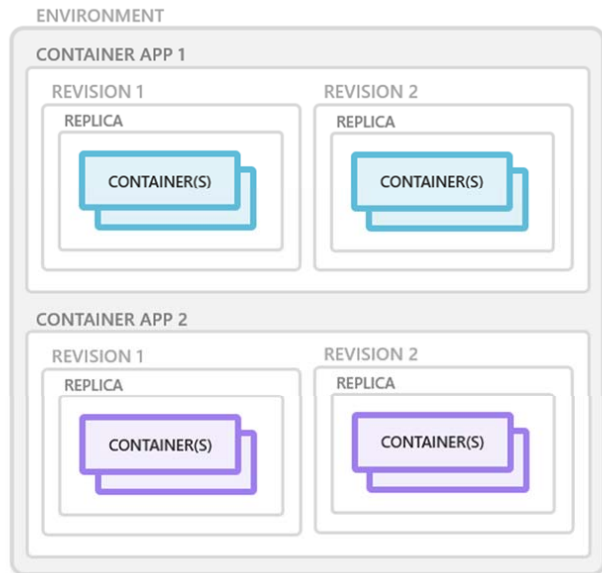
AUTO-SCALE CRITERIA

Individual microservices can scale according to any KEDA scale triggers.

TOUTVIRTUAL 002989-TOUTVIRTUAL 002991;



Containers in an Azure Container Apps environment are grouped together in pods inside revision snapshots.

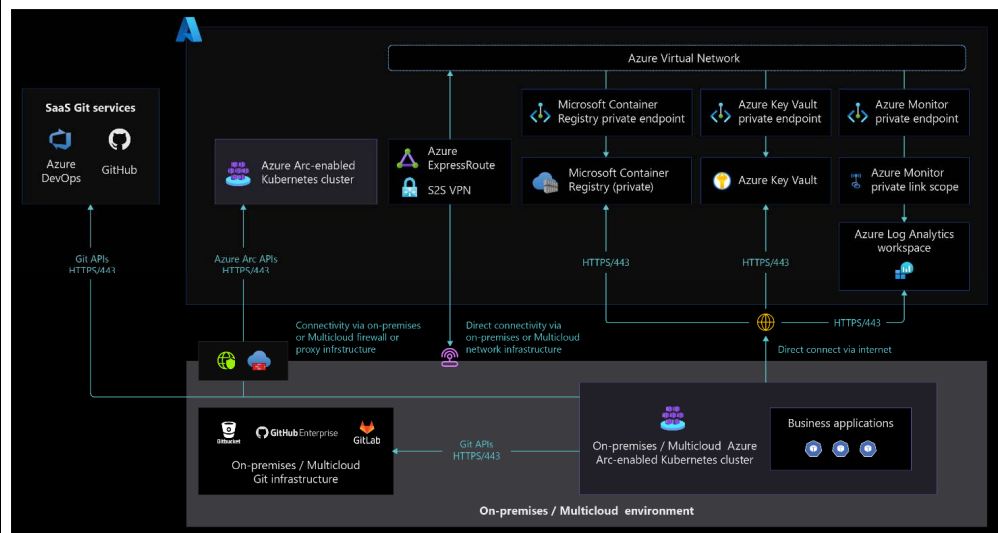


TOUTVIRTUAL 002992-TOUTVIRTUAL 002999; TOUTVIRTUAL 003000-TOUTVIRTUAL 003002; TOUTVIRTUAL 003003-TOUTVIRTUAL 003008.

The Accused Instrumentality provides Azure Arc, which extends management, governance, and Kubernetes orchestration capabilities to infrastructure running outside of the Azure environment, including on-premises servers, edge devices, and other cloud environments. TOUTVIRTUAL 002134-TOUTVIRTUAL 002137. Azure Arc also includes Azure Arc Resource Bridge, which is an appliance that runs in on-premises or edge environments and projects physical resources, such as servers, storage, and Kubernetes infrastructure, into the Azure Controllers (as defined below) as Azure resources. Azure Arc further projects these external systems into the Azure Portal or Windows Admin Center, allowing them to be managed through the same control plane as Azure physical resources and virtual assets. TOUTVIRTUAL 003039-TOUTVIRTUAL 003045.

Azure Arc-enabled Kubernetes integrates external Kubernetes clusters within Azure's control plane. These clusters may run on different environments, such as Hyper-V in on-premises environments,

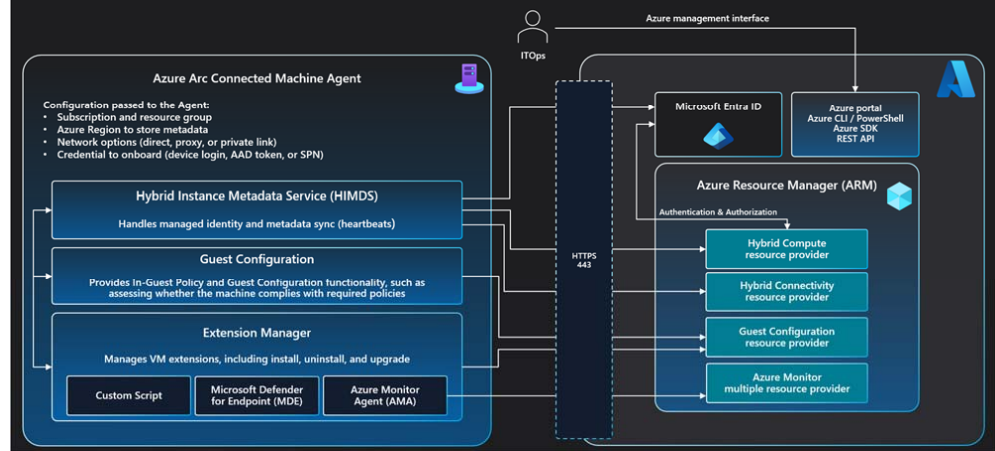
VMware ESXi, bare-metal hardware, or cloud virtual machines in Amazon Web Services, Google Cloud Platform, etc. Regardless of the underlying environment, Azure Arc views these systems as Azure-managed virtual assets. TOUTVIRTUAL 002646-TOUTVIRTUAL 002648; TOUTVIRTUAL 002649-TOUTVIRTUAL 002650; TOUTVIRTUAL 002810-TOUTVIRTUAL 002816;



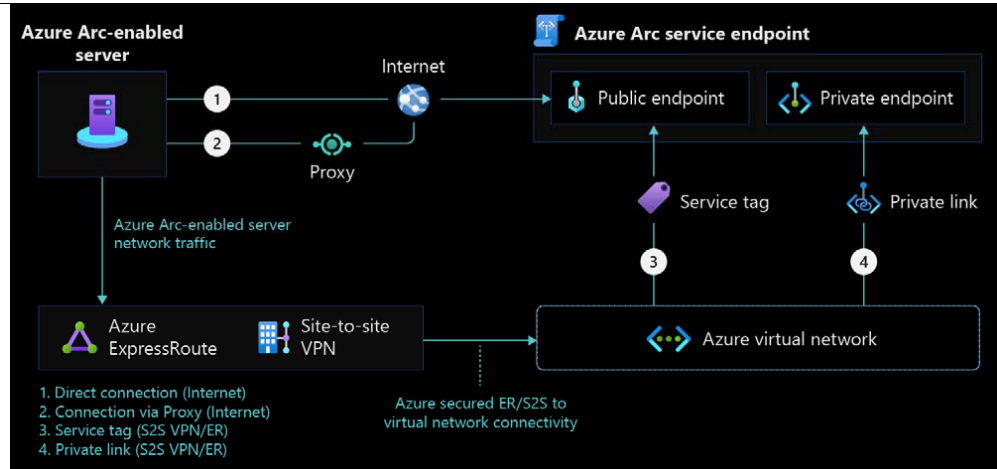
TOUTVIRTUAL 003211-TOUTVIRTUAL 003213; TOUTVIRTUAL 003217-TOUTVIRTUAL 003219; TOUTVIRTUAL 003220-TOUTVIRTUAL 003224.

Arc-enabled servers may run on a local virtualization layer (e.g., Microsoft Hyper-V, Linux KVM, or VMware ESXi) or on bare-metal hardware and connect to the Azure virtualization environment by using Azure Connected Machine agent. An Azure Monitor Agent is utilized to report the server's status to the Azure Portal or Windows Admin Center and to perform Azure functions, but the workloads may also be managed by the external virtualization layer.

Arc-enabled servers – Connected Machine agent architecture



TOUTVIRTUAL 003009-TOUTVIRTUAL 003017;

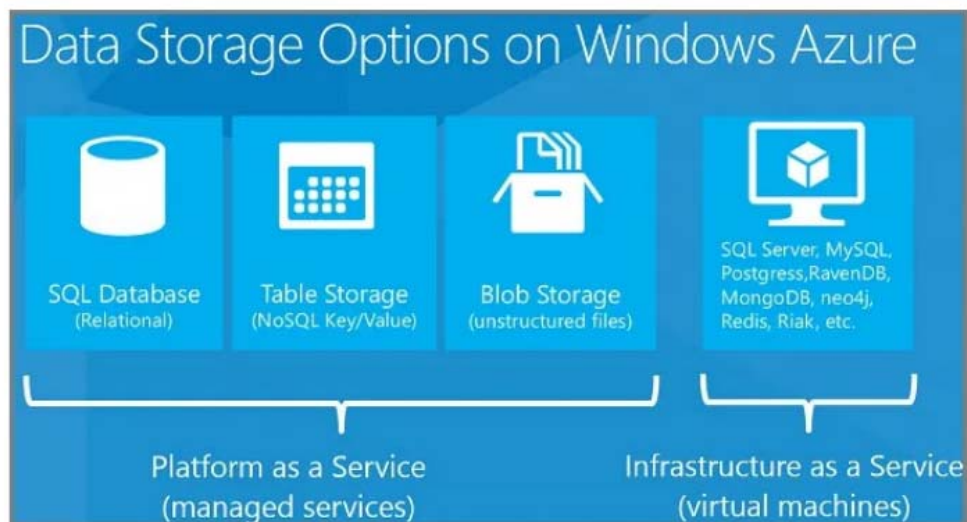


TOUTVIRTUAL 003205-TOUTVIRTUAL 003208.

The Accused Instrumentality provides a virtualization layer (i.e., Azure Hypervisor and/or Microsoft Hyper-V) on which its storage virtualization services operate, such as Azure Blob Storage, Azure Files, Azure Disk Storage, and Azure Elastic Storage Area Network (“SAN”). The Accused Instrumentality implements a virtualization layer on a physical server that abstracts physical storage hardware into logical, managed, network-accessible storage resources. This allows these services to run as virtualized processes or within virtualized partitions isolated from other workloads.

TOUTVIRTUAL 002192-TOUTVIRTUAL 002203; TOUTVIRTUAL 002210-TOUTVIRTUAL 002224;

Azure Storage Services



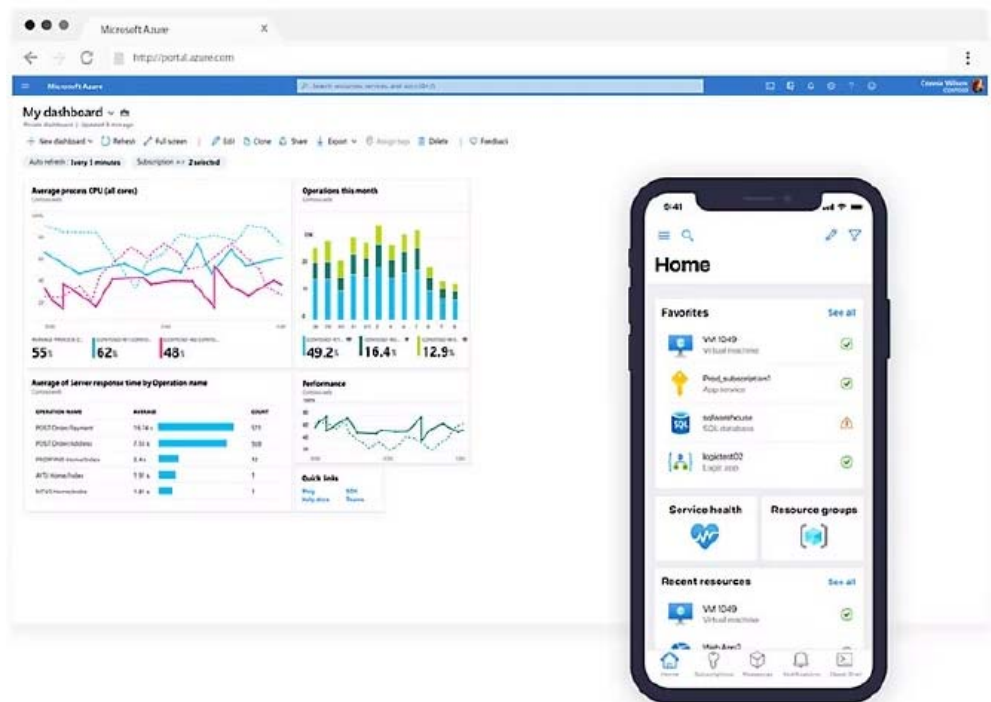
TOUTVIRTUAL 002790-TOUTVIRTUAL 002803; TOUTVIRTUAL 002883-TOUTVIRTUAL 002899.

The Accused Instrumentality provides Azure Blob Storage, which is a massively scalable object-storage platform used to store unstructured data, such as documents, images, logs, backups, and application data. Azure Blob Storage virtualizes physical storage hardware across Microsoft datacenters, presenting a logical, distributed object-storage system that automatically handles replication, redundancy, durability, and global accessibility. TOUTVIRTUAL 002204-TOUTVIRTUAL 002209.

The Accused Instrumentality provides Azure Files, which provides fully managed, cloud-based file shares accessible via SMB (Server Message Block) and NFS (Network File System) protocols. Azure Files virtualizes storage so that a user may receive network-attached file shares without managing physical NAS (Network Attached Storage) appliances, file servers, RAID (Redundant Array of Independent Disks) storage, or storage controllers. Azure Files runs on Azure storage

	cluster nodes, which are virtualized or containerized storage processes executing on servers in Microsoft datacenters. TOUTVIRTUAL 003021-TOUTVIRTUAL 003023. The Accused Instrumentality provides Azure Disk Storage, which provides block-level VHDs (Virtual Hard Disks) used by Azure virtual machines, AKS node pools, database systems, and other workloads requiring persistent block devices. Each managed disk is a virtual abstraction of block storage that is presented to a virtual machine as if it was an attached physical disk. Azure Disk Storage is supported by storage services running on servers in Microsoft datacenters. TOUTVIRTUAL 003024-TOUTVIRTUAL 003028. The Accused Instrumentality provides Azure Elastic SAN, which is Azure’s cloud-native storage service, providing high-performance block storage volumes grouped in SAN arrays accessible by multiple Azure virtual machines or compute clusters. Azure Elastic SAN replicates the architecture of on-premises SANs but fully virtualize the physical storage fabric and controllers. Azure Elastic SAN includes virtualized SAN arrays, virtualized storage pools, virtualized block volumes, and controllers for provisioning, zoning, and quality control. Azure Elastic SAN runs on Azure storage clusters built on physical servers in Microsoft datacenters. TOUTVIRTUAL 003029-TOUTVIRTUAL 003031. The Accused Instrumentality includes Azure Functions, which provides a virtualization environment that has a virtualization layer created by the Azure Hypervisors. Azure Functions automatically manages physical resources and virtual assets for the user without having the user manage the underlying infrastructure. Azure Functions provides an environment where program code is run on an event-driven basis in a virtual environment without the user specifying a particular environment. TOUTVIRTUAL 002804-TOUTVIRTUAL 002806. For example, Azure Functions may operate in response to events such as HTTP requests or the creation of files. Azure Functions creates virtual assets in the form of software instantiations of equipment objects in the virtualization environment automatically based on the needs of the operation of the program code that is being run, with the virtualization layer managing the virtual assets. Azure Functions operate in a virtualized manner where it may connect to other Azure services using bindings for compute, network, application, and storage. TOUTVIRTUAL 003032-TOUTVIRTUAL 003038.
1[b]. receiving a virtual asset provisioning request that specifies parameters to be	The Accused Instrumentality meets the recited claim language because it provides controllers, such as Azure Portal and/or Windows Admin Center (“WAC”) (both including all supporting functionality used for management, such as Azure Resource Manager (“ARM”) and Azure Automation) (hereinafter, “Azure Controllers”), that receive virtual asset provisioning requests that specify parameters to be considered. The Azure Controllers may run on a specific physical resource (i.e., server) located in Microsoft’s datacenters. TOUTVIRTUAL 003820-TOUTVIRTUAL

considered for the virtual asset provisioning request;	003823; TOUTVIRTUAL 003824-TOUTVIRTUAL 003828; TOUTVIRTUAL 003829-TOUTVIRTUAL 003831. Azure Portal and WAC include the different services identified below. The Accused Instrumentality provides Azure Portal, which may receive a virtual asset provisioning request either from a user, application, or automated network workflow. After receiving the request, Azure Portal may request additional resources or provision the necessary virtual assets through API-driven deployment, ARM templates, or Autoscale triggers (via Azure Monitor). Azure Portal may receive API calls from services, such as Azure Virtual Machine Scale Sets (“VMSS”), AKS, Azure Functions, and Azure Automation, for the provisioning of virtual assets. When Azure services detect increased network load or user activity, these services may communicate with Azure Portal over a network to provision additional virtual assets, such as new virtual machines, container pods, or serverless compute instances, on the virtualization layer. Azure Portal may then allocate compute, network, application, and storage resources from the available capacity in the Azure virtualization environment, configuring each new instance, and updating the system’s resource inventory in real time.
---	---

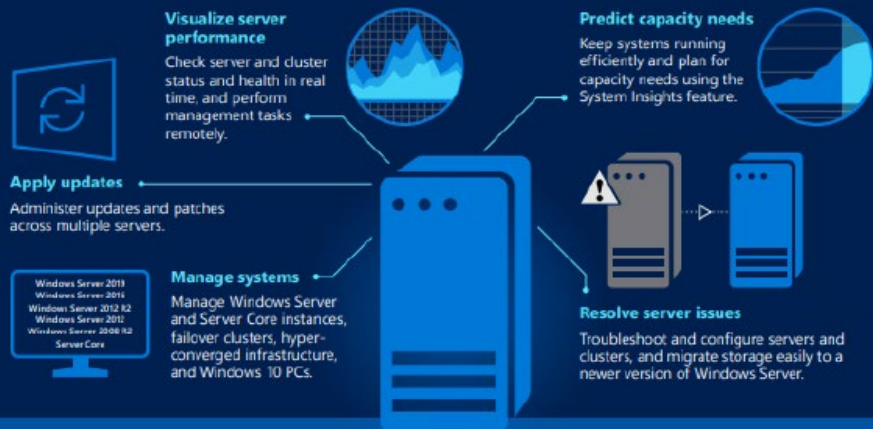


TOUTVIRTUAL 002509-TOUTVIRTUAL 002511; TOUTVIRTUAL 002124-TOUTVIRTUAL 002129; TOUTVIRTUAL 002503-TOUTVIRTUAL 002508.

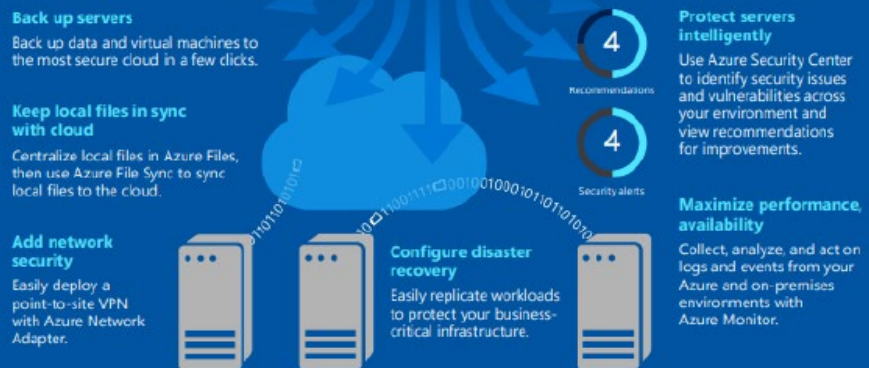
The Accused Instrumentality provides WAC, which integrates with Azure Arc to provision virtual assets in response to network workflow demands, particularly within hybrid Azure virtualization environments (i.e., virtualization environments consisting of Azure systems and non-Azure Arc-enabled systems). WAC communicates directly with hosts, servers or server clusters to deploy new virtual machines and virtual networks within or outside of the Azure infrastructure, including on-premises datacenters and other cloud platforms, in response to increased workload or network demand. WAC may initiate provisioning operations by receiving API calls from Azure VMSS, AKS, Azure Functions, and Azure Automation; and deploy virtual machines, containers, or

	serverless compute instances to handle workload surges originating from on-premises or edge environments. For example, users may submit virtual asset provisioning requests to WAC, which may include the parameters to be considered for the virtual asset provisioning request. WAC, via ARM, may then initialize the virtual asset. TOUTVIRTUAL 002571-TOUTVIRTUAL 002575; TOUTVIRTUAL 002130-TOUTVIRTUAL 002133;
--	--

Streamline management tasks



Extend your on-premises environment with Azure integrations



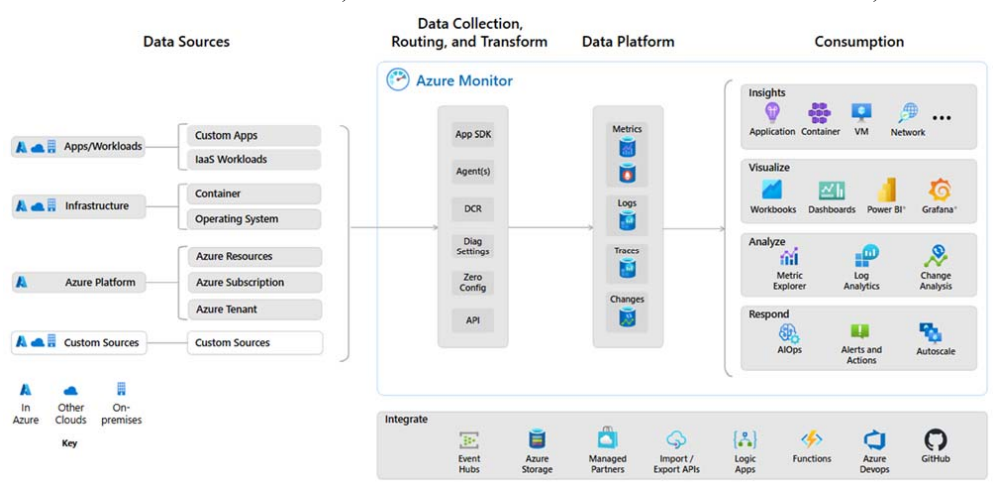
	TOUTVIRTUAL 002596-TOUTVIRTUAL 002597. The Accused Instrumentality provides Azure Controllers that may perform this provisioning functionality for an Azure Container Apps environment. TOUTVIRTUAL 003225-TOUTVIRTUAL 003237. For example, when workflow demands increase (e.g., rising HTTP request rates, queue depth, event stream activity, or custom metric thresholds), Azure Container Apps’s Kubernetes Event-Driven Autoscaling (“KEDA”) rules generate signals that Azure Controllers evaluate against the physical resource’s configuration. TOUTVIRTUAL 003095-TOUTVIRTUAL 003103. These virtual asset provisioning requests specify the parameters of the virtual assets that are being requested. Azure Controllers may then provision additional container replicas, new revisions, or job executions within the Azure Container Apps environment. Azure Controllers may also provision supporting physical resources whenever Azure Container Apps workloads scale or new applications are deployed. TOUTVIRTUAL 003238-TOUTVIRTUAL 003239. The Azure Controllers may perform this provisioning functionality for applications running in AKS. TOUTVIRTUAL 003240-TOUTVIRTUAL 003241. Workflow signals from Kubernetes components, such as Horizontal Pod Autoscaler metrics, Vertical Pod Autoscaler recommendations, or Cluster Autoscaler node-capacity triggers, cause Azure Controllers to request additional underlying resources based on the specified parameters in the provisioning request. Azure Controllers may then respond to this request by provisioning new virtual machines, expanding node pools, or deploying additional Kubernetes workloads as specified, thereby establishing a provisioned virtualization environment. TOUTVIRTUAL 003104-TOUTVIRTUAL 003108. The Azure Controllers may perform this provisioning functionality for applications running within private or on-premises environments, or Arc-enabled Kubernetes through Azure Arc. The Azure Controllers, via Azure Arc Resource Bridge, may provide custom locations within the private or on-premises environments, Kubernetes nodes, pods, container workloads, network endpoints, or security configurations which are considered when a virtual asset provisioning request is made. TOUTVIRTUAL 003039-TOUTVIRTUAL 003045; TOUTVIRTUAL 005089-TOUTVIRTUAL 005091. After validating the virtual asset provisioning request, the Azure Controllers, via Azure Arc, may use the custom locations to automatically provision on-premises environment or Kubernetes resources to fulfill the virtual asset provisioning request. For example, if a virtual asset’s workload increases, the Azure Controllers via Azure Arc may automatically provision more resources from the on-premises environment or Kubernetes nodes pods, container workloads, network endpoints, and security configurations.
--	--

	The Azure Controllers may provision storage virtual assets in response to workflow demands, such as Blob Storage accounts, file shares, managed disks, Elastic SAN volumes, and other storage service instances. This enables Azure Controllers to allocate the required storage capacity or resources to the provisioning request based on the specified parameters. For example, if an application workload experiences heavy growth, Azure Controllers may determine via Autoscale rules or workflow logic that additional storage throughput or capacity is required. TOUTVIRTUAL 002869-TOUTVIRTUAL 002882. Azure Controllers may then provision additional Blob Storage containers, create new managed disk volumes for new virtual machines being scaled out, or configures additional Elastic SAN volumes and attaches them to VMSS. Azure Controllers may also create or dynamically scale storage accounts using ARM templates or Automation runbooks triggered by workflow conditions (e.g., data ingestion spike). TOUTVIRTUAL 002166-TOUTVIRTUAL 002171; TOUTVIRTUAL 002598-TOUTVIRTUAL 002603; TOUTVIRTUAL 002604-TOUTVIRTUAL 002613; TOUTVIRTUAL 002937-TOUTVIRTUAL 002946. When storage demand decreases or shifts, Azure Controllers may also de-provision or reallocate storage assets (e.g., shrink file share quotas, decommission unused managed disks) through Automation tasks. The Accused Instrumentality provides VMSS, AKS, Azure Functions, and Azure Automation, which represent specific Azure services that implement the provisioning actions directed by the Azure Controllers. VMSS provisions and scales virtual machines based on demand metrics. AKS provisions container pods and cluster nodes in response to network traffic and workload signals. Azure Functions provisions containers in response to network-based triggers such as HTTP requests or message events. Azure Automation provisions virtual assets in response to network workflow demands by executing runbooks and workflows that monitor operational metrics and automatically trigger provisioning events. TOUTVIRTUAL 002166-TOUTVIRTUAL 002171. Each of these services provides virtual asset provisioning requests that specify parameters to be considered, and each service communicates via the virtualization layers to create, configure, and manage the resulting virtual assets. TOUTVIRTUAL 003126-TOUTVIRTUAL 003135; TOUTVIRTUAL 003136-TOUTVIRTUAL 003142; TOUTVIRTUAL 003143-TOUTVIRTUAL 003147; TOUTVIRTUAL 003148-TOUTVIRTUAL 003153. Azure Controllers may also provision virtual resources in response to workflow demands for event-driven actions, such as through the Azure Functions to establish a provisioned virtualization environment. TOUTVIRTUAL 003154-TOUTVIRTUAL 003162.
--	--

1[c].
receiving data on inventory
available in the virtualization
system;

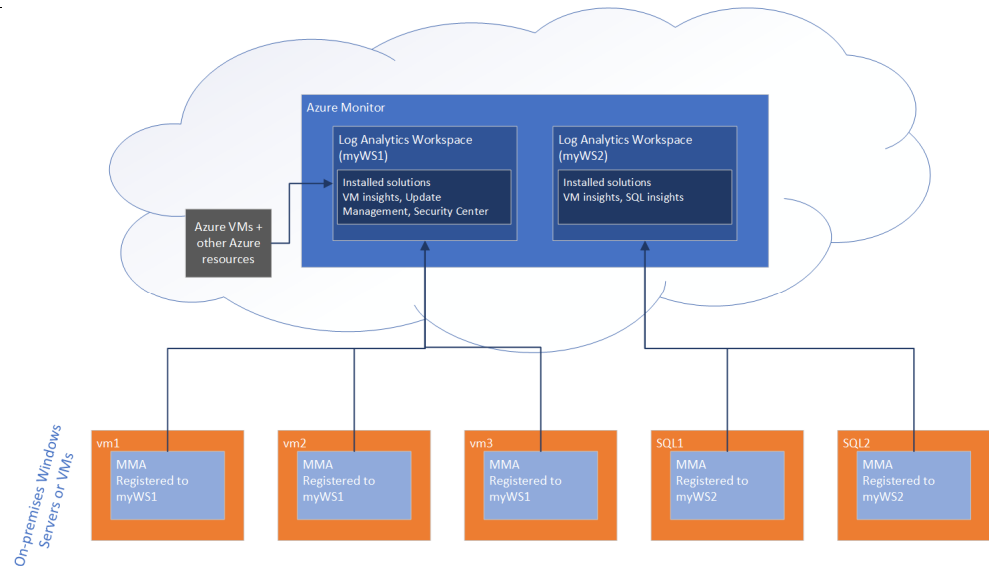
The Accused Instrumentality meets the recited claim language because each Azure Controller receives data on inventory available in the virtualization system.

The Accused Instrumentality provides Azure Portal, which may receive data on inventory available in the virtualization system and maintains a real-time inventory, for example, via the Azure Monitor (TOUTVIRTUAL 002733-TOUTVIRTUAL 002737; TOUTVIRTUAL 002738-TOUTVIRTUAL 002745), Azure Automation (TOUTVIRTUAL 002166-TOUTVIRTUAL 002171; TOUTVIRTUAL 003178-TOUTVIRTUAL 003190), Azure Resource Graph (TOUTVIRTUAL 003191-TOUTVIRTUAL 003194; TOUTVIRTUAL 002721-TOUTVIRTUAL 002727; TOUTVIRTUAL 002817-TOUTVIRTUAL 002834; TOUTVIRTUAL 002835-TOUTVIRTUAL 002840), Azure Policy (TOUTVIRTUAL 002172-TOUTVIRTUAL 002181), or Azure Role-Based Access Control (“RBAC”) (TOUTVIRTUAL 002182-TOUTVIRTUAL 002189) of all virtual assets and physical resources within a user’s network. Azure Portal, via ARM, may assign each asset and resource with a unique identifier, resource type, and metadata that defines its state, dependencies, and relationships to other components in the virtualization environment. This metadata is stored and continuously updated within Azure Portal’s resource management database. TOUTVIRTUAL 002124-TOUTVIRTUAL 002129; TOUTVIRTUAL 002638-TOUTVIRTUAL 002639;



TOUTVIRTUAL 002265-TOUTVIRTUAL 002280; TOUTVIRTUAL 003169-TOUTVIRTUAL 003173.

	The Accused Instrumentality provides WAC, which may provide identification and management capabilities for hosts, servers, server clusters, and virtual machines, running outside of the infrastructure of the Accused Instrumentality, including on-premises datacenters and other cloud platforms, including those provided by other vendors. WAC connects to the virtualization layers over a network and identifies the available virtual machines, networks, and storage pools. When integrated with Azure Arc (TOUTVIRTUAL 002134-TOUTVIRTUAL 002137), WAC extends this management to connected resources outside of the Azure infrastructure and synchronizes inventory and status data with the Azure virtualization environment, providing a user an inventory of all its connections and other identification and management Azure products that may be used with Azure Portal, like Azure Monitor (TOUTVIRTUAL 002265-TOUTVIRTUAL 002280; TOUTVIRTUAL 002733-TOUTVIRTUAL 002737; TOUTVIRTUAL 002738-TOUTVIRTUAL 002745), Azure Automation (TOUTVIRTUAL 002166-TOUTVIRTUAL 002171; TOUTVIRTUAL 003178-TOUTVIRTUAL 003190), Azure Resource Graph (TOUTVIRTUAL 003191-TOUTVIRTUAL 003194; TOUTVIRTUAL 002721-TOUTVIRTUAL 002727, TOUTVIRTUAL 002817-TOUTVIRTUAL 002834; TOUTVIRTUAL 002835-TOUTVIRTUAL 002840), Azure Policy (TOUTVIRTUAL 002172-TOUTVIRTUAL 002181), and Azure RBAC (TOUTVIRTUAL 002182-TOUTVIRTUAL 002189). Through this connection, the user may view, configure, or migrate virtual assets between local and cloud environments, all while maintaining a single identified resource set. TOUTVIRTUAL 002571-TOUTVIRTUAL 002575; TOUTVIRTUAL 002130-TOUTVIRTUAL 002133;
--	---

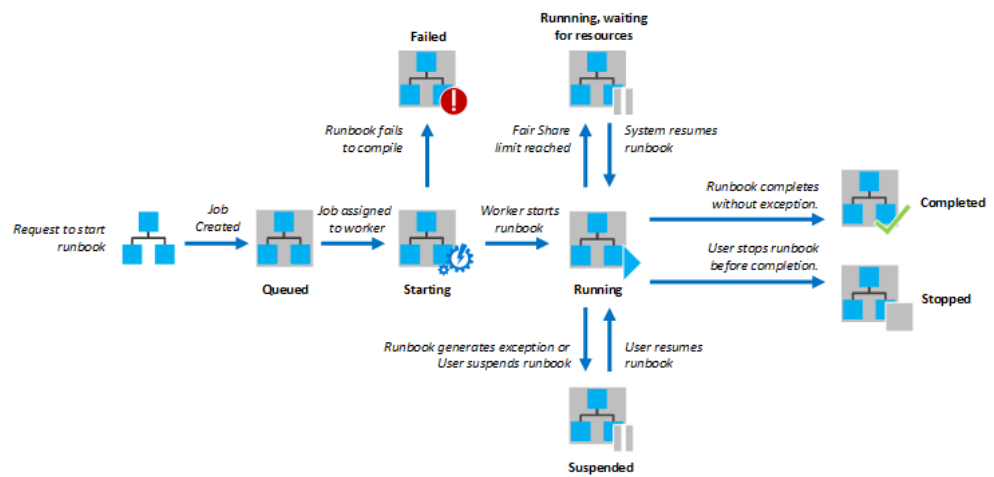


TOUTVIRTUAL 003174-TOUTVIRTUAL 003177.

The Azure Controllers may retrieve, display, and manage the identified physical resources and virtual assets. Azure Controllers visualize this information as a hierarchical resource map that shows, for example, how a virtual machine connects to a network, subnet, and virtual network, providing the relationships and configurations of the virtual assets. Through the Azure Controllers, a user can perform management actions (such as start, stop, reconfigure, or delete) that are transmitted to ARM, which in turn executes those commands on the virtualization layers. TOUTVIRTUAL 002143-TOUTVIRTUAL 002149.

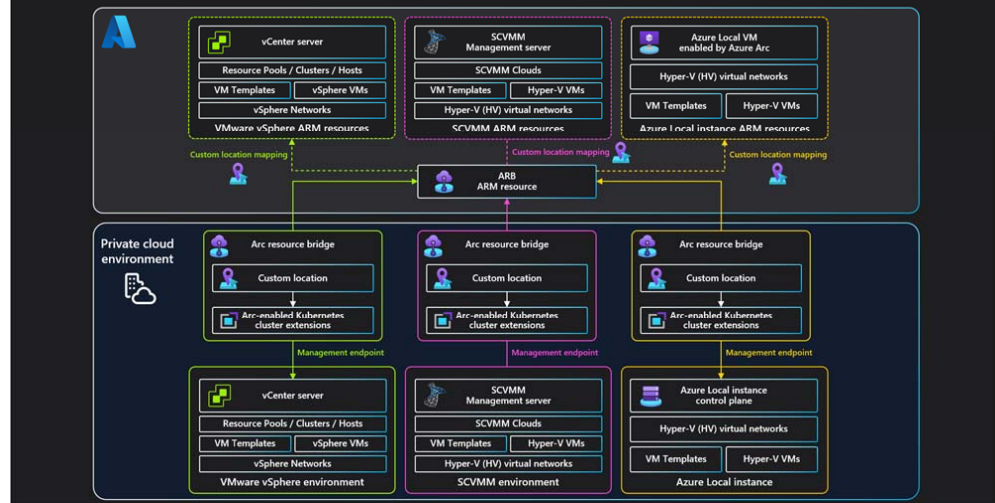
The Azure Controllers may utilize other identification and management Azure products, like Azure Monitor (TOUTVIRTUAL 002265-TOUTVIRTUAL 002280; TOUTVIRTUAL 002733-TOUTVIRTUAL 002737; TOUTVIRTUAL 002738-TOUTVIRTUAL 002745), Azure Automation (TOUTVIRTUAL 002166-TOUTVIRTUAL 002171; TOUTVIRTUAL 003178-TOUTVIRTUAL 003190), Azure Resource Graph (TOUTVIRTUAL 003191-TOUTVIRTUAL 003194; TOUTVIRTUAL 002721-TOUTVIRTUAL 002727; TOUTVIRTUAL 002817-TOUTVIRTUAL 002834; TOUTVIRTUAL 002835-TOUTVIRTUAL 002840), Azure Policy (TOUTVIRTUAL

002172-TOUTVIRTUAL 002181), and Azure RBAC (TOUTVIRTUAL 002182-TOUTVIRTUAL 002189). Azure Monitor collects, analyzes, and responds to monitoring data. Azure Automation integrates with Azure Monitor, enabling Azure Controllers to retrieve telemetry data and apply management policies based on resource health or performance status. Using runbooks (scripted workflows), Azure Automation continuously checks the configurations and status of virtual machines, networks, and storage registered with the Azure Controllers. Azure Resource Graph enables cross-resource querying and inventory management, while Azure Policy and Azure RBAC enforce consistent management and compliance rules across identified assets. The Azure Controllers may present this data and these identification and management Azure products visually, allowing users to apply, modify, or audit them. TOUTVIRTUAL 002937-TOUTVIRTUAL 002946;

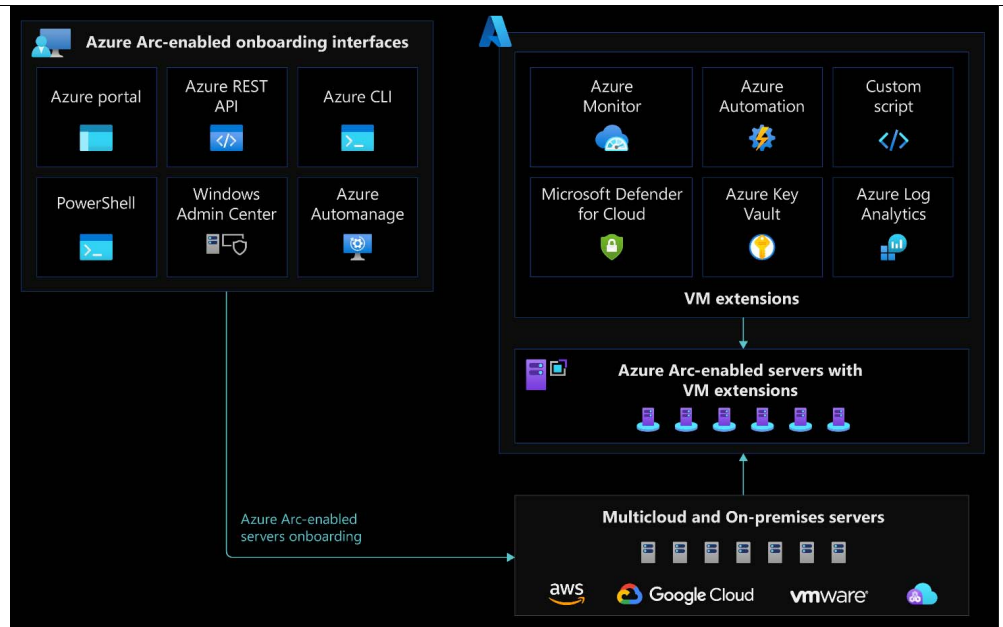


TOUTVIRTUAL 002947-TOUTVIRTUAL 002956;

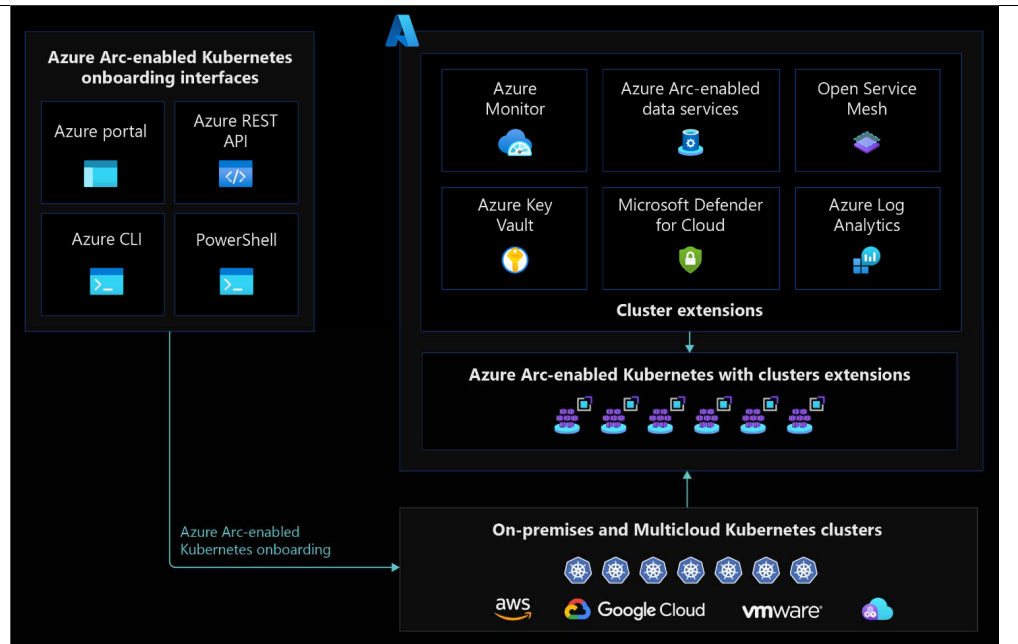
Arc resource bridge (ARB) – Solution architecture



TOUTVIRTUAL 003039-TOUTVIRTUAL 003045. By establishing a secure control-plane connection between the external infrastructure and the Azure infrastructure with Azure Arc and Azure Arc Resource Bridge, the Azure Controllers automatically discovers and inventories the external systems' physical resources and virtual assets, such as Arc-enabled virtual machines, physical or virtual servers, Arc-enabled Kubernetes nodes, pods, container workloads, network endpoints, and security configurations. TOUTVIRTUAL 002746-TOUTVIRTUAL 002748; TOUTVIRTUAL 002749-TOUTVIRTUAL 002759; TOUTVIRTUAL 002810-TOUTVIRTUAL 002816;



TOUTVIRTUAL 003201-TOUTVIRTUAL 003204;



TOUTVIRTUAL 003214-TOUTVIRTUAL 003216.

The Azure Controllers may receive data on the inventory available of container-based virtual assets with AKS. Azure Controllers may automatically inventory clusters, node pools, pods, deployments, load balancers, Kubernetes components, and persistent volumes. TOUTVIRTUAL 002640-TOUTVIRTUAL 002645.

The Azure Controllers may receive data on inventory available within an Azure Container Apps environment, which functions as a secure boundary that contains multiple container apps, jobs, and revisions. TOUTVIRTUAL 003046-TOUTVIRTUAL 003049. Azure Controllers automatically identify and manage the container apps deployed in each environment, along with their associated virtual assets such as revisions, scaling rules, ingress, configurations, and container replicas. An Azure Container Apps environment is associated with physical resources, including virtual networks, subnets, container network interfaces, and ingress endpoints, that Azure identifies for

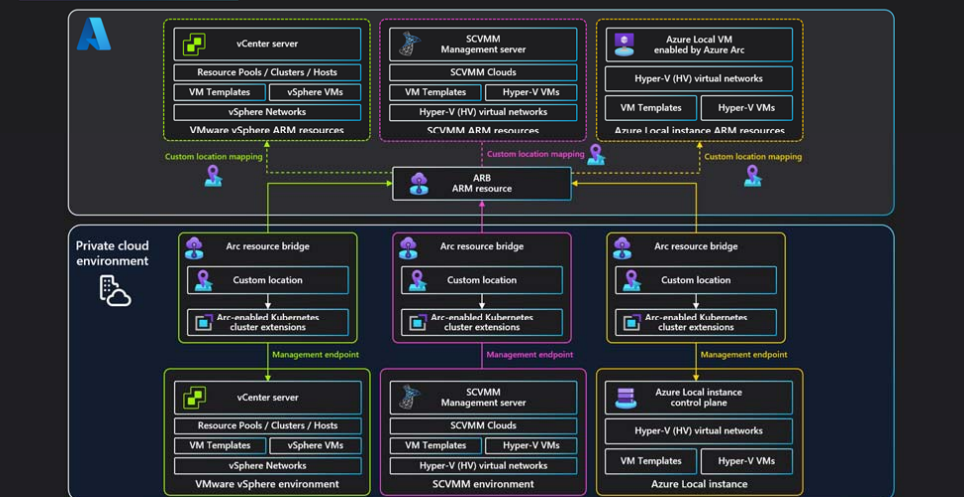
	management. TOUTVIRTUAL 003058-TOUTVIRTUAL 003061. An Azure Container Apps environment also shares a centralized logging and monitoring workspace, allowing Azure Controllers to uniformly track and manage virtual assets across all applications connected to the Azure virtualization environment and determine an inventory of network resources and virtual assets available to the virtualization environment. TOUTVIRTUAL 003000-TOUTVIRTUAL 003002; TOUTVIRTUAL 003050-TOUTVIRTUAL 003057; TOUTVIRTUAL 002225-TOUTVIRTUAL 002226; TOUTVIRTUAL 002900-TOUTVIRTUAL 002908; TOUTVIRTUAL 003729-TOUTVIRTUAL 003736. The Azure Controllers may identify each storage account or container as a managed object, tracks its provisioning, configuration, replication settings, encryption status, lifecycle policies, and cost/performance metadata. Through Azure Monitor and Azure Resource Graph, Azure Controllers may receive metrics, like latency, capacity, throughput, for each storage virtual asset, enabling Azure Controllers to manage them alongside compute, network, applications, and storage resources. TOUTVIRTUAL 002855-TOUTVIRTUAL 002868; TOUTVIRTUAL 002810-TOUTVIRTUAL 002816; TOUTVIRTUAL 002817-TOUTVIRTUAL 002834; TOUTVIRTUAL 002835-TOUTVIRTUAL 002840; TOUTVIRTUAL 002841-TOUTVIRTUAL 002847. Through AKS and Azure Container Apps, container workloads and Kubernetes pods often rely on persistent volumes, file shares, or blob storage. Azure Controllers may identify these storage assets and their relationships to workloads, enabling unified lifecycle and performance management across compute, network, applications, and storage domains. Through Azure Arc, Arc-enabled servers and Kubernetes clusters may run workloads that access on-premises SANs, file shares, or cloud storage. Azure Controllers may identify and manage these storage resources through Arc agents, treating external storage shares, caching gateways, and edge-appliances as virtual assets within the same Azure inventory. TOUTVIRTUAL 002134-TOUTVIRTUAL 002137; TOUTVIRTUAL 002746-TOUTVIRTUAL 002748; TOUTVIRTUAL 002749-TOUTVIRTUAL 002759; TOUTVIRTUAL 003109-TOUTVIRTUAL 003118. The Azure Controllers may also receive data of the inventory available of physical resources and virtual assets in response to event-driven events, such as through Azure Functions. The Azure Controllers will automatically manage the physical resources and virtual assets as needed in response to the code that is being run in Azure Functions. TOUTVIRTUAL 002804-TOUTVIRTUAL 002806; TOUTVIRTUAL 003062-TOUTVIRTUAL 003079.
--	---

1[d]. automatically provisioning of a particular virtual asset to a particular physical resource in the virtualization system that matches the parameters in the virtual asset provisioning request;	The Accused Instrumentality meets the recited claim language because each Azure Controller automatically provisions a particular virtual asset to a particular physical resource in the virtualization system that matches the parameters in the virtual asset provisioning request. The Accused Instrumentality provides Azure Portal, which may receive a virtual asset provisioning request either from a user, application, or automated network workflow. After receiving the request, Azure Portal may request additional resources, or Azure Portal may provision the necessary virtual assets through API-driven deployment, ARM templates, or Autoscale triggers (via Azure Monitor). TOUTVIRTUAL 002704-TOUTVIRTUAL 002710; TOUTVIRTUAL 002711-TOUTVIRTUAL 002720. Azure Portal receives API calls from services including Azure VMSS (TOUTVIRTUAL 002964-TOUTVIRTUAL 002977), AKS, Azure Functions, and Azure Automation for provisioning of virtual assets. When these services detect increased network load or user activity, they communicate with Azure Portal over a network to provision particular, additional virtual assets, such as new virtual machines, container pods, or serverless compute instances, on the virtualization layer. Azure Portal then allocates particular compute, network, application, and storage resources from the available capacity in the Azure virtualization environment, configuring each new instance, and updating the system's resource inventory in real time, thereby establishing a provisioned virtualization environment. TOUTVIRTUAL 002721-TOUTVIRTUAL 002727; TOUTVIRTUAL 002728-TOUTVIRTUAL 002732; TOUTVIRTUAL 002869-TOUTVIRTUAL 002882. The Accused Instrumentality provides WAC, which may integrate with Azure Arc to provision virtual assets in response to network workflow demands, particularly within hybrid Azure virtualization environments (i.e., virtualization environments consisting of Azure systems and non-Azure Arc-enabled systems). WAC communicates directly with hosts, servers or server clusters to deploy new virtual machines and virtual networks within or outside of the Azure infrastructure, including on-premises datacenters and other cloud platforms, in response to increased workload or network demand. WAC may initiate provisioning operations by receiving API calls from Azure VMSS, AKS, Azure Functions, and Azure Automation; and deploy virtual machines, containers, or serverless compute instances to handle workload surges originating from on-premises or edge environments. TOUTVIRTUAL 002543-TOUTVIRTUAL 002552; TOUTVIRTUAL 003084-TOUTVIRTUAL 003088; TOUTVIRTUAL 003089-TOUTVIRTUAL 003094. The Azure Controllers may perform this provisioning functionality for an Azure Container Apps environment. TOUTVIRTUAL 003225-TOUTVIRTUAL 003237. When workflow demands increase (e.g., rising HTTP request rates, queue depth, event stream activity, or custom metric thresholds), Azure Container Apps's Kubernetes Event-Driven Autoscaling ("KEDA") rules generate signals that Azure Controllers evaluate against the physical resource's configuration. TOUTVIRTUAL 003095-TOUTVIRTUAL 003103. Azure Controllers may then provision
--	---

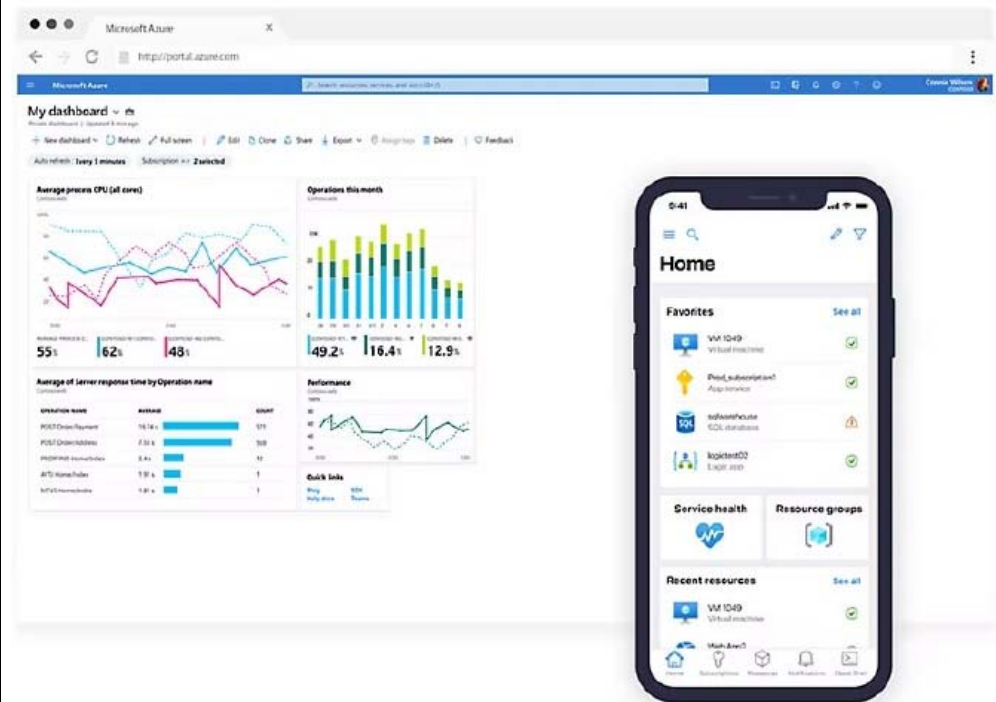
	additional container replicas, new revisions, or job executions within the Azure Container Apps environment. Azure Controllers may also provision supporting physical resources whenever Azure Container Apps workloads scale or new applications are deployed. TOUTVIRTUAL 003238-TOUTVIRTUAL 003239; TOUTVIRTUAL 003737-TOUTVIRTUAL 003740. The Azure Controllers may perform this provisioning functionality for applications running in AKS. TOUTVIRTUAL 003240-TOUTVIRTUAL 003241. Workflow signals from Kubernetes components, such as Horizontal Pod Autoscaler metrics, Vertical Pod Autoscaler recommendations, or Cluster Autoscaler node-capacity triggers, cause Azure Controllers to request additional underlying resources. Azure Controllers may then respond to this request by provisioning new virtual machines, expanding node pools, or deploying additional Kubernetes workloads as specified, thereby establishing a provisioned virtualization environment. TOUTVIRTUAL 003104-TOUTVIRTUAL 003108. The Azure Controllers may perform this provisioning functionality for applications running within private or on-premises environments, or Arc-enabled Kubernetes through Azure Arc. The Azure Controllers, via Azure Arc Resource Bridge, may provide custom locations within the private or on-premises environments, Kubernetes nodes, pods, container workloads, network endpoints, or security configurations which are considered when a virtual asset provisioning request is made. TOUTVIRTUAL 003039-TOUTVIRTUAL 003045; TOUTVIRTUAL 005089-TOUTVIRTUAL 005091. After validating the virtual asset provisioning request, the Azure Controllers, via Azure Arc, may use the custom locations to automatically provision on-premises environment or Kubernetes resources to fulfill the virtual asset provisioning request. For example, if a virtual asset's workload increases, the Azure Controllers via Azure Arc may automatically provision more resources from the on-premises environment or Kubernetes nodes pods, container workloads, network endpoints, and security configurations. The Azure Controllers may provision storage virtual assets in response to workflow demands, such as Blob Storage accounts, file shares, managed disks, Elastic SAN volumes, and other storage service instances. This enables Azure Controllers to allocate the required storage capacity or resources. For example, if an application workload experiences heavy growth, Azure Controllers may determine via Autoscale rules or workflow logic that additional storage throughput or capacity is required. TOUTVIRTUAL 002869-TOUTVIRTUAL 002882. Azure Controllers may then provision additional Blob Storage containers, create new managed disk volumes for new virtual machines being scaled out, or configures additional Elastic SAN volumes and attaches them to VMSS. Azure Controllers may also create or dynamically scale storage accounts using ARM templates or Automation runbooks triggered by workflow conditions (e.g., data ingestion spike). TOUTVIRTUAL 002166-TOUTVIRTUAL 002171; TOUTVIRTUAL 002598-TOUTVIRTUAL
--	--

	002603; TOUTVIRTUAL 002604-TOUTVIRTUAL 002613; TOUTVIRTUAL 002937-TOUTVIRTUAL 002946. When storage demand decreases or shifts, Azure Controllers may also de-provision or reallocate storage assets (e.g., shrink file share quotas, decommission unused managed disks) through Automation tasks. The Accused Instrumentality provides VMSS, AKS, Azure Functions, and Azure Automation which represent specific Azure services that implement the provisioning actions directed by the Azure Controllers. VMSS provisions and scales virtual machines based on demand metrics. AKS provisions container pods and cluster nodes in response to network traffic and workload signals. Azure Functions provisions containers in response to network-based triggers such as HTTP requests or message events. Azure Automation provisions virtual assets in response to network workflow demands by executing runbooks and workflows that monitor operational metrics and automatically trigger provisioning events. TOUTVIRTUAL 002166-TOUTVIRTUAL 002171. Each of these services communicates via the virtualization layers to create, configure, and manage the resulting virtual assets. TOUTVIRTUAL 003126-TOUTVIRTUAL 003135; TOUTVIRTUAL 003136-TOUTVIRTUAL 003142; TOUTVIRTUAL 003143-TOUTVIRTUAL 003147; TOUTVIRTUAL 003148-TOUTVIRTUAL 003153. Azure Controllers can also provision virtual resources to, for example, respond to workflow demands for event-driven actions, such as through the Azure Functions to establish a provisioned virtualization environment. TOUTVIRTUAL 003154-TOUTVIRTUAL 003162.
1[e]. assigning the provisioned virtual asset to the virtual asset provisioning request; and	The Accused Instrumentality meets the recited claim language because after provisioning a virtual asset in response to a user or API-initiated provisioning request, each Azure Controller assigns the provisioned virtual asset to the corresponding virtual asset provisioning request by mapping the newly provisioned asset to the request's parameters and metadata. The Accused Instrumentality provides Azure Controllers, which may process the request and execute the provisioning of the virtual asset through the appropriate Azure resource provider (e.g., Microsoft.Compute, Microsoft.ContainerService, Microsoft.Storage). TOUTVIRTUAL 005092-TOUTVIRTUAL 005106; TOUTVIRTUAL 005115-TOUTVIRTUAL 005303; TOUTVIRTUAL 005304-TOUTVIRTUAL 005348, TOUTVIRTUAL 005349-TOUTVIRTUAL 005371; TOUTVIRTUAL 005372-TOUTVIRTUAL 005378; TOUTVIRTUAL 005379-TOUTVIRTUAL 005617. For example, once the virtual asset is provisioned, the Azure Controllers assign that asset to the original provisioning request by associating the provisioned virtual asset (i.e., virtual machine, managed disk, AKS node, container replica) to the virtual asset provisioning request (i.e., originating deployment request, resource group, subscription, Autoscale rule, or orchestration policy that triggered the provisioning). The Azure Controllers may further record the asset as the resulting

	object of that provisioning operation in activity logs and deployment records. The Azure Controllers may also apply the requested identities, role assignments, policies, and tags specified in the request and link the asset to the deployment operation ID (<i>i.e.</i>, a user, the scale set, AKS node pool, ACA revision, deployment template, or automation runbook that requested it), enabling traceability between the request and the provisioned virtual asset. TOUTVIRTUAL 005618-TOUTVIRTUAL 005645; TOUTVIRTUAL 005646-TOUTVIRTUAL 005675. The Accused Instrumentality provides Azure Controllers that may receive a provisioning request from the Azure Load Balancer, which may assign the newly provisioned asset to the active network traffic. For example, when a virtual machine or VMSS instance is provisioned, it is automatically added to a backend pool, health probes verify the asset's readiness, and traffic is routed to the new asset. The Azure Load Balancer may assign the asset to the original workload demand (e.g., increased traffic). TOUTVIRTUAL 004035-TOUTVIRTUAL 004038. The Accused Instrumentality provides Azure Controllers that may receive a provisioning request from AKS, which may assign provisioned virtual assets through node provisioning or pod scheduling. For example, when virtual machines nodes are provisioned, new virtual machine nodes are added to a node pool, assigned to a cluster scheduling, and used by the workloads that triggered the autoscaling. AKS may also define resource quotas, such that when multiple replicas of pods are necessary during a disruption, the newly provisioned pods are assigned to nodes, such that services and ingress controllers may continue to route traffic through these new pods. TOUTVIRTUAL 002260-TOUTVIRTUAL 002264; TOUTVIRTUAL 002614-TOUTVIRTUAL 002620. The Accused Instrumentality provides Azure Controllers that may receive a provisioning request from Azure Container Apps, which may assign provisioned container replicas automatically. For example, when new container replicas are provisioned, the new replicas are associated with a specific revision, registered with the ingress routing, and assigned to handle the event or HTTP load that triggered the scaling. TOUTVIRTUAL 002989-TOUTVIRTUAL 002991. The Accused Instrumentality provides Azure Controllers that may receive a provisioning request from Azure Arc Resource Bridge or Azure Arc-enabled Kubernetes via Azure Arc, which may assign provisioned virtual assets to the virtual asset provisioning request. For example, Azure Arc Resource Bridge may interpret the validated virtual asset provisioning request and create a virtual asset in the private infrastructure, which will be represented within the Azure Controllers.
--	---

	Arc resource bridge (ARB) – Solution architecture  The diagram illustrates the Arc resource bridge (ARB) solution architecture. It shows three main environments at the top: vCenter server, SCVMM Management server, and Azure Local VM enabled by Azure Arc. Each environment contains specific components like Resource Pools, VM Templates, and virtual networks. These environments are connected to a central ARB resource through custom location mappings. Below this, three Arc resource bridges are shown, each connecting a specific environment to a Private cloud environment. Each bridge includes a Custom location and Arc-enabled Kubernetes cluster extensions. The Private cloud environment at the bottom contains vCenter, SCVMM, and Azure Local instance control planes, which are managed via management endpoints from the bridges. TOUTVIRTUAL 003039-TOUTVIRTUAL 003045. The Accused Instrumentality provides Azure Controllers that may receive provisioning requests from the Azure storage virtualization services, which may assign the newly provisioned virtual asset to the request that caused the provisioning. For example, new managed disks may be attached to specific virtual machines, new file shares may be mounted to specific workloads, or new containers may be bound to specific application or pipelines that caused the provisioning. TOUTVIRTUAL 003388-TOUTVIRTUAL 003397, TOUTVIRTUAL 003398-TOUTVIRTUAL 003405, TOUTVIRTUAL 003406-TOUTVIRTUAL 003413, TOUTVIRTUAL 003414-TOUTVIRTUAL 003416.
1[f]. providing user access to the provisioned virtual asset.	The Accused Instrumentality meets the recited claim language because each Azure Controller provides the user access to the provisioned virtual asset. The Accused Instrumentality provides Azure Portal, which is a controller that provides a user with a unified, web-based console for creating, managing, and monitoring Azure resources, ranging from simple web apps to complex deployments through a graphical interface with integrated support. Azure Portal communicates with its users over a network (such as the Internet or a local network)

with the virtualization layers to create, configure, monitor, and deallocate virtual resources. Azure Portal interacts with and allows users to visually manage and provision virtual machines, networks, storage resources, and functions over a network.

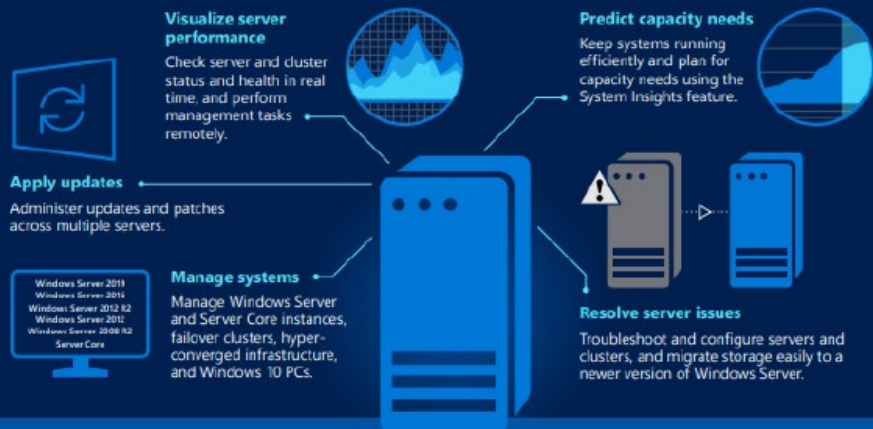


TOUTVIRTUAL 002509-TOUTVIRTUAL 002511; TOUTVIRTUAL 002124-TOUTVIRTUAL 002129; TOUTVIRTUAL 002503-TOUTVIRTUAL 002508.

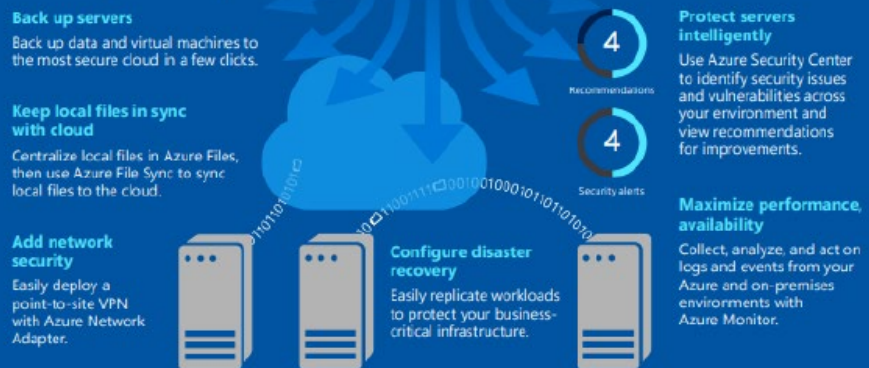
The Accused Instrumentality provides WAC, which acts as a network-coupled controller that communicates directly with the host servers or server clusters to provision and manage virtual machines, including environment connected through Azure Arc. TOUTVIRTUAL 002134-TOUTVIRTUAL 002137. WAC is a locally deployed management tool set that can manage Windows Clients, Servers, and Clusters without needing to connect to the cloud and provides full

	control over all aspects of server infrastructure including managing servers on private networks that are not connected to the Internet. WAC interacts with and allows users to perform actions such as management and provisioning of virtual machines, networks, storage resources, and functions over a network. TOUTVIRTUAL 002571-TOUTVIRTUAL 002575; TOUTVIRTUAL 002130-TOUTVIRTUAL 002133;
--	---

Streamline management tasks

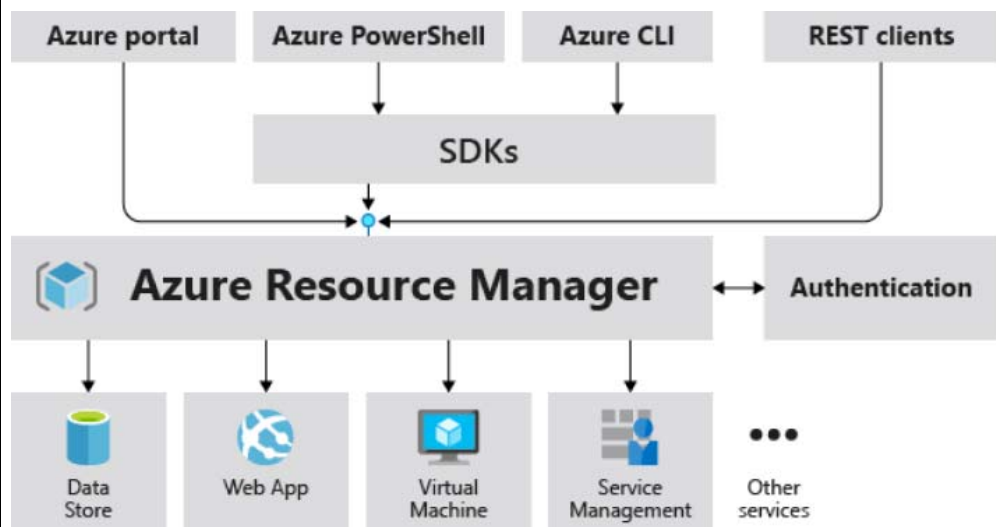


Extend your on-premises environment with Azure integrations



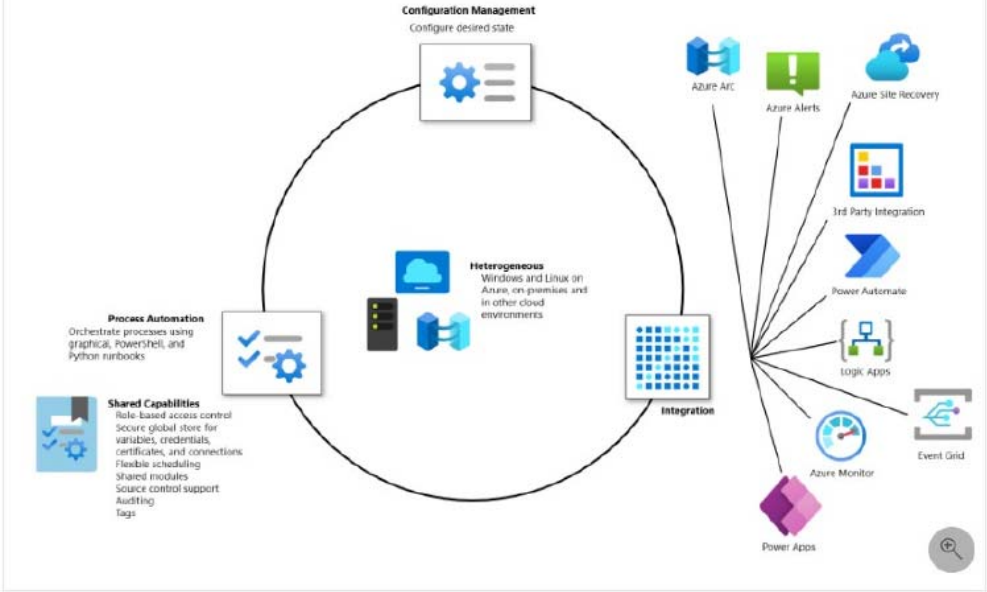
TOUTVIRTUAL 002596-TOUTVIRTUAL 002597.

The Accused Instrumentality provides Azure Resource Manager (“ARM”), which provides a deployment and management service that can create, update, and delete resources such as virtual machines, storage accounts, web apps, databases, and virtual networks within the Azure virtualization environment. TOUTVIRTUAL 002150-TOUTVIRTUAL 002151;

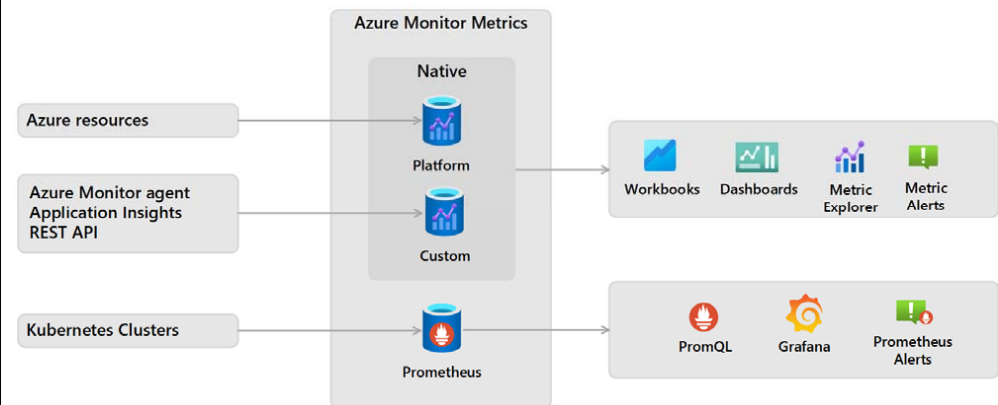


TOUTVIRTUAL 002143-TOUTVIRTUAL 002149.

The Accused Instrumentality provides Azure Controllers that provide Azure Automation, which supports the Azure Controllers by executing runbooks and scripts that automatically manage and reconfigure virtual resources through network-based APIs across the virtualization environment.

	 The diagram illustrates the Azure Automation framework. It features a central circle labeled 'Heterogeneous' containing 'Windows and Linux on Azure, on-premises and in other cloud environments'. Surrounding this circle are four main components: 'Configuration Management' (top, 'Configure desired state'), 'Process Automation' (left, 'Orchestrate processes using graphical, PowerShell, and Python runbooks'), 'Shared Capabilities' (bottom-left, listing 'Rule-based access control', 'Secure global store for variables, credentials, certificates, and connections', 'Flexible scheduling', 'Shared modules', 'Source control support', 'Auditing', and 'Tags'), and 'Integration' (right). To the right of the Integration component, a hub connects to various Azure services: Azure ARC, Azure Alerts, Azure Site Recovery, 3rd Party Integration, Power Automate, Logic Apps, Azure Monitor, Event Grid, and Power Apps. TOUTVIRTUAL 002166-TOUTVIRTUAL 002171; TOUTVIRTUAL 002760-TOUTVIRTUAL 002770; TOUTVIRTUAL 002771-TOUTVIRTUAL 002780. After executing the runbooks and scripts, the Azure Controllers via Azure Automation assign Hybrid Runbook workers to ensure virtual asset provisioning requests are fulfilled. Once the Azure Automation runbook is complete, the virtual asset may be available to the user in the Azure Controllers.
Claim 2	
2. The method of <i>claim 1</i> further comprising determining one or more performance metrics of the provisioned virtual asset.	See Claims 1[c] and 1[d]. The Accused Instrumentality meets the recited claim language because each Azure Controller determines one or more performance metrics of the provisioned virtual asset. The Accused Instrumentality provides Azure Portal, which determines one or more performance metrics of the provisioned virtual asset because it tracks the operational state and configuration of all provisioned virtual assets, including VMs, VMSS, AKS nodes and pods, storage, and other

physical resources. Azure Portal integrates Azure Monitor and Azure Service Health, which includes Azure Status, Service Health, and Resource Health, to collect key telemetry such as CPU utilization, network throughput, disk I/O, and availability for each resource and asset. These measurements are continuously reported through the Azure Portal, ARM APIs, and the Azure Metrics Explorer interface. Azure Portal's telemetry data is also made available to automation workflows and alerting mechanisms for performance-based management.



TOUTVIRTUAL 003163-TOUTVIRTUAL 003168.

The Accused Instrumentality provides WAC, which determines one or more performance metrics of the provisioned virtual asset because WAC continuously collects telemetry from host servers, server clusters, and VMs running within or outside of the Azure infrastructure, including on-premises datacenters and other cloud platforms, displaying metrics such as CPU, memory, disk, and network usage. When integrated with Azure Arc (TOUTVIRTUAL 002134-TOUTVIRTUAL 002137), WAC forwards this measurement data from these non-Azure systems to the Azure Portal for aggregation and reporting. Users may view detailed performance dashboards, generate usage reports, and receive notification of performance degradation through the WAC interface. This enables consistent performance measurement and reporting across both cloud-based and on-premise virtual assets and physical resources. TOUTVIRTUAL 002543-TOUTVIRTUAL 002552; TOUTVIRTUAL 002553-TOUTVIRTUAL 002570; TOUTVIRTUAL 002576-TOUTVIRTUAL 002595.

The Accused Instrumentality provides Azure Service Health, which keeps users informed about the health of its cloud resources, including current and upcoming issues, such as service impacting events, planned maintenance, and other changes that might affect network availability. As provided above, Azure Service Health includes (1) Azure Status, which informs users of service outages in the Azure virtualization environment globally; (2) Service Health, which provides users a personalized view of the health of the user’s Azure virtualization environment and notification through a preferred communication channel about issues or changes that may affect the user’s resources and assets; and (3) Resource Health, which provides information about the health of the user’s individual cloud resources, such as a specific virtual machine instance and is able to help determine metrics for the provisioned virtualization environment.

Microsoft Azure

My accountPortal

Welcome to the new Azure status page. Don't forget to update this page in your bookmarks. [Learn More](#)

Azure status

RSS

This page is only used for widespread incidents.

Sign in to view incidents that may be affecting your services

[Go to Azure Service Health >](#)

HELPFUL LINKS

[Azure status history](#)
Learn when we use this page
[Get notified of outages that impact you](#)
[Building reliable applications on Azure](#)

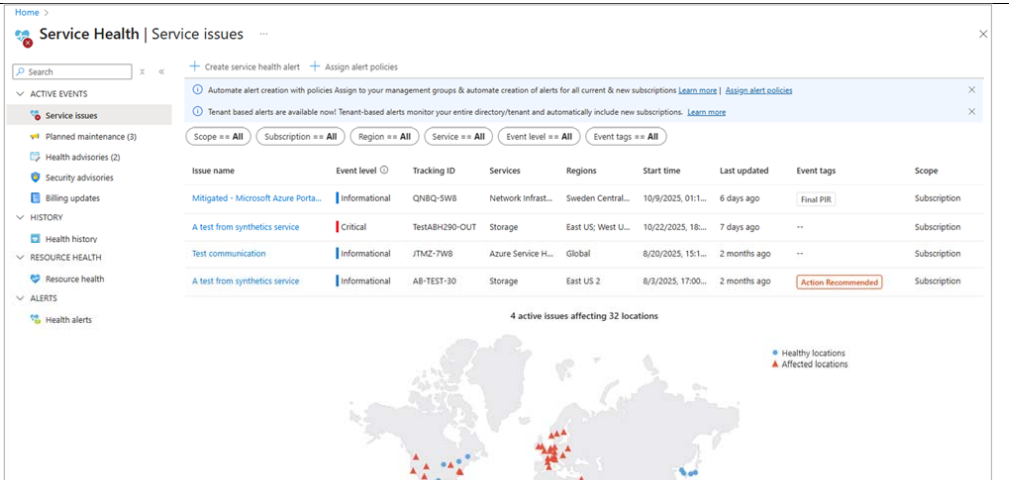
Updated 34 seconds ago | Refresh every 2 minutes

Good Information Warning Critical -- N/A

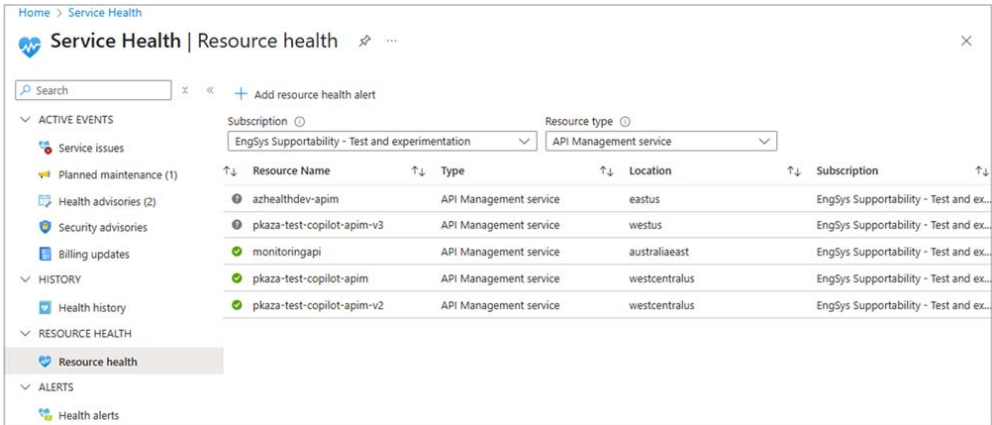
Current ImpactAmericasEuropeAsia PacificMiddle East and AfricaAzure GovernmentAzure ChinaJio¹

Products And Services	North-Regional ⓘ	East US	East US 2	Central US	North Central US	South Central US	West Central US	West US	West US 2	West US 3	Canada East	Canada Central	Brazil South	Brazil Southeast	Mexico Central	Chile Central
COMPUTE																
Azure Compute Fleet	--	Good	Good	Good	Good	Good	Good	Good	Good	Good	Good	Good	Good	Good	Good	Good
Azure VMware Solution	--	Good	Good	Good	Good	Good	--	Good	Good	Good	Good	Good	Good	--	--	--
Azure VMware Solution by CloudSimple	--	Good	--	--	--	Good	--	Good	--	--	--	--	--	--	--	--
Batch	--	Good	Good	Good	Good	Good	Good	Good	Good	Good	Good	Good	Good	Good	--	Good

TOUTVIRTUAL 003244-TOUTVIRTUAL 003247;

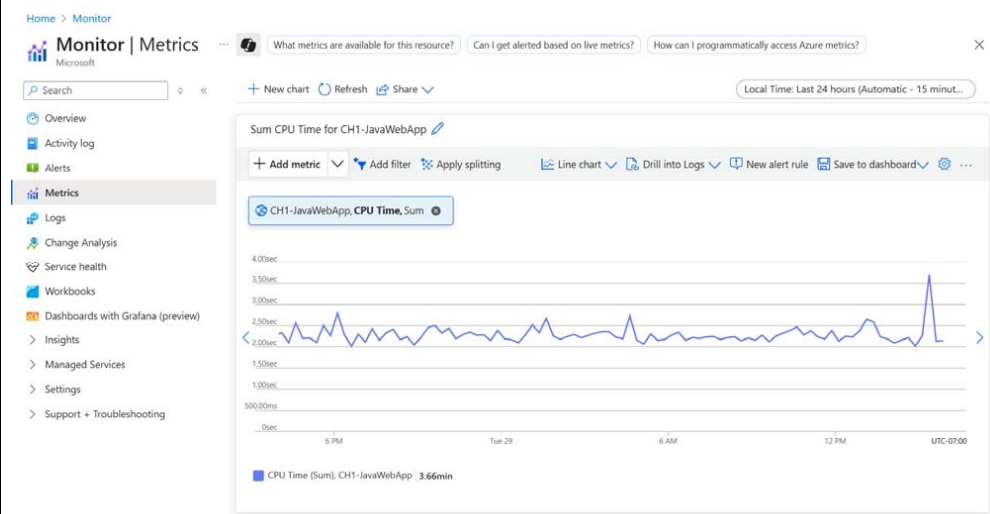


TOUTVIRTUAL 003242-TOUTVIRTUAL 003243;



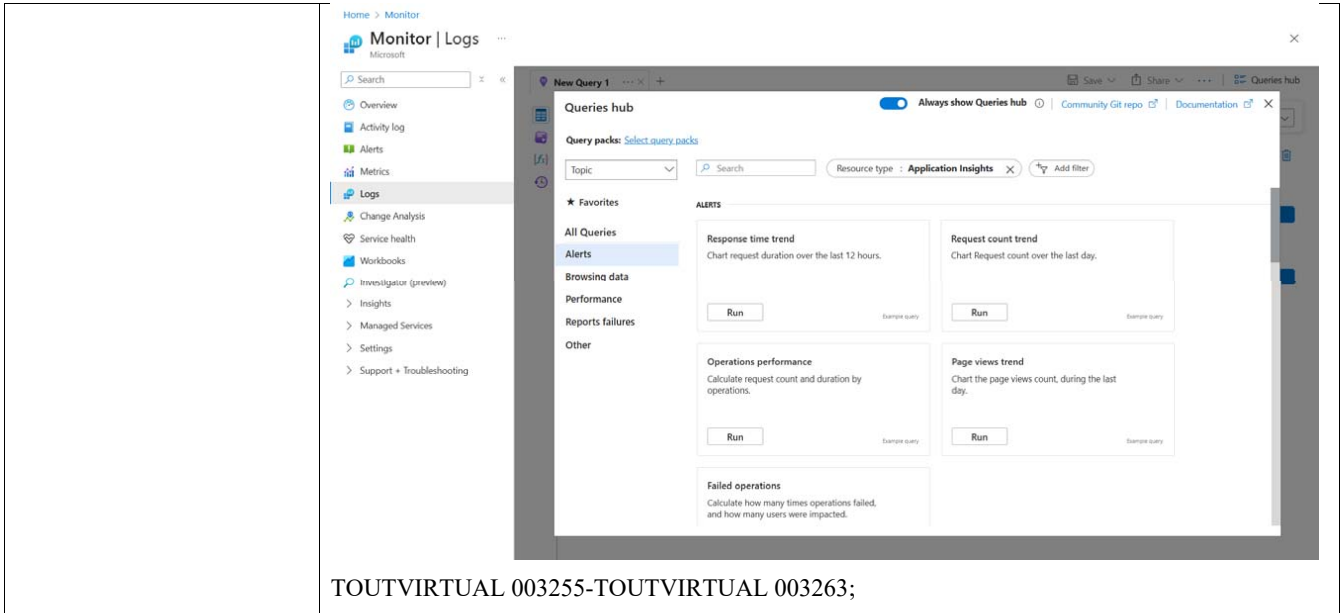
TOUTVIRTUAL 003248-TOUTVIRTUAL 003254.

The Accused Instrumentality provides Azure Monitor, which includes Metrics Explorer, which helps users plot charts, visually correlate trends, and investigate spikes and dips in metrics values. Metrics Explorer enables users to investigate the health and utilization of the user's resources and assets and determine metrics for the provisioned virtualization environment.

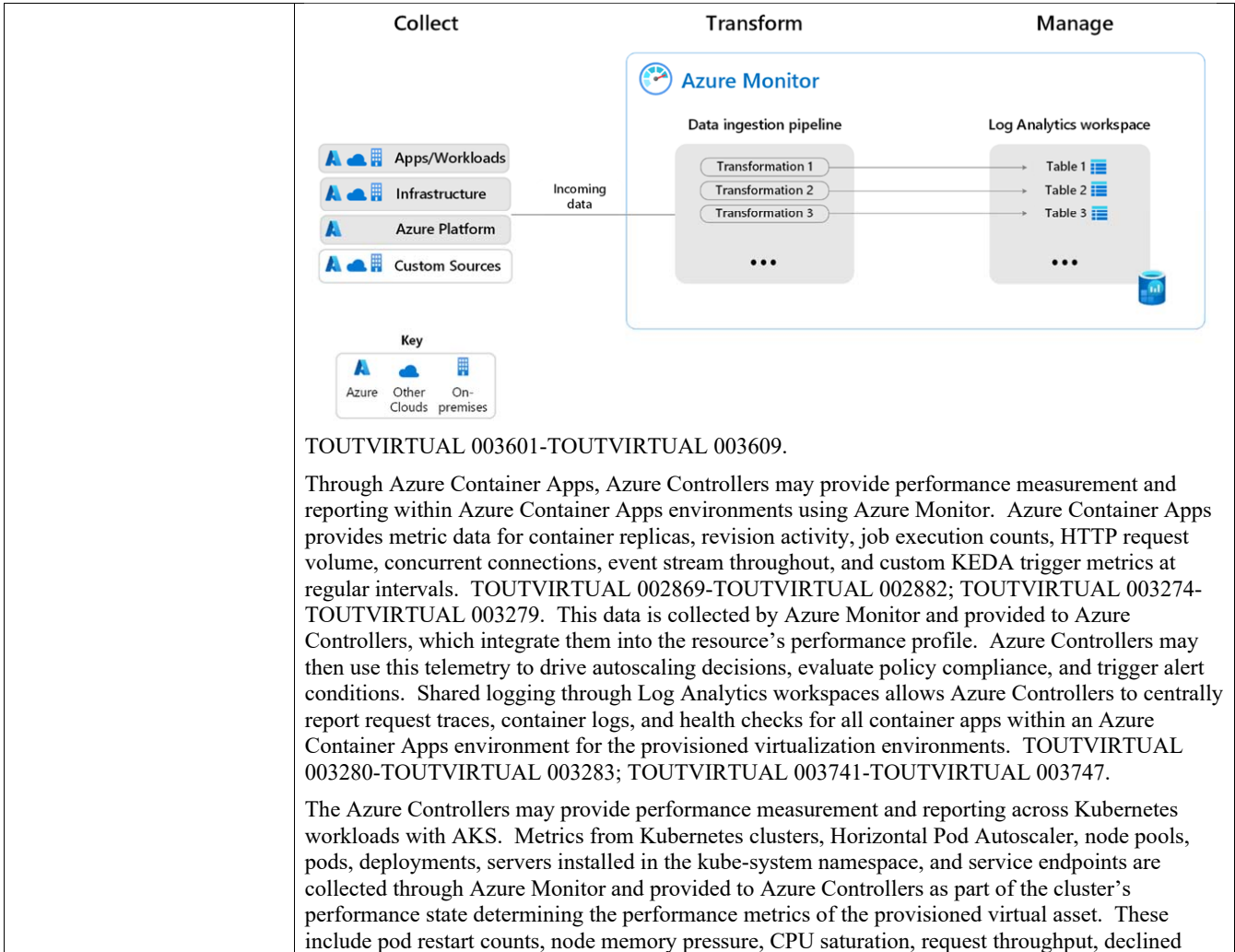


TOUTVIRTUAL 002281-TOUTVIRTUAL 002312.

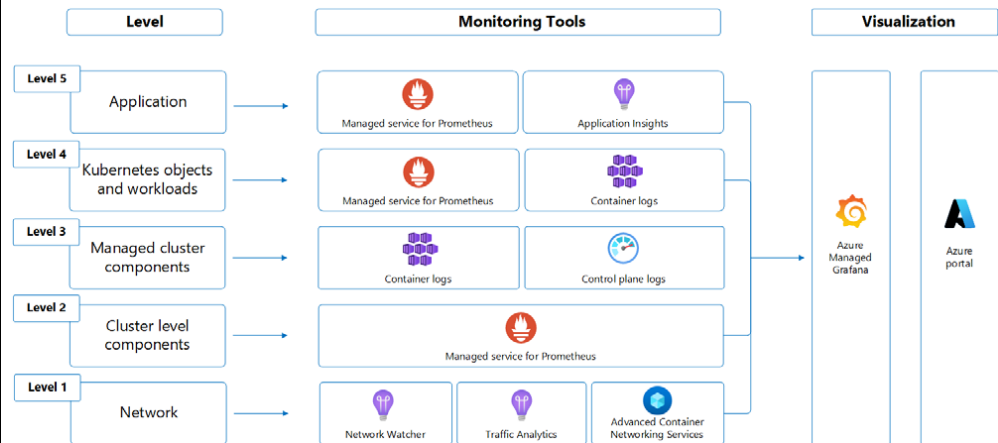
Azure Monitor further includes Log Analytics that allows users to explore and analyze data collected by Azure Monitor Logs. A user may edit and run log queries to filter records, uncover trends, analyze patterns, and gain meaningful insights into the user's Azure virtualization environment and is able to help determine metrics for the provisioned virtualization environment.



TOUTVIRTUAL 003255-TOUTVIRTUAL 003263;

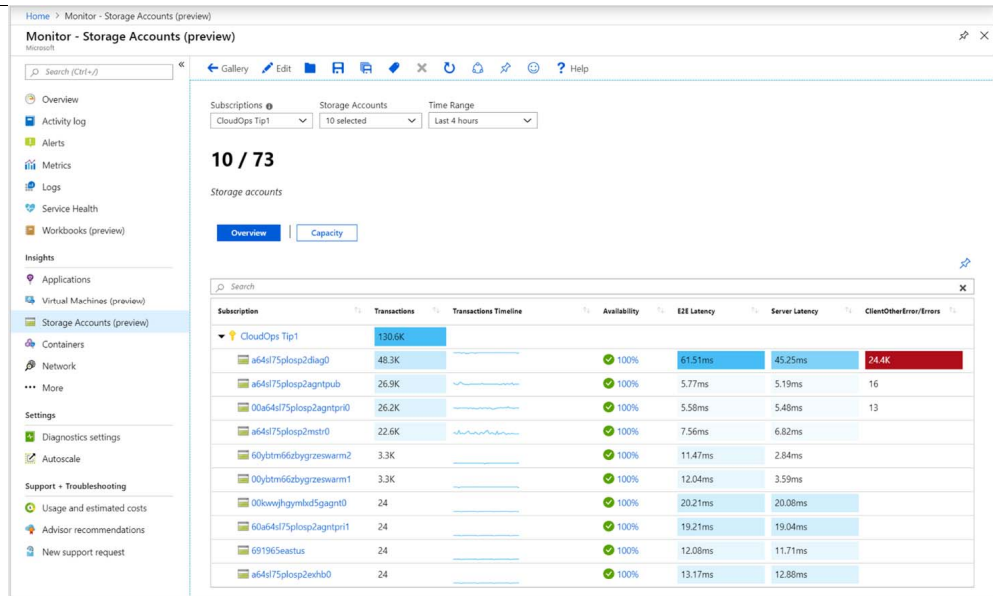


scheduling attempts, and container-level health signals. Azure Controllers use this performance data to generate reports, drive autoscaling logic, trigger alerts, and support automatic remediation in an AKS environment for the provisioned virtualization environments.



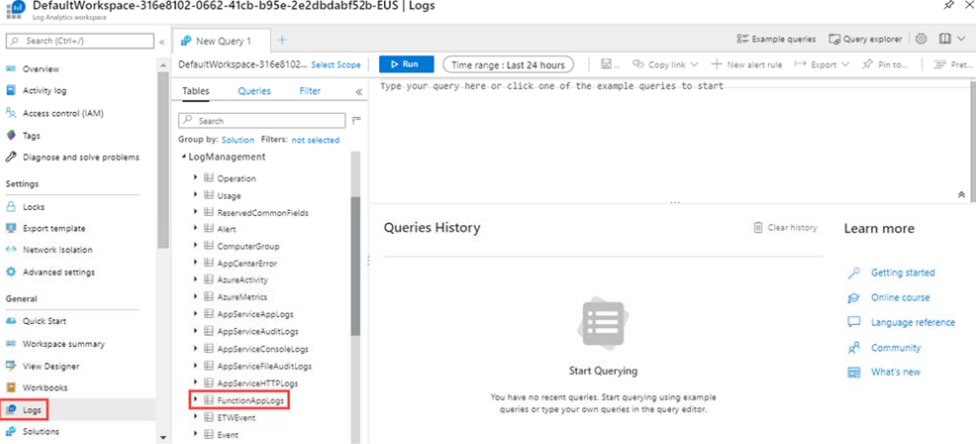
TOUTVIRTUAL 003284-TOUTVIRTUAL 003287.

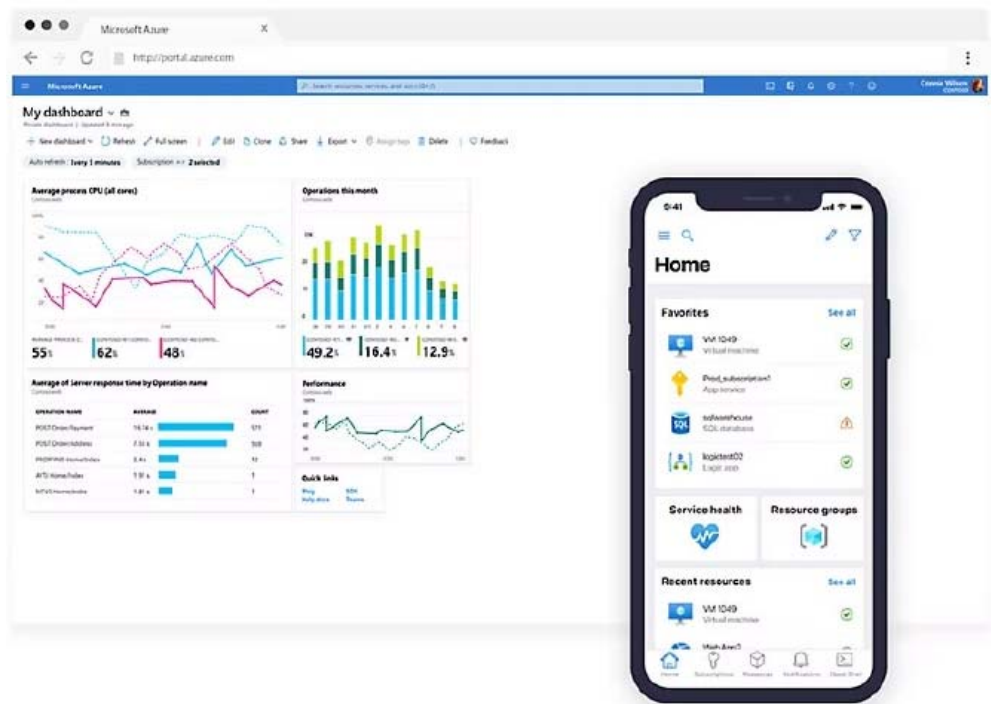
The Azure Controllers may receive performance measurements and reports for storage-virtualized assets from Azure Monitor. From Azure Blob Storage, Azure Monitor automatically collects metrics related to latency, throughput, throttling events, replication health, and capacity usage. From Azure Files, Azure Monitor automatically collects metrics related to SMB and NFS latency, IOPS, quota usage, and share health. From Azure Disk Storage, Azure Monitor automatically collects metrics related to IOPS, throughput, queue depth, read and write latency, and disk health signals. From Azure Elastic SAN, Azure Monitor automatically collects metrics related to volume throughput, SAN controller health, redundancy status, and capacity utilization. Azure Monitor collects these metrics automatically and provides these metrics to Azure Controllers, so that Azure Controllers may aggregate these metrics, provide continuous reporting, and support reallocation or deployment decisions for the provisioned virtualization environments.



TOUTVIRTUAL 003288-TOUTVIRTUAL 003303; TOUTVIRTUAL 003398-TOUTVIRTUAL 003405; TOUTVIRTUAL 003406-TOUTVIRTUAL 003413; TOUTVIRTUAL 003414-TOUTVIRTUAL 003416.

The Azure Controllers may also determine one or more performance metrics of the provisioned virtual assets through Azure Functions. Performance metrics of the provisioned virtual assets may be measured and reported, along with the other available resources within the virtualization environment, via Azure Functions based on different demand loads and over certain time periods that Azure Functions has been operating for the provisioned virtualization environments.

	 TOUTVIRTUAL 003304-TOUTVIRTUAL 003313.
Claim 3	
3. The method of <i>claim 1</i> further comprising providing a user interface for submitting the virtual asset provisioning request.	See Claim 1[b]. The Accused Instrumentality meets the recited claim language because the Azure Controllers provide a user interface for submitting the virtual asset provisioning request. The Accused Instrumentality provides Azure Portal, which is a controller that provides a user with a unified, web-based console for creating, managing, and monitoring Azure resources, ranging from simple web apps to complex deployments through a graphical interface with integrated support. Azure Portal communicates over a network (such as the Internet or a local network) with the virtualization layers to create, configure, monitor, and deallocate virtual resources. Azure Portal interacts with and allows users to visually manage and provision virtual machines, networks, storage resources, and functions over a network.

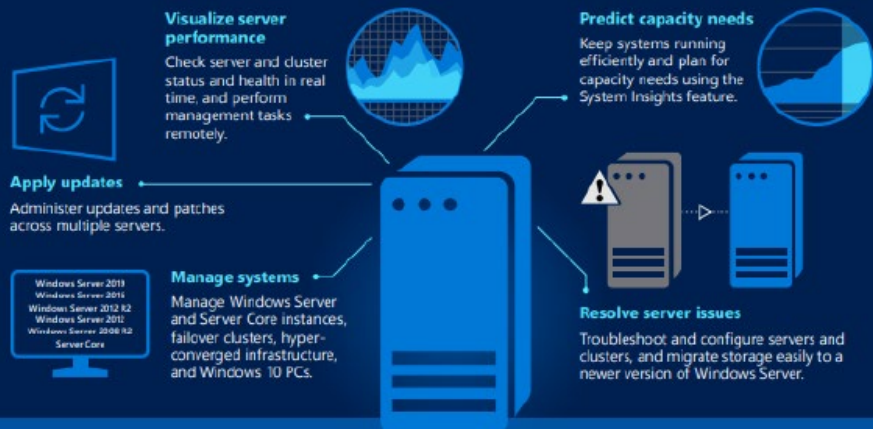


TOUTVIRTUAL 002509-TOUTVIRTUAL 002511; TOUTVIRTUAL 002124-TOUTVIRTUAL 002129; TOUTVIRTUAL 002503-TOUTVIRTUAL 002508.

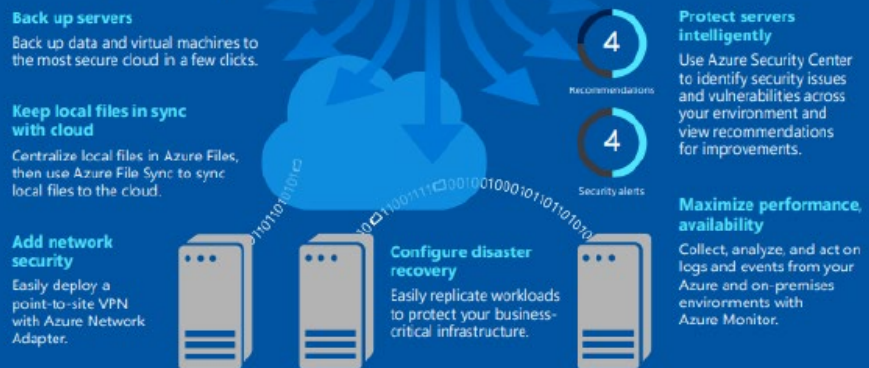
The Accused Instrumentality provides WAC, which acts as a network-coupled controller that communicates directly with the host servers or server clusters to provision and manage virtual machines, including environment connected through Azure Arc. TOUTVIRTUAL 002134-TOUTVIRTUAL 002137. WAC is a locally deployed management tool set that can manage Windows Clients, Servers, and Clusters without needing to connect to the cloud and provides full control over all aspects of server infrastructure including managing servers on private networks that are not connected to the Internet. WAC interacts with and allows users to perform actions such as management and provisioning of virtual machines, networks, storage resources, and functions over a

	network. TOUTVIRTUAL 002571-TOUTVIRTUAL 002575; TOUTVIRTUAL 002130-TOUTVIRTUAL 002133;
--	--

Streamline management tasks

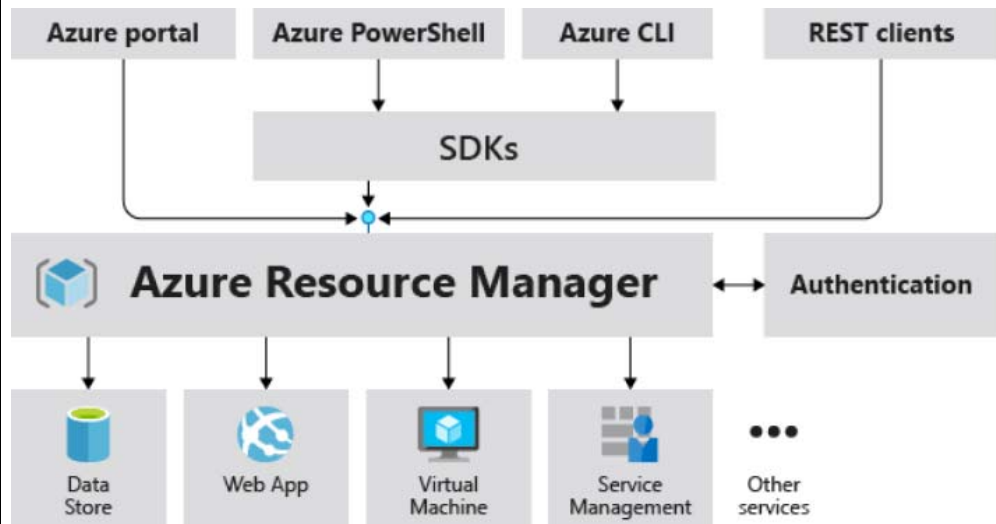


Extend your on-premises environment with Azure integrations



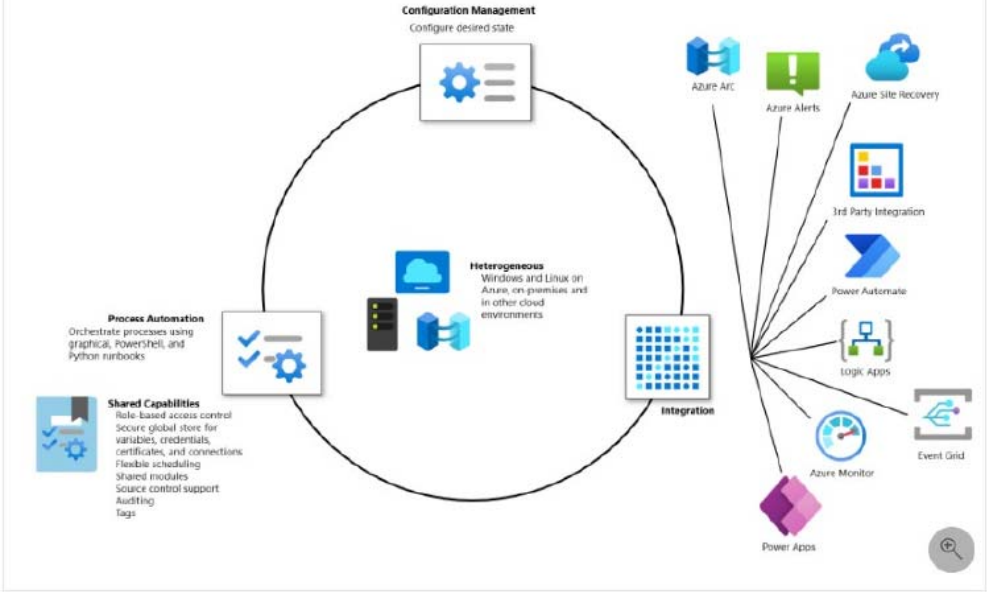
TOUTVIRTUAL 002596-TOUTVIRTUAL 002597.

The Accused Instrumentality provides ARM, which provides a user with an interface via the Azure Controllers, which allows the user to submit virtual asset provisioning requests. When users submit virtual asset provisioning requests via the Azure Controllers, ARM may validate and execute the request. TOUTVIRTUAL 002150-TOUTVIRTUAL 002151;

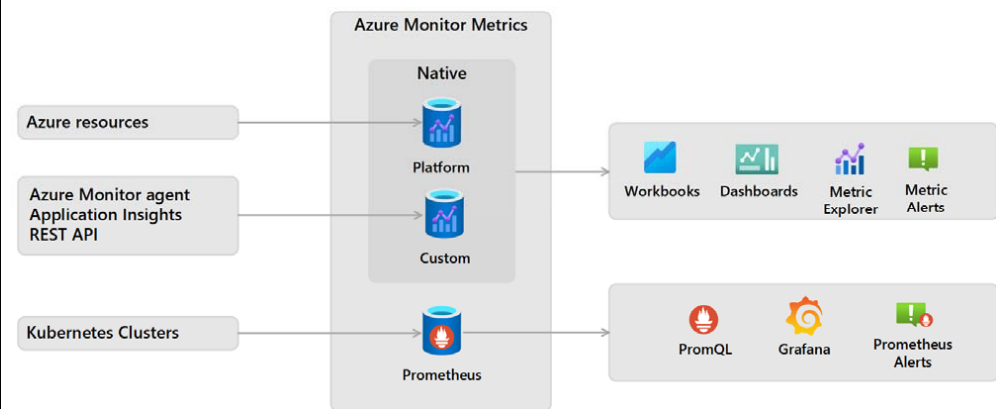


TOUTVIRTUAL 002143-TOUTVIRTUAL 002149.

The Accused Instrumentality provides Azure Automation, which supports the Azure Controllers by executing runbooks and scripts that automatically manage and reconfigure virtual resources through network-based APIs across the virtualization environment.

	 The diagram illustrates the Azure Portal architecture. At the center is a circle labeled "Heterogeneous" containing icons for Windows and Linux on Azure, on-premises, and in other cloud environments. Surrounding this central hub are several functional areas: Configuration Management (top): "Configure desired state" with a gear icon. Process Automation (left): "Orchestrate processes using graphical, PowerShell, and Python runbooks" with a checkmark and gear icon. Shared Capabilities (bottom-left): "Role-based access control, Secure global store for variables, credentials, certificates, and connections, Flexible scheduling, Shared modules, Source control support, Auditing, Tags" with a gear icon. Integration (right): A large box with a grid pattern, connected to various Azure services including Azure ARC, Azure Alerts, Azure Site Recovery, 3rd Party Integration, Power Automate, Logic Apps, Azure Monitor, Event Grid, and Power Apps. TOUTVIRTUAL 002166-TOUTVIRTUAL 002171; TOUTVIRTUAL 002760-TOUTVIRTUAL 002770; TOUTVIRTUAL 002771-TOUTVIRTUAL 002780.
Claim 5	
5. The method of <i>claim 2</i>, wherein determining the one or more performance metrics further comprises determining one or more real time performance metrics.	See Claim 2. The Accused Instrumentality meets the recited claim language because each Azure Controller determines one or more performance metrics which further comprise determining one or more real time performance metrics. The Accused Instrumentality provides Azure Portal, which determines real time performance metrics of the virtual assets because it tracks the operational state and configuration of all provisioned virtual assets. Through Azure Portal's integration of Azure Monitor and Azure Service Health which includes Azure Status, Service Health, and Resource Health, Azure Portal collects real time telemetry such as CPU utilization, network throughput, disk I/O, and availability for each

virtual asset at regular intervals. These measurements are continuously reported through the Azure Portal, ARM APIs, and the Azure Metrics Explorer interface. Azure Portal's telemetry data is also made available to automation workflows and alerting mechanisms for performance-based management.



TOUTVIRTUAL 003163-TOUTVIRTUAL 003168.

The Accused Instrumentality provides WAC, which determines real time performance metrics of the provisioned virtual asset because WAC continuously collects real time telemetry from host servers, server clusters, and VMs running within or outside of the Azure infrastructure, including on-premises datacenters and other cloud platforms, displaying metrics such as CPU, memory, disk, and network usage. When integrated with Azure Arc (TOUTVIRTUAL 002134-TOUTVIRTUAL 002137), WAC forwards this measurement data from these non-Azure systems to the Azure Portal for aggregation of the data and reporting of the real time performance metrics. Users may view detailed performance dashboards, generate usage reports, and receive notification of performance degradation through the WAC interface which is continuously collecting real time telemetry. This enables consistent performance measurement and reporting across both cloud-based and on-premises virtual assets and physical resources. TOUTVIRTUAL 002543-TOUTVIRTUAL 002552; TOUTVIRTUAL 002553-TOUTVIRTUAL 002570; TOUTVIRTUAL 002576-TOUTVIRTUAL 002595.

The Accused Instrumentality provides Azure Service Health, which keeps users informed in real time about the health of its cloud resources, including current and upcoming issues, such as service

impacting events, planned maintenance, and other changes that might affect network availability. As provided above, Azure Service Health Service includes (1) Azure Status, which informs users of service outages in the Azure virtualization environment globally; (2) Service Health, which provides users a personalized view of the health of the user's Azure virtualization environment and notification through a preferred communication channel about issues or changes that may affect the user's resources and assets; and (3) Resource Health, which provides information about the health of the user's individual cloud resources, such as a specific virtual machine instance.

My account

Portal

Welcome to the new Azure status page. Don't forget to update this page in your bookmarks. [Learn More](#)

Azure status

This page is only used for widespread incidents.

Sign in to view incidents that may be affecting your services

Go to Azure Service Health

HELPFUL LINKS

[Azure status history](#)
[Learn when we use this page](#)
[Get notified of outages that impact you](#)
[Building reliable applications on Azure](#)

Updated 34 seconds ago

Refresh every

2 minutes

Good

Information

Warning

Critical

--

N/A

Current Impact

Americas

Europe

Asia Pacific

Middle East and Africa

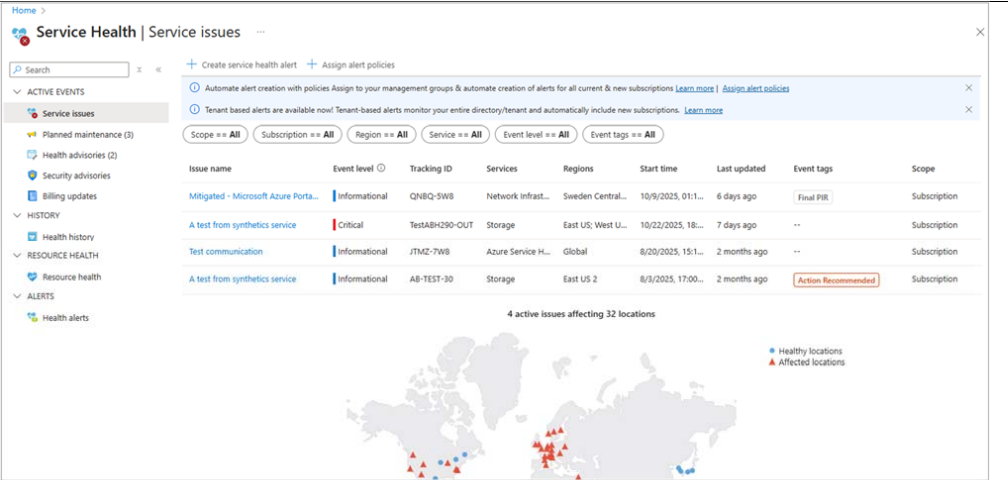
Azure Government

Azure China

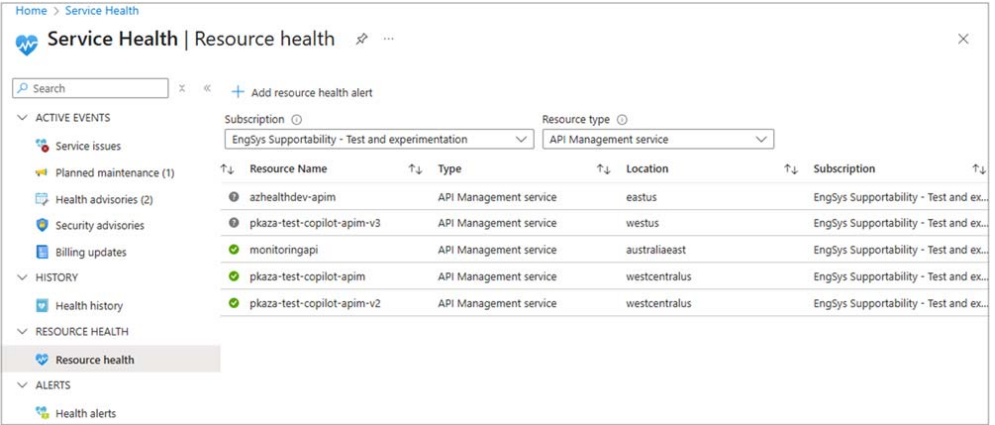
Jio¹

Products And Services	*Non-Regional ⓘ	East US	East US 2	Central US	North Central US	South Central US	West Central US	West US	West US 2	*West US 3	Canada East	Canada Central	Brazil South	Brazil Southeast	Mexico Central	Chile Central
COMPUTE																
Azure Compute Fleet	--	Good	Good	Good	Good	Good	Good	Good	Good	Good	Good	Good	Good	Good	Good	Good
Azure VMware Solution	--	Good	Good	Good	Good	Good	--	Good	Good	Good	Good	Good	Good	--	--	--
Azure VMware Solution by CloudSimple	--	Good	--	--	--	Good	--	Good	--	--	--	--	--	--	--	--
Batch	--	Good	Good	Good	Good	Good	Good	Good	Good	Good	Good	Good	Good	Good	--	Good

TOUTVIRTUAL 003244-TOUTVIRTUAL 003247;

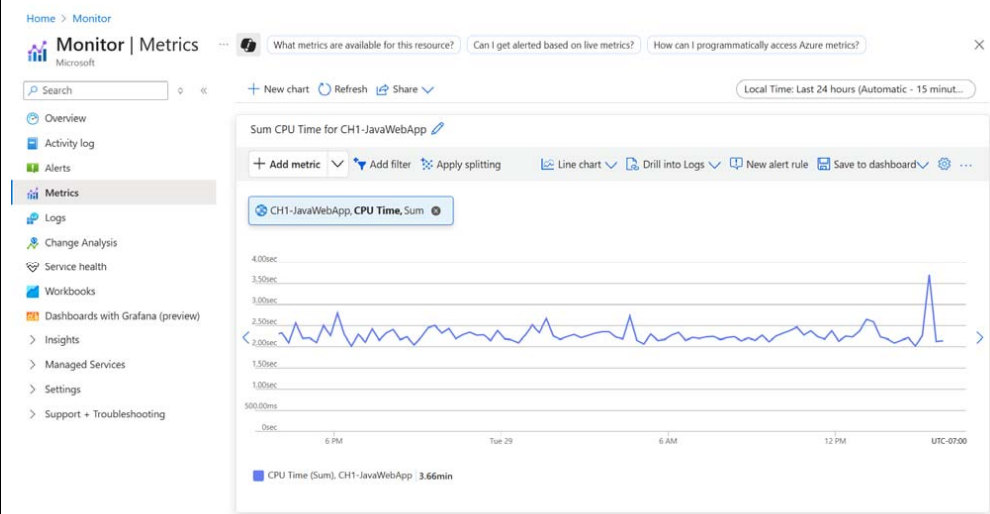


TOUTVIRTUAL 003242-TOUTVIRTUAL 003243;



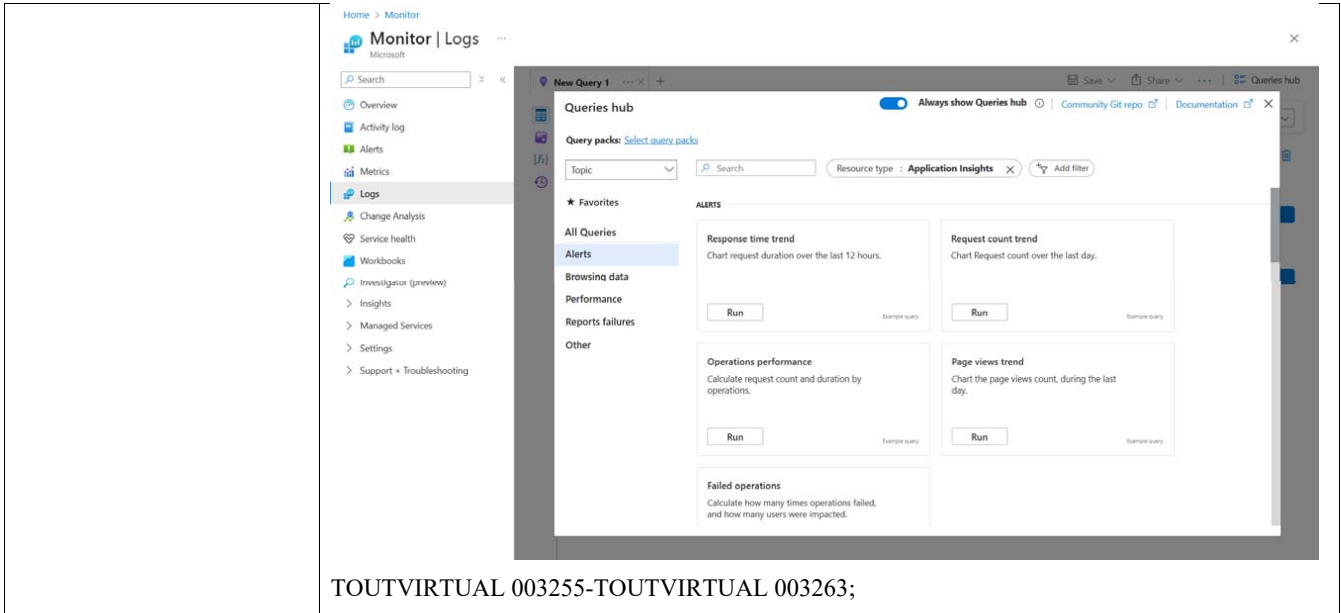
TOUTVIRTUAL 003248-TOUTVIRTUAL 003254.

The Accused Instrumentality provides Azure Monitor, which includes Metrics Explorer, which helps users plot charts, visually correlate trends, and investigate spikes and dips in metrics values. Metrics Explorer enables users to investigate the health and utilization of the user's resources and assets in real time.

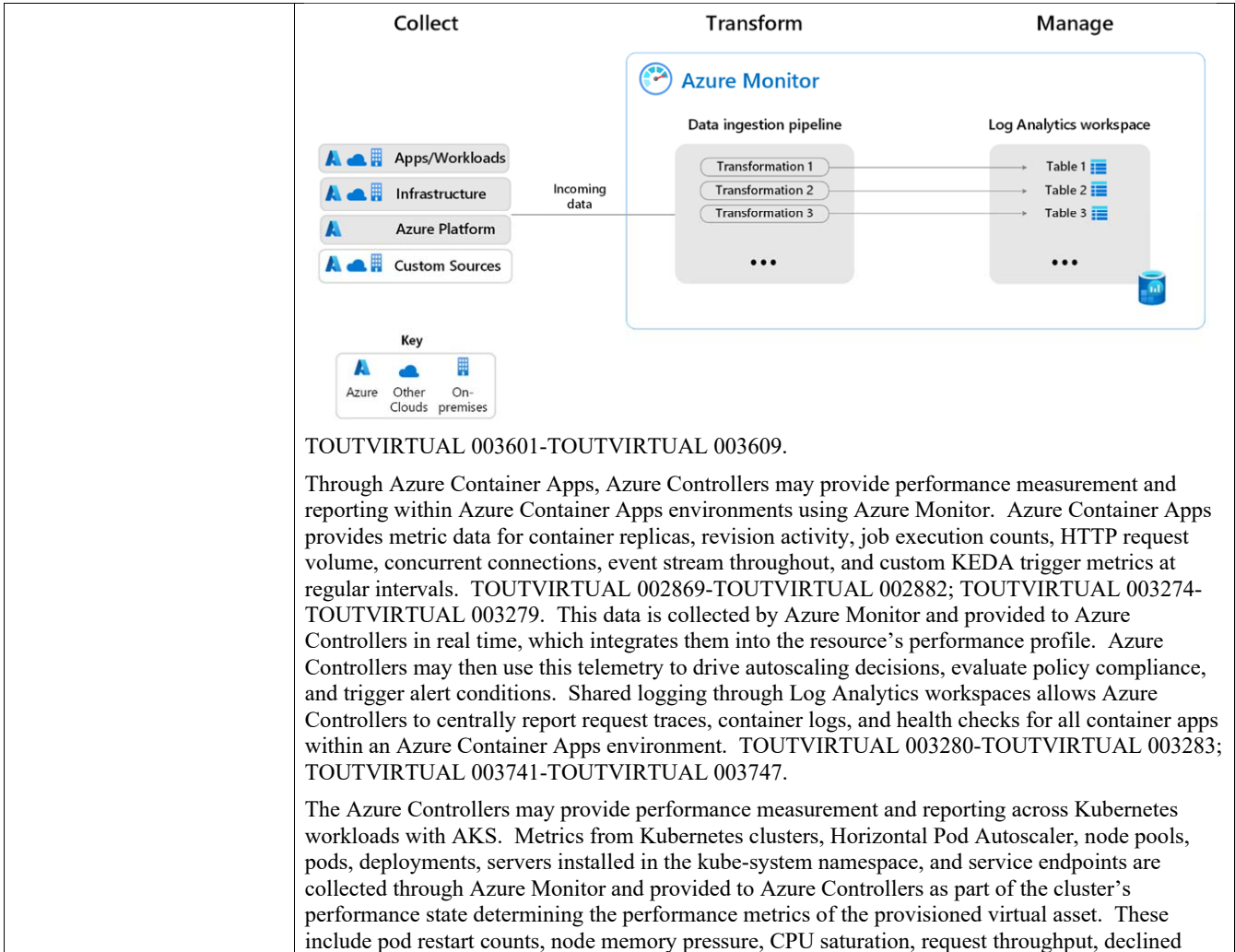


TOUTVIRTUAL 002281-TOUTVIRTUAL 002312.

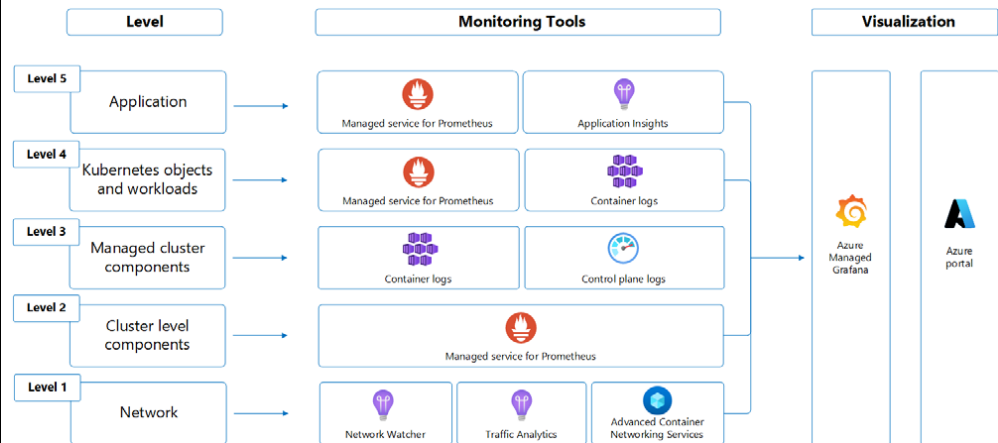
Azure Monitor further includes Log Analytics that allows users to explore and analyze data collected by Azure Monitor Logs. A user may edit and run log queries to filter records, uncover trends, analyze patterns, and gain meaningful insights into the user's Azure virtualization environment in real time.



TOUTVIRTUAL 003255-TOUTVIRTUAL 003263;

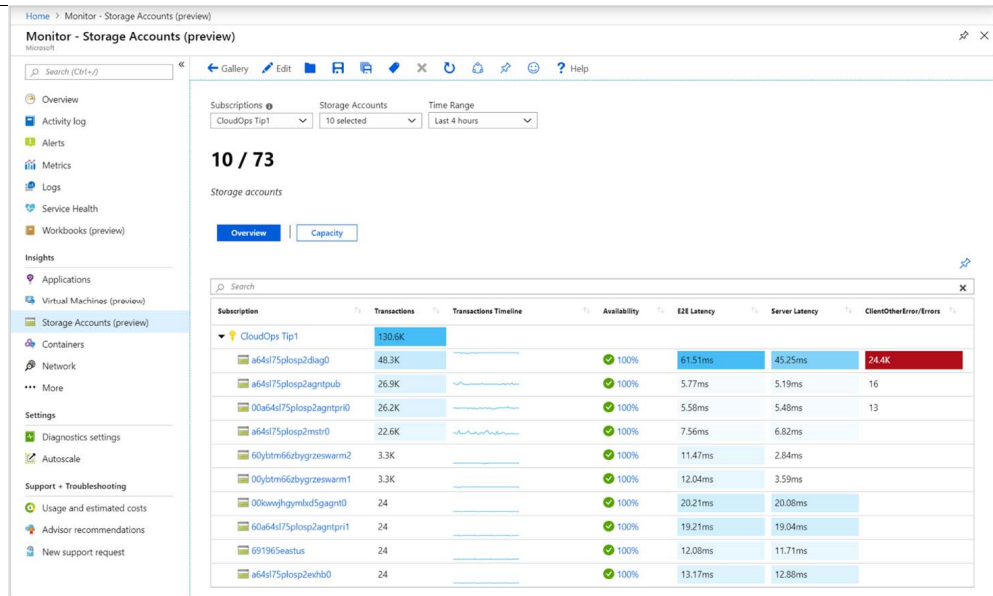


scheduling attempts, and container-level health signals. Azure Controllers use this performance data to generate reports, drive autoscaling logic, trigger alerts, and support automatic remediation in an AKS environment.



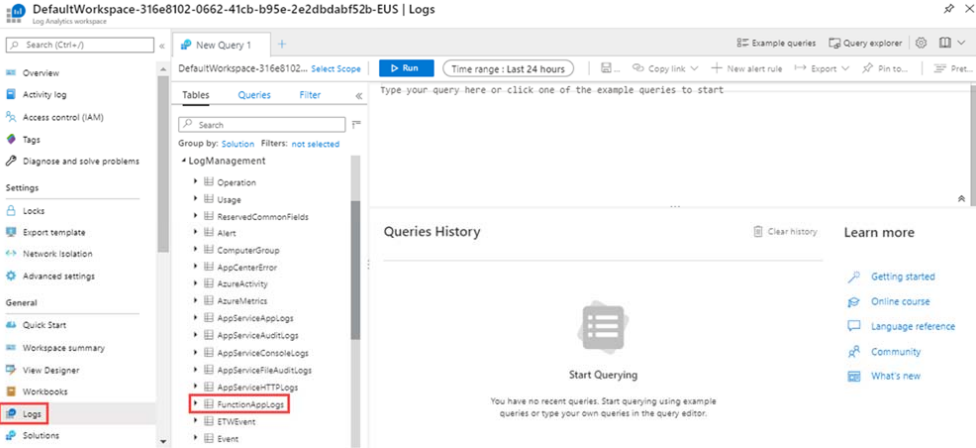
TOUTVIRTUAL 003284-TOUTVIRTUAL 003287.

The Azure Controllers may receive real time performance measurements and reports for storage-virtualized assets from Azure Monitor in real time. From Azure Blob Storage, Azure Monitor automatically collects metrics related to latency, throughput, throttling events, replication health, and capacity usage. From Azure Files, Azure Monitor automatically collects metrics related to SMB and NFS latency, IOPS, quota usage, and share health. From Azure Disk Storage, Azure Monitor automatically collects metrics related to IOPS, throughput, queue depth, read and write latency, and disk health signals. From Azure Elastic SAN, Azure Monitor automatically collects metrics related to volume throughput, SAN controller health, redundancy status, and capacity utilization. Azure Monitor collects these metrics automatically and provides these metrics to Azure Controllers, so that Azure Controllers may aggregate these metrics, provide continuous reporting, and support reallocation or deployment decisions.



TOUTVIRTUAL 003288-TOUTVIRTUAL 003303; TOUTVIRTUAL 003388-TOUTVIRTUAL 003397; TOUTVIRTUAL 003398-TOUTVIRTUAL 003405; TOUTVIRTUAL 003406-TOUTVIRTUAL 003413; TOUTVIRTUAL 003414-TOUTVIRTUAL 003416.

The Azure Controllers will also, in real time, determine performance metrics of the provisioned virtual asset through Azure Functions. Real time performance metrics will be measured and reported, along with other available resources, via Azure Functions based on different demand loads and over certain time periods that Azure Functions has been operating.

	 TOUTVIRTUAL 003304-TOUTVIRTUAL 003313.
Claim 6 6. The method of <i>claim 1</i>, wherein the inventory further comprises one or more application programs.	See Claims 1[a] and 1[c]. The Accused Instrumentality meets the recited claim language because the virtualization environment's inventory comprises one or more application programs. The Accused Instrumentality's inventory includes but is not limited to application programs, such as Azure App Service, Azure Container Apps, Azure Kubernetes Service, Arc-enabled Kubernetes, and Azure Functions, that operate as virtual assets within the virtualization environment. TOUTVIRTUAL 002225-TOUTVIRTUAL 002226; TOUTVIRTUAL 002989-TOUTVIRTUAL 002991; TOUTVIRTUAL 002260-TOUTVIRTUAL 002264; TOUTVIRTUAL 002649-TOUTVIRTUAL 002650; TOUTVIRTUAL 002804-TOUTVIRTUAL 002806. These application programs allow the user to build, deploy, and manage tasks and solutions without regard to underlying infrastructure because the application programs are operating on a virtual asset. The Accused Instrumentality provides Azure App Service, which is a platform that manages infrastructure which allows the operation of web applications, mobile backends, and other APIs. TOUTVIRTUAL 002225-TOUTVIRTUAL 002226; TOUTVIRTUAL 002900-TOUTVIRTUAL 002908.

The Accused Instrumentality provides Azure Container Apps, which is a container platform that runs microservices, event-driven applications, Application Programming Interfaces (“APIs”), and background jobs without requiring a user to manage the underlying Kubernetes clusters directly. TOUTVIRTUAL 002986-TOUTVIRTUAL 002988. Azure Container Apps leverages Kubernetes, Kubernetes Event-driven Autoscaling (“KEDA”), Distributed Application Runtime (“Dapr”), and Microsoft-managed scale controllers to automatically scale containers based on events, HTTP load, or resource metrics. TOUTVIRTUAL 003095-TOUTVIRTUAL 003103. Container workloads from Azure Container Apps are executed inside managed Kubernetes clusters that run on Azure compute infrastructure. These Azure Container Apps compute hosts are implemented as Azure virtual machines, which run on physical servers controlled by the virtualization layer.



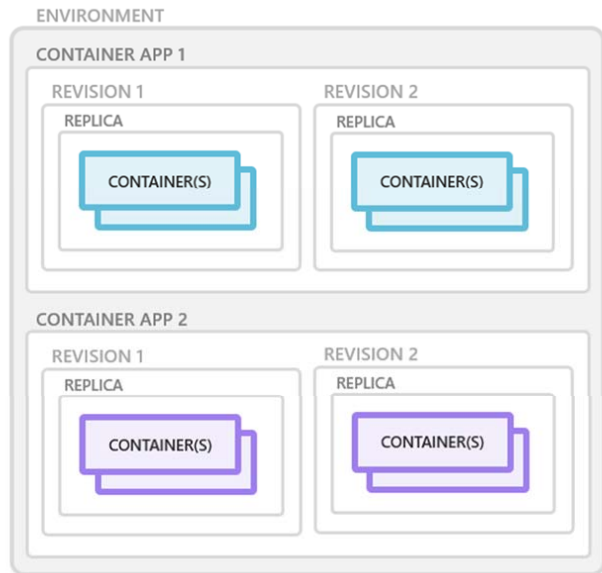
Azure Container Apps: Example scenarios

PUBLIC API ENDPOINTS	BACKGROUND PROCESSING	EVENT-DRIVEN PROCESSING	MICROSERVICES
 HTTP requests are split between two versions of the container app where the first revision gets 80% of the traffic, while a new revision receives the remaining 20%.	 A background job that transforms data in a database.	 A queue reader application that processes messages as they arrive in a queue.	 Deploy and manage a microservices architecture with the option to integrate with Dapr.
AUTO-SCALE CRITERIA Scaling is determined by the number of concurrent HTTP requests.	AUTO-SCALE CRITERIA Triggered by a schedule, on demand, or based on events.	AUTO-SCALE CRITERIA Scaling is determined by the number of messages in the queue.	AUTO-SCALE CRITERIA Individual microservices can scale according to any KEDA scale triggers.

TOUTVIRTUAL 002989-TOUTVIRTUAL 002991;



Containers in an Azure Container Apps environment are grouped together in pods inside revision snapshots.



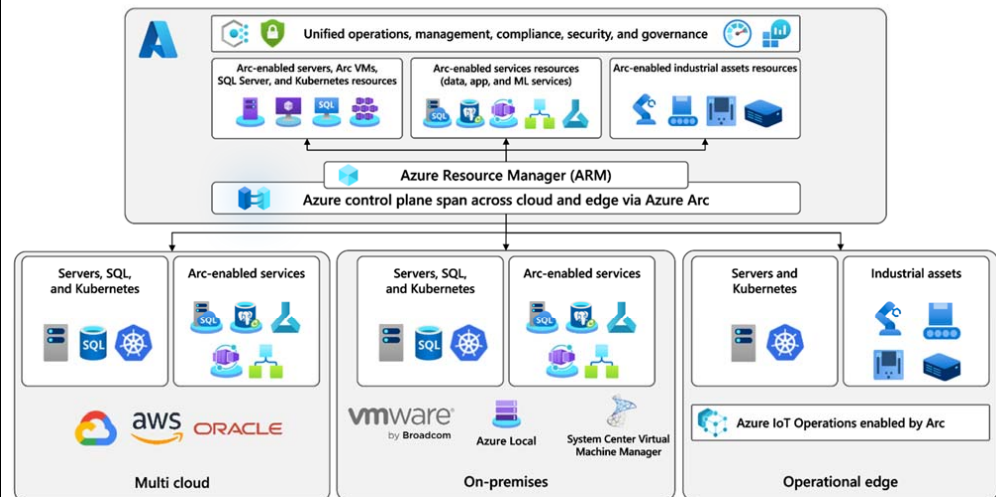
TOUTVIRTUAL 002992-TOUTVIRTUAL 002999; TOUTVIRTUAL 003000-TOUTVIRTUAL 003002; TOUTVIRTUAL 003003-TOUTVIRTUAL 003008.

The Accused Instrumentality provides AKS, which is a Kubernetes management service that allows users to deploy, scale, and manage containerized applications. AKS provides automated upgrades, node health monitoring, workload scheduling, and integration with Azure networking, storage, and security services. AKS relies on Azure virtual machines to serve as Kubernetes worker nodes. TOUTVIRTUAL 002260-TOUTVIRTUAL 002264; TOUTVIRTUAL 002614-TOUTVIRTUAL 002620, TOUTVIRTUAL 002640-TOUTVIRTUAL 002645; TOUTVIRTUAL 002646-TOUTVIRTUAL 002648; TOUTVIRTUAL 002649-TOUTVIRTUAL 002650.

The Accused Instrumentality provides Azure Arc, which extends management, governance, and Kubernetes orchestration capabilities to infrastructure running outside of the Azure environment, including on-premises servers, edge devices, and other cloud environments. TOUTVIRTUAL 002134-TOUTVIRTUAL 002137. Azure Arc also includes Azure Arc Resource Bridge, which is

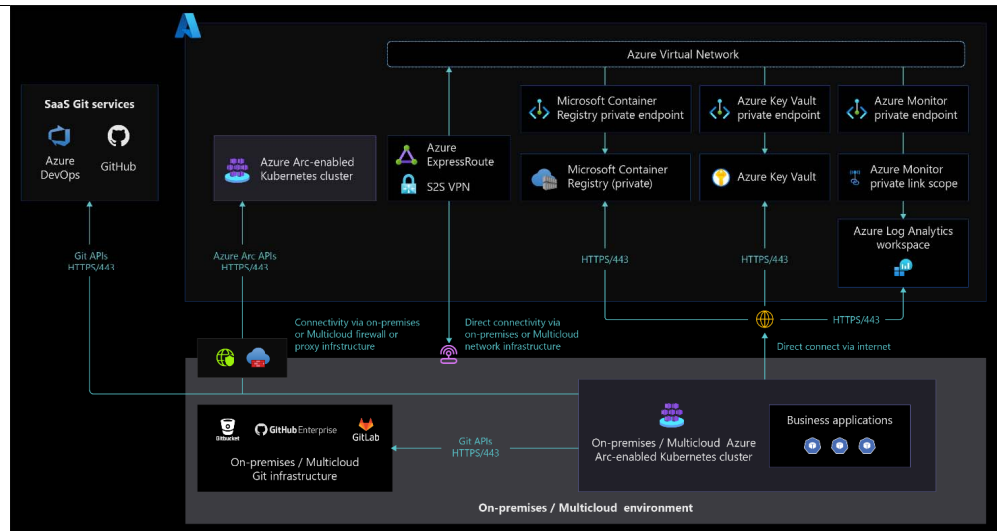
an appliance that runs in on-premises or edge environments and projects physical resources, such as servers, storage, and Kubernetes infrastructure, into the Azure Controllers as Azure resources. TOUTVIRTUAL 003039-TOUTVIRTUAL 003045. Azure Arc further projects these external systems into the Azure Portal or Windows Admin Center, allowing them to be managed through the same control plane as Azure physical resources and virtual assets.

Azure Arc solution overview architecture



TOUTVIRTUAL 002138-TOUTVIRTUAL 002142; TOUTVIRTUAL 002553-TOUTVIRTUAL 002570.

Azure Arc-enabled Kubernetes integrates external Kubernetes clusters within Azure's control plane. These clusters may run on different environments, such as Hyper-V in on-premises environments, VMware ESXi, bare-metal hardware, or cloud virtual machines in Amazon Web Services, Google Cloud Platform, etc. Regardless of the underlying environment, Azure Arc views these systems as Azure-managed virtual assets. TOUTVIRTUAL 002646-TOUTVIRTUAL 002648; TOUTVIRTUAL 002649-TOUTVIRTUAL 002650; TOUTVIRTUAL 002810-TOUTVIRTUAL 002816;



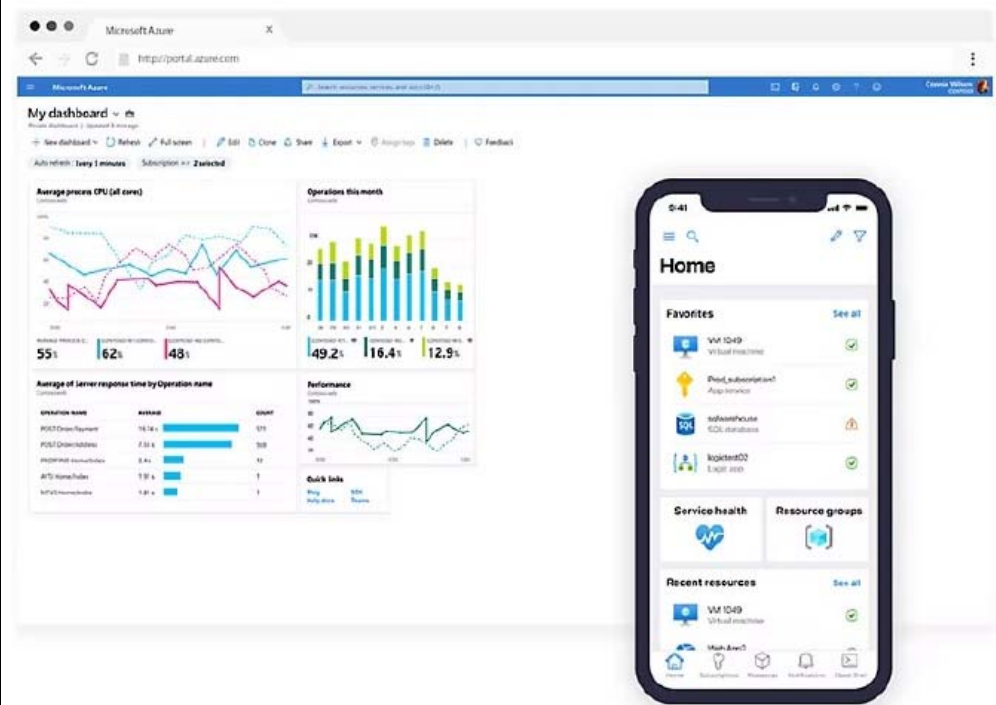
TOUTVIRTUAL 003211-TOUTVIRTUAL 003213; TOUTVIRTUAL 003217-TOUTVIRTUAL 003219; TOUTVIRTUAL 003220-TOUTVIRTUAL 003224.

The Accused Instrumentality provides Azure Functions, which extend Azure App Service’s functionality such that code may be implemented based on a trigger event. This functionality leverages Azure App Service such that code may be initiated automatically once a trigger event occurs so that the virtual environment may respond to changes instantaneously. TOUTVIRTUAL 002225-TOUTVIRTUAL 002226; TOUTVIRTUAL 002804-TOUTVIRTUAL 002806; TOUTVIRTUAL 005107-TOUTVIRTUAL 005114.

Claim 9	
9[pre]. An apparatus that performs automatic management of a virtualization environment in a computer network comprising:	The Accused Instrumentality meets the recited claim language because it provides an infringing apparatus that performs the automatic management of a virtualization environment in a computer network, as set forth below. The Accused Instrumentality is controlled by hardware owned and controlled by Microsoft, such that all steps are performed by it. The Accused Instrumentality is a cloud-based computing system that generates and automatically manages a distributed virtualization environment in a computer network, enabling users to deploy,

	configure, and operate virtual machines, containers, and other virtualized resources on demand without managing the underlying physical and software infrastructure. The Accused Instrumentality includes every component of the claimed apparatus, as set forth below.
9[a][i]. a virtualization environment having a computer device with a processor and memory and	The Accused Instrumentality meets the recited claim language because it provides a virtualization environment that has a computer device with a processor and memory. The Accused Instrumentality provides Microsoft's datacenters, which are where the physical servers that operate the Accused Instrumentality may be located. For example, these datacenters host physical resources (<i>i.e.</i>, servers), which are necessary for a virtualization environment to operate. Each of these physical resources is a computer device equipped with processors (CPUs) and system memory (RAM). These physical resources run a virtualization layer (<i>i.e.</i>, Azure Hypervisor or Microsoft Hyper-V), which virtualizes the underlying processor and memory resources to create and support virtual machines, container hosts, and other virtual assets. Microsoft's datacenters are in various regions to ensure that if one datacenter malfunctions, user data and operations will not be disrupted. TOUTVIRTUAL 003820-TOUTVIRTUAL 003823; TOUTVIRTUAL 003824-TOUTVIRTUAL 003828; TOUTVIRTUAL 003829-TOUTVIRTUAL 003831. The Accused Instrumentality provides Azure Dedicated Hosts, which are also physical resources located within Microsoft's datacenters. Azure Dedicated Hosts may host one or more virtual machines. Azure Dedicated Hosts provide users with the physical hardware resource meaning that the user has a computer device that has a processor and memory. While users who operate their virtualization environment with physical resources located in Microsoft's datacenters must share resources with other users, users who use Azure Dedicated Hosts have complete control over the processors and memory that are included in the computer device within their virtualization environment. TOUTVIRTUAL 002152-TOUTVIRTUAL 002156; TOUTVIRTUAL 002157-TOUTVIRTUAL 002165; TOUTVIRTUAL 002630-TOUTVIRTUAL 002637.
9[a][ii]. a control center computer coupled to the computer device,	See Claims 1[f] and 3. The Accused Instrumentality meets the recited claim language because Azure Controllers are control center computers that are coupled to the virtualization environment. The Accused Instrumentality provides Azure Portal, which is a control center computer that provides a unified, web-based console for creating, managing, and monitoring Azure resources, ranging from simple web apps to complex deployments through a graphical interface with integrated support. Azure Portal communicates over a network (such as the Internet or a local network) with the virtualization layers to create, configure, monitor, and deallocate virtual resources. Azure Portal

interacts with and allows users to visually manage and provision virtual machines, networks, storage resources, and functions over a network.

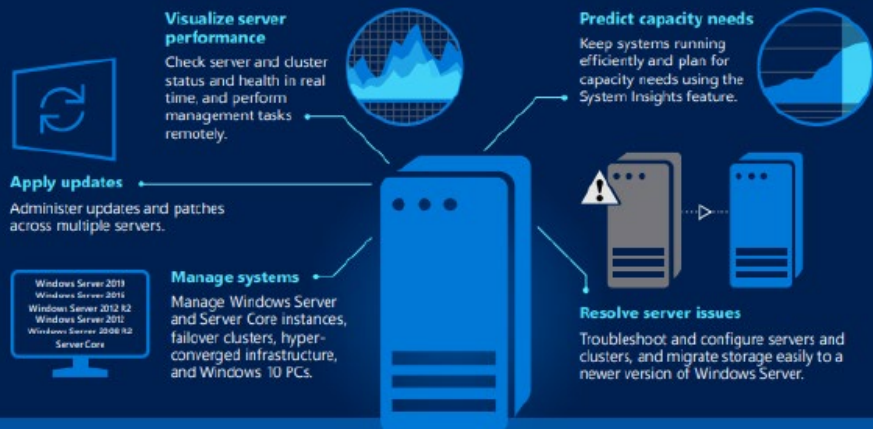


TOUTVIRTUAL 002509-TOUTVIRTUAL 002511; TOUTVIRTUAL 002124-TOUTVIRTUAL 002129; TOUTVIRTUAL 002503-TOUTVIRTUAL 002508.

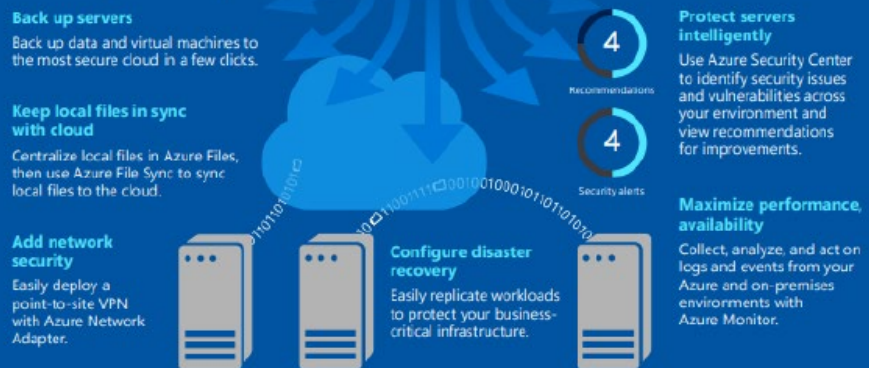
The Accused Instrumentality provides WAC, which acts as a network-coupled control center computer that communicates directly with the host servers or server clusters to provision and manage virtual machines, including environment connected through Azure Arc. TOUTVIRTUAL 002134-TOUTVIRTUAL 002137. WAC is a locally deployed management tool set that can manage Windows Clients, Servers, and Clusters without needing to connect to the cloud and provides full control over all aspects of server infrastructure including managing servers on private

	networks that are not connected to the Internet. WAC interacts with and allows users to perform actions such as management and provisioning of virtual machines, networks, storage resources, and functions over a network. TOUTVIRTUAL 002571-TOUTVIRTUAL 002575; TOUTVIRTUAL 002130-TOUTVIRTUAL 002133;
--	---

Streamline management tasks

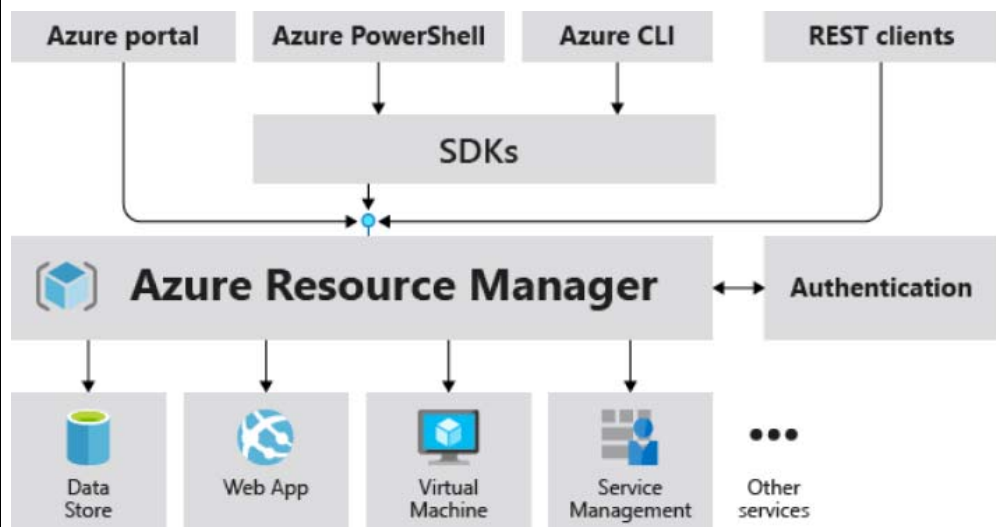


Extend your on-premises environment with Azure integrations



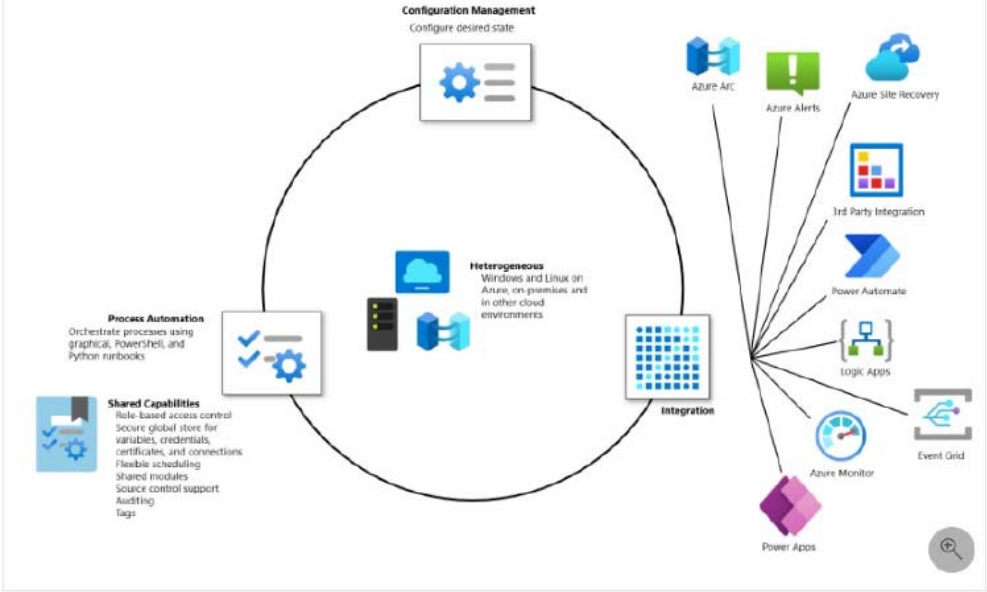
TOUTVIRTUAL 002596-TOUTVIRTUAL 002597.

The Accused Instrumentality provides Azure Resource Manager (“ARM”), which provides a deployment and management service that can create, update, and delete resource resources such as virtual machines, storage accounts, web apps, databases, and virtual networks within the Azure virtualization environment. TOUTVIRTUAL 002150-TOUTVIRTUAL 002151;



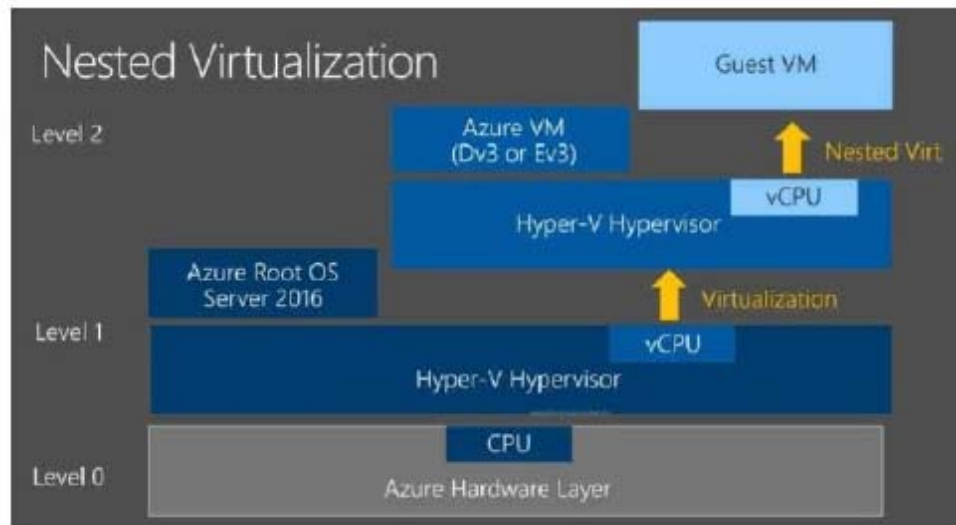
TOUTVIRTUAL 002143-TOUTVIRTUAL 002149.

The Accused Instrumentality provides Azure Automation, which supports the Azure Controllers by executing runbooks and scripts that automatically manage and reconfigure virtual resources through network-based APIs across the virtualization environment.

	 TOUTVIRTUAL 002166-TOUTVIRTUAL 002171; TOUTVIRTUAL 002760-TOUTVIRTUAL 002770; TOUTVIRTUAL 002771-TOUTVIRTUAL 002780.
9[a][iii]. the virtualization environment having an inventory that includes network resources and virtual assets being software instantiations of computer systems hosted on the computer device and a virtualization layer executed	The Accused Instrumentality meets the recited claim language because it includes a technology stack of hardware and software that performs steps of generating and operating a virtualization environment that has a virtualization layer, network resources, and virtual assets. The Accused Instrumentality provides a cloud-based environment that operates hypervisor technology (including Azure Hypervisor and/or Hyper-V), which creates the virtualization layer. This virtualization layer is the software that runs in conjunction with the physical servers in the datacenters or the Azure Dedicated Hosts to virtualize network resources and assets. The hypervisors used in the Accused Instrumentality is software technology that creates and manages virtual machines by virtualizing and allocating hardware resources like compute, network, and storage. Hypervisors serve as the foundational virtualization layer upon which compute

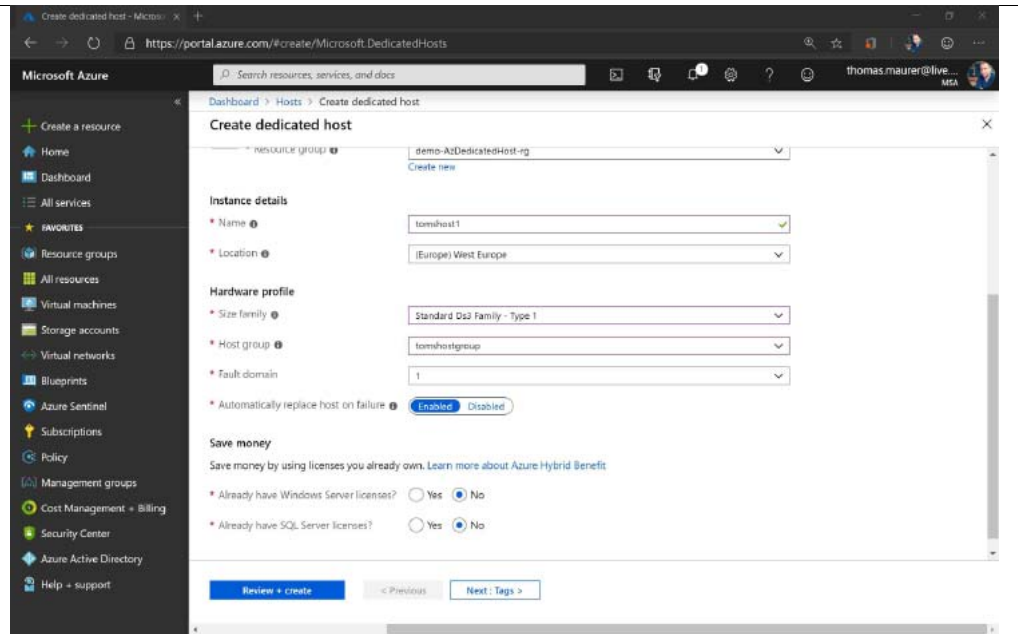
by the computer device that manages the virtual assets;

virtualization, network virtualization, application virtualization, and storage virtualization operate within the virtualization environment.



TOUTVIRTUAL 002658-TOUTVIRTUAL 002663; TOUTVIRTUAL 002651-TOUTVIRTUAL 002657; TOUTVIRTUAL 002664-TOUTVIRTUAL 002703.

The Accused Instrumentality provides network resources which include, but are not limited to, physical resources like processors, storage, and networking infrastructure components. Network resources also include software corresponding to processors, storage, and networking infrastructure components. Network resources further include the physical resources in the datacenters hosting the Accused Instrumentality and Azure Dedicated Hosts. TOUTVIRTUAL 002152-TOUTVIRTUAL 002156; TOUTVIRTUAL 002157-TOUTVIRTUAL 002165; TOUTVIRTUAL 002630-TOUTVIRTUAL 002637. These physical network resources are utilized to run the virtualization layer and enable communication, connectivity, security, and management among the virtual assets.

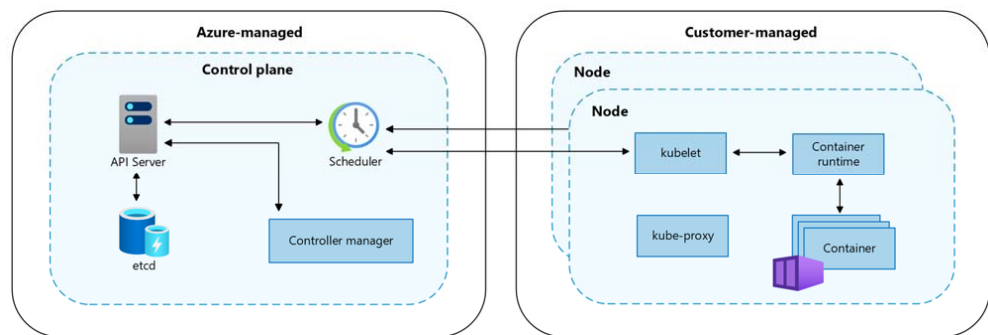


TOUTVIRTUAL 002621-TOUTVIRTUAL 002629.

The Accused Instrumentality provides virtual assets by abstracting hardware components within the virtualization environment that provide compute, network, applications, storage, etc. These virtual assets include, but are not limited to, software-based instantiations of equipment objects such as Azure Virtual Machines (servers) (TOUTVIRTUAL 002238-TOUTVIRTUAL 002246), Azure Virtual Desktop session hosts (desktops) (TOUTVIRTUAL 002247-TOUTVIRTUAL 002249), Azure Kubernetes Service (“AKS”) nodes and pods (application servers) (TOUTVIRTUAL 002260-TOUTVIRTUAL 002264), Arc-enabled virtual machines and Kubernetes nodes (on-premises and non-Azure servers) (TOUTVIRTUAL 003217-TOUTVIRTUAL 003219; TOUTVIRTUAL 003220-TOUTVIRTUAL 003224), and Azure storage services (storage) (TOUTVIRTUAL 002192-TOUTVIRTUAL 002203). Microsoft Azure’s virtualization layer manages these virtual assets by

allocating underlying physical resources and controlling execution within the Azure virtualization environment.

The Accused Instrumentality provides a virtualization layer (*i.e.*, Azure Hypervisor and/or Microsoft Hyper-V) on which its Kubernetes-based virtualization services operate, such as AKS, Azure Container Apps, Arc-enabled Kubernetes clusters, and Arc-enabled servers. TOUTVIRTUAL 002986-TOUTVIRTUAL 002988. The Accused Instrumentality implements a virtualization layer, which is executed by the physical servers, that abstracts the underlying system and provides a virtualization environment for services and applications, regardless of whether they run in the Azure virtualization environment or on an Arc-enabled infrastructure outside the Azure environment. The Kubernetes-based virtualization services allow for the deployment and management of containerized applications. TOUTVIRTUAL 002260-TOUTVIRTUAL 002264;



TOUTVIRTUAL 002614-TOUTVIRTUAL 002620.

The Accused Instrumentality's virtualization environment provides virtual assets, which include pods, containers, container groups, AKS nodes, Arc-enabled Kubernetes nodes, and deployments. These virtual assets are software instantiations of equipment objects, such as application servers, microservice components, data processing nodes, and workload endpoints. TOUTVIRTUAL 002260-TOUTVIRTUAL 002264; TOUTVIRTUAL 002614-TOUTVIRTUAL 002620; TOUTVIRTUAL 002649-TOUTVIRTUAL 002650.

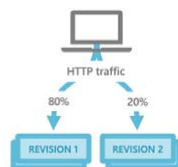
The Accused Instrumentality's virtualization environment provides network resources that support these virtual assets, including Azure Virtual Networks, container network interfaces, AKS networking, ingress controllers, and load balancers that route traffic internally and externally across the virtualization environment. Through Azure Arc, these same network and management

	capabilities extend to Arc-enabled servers and AKS clusters, allowing Microsoft Azure, including the Accused Instrumentality, to create, configure, monitor, inventory, and control virtualized applications running on non-Azure infrastructure. TOUTVIRTUAL 002134-TOUTVIRTUAL 002137; TOUTVIRTUAL 002138-TOUTVIRTUAL 002142; TOUTVIRTUAL 002646-TOUTVIRTUAL 002648; TOUTVIRTUAL 002649-TOUTVIRTUAL 002650; TOUTVIRTUAL 003205-TOUTVIRTUAL 003208. The Accused Instrumentality provides AKS, which is a Kubernetes management service that allows users to deploy, scale, and manage containerized applications. AKS provides automated upgrades, node health monitoring, workload scheduling, and integration with Azure networking, storage, and security services. AKS relies on Azure virtual machines to serve as Kubernetes worker nodes. TOUTVIRTUAL 002260-TOUTVIRTUAL 002264; TOUTVIRTUAL 002614-TOUTVIRTUAL 002620, TOUTVIRTUAL 002640-TOUTVIRTUAL 002645; TOUTVIRTUAL 002646-TOUTVIRTUAL 002648; TOUTVIRTUAL 002649-TOUTVIRTUAL 002650. The Accused Instrumentality provides Azure Container Apps, which is a container platform that runs microservices, event-driven applications, Application Programming Interfaces (“APIs”), and background jobs without requiring a user to manage the underlying Kubernetes clusters directly. TOUTVIRTUAL 002986-TOUTVIRTUAL 002988. Azure Container Apps leverages Kubernetes, Kubernetes Event-driven Autoscaling (“KEDA”), Distributed Application Runtime (“Dapr”), and Microsoft-managed scale controllers to automatically scale containers based on events, HTTP load, or resource metrics. TOUTVIRTUAL 003095-TOUTVIRTUAL 003103. Container workloads from Azure Container Apps are executed inside managed Kubernetes clusters that run on Azure compute infrastructure. These Azure Container Apps compute hosts are implemented as Azure virtual machines, which run on physical servers controlled by the virtualization layer.
--	---



Azure Container Apps: Example scenarios

PUBLIC API ENDPOINTS



HTTP requests are split between two versions of the container app where the first revision gets 80% of the traffic, while a new revision receives the remaining 20%.

AUTO-SCALE CRITERIA

Scaling is determined by the number of concurrent HTTP requests.

BACKGROUND PROCESSING



A background job that transforms data in a database.

AUTO-SCALE CRITERIA

Triggered by a schedule, on demand, or based on events.

EVENT-DRIVEN PROCESSING

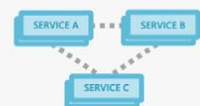


A queue reader application that processes messages as they arrive in a queue.

AUTO-SCALE CRITERIA

Scaling is determined by the number of messages in the queue.

MICROSERVICES



Deploy and manage a microservices architecture with the option to integrate with Dapr.

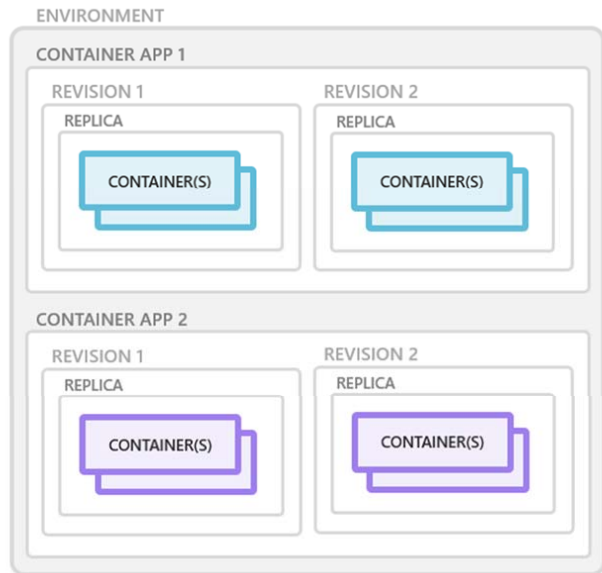
AUTO-SCALE CRITERIA

Individual microservices can scale according to any KEDA scale triggers.

TOUTVIRTUAL 002989-TOUTVIRTUAL 002991;



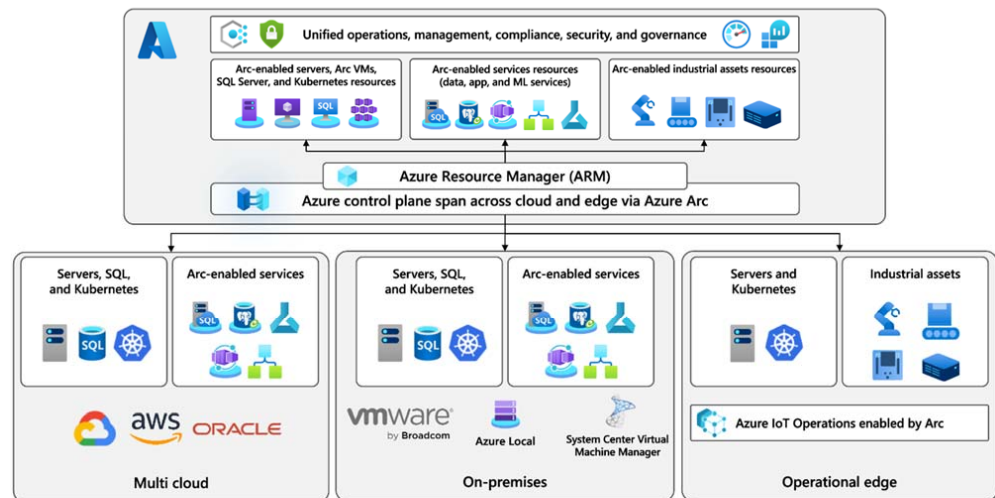
Containers in an Azure Container Apps environment are grouped together in pods inside revision snapshots.



TOUTVIRTUAL 002992-TOUTVIRTUAL 002999; TOUTVIRTUAL 003000-TOUTVIRTUAL 003002; TOUTVIRTUAL 003003-TOUTVIRTUAL 003008.

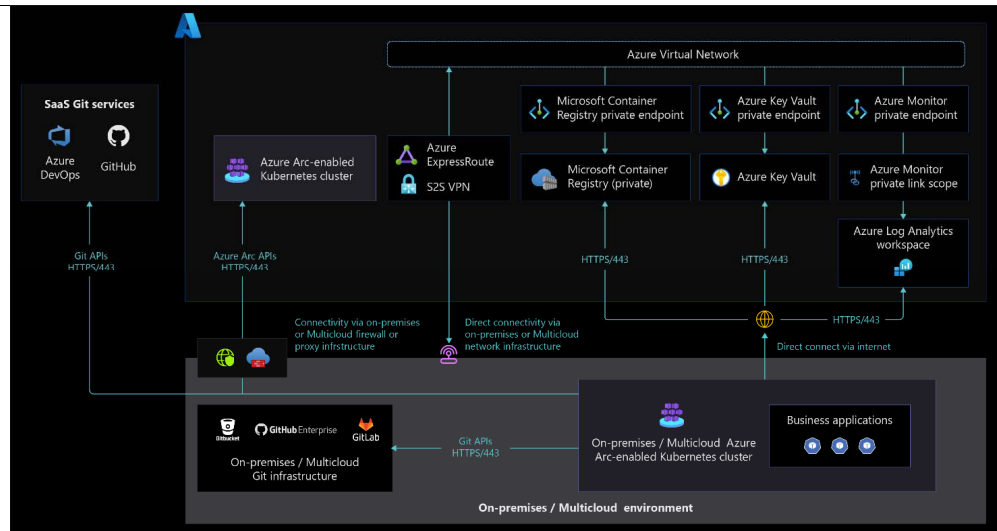
The Accused Instrumentality provides Azure Arc, which extends management, governance, and Kubernetes orchestration capabilities to infrastructure running outside of the Azure environment, including on-premises servers, edge devices, and other cloud environments. TOUTVIRTUAL 002134-TOUTVIRTUAL 002137. Azure Arc also includes Azure Arc Resource Bridge, which is an appliance that runs in on-premises or edge environments and projects physical resources, such as servers, storage, and Kubernetes infrastructure, into the Azure Controllers as Azure resources. TOUTVIRTUAL 003039-TOUTVIRTUAL 003045. Azure Arc further projects these external systems into the Azure Portal or Windows Admin Center, allowing them to be managed through the same control plane as Azure network resources and virtual assets.

Azure Arc solution overview architecture



TOUTVIRTUAL 002138-TOUTVIRTUAL 002142; TOUTVIRTUAL 002553-TOUTVIRTUAL 002570.

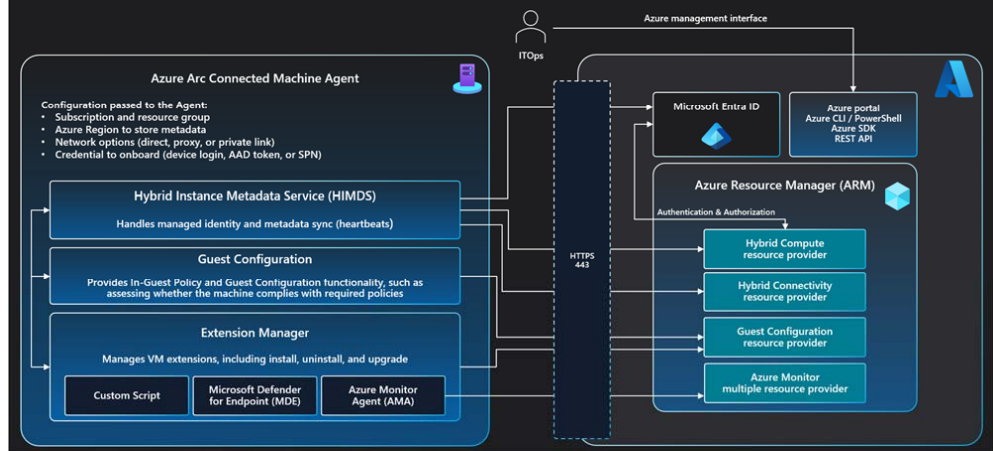
Azure Arc-enabled Kubernetes integrates external Kubernetes clusters within Azure's control plane. These clusters may run on different environments, such as Hyper-V in on-premises environments, VMware ESXi, bare-metal hardware, or cloud virtual machines in Amazon Web Services, Google Cloud Platform, etc. Regardless of the underlying environment, Azure Arc views these systems as Azure-managed virtual assets. TOUTVIRTUAL 002646-TOUTVIRTUAL 002648; TOUTVIRTUAL 002649-TOUTVIRTUAL 002650; TOUTVIRTUAL 002810-TOUTVIRTUAL 002816;



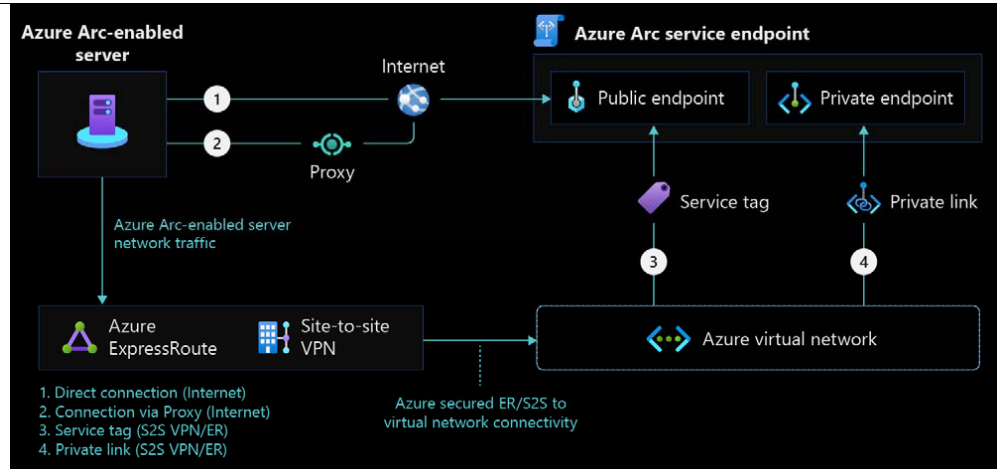
TOUTVIRTUAL 003211-TOUTVIRTUAL 003213; TOUTVIRTUAL 003217-TOUTVIRTUAL 003219; TOUTVIRTUAL 003220-TOUTVIRTUAL 003224.

Arc-enabled servers may run on a local virtualization layer (e.g., Microsoft Hyper-V, Linux KVM, or VMware ESXi) or on bare-metal hardware and connect to the Azure virtualization environment by using Azure Connected Machine agent. An Azure Monitor Agent is utilized to report the server's status to the Azure Portal or Windows Admin Center and to perform Azure functions, but the workloads may also be managed by the external virtualization layer.

Arc-enabled servers – Connected Machine agent architecture



TOUTVIRTUAL 003009-TOUTVIRTUAL 003017; TOUTVIRTUAL 003018-TOUTVIRTUAL 003020;

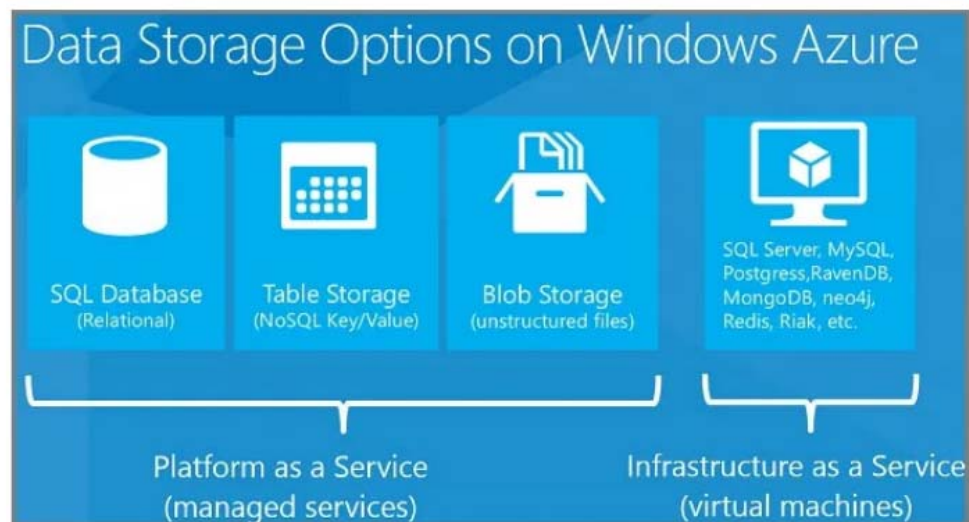


TOUTVIRTUAL 003205-TOUTVIRTUAL 003208.

The Accused Instrumentality provides a virtualization layer (*i.e.*, Azure Hypervisor and/or Microsoft Hyper-V) on which its storage virtualization services operate, such as Azure Blob Storage, Azure Files, Azure Disk Storage, and Azure Elastic Storage Area Network (“SAN”). The Accused Instrumentality implements a virtualization layer on a physical server that abstracts physical storage hardware into logical, managed, network-accessible storage resources. This allows these services to run as virtualized processes or within virtualized partitions isolated from other workloads.

TOUTVIRTUAL 002192-TOUTVIRTUAL 002203; TOUTVIRTUAL 002210-TOUTVIRTUAL 002224;

Azure Storage Services



TOUTVIRTUAL 002790-TOUTVIRTUAL 002803; TOUTVIRTUAL 002883-TOUTVIRTUAL 002899.

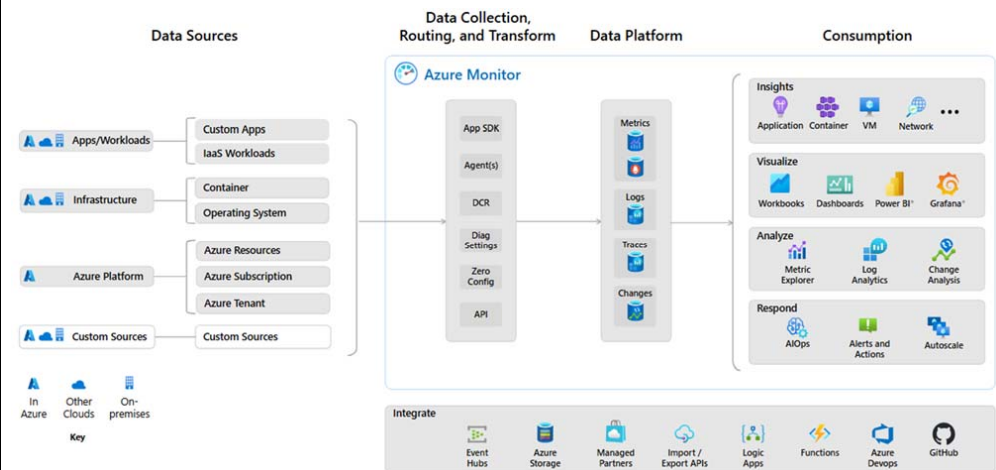
The Accused Instrumentality provides Azure Blob Storage, which is a massively scalable object-storage platform used to store unstructured data, such as documents, images, logs, backups, and application data. Azure Blob Storage virtualizes physical storage hardware across Microsoft datacenters, presenting a logical, distributed object-storage system that automatically handles replication, redundancy, durability, and global accessibility. TOUTVIRTUAL 002204-TOUTVIRTUAL 002209.

The Accused Instrumentality provides Azure Files, which provides fully managed, cloud-based file shares accessible via SMB (Server Message Block) and NFS (Network File System) protocols. Azure Files virtualizes storage so that a user can receive network-attached file shares without managing physical NAS (Network Attached Storage) appliances, file servers, RAID (Redundant Array of Independent Disks) storage, or storage controllers. Azure Files runs on Azure storage

	cluster nodes, which are virtualized or containerized storage processes executing on servers in Microsoft datacenters. TOUTVIRTUAL 003021-TOUTVIRTUAL 003023. The Accused Instrumentality provides Azure Disk Storage, which provides block-level VHDs (Virtual Hard Disks) used by Azure virtual machines, AKS node pools, database systems, and other workloads requiring persistent block devices. Each managed disk is a virtual abstraction of block storage that is presented to a virtual machine as if it was an attached physical disk. Azure Disk Storage is supported by storage services running on servers in Microsoft datacenters. TOUTVIRTUAL 003024-TOUTVIRTUAL 003028. The Accused Instrumentality provides Azure Elastic SAN, which is Azure's cloud-native storage service, providing high-performance block storage volumes grouped in SAN arrays accessible by multiple Azure virtual machines or compute clusters. Azure Elastic SAN replicates the architecture of on-premises SANs but fully virtualize the physical storage fabric and controllers. Azure Elastic SAN includes virtualized SAN arrays, virtualized storage pools, virtualized block volumes, and controllers for provisioning, zoning, and quality control. Azure Elastic SAN runs on Azure storage clusters built on physical servers in Microsoft datacenters. TOUTVIRTUAL 003029-TOUTVIRTUAL 003031. The Accused Instrumentality includes Azure Functions, which provides a virtualization environment that has a virtualization layer created by the Azure Hypervisors. Azure Functions automatically manages network resources and virtual assets for the user without having the user manage the underlying infrastructure. Azure Functions provides an environment where program code is run on an event-driven basis in a virtual environment without the user specifying a particular environment. TOUTVIRTUAL 002804-TOUTVIRTUAL 002806. For example, Azure Functions can operate in response to events such as HTTP requests or the creation of files. Azure Functions creates virtual assets in the form of software instantiations of equipment objects in the virtualization environment automatically based on the needs of the operation of the program code that is being run, with the virtualization layer managing the virtual assets. Azure Functions operate in a virtualized manner where it can connect to other Azure services using bindings for compute, network, application, and storage. TOUTVIRTUAL 003032-TOUTVIRTUAL 003038.
9[b][i]. the control center computer executing a virtual mapping layer that determines an inventory of network resources and virtual assets	The Accused Instrumentality meets the recited claim language because each Azure Controller executes a virtual mapping layer, Azure Resource Manager (ARM), that determines an inventory of network resources and virtual assets available to the virtualization environment. The Accused Instrumentality provides Azure Portal, which receives data on inventory available in the virtualization system and maintains a real-time inventory (for example, via the Azure Monitor (TOUTVIRTUAL 002733-TOUTVIRTUAL 002737; TOUTVIRTUAL 002738-TOUTVIRTUAL

available to the virtualization environment,

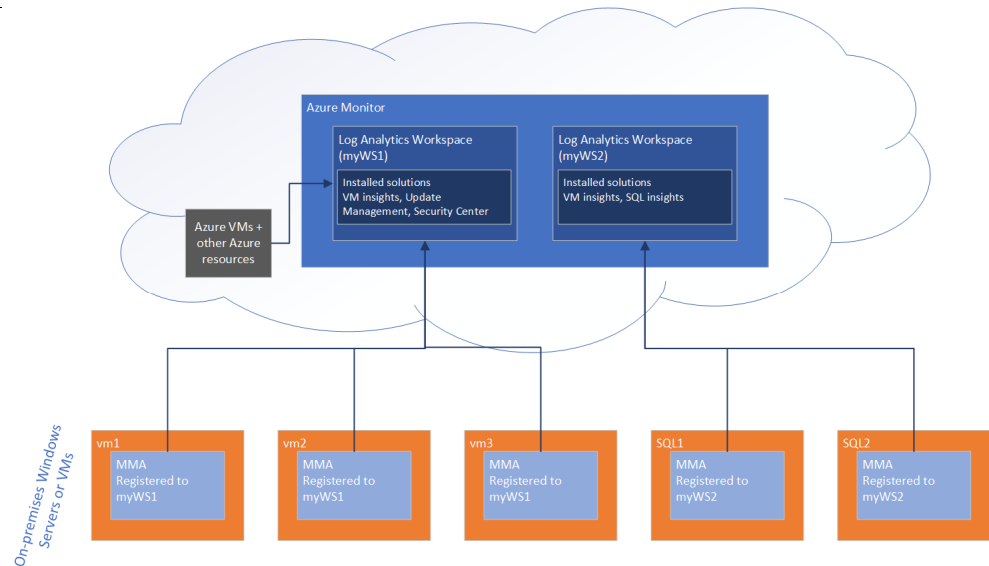
002745), Azure Automation (TOUTVIRTUAL 002166-TOUTVIRTUAL 002171; TOUTVIRTUAL 003178-TOUTVIRTUAL 003190), Azure Resource Graph (TOUTVIRTUAL 003191-TOUTVIRTUAL 003194; TOUTVIRTUAL 002721-TOUTVIRTUAL 002727; TOUTVIRTUAL 002817-TOUTVIRTUAL 002834; TOUTVIRTUAL 002835-TOUTVIRTUAL 002840), Azure Policy (TOUTVIRTUAL 002172-TOUTVIRTUAL 002181), and Azure Role-Based Access Control (“RBAC”) (TOUTVIRTUAL 002182-TOUTVIRTUAL 002189) of all virtual assets and network resources within a user’s network. Azure Portal executes ARM, which assigns each asset and resource with a unique identifier, resource type, and metadata that defines its state, dependencies, and relationships to other components in the virtualization environment. This metadata is stored and continuously updated within Azure Portal’s resource management database. TOUTVIRTUAL 002124-TOUTVIRTUAL 002129; TOUTVIRTUAL 002638-TOUTVIRTUAL 002639;



TOUTVIRTUAL 002265-TOUTVIRTUAL 002280; TOUTVIRTUAL 003169-TOUTVIRTUAL 003173.

The Accused Instrumentality provides WAC, which provides identification and management capabilities for hosts, servers, server clusters, and virtual machines, running outside of the infrastructure of the Accused Instrumentality, including on-premises datacenters and other cloud platforms, including those provided by other vendors. WAC connects to the virtualization layers

	over a network and executes ARM, which identifies the available virtual machines, networks, and storage pools. When integrated with Azure Arc (TOUTVIRTUAL 002134-TOUTVIRTUAL 002137), WAC extends ARM's management functionality to connected resources outside of the Azure infrastructure and synchronizes inventory and status data with the Azure virtualization environment, providing a user an inventory of all its connections and other identification and management Azure products that can be used with Azure Portal, like Azure Monitor (TOUTVIRTUAL 002265-TOUTVIRTUAL 002280; TOUTVIRTUAL 002733-TOUTVIRTUAL 002737; TOUTVIRTUAL 002738-TOUTVIRTUAL 002745), Azure Automation (TOUTVIRTUAL 002166-TOUTVIRTUAL 002171; TOUTVIRTUAL 003178-TOUTVIRTUAL 003190), Azure Resource Graph (TOUTVIRTUAL 003191-TOUTVIRTUAL 003194; TOUTVIRTUAL 002721-TOUTVIRTUAL 002727, TOUTVIRTUAL 002817-TOUTVIRTUAL 002834; TOUTVIRTUAL 002835-TOUTVIRTUAL 002840), Azure Policy (TOUTVIRTUAL 002172-TOUTVIRTUAL 002181), and Azure Role-Based Access Control (TOUTVIRTUAL 002182-TOUTVIRTUAL 002189). Through this connection, the user can view, configure, or migrate virtual assets between local and cloud environments, all while maintaining a single identified resource set. TOUTVIRTUAL 002571-TOUTVIRTUAL 002575; TOUTVIRTUAL 002130-TOUTVIRTUAL 002133;
--	---

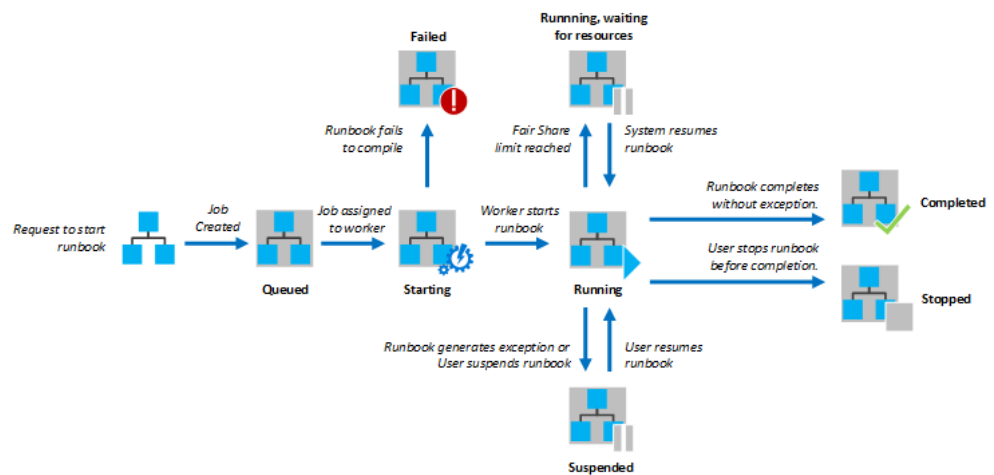


TOUTVIRTUAL 003174-TOUTVIRTUAL 003177.

The Azure Controllers, in conjunction with ARM, may retrieve, display, and manage the identified network resources and virtual assets. Azure Controllers visualize this information as a hierarchical resource map that shows, for example, how a virtual machine connects to a network, subnet, and virtual network, providing the relationships and configurations of the virtual assets. Through the Azure Controllers, a user can perform management actions (such as start, stop, reconfigure, or delete) that are transmitted to ARM, which in turn executes those commands on the virtualization layers. TOUTVIRTUAL 002143-TOUTVIRTUAL 002149.

The Azure Controllers, in conjunction with ARM, may utilize other identification and management Azure products to operate as a virtual mapping layer, like Azure Monitor (TOUTVIRTUAL 002265-TOUTVIRTUAL 002280; TOUTVIRTUAL 002733-TOUTVIRTUAL 002737; TOUTVIRTUAL 002738-TOUTVIRTUAL 002745), Azure Automation (TOUTVIRTUAL 002166-TOUTVIRTUAL 002171; TOUTVIRTUAL 003178-TOUTVIRTUAL 003190), Azure Resource Graph (TOUTVIRTUAL 003191-TOUTVIRTUAL 003194; TOUTVIRTUAL 002721-TOUTVIRTUAL 002727; TOUTVIRTUAL 002817-TOUTVIRTUAL 002834; TOUTVIRTUAL

002835-TOUTVIRTUAL 002840), Azure Policy (TOUTVIRTUAL 002172-TOUTVIRTUAL 002181), and Azure RBAC (TOUTVIRTUAL 002182-TOUTVIRTUAL 002189). Azure Monitor collects, analyzes, and responds to monitoring data. Azure Automation integrates with Azure Monitor, enabling Azure Controllers to retrieve telemetry data and apply management policies based on resource health or performance status. Using runbooks (scripted workflows), Azure Automation continuously checks the configurations and status of virtual machines, networks, and storage registered with the Azure Controllers. Azure Resource Graph enables cross-resource querying and inventory management, while Azure Policy and Azure RBAC enforce consistent management and compliance rules across identified assets. The Azure Controllers may present this data and these identification and management Azure products visually, allowing users to apply, modify, or audit them. TOUTVIRTUAL 002937-TOUTVIRTUAL 002946;



TOUTVIRTUAL 002947-TOUTVIRTUAL 002956;

←

↺

🏠

🔍

🌐

https://portal.azure.com/

Microsoft Azure

🔍 resource graph

✕

Azure services

+

Create a resource

🔗

Resource Graph Explorer

All

Services (18)

Documentation (99+)

More (4)

Services

See all

🔗 Resource Graph Explorer

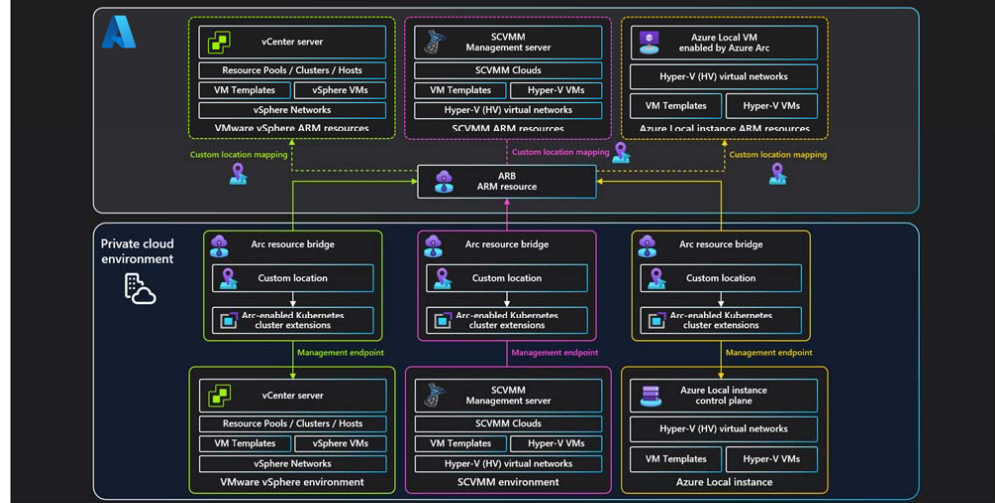
📄 Resource Graph queries

👤 Resource groups

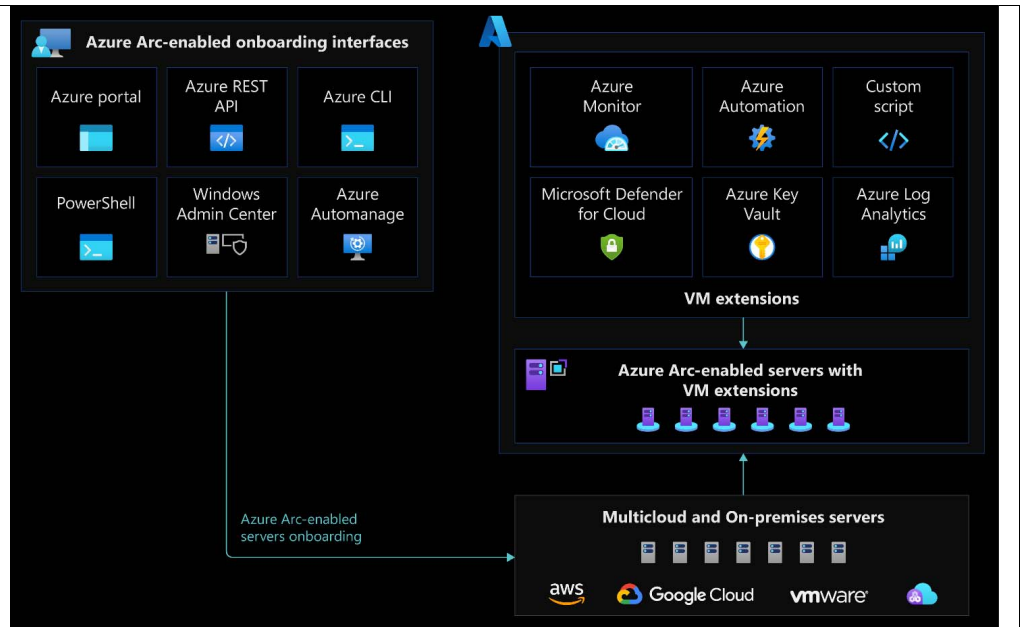
TOUTVIRTUAL 003195-TOUTVIRTUAL 003200.

The Azure Controllers, in conjunction with ARM, may determine an inventory of network resources and virtual assets available to the virtualization environment Arc-enabled servers, Kubernetes clusters, and virtual machines running outside of the Azure infrastructure with Azure Arc, including on-premises datacenters and other cloud platforms. TOUTVIRTUAL 002640-TOUTVIRTUAL 002645. Through Azure Arc, an Azure Connected Machine agent is installed on external systems and registers the resources on those systems with the Azure Controllers. TOUTVIRTUAL 002134-TOUTVIRTUAL 002137; TOUTVIRTUAL 003009-TOUTVIRTUAL 003017. Azure Arc further includes Azure Arc Resource Bridge, which is an appliance that runs in on-premises or edge environments and projects physical resources, such as servers, storage, and Kubernetes infrastructure, into the Azure Controllers as Azure resources.

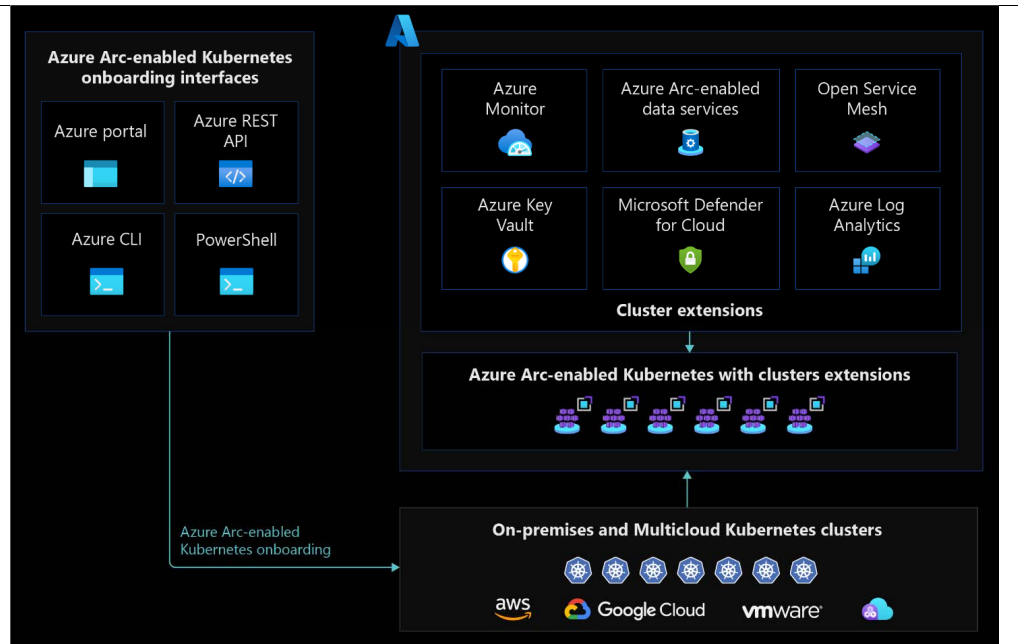
Arc resource bridge (ARB) – Solution architecture



TOUTVIRTUAL 003039-TOUTVIRTUAL 003045. By establishing a secure control-plane connection between the external infrastructure and the Azure infrastructure with Azure Arc and Azure Arc Resource Bridge, the Azure Controllers automatically discovers and inventories the external systems' network resources and virtual assets, such as Arc-enabled virtual machines, physical or virtual servers, Arc-enabled Kubernetes nodes, pods, container workloads, network endpoints, and security configurations. TOUTVIRTUAL 002746-TOUTVIRTUAL 002748; TOUTVIRTUAL 002749-TOUTVIRTUAL 002759; TOUTVIRTUAL 002810-TOUTVIRTUAL 002816;



TOUTVIRTUAL 003201-TOUTVIRTUAL 003204;



TOUTVIRTUAL 003214-TOUTVIRTUAL 003216.

The Azure Controllers, in conjunction with ARM, may receive data on the inventory available of container-based virtual assets with AKS. Azure Controllers can automatically inventory clusters, node pools, pods, deployments, load balancers, Kubernetes components, and persistent volumes. TOUTVIRTUAL 002640-TOUTVIRTUAL 002645.

The Azure Controllers, in conjunction with ARM, may receive data on inventory available within an Azure Container Apps environment, which functions as a secure boundary that contains multiple container apps, jobs, and revisions. TOUTVIRTUAL 003046-TOUTVIRTUAL 003049. Azure Controllers automatically identify and manage the container apps deployed in each environment, along with their associated virtual assets such as revisions, scaling rules, ingress, configurations, and container replicas. An Azure Container Apps environment is associated with network resources, including virtual networks, subnets, container network interfaces, and ingress endpoints, that Azure

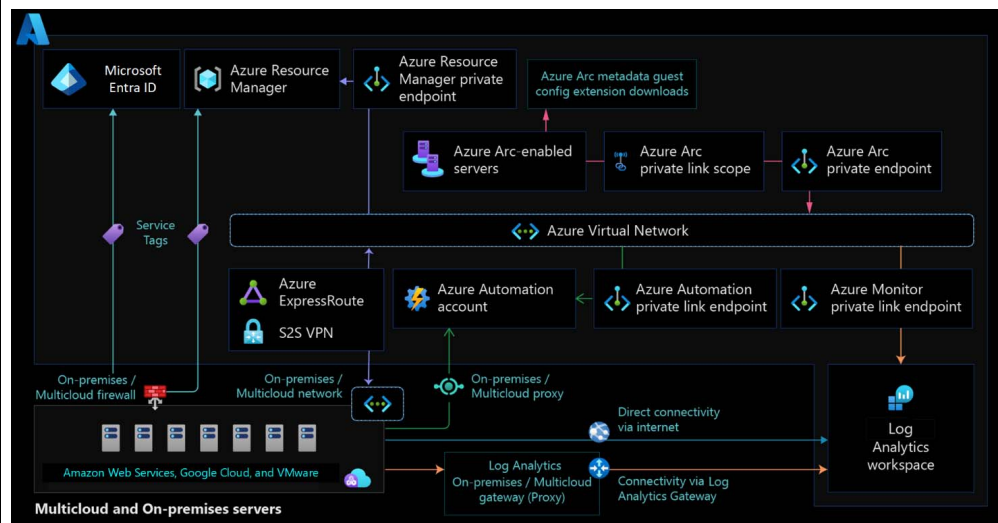
	identifies for management. TOUTVIRTUAL 003058-TOUTVIRTUAL 003061. An Azure Container Apps environment also shares a centralized logging and monitoring workspace, allowing Azure Controllers to uniformly track and manage virtual assets across all applications connected to the Azure virtualization environment and determine an inventory of network resources and virtual assets available to the virtualization environment. TOUTVIRTUAL 003000-TOUTVIRTUAL 003002; TOUTVIRTUAL 003050-TOUTVIRTUAL 003057; TOUTVIRTUAL 002225-TOUTVIRTUAL 002226; TOUTVIRTUAL 002900-TOUTVIRTUAL 002908; TOUTVIRTUAL 003729-TOUTVIRTUAL 003736. The Azure Controllers, in conjunction with ARM, may identify each storage account or container as a managed object, track its provisioning, configuration, replication settings, encryption status, lifecycle policies, and cost/performance metadata. Through Azure Monitor and Azure Resource Graph, Azure Controllers may receive metrics, like latency, capacity, throughput, for each storage virtual asset, enabling Azure Controllers to manage them alongside compute, network, applications, and storage resources. TOUTVIRTUAL 002855-TOUTVIRTUAL 002868; TOUTVIRTUAL 002810-TOUTVIRTUAL 002816; TOUTVIRTUAL 002817-TOUTVIRTUAL 002834; TOUTVIRTUAL 002835-TOUTVIRTUAL 002840; TOUTVIRTUAL 002841-TOUTVIRTUAL 002847. Through AKS and Azure Container Apps, container workloads and Kubernetes pods often rely on persistent volumes, file shares, or blob storage. Azure Controllers may identify these storage assets and their relationships to workloads, enabling unified lifecycle and performance management across compute, network, applications, and storage domains. Through Azure Arc, Arc-enabled servers and Kubernetes clusters may run workloads that access on-premises SANs, file shares, or cloud storage. Azure Controllers can identify and manage these storage resources through Arc agents, treating external storage shares, caching gateways, and edge-appliances as virtual assets within the same Azure inventory. TOUTVIRTUAL 002746-TOUTVIRTUAL 002748; TOUTVIRTUAL 002749-TOUTVIRTUAL 002759; TOUTVIRTUAL 003109-TOUTVIRTUAL 003118. The Azure Controllers, in conjunction with ARM, may receive the inventory available of network resources and virtual assets in response to event-driven events, such as through Azure Functions. The Azure Controllers will automatically manage the network resources and virtual assets as needed in response to the code that is being run in Azure Functions. TOUTVIRTUAL 002804-TOUTVIRTUAL 002806; TOUTVIRTUAL 003062-TOUTVIRTUAL 003079.
--	---

9[b][ii].

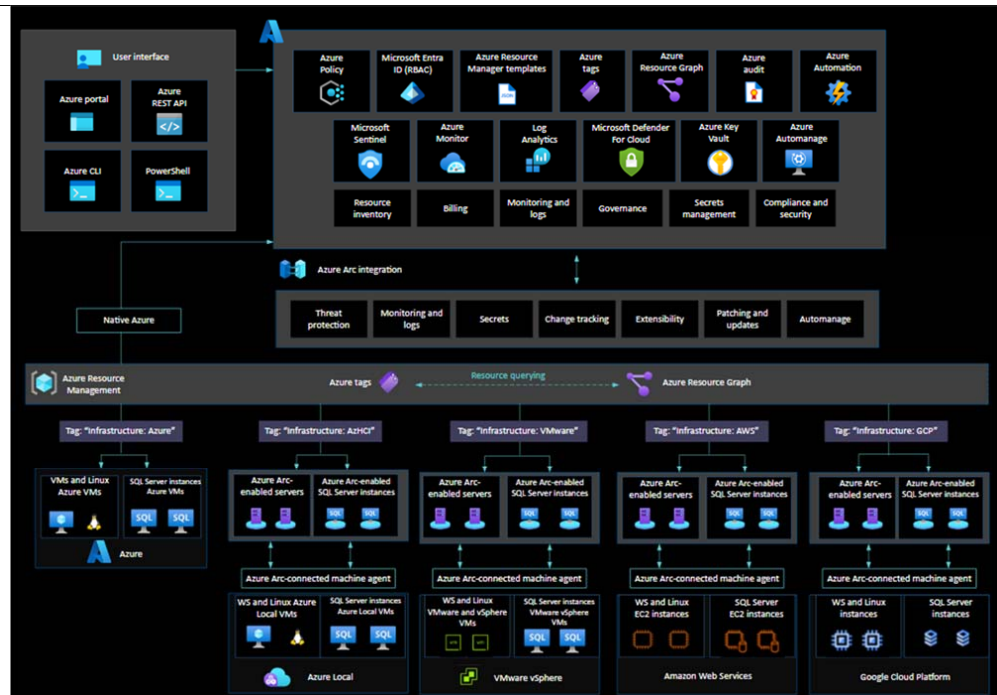
wherein the virtual mapping layer determines the inventory without regard to processors, operating systems, virtualization platforms, and application software of the virtualization environment; and

The Accused Instrumentality meets the recited claim language because it provides the virtual mapping layer which determines the inventory without regard to the specific processors, operating systems, virtualization platforms, and application software of the virtualization environment.

The Accused Instrumentality includes a virtual mapping layer, ARM, which monitors resources and applications that are running in other clouds, such as Amazon Web Services (AWS) and Google Cloud Platform (GCP). TOUTVIRTUAL 002746-TOUTVIRTUAL 002748. The virtual mapping layer abstracts the specific implementation details of the processors, operating systems, virtualization platforms, and application software, allowing the functionality to be carried out for a particular user without regard to their specific implementation details and not be contingent on specific lower-level details of the system.



TOUTVIRTUAL 003205-TOUTVIRTUAL 003208;



TOUTVIRTUAL 003209-TOUTVIRTUAL 003210.

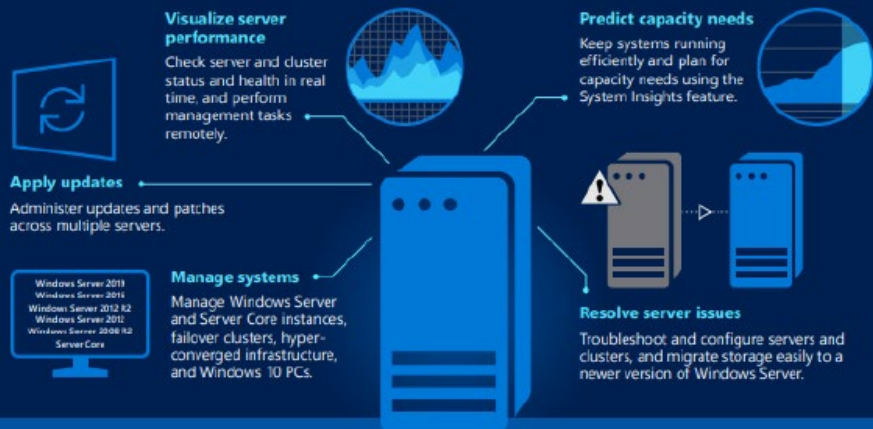
The Accused Instrumentality operates on the Azure Hypervisor and/or Hyper-V. The Azure Controllers do not depend on the specific processor type (i.e., Intel, AMD, or ARM-based hardware), nor does it rely on the OS running inside the virtual machines or containers it manages. Whether the underlying resources run Windows or Linux, or whether they host virtual machines, AKS nodes, Azure Container Apps containers, or Arc-enabled servers, the Azure Controllers interact with their resource representations, enabling uniform control regardless of differences in the underlying platform.

The Accused Instrumentality operates Azure Arc, which allows the Azure Controllers to execute ARM to discover, monitor, and control external network resources and virtual assets, including

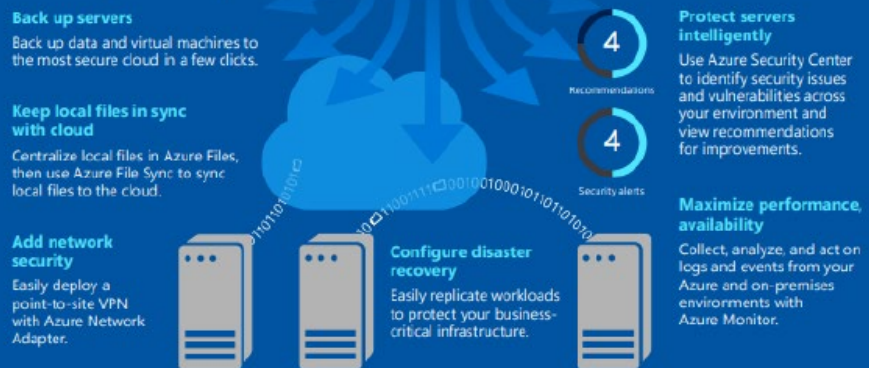
	Linux VMs, Windows servers, and Kubernetes clusters hosted on-premises, either in AWS or GCP. Azure Arc Resource Bridge, Arc-enabled servers, and Arc-enabled Kubernetes clusters may run on entirely different infrastructures, such as VMware vSphere, on-premises bare metal, AWS EC2, or Google Compute Engine, and may run different operating systems or virtualization stacks. Azure Arc translates virtual mapping layer policies and actions into platform-specific instructions automatically, so the same control logic applies uniformly across all environments, including other cloud platforms where the internal underlying infrastructure is not known. The Accused Instrumentality provides AKS and Azure Container Apps. Azure Container Apps workloads run on Azure-managed container hosts, while AKS workloads run on Kubernetes nodes based on virtual machines. These hosts and nodes may run different Linux distributions, different container runtimes, and different Kubernetes versions. However, the Azure Controllers may execute the virtual mapping layer to discover and inventory these resources through standardized ARM templates, APIs, and policy definitions that operate independently of operating systems or application software differences. The Accused Instrumentality may also provide Azure Functions, which operates code to be run without regard to any particular infrastructure that it is run in. To the extent that this element is not met literally, it is met under the Doctrine of Equivalents. In particular, the virtual mapping layer performs its function in a way to achieve the same result. Namely, the Accused Instrumentality allows for virtual mapping of different systems with different, potentially unknown, implementations.
9[c]. the control center computer executing a provisioning manager that communicates with the virtual mapping layer,	The Accused Instrumentality meets the recited claim language because each Azure Controller executes a provisioning manager that communicates with the virtual mapping layer. The Accused Instrumentality provides Azure Portal, which may be coupled a computer device with processors and memory and may receive virtual asset provisioning requests from users, applications, or automated network workflows, such as Azure Resource Manager, Azure Logic Apps, Azure Monitor, and related Azure services. Azure Portal may then execute Azure Logic Apps, which may communicate with Azure Resource Manager to provide an on-demand solution for the provisioning of virtual assets for an automated workflow management. TOUTVIRTUAL 004005-TOUTVIRTUAL 004016; TOUTVIRTUAL 005751-TOUTVIRTUAL 005765; TOUTVIRTUAL 005766-TOUTVIRTUAL 005796; TOUTVIRTUAL 005797-TOUTVIRTUAL 005801. For example, Azure Logic Apps may receive provisioning requests or triggers (<i>i.e.</i>, user input, API calls, alerts, schedules, or events), and evaluate parameters associated with the provisioning requests (<i>i.e.</i>, resource type, size, region, performance tier, priority, dependencies, or timing). Azure Logic Apps may then determine the sequence of provisioning actions required to satisfy the request based on the

	prioritization configurations set by an administrator. TOUTVIRTUAL 005676-TOUTVIRTUAL 005697; TOUTVIRTUAL 005698-TOUTVIRTUAL 005716; TOUTVIRTUAL 005717-TOUTVIRTUAL 005750. Azure Portal may also execute Azure Arc, which may communicate with Azure Resource Manager to provide an option to provision virtual assets for automated workflow management via on-premises or Arc-enabled Kubernetes infrastructure. TOUTVIRTUAL 002134-TOUTVIRTUAL 002137; TOUTVIRTUAL 003039-TOUTVIRTUAL 003045. The Accused Instrumentality provides WAC, which integrates with Azure Arc, as the control center computer within on-premises infrastructure to execute Azure Logic Apps. Azure Logic Apps may communicate with Azure Resource Manager to provide central management of global virtual assets and an enterprise workflow system for adds, moves, and changes within on-premises infrastructure. TOUTVIRTUAL 002571-TOUTVIRTUAL 002575; TOUTVIRTUAL 002130-TOUTVIRTUAL 002133;
--	--

Streamline management tasks



Extend your on-premises environment with Azure integrations



	TOUTVIRTUAL 002596-TOUTVIRTUAL 002597.
9[d][i]. the processor being configured to receive a virtual asset provisioning request that specifies parameters to be considered for the virtual asset provisioning request,	The Accused Instrumentality meets the recited claim language because the processor, in conjunction with the control center computer (Azure Controllers), is configured to receive a virtual asset provisioning request that specifies the parameters to be considered for the virtual asset provisioning request. The Accused Instrumentality provides a processor, which in conjunction with the Azure Portal may receive a virtual asset provisioning request either from a user, application, or automated network workflow. After receiving the request, the processor in conjunction with the Azure Portal may request additional resources or provision the necessary virtual assets through API-driven deployment, ARM templates, or Autoscale triggers (via Azure Monitor). TOUTVIRTUAL 002704-TOUTVIRTUAL 002710; TOUTVIRTUAL 002711-TOUTVIRTUAL 002720. The processor in conjunction with the Azure Portal may receive API calls from services, such as Azure Virtual Machine Scale Sets (“VMSS”) (TOUTVIRTUAL 002964-TOUTVIRTUAL 002977), AKS, Azure Functions, and Azure Automation, for the provisioning of virtual assets. When Azure services detect increased network load or user activity, these services may communicate with the processor and the Azure Portal over a network to provision additional virtual assets, such as new virtual machines, container pods, or serverless compute instances, on the virtualization layer. The processor and the Azure Portal may then allocate compute, network, application, and storage resources from the available capacity in the Azure virtualization environment, configuring each new instance, and updating the system’s resource inventory in real time. TOUTVIRTUAL 002721-TOUTVIRTUAL 002727; TOUTVIRTUAL 002728-TOUTVIRTUAL 002732; TOUTVIRTUAL 002869-TOUTVIRTUAL 002882. The Accused Instrumentality provides a processor, which in conjunction with WAC integrates with Azure Arc to provision virtual assets in response to network workflow demands, particularly within hybrid Azure virtualization environments (i.e., virtualization environments consisting of Azure systems and non-Azure Arc-enabled systems). The processor in conjunction with WAC communicates directly with hosts, servers or server clusters to deploy new virtual machines and virtual networks within or outside of the Azure infrastructure, including on-premises datacenters and other cloud platforms, in response to increased workload or network demand. The processor in conjunction with WAC may initiate provisioning operations by receiving API calls from Azure VMSS, AKS, Azure Functions, and Azure Automation; and deploy virtual machines, containers, or serverless compute instances to handle workload surges originating from on-premises or edge environments. TOUTVIRTUAL 002543-TOUTVIRTUAL 002552; TOUTVIRTUAL 003084-TOUTVIRTUAL 003088; TOUTVIRTUAL 003089-TOUTVIRTUAL 003094. For example, users may submit virtual asset provisioning requests to the processor and WAC, which may include the

	parameters to be considered for the virtual asset provisioning request. The processor and WAC, via ARM, may then initialize the virtual asset. The processor in conjunction with the Azure Controllers may perform this provisioning functionality for Arc-enabled servers and external systems not hosted within the Azure infrastructure. Using Azure Arc-enabled servers and Arc-enabled Kubernetes clusters, users can deploy virtual assets, such as containerized workloads, configuration profiles, applications, policies, extensions, and management agents, directly onto non-Azure servers or server clusters from the processor and Azure Controllers. TOUTVIRTUAL 003080-TOUTVIRTUAL 003083; TOUTVIRTUAL 003201-TOUTVIRTUAL 003204; TOUTVIRTUAL 003214-TOUTVIRTUAL 003216. The processor and the Azure Controllers treat Arc-enabled systems as Azure resources, allowing Azure Portal to provision assets via deployments, ARM templates, Azure Policy assignments, or Automation runbooks in response to workflow demands detected in Azure Monitor or by an Arc Connected Machine agent. TOUTVIRTUAL 003009-TOUTVIRTUAL 003017. The Accused Instrumentality provides a processor in conjunction with the Azure Controllers that may perform this provisioning functionality for an Azure Container Apps environment. TOUTVIRTUAL 003225-TOUTVIRTUAL 003237. When workflow demands increase (e.g., rising HTTP request rates, queue depth, event stream activity, or custom metric thresholds), Azure Container Apps's Kubernetes Event-Driven Autoscaling ("KEDA") rules generate signals that the processor and the Azure Controllers may evaluate against the physical resource's configuration. TOUTVIRTUAL 003095-TOUTVIRTUAL 003103. These virtual asset provisioning requests specify the parameters of the virtual assets that are being requested. The processor and the Azure Controllers may then provision additional container replicas, new revisions, or job executions within the Azure Container Apps environment. The processor and the Azure Controllers may also provision supporting physical resources whenever Azure Container Apps workloads scale or new applications are deployed. TOUTVIRTUAL 003238-TOUTVIRTUAL 003239; TOUTVIRTUAL 003737-TOUTVIRTUAL 003740. The processor in conjunction with the Azure Controllers may perform this provisioning functionality for applications running in AKS. TOUTVIRTUAL 003240-TOUTVIRTUAL 003241. Workflow signals from Kubernetes components, such as Horizontal Pod Autoscaler metrics, Vertical Pod Autoscaler recommendations, or Cluster Autoscaler node-capacity triggers, may cause the processor and the Azure Controllers to request additional underlying resources based on the specified parameters in the provisioning request. The processor and the Azure Controllers may then respond to this request by provisioning new virtual machines, expanding node pools, or deploying additional
--	---

	Kubernetes workloads as specified, thereby establishing a provisioned virtualization environment. TOUTVIRTUAL 003104-TOUTVIRTUAL 003108. The Azure Controllers may perform this provisioning functionality for applications running within private or on-premises environments, or Arc-enabled Kubernetes through Azure Arc. The Azure Controllers, via Azure Arc Resource Bridge, may provide custom locations within the private or on-premises environments, Kubernetes nodes, pods, container workloads, network endpoints, or security configurations which are considered when a virtual asset provisioning request is made. TOUTVIRTUAL 003039-TOUTVIRTUAL 003045; TOUTVIRTUAL 005089-TOUTVIRTUAL 005091. After validating the virtual asset provisioning request, the Azure Controllers, via Azure Arc, may use the custom locations to automatically provision on-premises environment or Kubernetes resources to fulfill the virtual asset provisioning request. For example, if a virtual asset's workload increases, the Azure Controllers via Azure Arc may automatically provision more resources from the on-premises environment or Kubernetes nodes pods, container workloads, network endpoints, and security configurations. The processor in conjunction with the Azure Controllers may provision storage virtual assets in response to workflow demands, such as Blob Storage accounts, file shares, managed disks, Elastic SAN volumes, and other storage service instances. This enables the processor and the Azure Controllers to allocate the required storage capacity or resources to the provisioning request based on the specified parameters. For example, if an application workload experiences heavy growth, the processor in conjunction with the Azure Controllers may determine via Autoscale rules or workflow logic that additional storage throughput or capacity is required. TOUTVIRTUAL 002869-TOUTVIRTUAL 002882. The processor and the Azure Controllers may then provision additional Blob Storage containers, create new managed disk volumes for new virtual machines being scaled out, or configures additional Elastic SAN volumes and attaches them to VMSS. The processor in conjunction with the Azure Controllers may also create or dynamically scale storage accounts using ARM templates or Automation runbooks triggered by workflow conditions (<i>e.g.</i>, data ingestion spike). TOUTVIRTUAL 002166-TOUTVIRTUAL 002171; TOUTVIRTUAL 002598-TOUTVIRTUAL 002603; TOUTVIRTUAL 002604-TOUTVIRTUAL 002613; TOUTVIRTUAL 002937-TOUTVIRTUAL 002946. When storage demand decreases or shifts, the processor in conjunction with the Azure Controllers may also de-provision or reallocate storage assets (<i>e.g.</i>, shrink file share quotas, decommission unused managed disks) through Automation tasks. The Accused Instrumentality provides VMSS, AKS, Azure Functions, and Azure Automation, which represent specific Azure services that implement the provisioning actions directed by the processor in conjunction with the Azure Controllers. VMSS provisions and scales virtual machines based on demand metrics. AKS provisions container pods and cluster nodes in response to network
--	--

	traffic and workload signals. Azure Functions provisions containers in response to network-based triggers such as HTTP requests or message events. Azure Automation provisions virtual assets in response to network workflow demands by executing runbooks and workflows that monitor operational metrics and automatically trigger provisioning events. TOUTVIRTUAL 002166-TOUTVIRTUAL 002171. Each of these services provides virtual asset provisioning requests that specify parameters to be considered, and each service communicates via the virtualization layers to create, configure, and manage the resulting virtual assets. TOUTVIRTUAL 003126-TOUTVIRTUAL 003135; TOUTVIRTUAL 003136-TOUTVIRTUAL 003142; TOUTVIRTUAL 003143-TOUTVIRTUAL 003147; TOUTVIRTUAL 003148-TOUTVIRTUAL 003153. The processor in conjunction with the Azure Controllers may also provision virtual resources in response to workflow demands for event-driven actions, such as through the Azure Functions to establish a provisioned virtualization environment. TOUTVIRTUAL 003154-TOUTVIRTUAL 003162.
9[d][ii]. automatically provision a particular virtual asset to a particular physical resource in the virtualization system that matches the parameters in the virtual asset provisioning request,	The Accused Instrumentality meets the recited claim language because the processor, in conjunction with the control center computer (Azure Controllers), is configured to automatically provision a particular virtual asset to a particular physical resource in the virtualization system that matches the parameters in the virtual asset provisioning request. The Accused Instrumentality provides a processor, which in conjunction with the Azure Portal receives a virtual asset provisioning request either from a user, application, or automated network workflow to be considered for the virtual asset. After receiving the request, the processor in conjunction with the Azure Portal may request additional resources, or provision the necessary virtual assets through API-driven deployment ARM templates or Autoscale triggers (via Azure Monitor). TOUTVIRTUAL 002704-TOUTVIRTUAL 002710; TOUTVIRTUAL 002711-TOUTVIRTUAL 002720. The processor and the Azure Portal may receive API calls from services including Azure Virtual Machine Scale Sets (“VMSS”) (TOUTVIRTUAL 002964-TOUTVIRTUAL 002977), AKS, Azure Functions, and Azure Automation for provisioning of virtual assets. When these services detect increased network load or user activity, they communicate with the processor and the Azure Portal over a network to provision particular, additional virtual assets, such as new virtual machines, container pods, or serverless compute instances, on the virtualization layer. The processor in conjunction with the Azure Portal may then allocate particular compute, network, application, and storage resources from the available capacity in the Azure virtualization environment, configuring each new instance, and updating the system’s resource inventory in real time, thereby establishing a provisioned virtualization environment.

	TOUTVIRTUAL 002721-TOUTVIRTUAL 002727; TOUTVIRTUAL 002728-TOUTVIRTUAL 002732; TOUTVIRTUAL 002869-TOUTVIRTUAL 002882. The Accused Instrumentality provides a processor, which in conjunction with WAC integrates with Azure Arc to provision particular virtual assets in response to network workflow demands, particularly within hybrid Azure virtualization environments (<i>i.e.</i>, virtualization environments consisting of Azure systems and non-Azure Arc-enabled systems). The processor in conjunction with WAC communicates directly with hosts, servers or server clusters to deploy new virtual machines and virtual networks within or outside of the Azure infrastructure, including on-premises datacenters and other cloud platforms, in response to increased workload or network demand. The processor in conjunction with WAC can initiate provisioning operations by receiving API calls from Azure VMSS, AKS, Azure Functions, and Azure Automation; and deploy virtual machines, containers, or serverless compute instances to handle workload surges originating from on-premises or edge environments. TOUTVIRTUAL 002543-TOUTVIRTUAL 002552; TOUTVIRTUAL 003084-TOUTVIRTUAL 003088; TOUTVIRTUAL 003089-TOUTVIRTUAL 003094). The processor in conjunction with the Azure Controllers may perform this provisioning functionality for an Azure Container Apps environment. TOUTVIRTUAL 003225-TOUTVIRTUAL 003237. When workflow demands increase (<i>e.g.</i>, rising HTTP request rates, queue depth, event stream activity, or custom metric thresholds), Azure Container Apps’s Kubernetes Event-Driven Autoscaling (“KEDA”) rules generate signals that Azure Controllers evaluate against the network resource’s configuration. TOUTVIRTUAL 003095-TOUTVIRTUAL 003103. The processor in conjunction with the Azure Controllers may then provision additional container replicas, new revisions, or job executions within the Azure Container Apps environment. The processor in conjunction with the Azure Controllers may also provision supporting network resources whenever Azure Container Apps workloads scale or new applications are deployed. TOUTVIRTUAL 003238-TOUTVIRTUAL 003239; TOUTVIRTUAL 003737-TOUTVIRTUAL 003740. The processor in conjunction with the Azure Controllers may perform this provisioning functionality for applications running in AKS. TOUTVIRTUAL 003240-TOUTVIRTUAL 003241. Workflow signals from Kubernetes components, such as Horizontal Pod Autoscaler metrics, Vertical Pod Autoscaler recommendations, or Cluster Autoscaler node-capacity triggers, may cause the processor in conjunction with the Azure Controllers to request additional underlying resources. The processor in conjunction with the Azure Controllers may then respond to this request by provisioning new virtual machines, expanding node pools, or deploying additional Kubernetes workloads as specified, thereby establishing a provisioned virtualization environment. TOUTVIRTUAL 003104-TOUTVIRTUAL 003108.
--	---

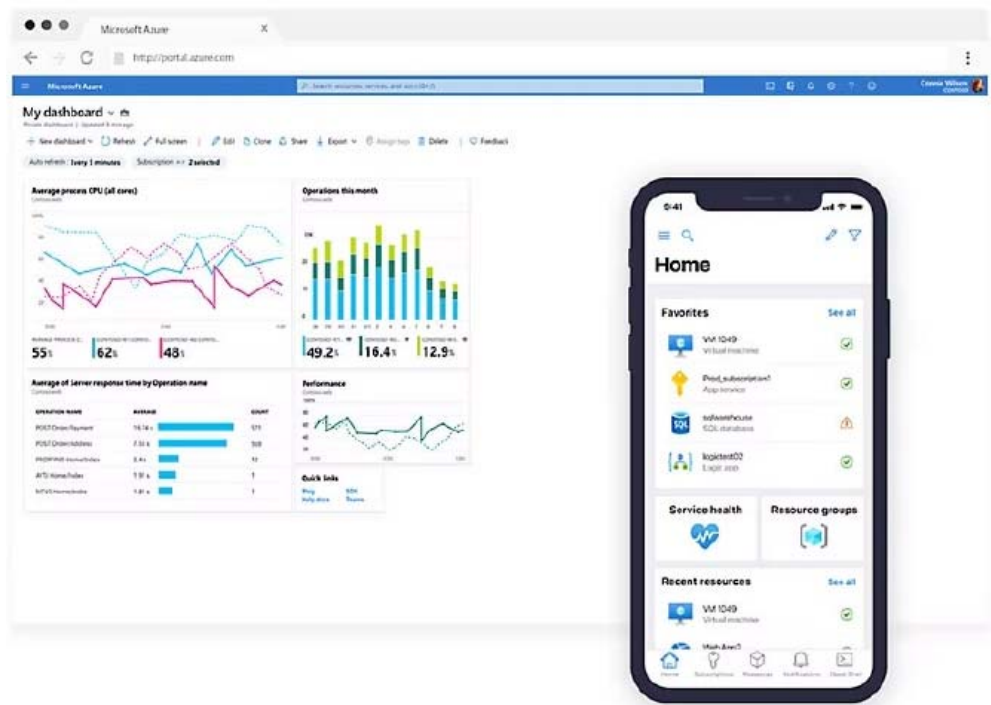
	The Azure Controllers may perform this provisioning functionality for applications running within private or on-premises environments, or Arc-enabled Kubernetes through Azure Arc. The Azure Controllers, via Azure Arc Resource Bridge, may provide custom locations within the private or on-premises environments, Kubernetes nodes, pods, container workloads, network endpoints, or security configurations which are considered when a virtual asset provisioning request is made. TOUTVIRTUAL 003039-TOUTVIRTUAL 003045; TOUTVIRTUAL 005089-TOUTVIRTUAL 005091. After validating the virtual asset provisioning request, the Azure Controllers, via Azure Arc, may use the custom locations to automatically provision on-premises environment or Kubernetes resources to fulfill the virtual asset provisioning request. For example, if a virtual asset's workload increases, the Azure Controllers via Azure Arc may automatically provision more resources from the on-premises environment or Kubernetes nodes pods, container workloads, network endpoints, and security configurations. The processor in conjunction with the Azure Controllers may provision storage virtual assets in response to workflow demands, such as Blob Storage accounts, file shares, managed disks, Elastic SAN volumes, and other storage service instances. This enables the processor and the Azure Controllers to allocate the required storage capacity or resources. For example, if an application workload experiences heavy growth, the processor in conjunction with the Azure Controllers may determine via Autoscale rules or workflow logic that additional storage throughput or capacity is required. TOUTVIRTUAL 002869-TOUTVIRTUAL 002882. The processor in conjunction with the Azure Controllers may then provision additional Blob Storage containers, create new managed disk volumes for new virtual machines being scaled out, or configures additional Elastic SAN volumes and attaches them to VMSS. The processor in conjunction with the Azure Controllers can also create or dynamically scale storage accounts using ARM templates or Automation runbooks triggered by workflow conditions (<i>e.g.</i>, data ingestion spike). TOUTVIRTUAL 002166-TOUTVIRTUAL 002171; TOUTVIRTUAL 002598-TOUTVIRTUAL 002603; TOUTVIRTUAL 002604-TOUTVIRTUAL 002613; TOUTVIRTUAL 002937-TOUTVIRTUAL 002946. When storage demand decreases or shifts, the processor and the Azure Controllers may also de-provision or reallocate storage assets (<i>e.g.</i>, shrink file share quotas, decommission unused managed disks) through Automation tasks. The Accused Instrumentality provides VMSS, AKS, Azure Functions, and Azure Automation which represent specific Azure services that implement the provisioning actions directed by the processor in conjunction with the Azure Controllers. VMSS provisions and scales virtual machines based on demand metrics. AKS provisions container pods and cluster nodes in response to network traffic and workload signals. Azure Functions provisions containers in response to network-based triggers such as HTTP requests or message events. Azure Automation provisions virtual assets in response to
--	--

	network workflow demands by executing runbooks and workflows that monitor operational metrics and automatically trigger provisioning events. Each of these services communicates via the virtualization layers to create, configure, and manage the resulting virtual assets. TOUTVIRTUAL 003126-TOUTVIRTUAL 003135; TOUTVIRTUAL 003136-TOUTVIRTUAL 003142; TOUTVIRTUAL 003143-TOUTVIRTUAL 003147; TOUTVIRTUAL 003148-TOUTVIRTUAL 003153. The processor in conjunction with the Azure Controllers may also provision virtual resources in response to workflow demands for event-driven actions, such as through the Azure Functions to establish a provisioned virtualization environment. TOUTVIRTUAL 003154-TOUTVIRTUAL 003162.
9[d][iii]. assign the provisioned virtual asset to the virtual asset provisioning request and	See Claim 1[c]. The Accused Instrumentality meets the recited claim language because after provisioning a virtual asset in response to a user or API-initiated provisioning request, the processor, in conjunction with the Azure Controllers, assigns the provisioned virtual asset to the corresponding virtual asset provisioning request by mapping the newly provisioned asset to the request's parameters and metadata. The Accused Instrumentality provides a processor, which in conjunction with the Azure Controllers may process the request and execute the provisioning of the virtual asset through the appropriate Azure resource provider (<i>e.g.</i>, Microsoft.Compute, Microsoft.ContainerService, Microsoft.Storage). TOUTVIRTUAL 005092-TOUTVIRTUAL 005106; TOUTVIRTUAL 005115-TOUTVIRTUAL 005303; TOUTVIRTUAL 005304-TOUTVIRTUAL 005348, TOUTVIRTUAL 005349-TOUTVIRTUAL 005371; TOUTVIRTUAL 005372-TOUTVIRTUAL 005378; TOUTVIRTUAL 005379-TOUTVIRTUAL 005617. For example, once the virtual asset is provisioned, the processor in conjunction with the Azure Controllers may assign that asset to the original provisioning request by associating the provisioned virtual asset (<i>i.e.</i>, virtual machine, managed disk, AKS node, container replica) to the virtual asset provisioning request (<i>i.e.</i>, originating deployment request, resource group, subscription, Autoscale rule, or orchestration policy that triggered the provisioning). The processor in conjunction with the Azure Controllers may further record the asset as the resulting object of that provisioning operation in activity logs and deployment records. The processor in conjunction with Azure Controllers may also apply the requested identities, role assignments, policies, and tags specified in the request and link the asset to the deployment operation ID (<i>i.e.</i>, a user, the scale set, AKS node pool, ACA revision, deployment template, or automation runbook that requested it), enabling traceability between the request and the provisioned virtual asset.

	TOUTVIRTUAL 005618-TOUTVIRTUAL 005645; TOUTVIRTUAL 005646-TOUTVIRTUAL 005675. The Accused Instrumentality provides a processor that in conjunction with the Azure Controllers may receive a provisioning request from the Azure Load Balancer, which may assign the newly provisioned asset to the active network traffic. For example, when a virtual machine or VMSS instance is provisioned, it is automatically added to a backend pool, health probes verify the asset's readiness, and traffic is routed to the new asset. The Azure Load Balancer may assign the asset to the original workload demand (<i>e.g.</i>, increased traffic). TOUTVIRTUAL 004035-TOUTVIRTUAL 004038. The Accused Instrumentality provides a processor that in conjunction with the Azure Controllers may receive a provisioning request from AKS, which may assign provisioned virtual assets through node provisioning or pod scheduling. For example, when virtual machines nodes are provisioned, new virtual machine nodes are added to a node pool, assigned to a cluster scheduling, and used by the workloads that triggered the autoscaling. AKS may also define resource quotas, such that when multiple replicas of pods are necessary during a disruption, the newly provisioned pods are assigned to nodes, such that services and ingress controllers may continue to route traffic through these new pods. TOUTVIRTUAL 002260-TOUTVIRTUAL 002264; TOUTVIRTUAL 002614-TOUTVIRTUAL 002620. The Accused Instrumentality provides a processor that in conjunction with the Azure Controllers may receive a provisioning request from Azure Container Apps, which may assign provisioned container replicas automatically. For example, when new container replicas are provisioned, the new replicas are associated with a specific revision, registered with the ingress routing, and assigned to handle the event or HTTP load that triggered the scaling. TOUTVIRTUAL 002989-TOUTVIRTUAL 002991. The Accused Instrumentality provides Azure Controllers that may receive a provisioning request from Azure Arc Resource Bridge or Azure Arc-enabled Kubernetes via Azure Arc, which may assign provisioned virtual assets to the virtual asset provisioning request. For example, Azure Arc Resource Bridge may interpret the validated virtual asset provisioning request and create a virtual asset in the private infrastructure, which will be represented within the Azure Controllers.
--	--

	Arc resource bridge (ARB) – Solution architecture The diagram illustrates the Arc resource bridge (ARB) solution architecture. It shows three main environments at the top: vCenter server, SCVMM Management server, and Azure Local VM enabled by Azure Arc. Each environment contains specific components like Resource Pools, VM Templates, and virtual networks. These environments are connected via 'Custom location mapping' to a central 'ARB ARM resource'. Below this, three 'Private cloud environment' blocks are shown, each containing an 'Arc resource bridge' and 'Custom location'. These private cloud environments are connected to the ARB ARM resource through 'Management endpoint' connections. The private cloud environments also contain their own vCenter, SCVMM, or Azure Local instance components. TOUTVIRTUAL 003039-TOUTVIRTUAL 003045. The Accused Instrumentality provides a processor that in conjunction with the Azure Controllers may receive provisioning requests from the Azure storage virtualization services, which may assign the newly provisioned virtual asset to the request that caused the provisioning. For example, new managed disks may be attached to specific virtual machines, new file shares may be mounted to specific workloads, or new containers may be bound to specific application or pipelines that caused the provisioning. TOUTVIRTUAL 003388-TOUTVIRTUAL 003397, TOUTVIRTUAL 003398-TOUTVIRTUAL 003405, TOUTVIRTUAL 003406-TOUTVIRTUAL 003413, TOUTVIRTUAL 003414-TOUTVIRTUAL 003416.
9[d][iv]. provide user access to the provisioned virtual asset.	The Accused Instrumentality meets the recited claim language because the processor, in conjunction with the control center computer (Azure Controllers), is configured to provide the user access to the provisioned virtual asset. The Accused Instrumentality provides a processor, which in conjunction with the Azure Portal includes a controller that provides a unified, web-based console for creating, managing, and monitoring Azure resources, ranging from simple web apps to complex deployments through a

graphical interface with integrated support. The processor, in conjunction with the Azure Portal, communicates over a network (such as the Internet or a local network) with the virtualization layers to create, configure, monitor, and deallocate virtual resources. The processor in conjunction with the Azure Portal interacts with and allows users to visually manage and provision virtual machines, networks, storage resources, and functions over a network.

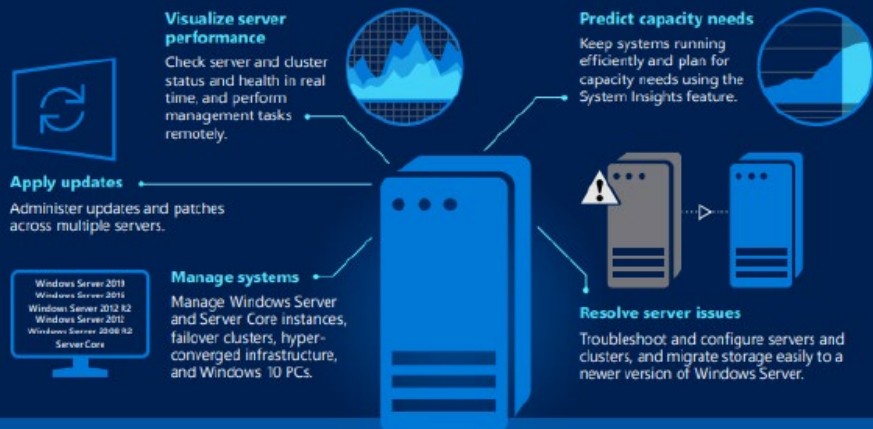


TOUTVIRTUAL 002509-TOUTVIRTUAL 002511; TOUTVIRTUAL 002124-TOUTVIRTUAL 002129; TOUTVIRTUAL 002503-TOUTVIRTUAL 002508.

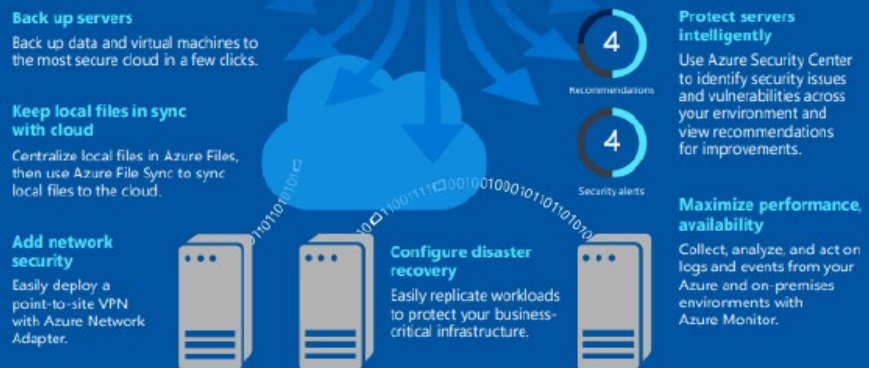
The Accused Instrumentality provides a processor, which in conjunction with WAC provides a network-coupled controller that communicates directly with the host servers or server clusters to provision and manage virtual machines, including environment connected through Azure Arc.

	TOUTVIRTUAL 002134-TOUTVIRTUAL 002137. WAC is a locally deployed management tool set that can manage Windows Clients, Servers, and Clusters without needing to connect to the cloud and provides full control over all aspects of server infrastructure including managing servers on private networks that are not connected to the Internet. The processor in conjunction with WAC interacts with and allows users to perform actions such as management and provisioning of virtual machines, networks, storage resources, and functions over a network. TOUTVIRTUAL 002571-TOUTVIRTUAL 002575; TOUTVIRTUAL 002130-TOUTVIRTUAL 002133;
--	--

Streamline management tasks

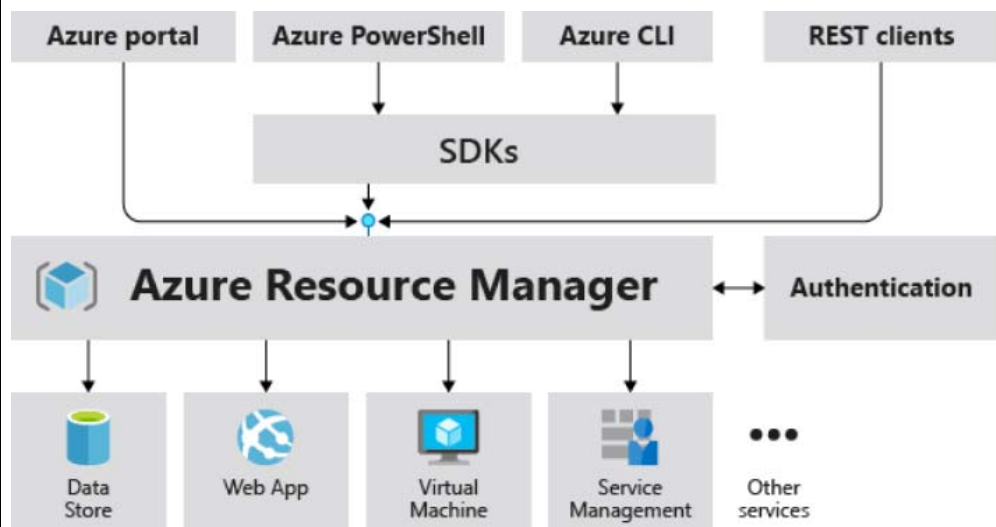


Extend your on-premises environment with Azure integrations



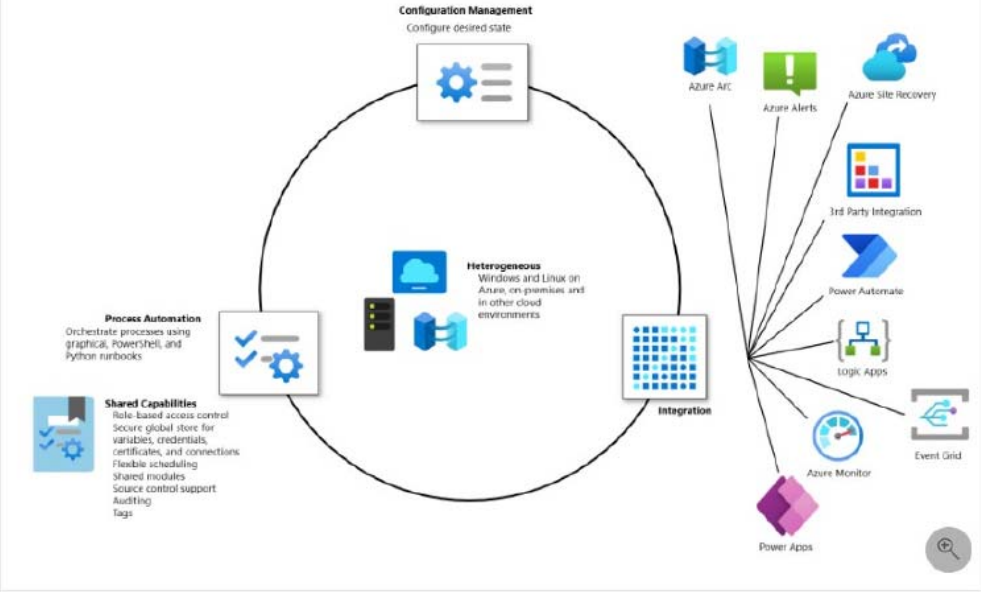
TOUTVIRTUAL 002596-TOUTVIRTUAL 002597.

The Accused Instrumentality includes Azure Resource Manager (“ARM”), which provides a deployment and management service that can create, update, and delete resources such as virtual machines, storage accounts, web apps, databases, and virtual networks within the Azure virtualization environment. TOUTVIRTUAL 002150-TOUTVIRTUAL 002151;

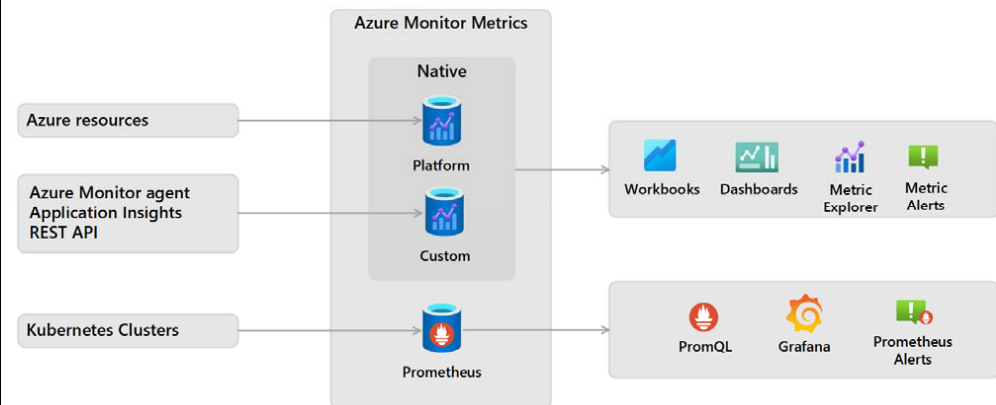


TOUTVIRTUAL 002143-TOUTVIRTUAL 002149.

The Accused Instrumentality includes Azure Controllers in conjunction with the processor that provide Azure Automation, which supports the Azure Controllers by executing runbooks and scripts that automatically manage and reconfigure virtual resources through network-based APIs across the virtualization environment.

	 The diagram illustrates the Azure Arc architecture. At the center is a circle labeled "Heterogeneous" containing icons for Windows and Linux, with text: "Windows and Linux on Azure, on-premises and in other cloud environments". Surrounding this central hub are five main functional areas, each with a gear icon: "Configuration Management" (top) with text "Configure desired state"; "Process Automation" (left) with text "Orchestrate processes using graphical, PowerShell, and Python runbooks"; "Shared Capabilities" (bottom-left) with text "Rule-based access control, Secure global store for variables, credentials, certificates, and connections, Flexible scheduling, Shared modules, Source control support, Auditing, Tags"; "Integration" (bottom-right) with text "Integration"; and "Azure Arc" (top-right) with text "Azure Arc". To the right of the central hub, a series of lines radiate outwards to various Azure services and components, including: "Azure Alerts", "Azure Site Recovery", "3rd Party Integration", "Power Automate", "Logic Apps", "Event Grid", "Azure Monitor", "Power Apps", and "Azure Arc" (repeated). A magnifying glass icon is located at the bottom right of the diagram. TOUTVIRTUAL 002166-TOUTVIRTUAL 002171; TOUTVIRTUAL 002760-TOUTVIRTUAL 002770; TOUTVIRTUAL 002771-TOUTVIRTUAL 002780.
Claim 10	
10. The apparatus of <i>claim 9</i>, wherein the virtualization environment determines one or more performance metrics of the provisioned virtual asset.	See Claims 9[b][i] and 9[d][ii]. The Accused Instrumentality meets the recited claim language because each Azure Controller determines one or more performance metrics of the provisioned virtual asset. The Accused Instrumentality provides Azure Portal, which determines one or more performance metrics of the provisioned virtual asset because it tracks the operational state and configuration of all provisioned virtual assets, including VMs, VMSS, AKS nodes and pods, storage, and other physical resources. Azure Portal integrates Azure Monitor and Azure Service Health, which includes Azure Status, Service Health, and Resource Health, to collect key telemetry such as CPU utilization, network throughput, disk I/O, and availability for each resource and asset. These

measurements are continuously reported through the Azure Portal, ARM APIs, and the Azure Metrics Explorer interface. Azure Portal's telemetry data is also made available to automation workflows and alerting mechanisms for performance-based management.



TOUTVIRTUAL 003163-TOUTVIRTUAL 003168.

The Accused Instrumentality provides WAC, which determines one or more performance metrics of the provisioned virtual asset because WAC continuously collects telemetry from host servers, server clusters, and VMs running within or outside of the Azure infrastructure, including on-premises datacenters and other cloud platforms, displaying metrics such as CPU, memory, disk, and network usage. When integrated with Azure Arc (TOUTVIRTUAL 002134-TOUTVIRTUAL 002137), WAC forwards this measurement data from these non-Azure systems to the Azure Portal for aggregation and reporting. Users may view detailed performance dashboards, generate usage reports, and receive notification of performance degradation through the WAC interface. This enables consistent performance measurement and reporting across both cloud-based and on-premise virtual assets and physical resources for the provisioned virtualization environment.

TOUTVIRTUAL 002543-TOUTVIRTUAL 002552; TOUTVIRTUAL 002553-TOUTVIRTUAL 002570; TOUTVIRTUAL 002576-TOUTVIRTUAL 002595.

The Accused Instrumentality provides Azure Service Health, which keeps users informed about the health of its cloud resources, including current and upcoming issues, such as service impacting events, planned maintenance, and other changes that might affect network availability. As provided above, Azure Service Health includes (1) Azure Status, which informs users of service outages in

the Azure virtualization environment globally; (2) Service Health, which provides users a personalized view of the health of the user’s Azure virtualization environment and notification through a preferred communication channel about issues or changes that may affect the user’s resources and assets; and (3) Resource Health, which provides information about the health of the user’s individual cloud resources, such as a specific virtual machine instance and is able to help determine metrics for the provisioned virtualization environment.

Microsoft Azure

My account Portal

Welcome to the new Azure status page. Don't forget to update this page in your bookmarks. [Learn More](#)

Azure status

RSS

This page is only used for widespread incidents.

Sign in to view incidents that may be affecting your services

[Go to Azure Service Health >](#)

HELPFUL LINKS

[Azure status history](#)

[Learn when we use this page](#)

[Get notified of outages that impact you](#)

[Building reliable applications on Azure](#)

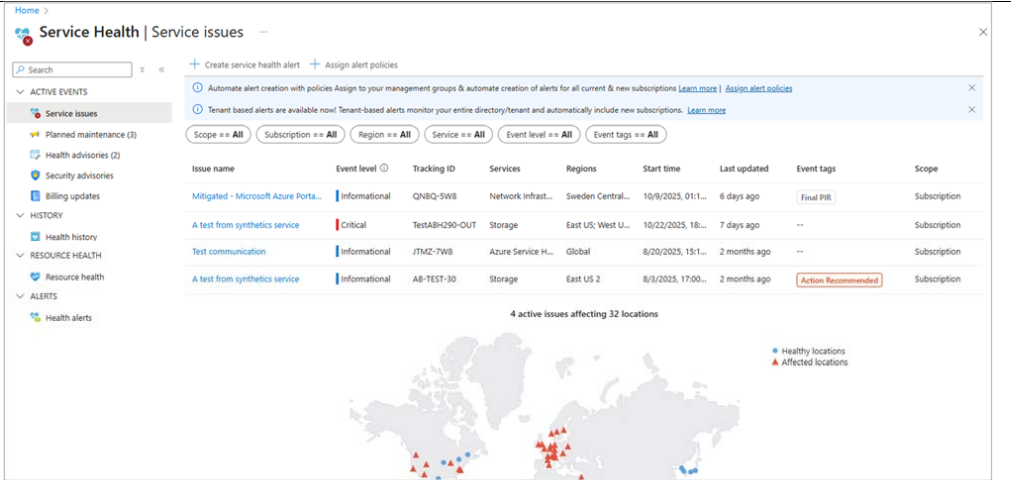
Updated 34 seconds ago | Refresh every 2 minutes

Good Information Warning Critical N/A

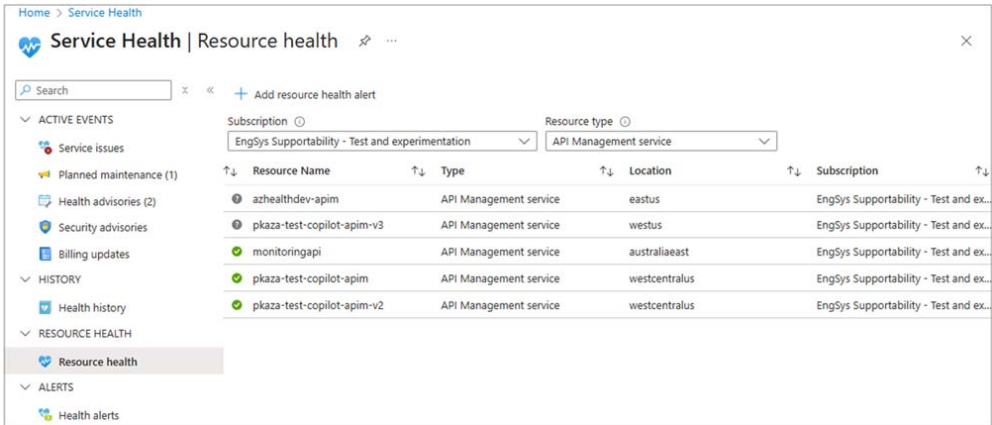
Current Impact Americas Europe Asia Pacific Middle East and Africa Azure Government Azure China Jio³

Products And Services	*Non-Regional ⓘ	East US	East US 2	Central US	North Central US	South Central US	West Central US	West US	West US 2	*West US 3	Canada East	Canada Central	Brazil South	Brazil Southeast	Mexico Central	Chile Central
COMPUTE																
Azure Compute Fleet	--	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure VMware Solution	--	✓	✓	✓	✓	✓	--	✓	✓	✓	✓	✓	✓	--	--	--
Azure VMware Solution by CloudSimple	--	✓	--	--	--	✓	--	✓	--	--	--	--	--	--	--	--
Batch	--	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	--	✓

TOUTVIRTUAL 003244-TOUTVIRTUAL 003247;

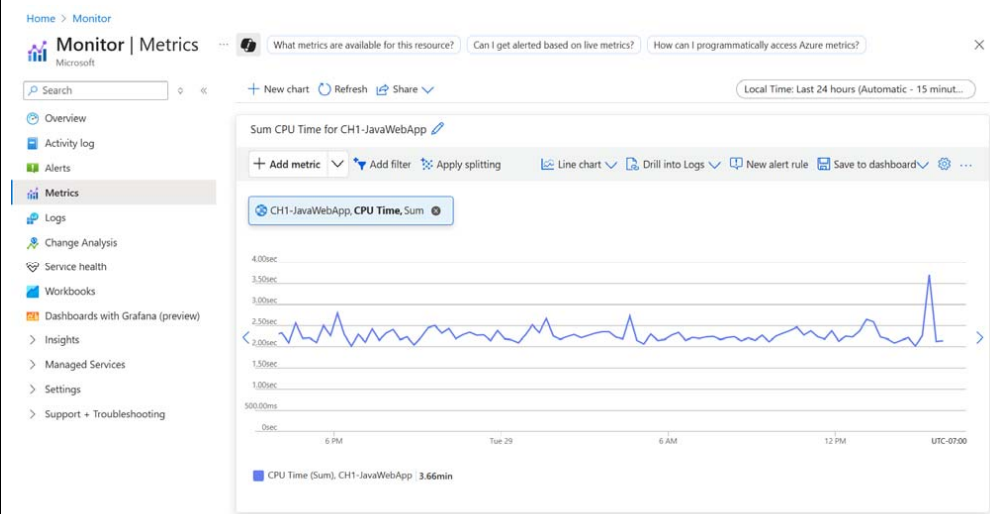


TOUTVIRTUAL 003242-TOUTVIRTUAL 003243;



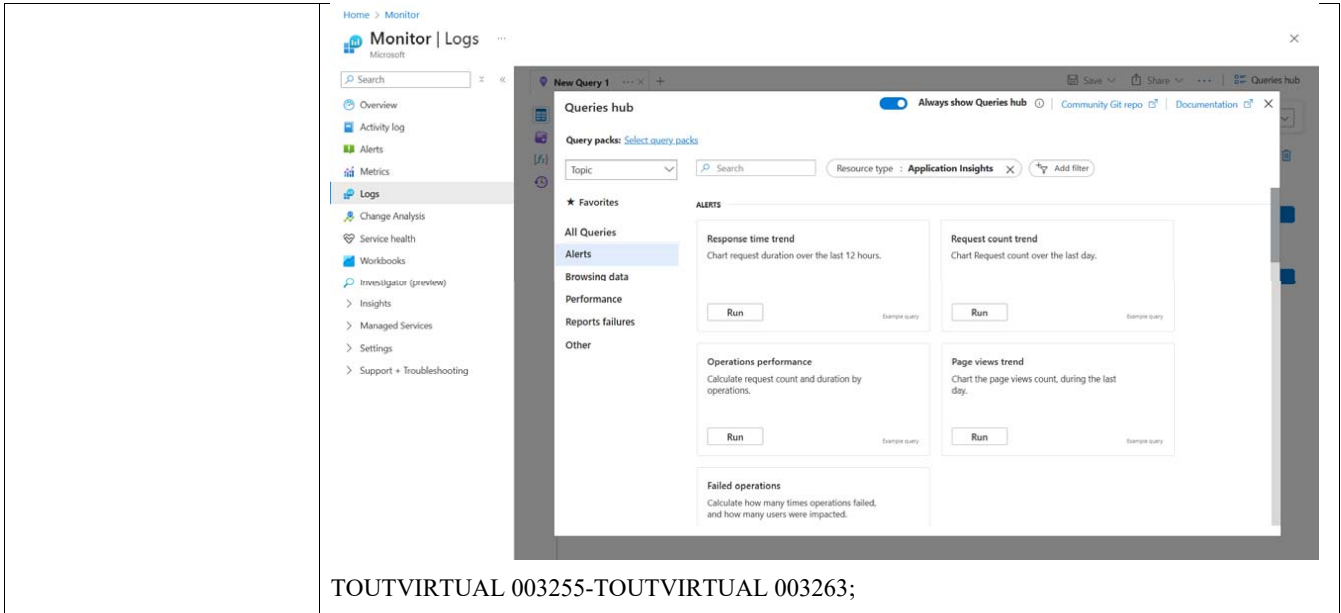
TOUTVIRTUAL 003248-TOUTVIRTUAL 003254.

The Accused Instrumentality provides Azure Monitor, which includes Metrics Explorer, which helps users plot charts, visually correlate trends, and investigate spikes and dips in metrics values. Metrics Explorer enables users to investigate the health and utilization of the user's resources and assets and determine metrics for the provisioned virtualization environment.

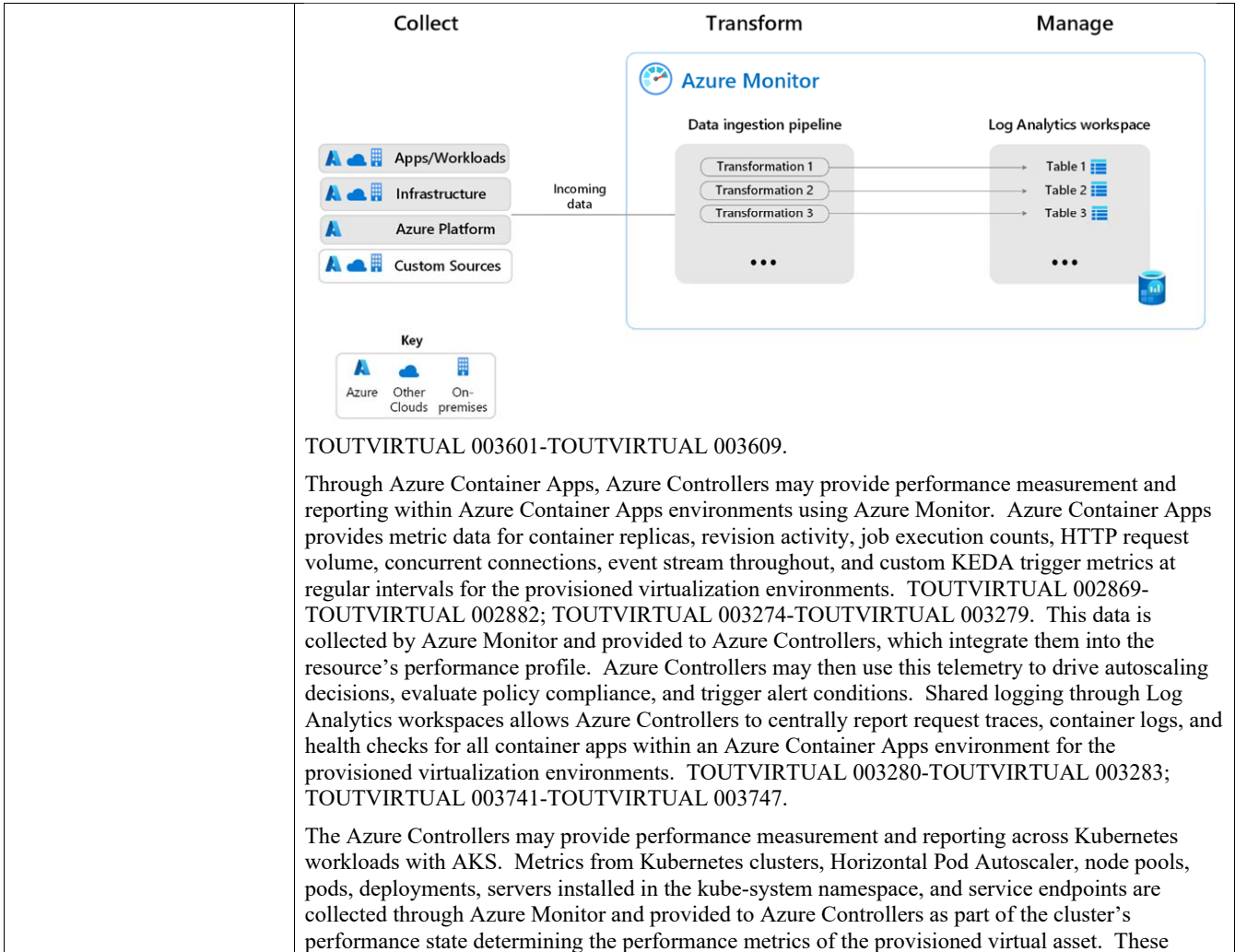


TOUTVIRTUAL 002281-TOUTVIRTUAL 002312.

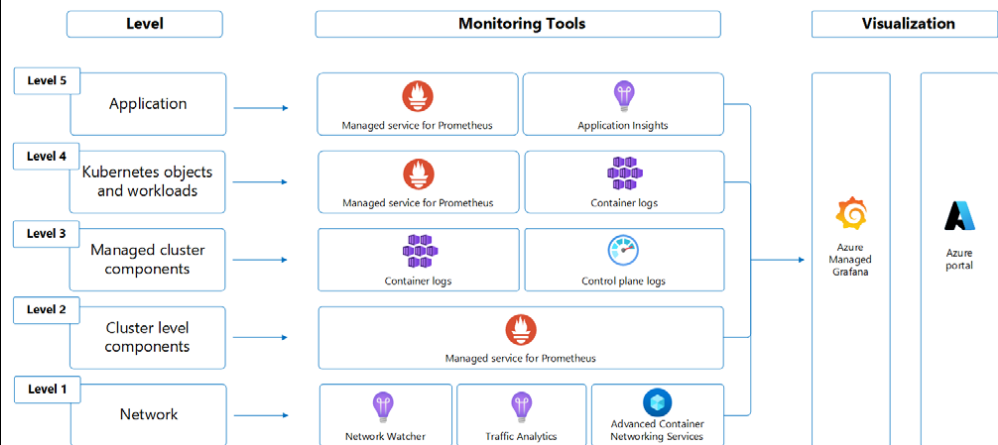
Azure Monitor further includes Log Analytics that allows users to explore and analyze data collected by Azure Monitor Logs. A user may edit and run log queries to filter records, uncover trends, analyze patterns, and gain meaningful insights into the user's Azure virtualization environment and is able to help determine metrics for the provisioned virtualization environment.



TOUTVIRTUAL 003255-TOUTVIRTUAL 003263;

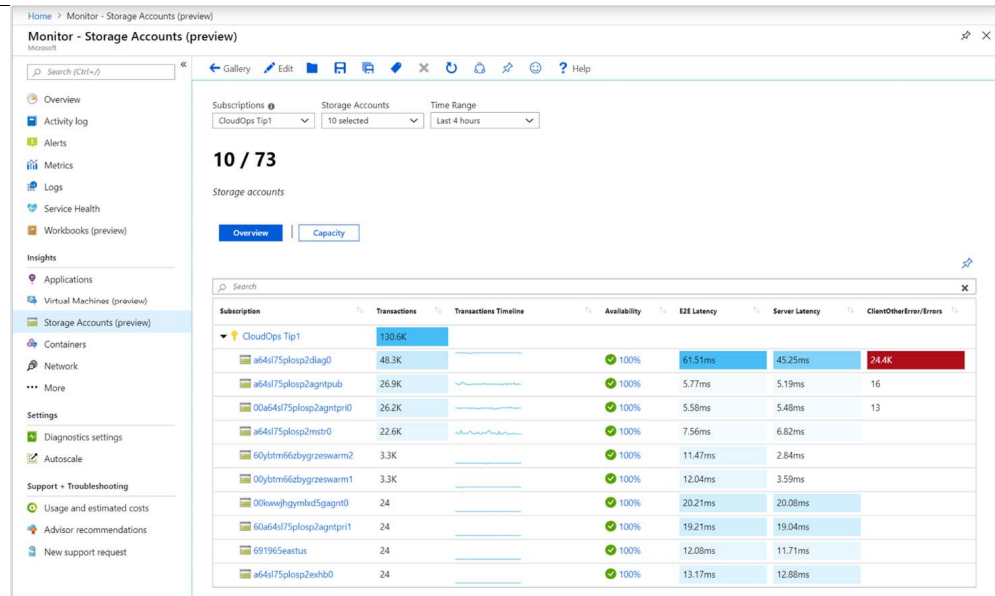


include pod restart counts, node memory pressure, CPU saturation, request throughput, declined scheduling attempts, and container-level health signals. Azure Controllers use this performance data to generate reports, drive autoscaling logic, trigger alerts, and support automatic remediation in an AKS environment for the provisioned virtualization environments.



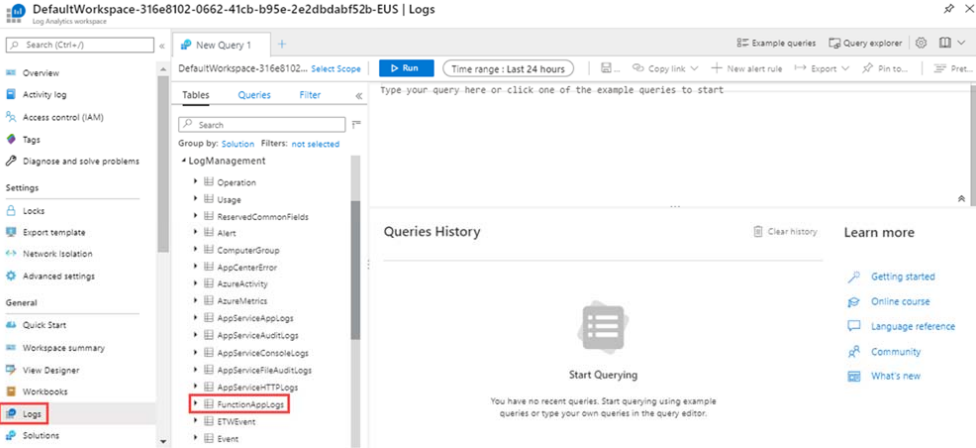
TOUTVIRTUAL 003284-TOUTVIRTUAL 003287.

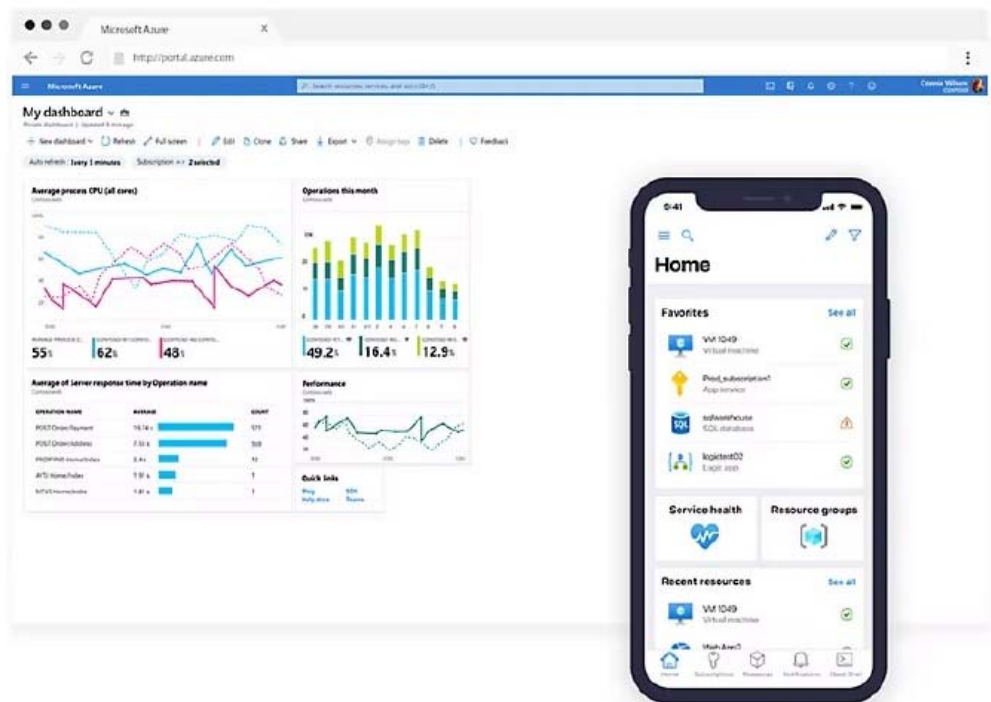
The Azure Controllers may receive performance measurements and reports for storage-virtualized assets from Azure Monitor. From Azure Blob Storage, Azure Monitor automatically collects metrics related to latency, throughput, throttling events, replication health, and capacity usage. From Azure Files, Azure Monitor automatically collects metrics related to SMB and NFS latency, IOPS, quota usage, and share health. From Azure Disk Storage, Azure Monitor automatically collects metrics related to IOPS, throughput, queue depth, read and write latency, and disk health signals. From Azure Elastic SAN, Azure Monitor automatically collects metrics related to volume throughput, SAN controller health, redundancy status, and capacity utilization. Azure Monitor collects these metrics automatically and provides these metrics to Azure Controllers, so that Azure Controllers may aggregate these metrics, provide continuous reporting, and support reallocation or deployment decisions for the provisioned virtualization environments.



TOUTVIRTUAL 003288-TOUTVIRTUAL 003303; TOUTVIRTUAL 003388-TOUTVIRTUAL 003397; TOUTVIRTUAL 003398-TOUTVIRTUAL 003405; TOUTVIRTUAL 003406-TOUTVIRTUAL 003413; TOUTVIRTUAL 003414-TOUTVIRTUAL 003416.

The Azure Controllers may also determine one or more performance metrics of the provisioned virtual assets through Azure Functions. Performance metrics of the provisioned virtual assets may be measured and reported, along with the other available resources within the virtualization environment, via Azure Functions based on different demand loads and over certain time periods that Azure Functions has been operating for the provisioned virtualization environments.

	 TOUTVIRTUAL 003304-TOUTVIRTUAL 003313.
Claim 11 11. The apparatus of <i>claim 9</i>, wherein the provisioning manager provides a user interface for submitting the virtual asset provisioning request.	See Claim 9[d][i]. The Accused Instrumentality meets the recited claim language because the Azure Controllers in conjunction with the provisioning manager provide a user interface for submitting the virtual asset provisioning request. The Accused Instrumentality provides Azure Portal, which is a controller that provides a user with a unified, web-based console for creating, managing, and monitoring Azure resources through functionalities including but not limited to Azure Logic Apps. As the controller, Azure Portal in conjunction with Azure Logic Apps interacts with and allows users to visually manage and provision virtual machines, networks, storage resources, and functions over a network. TOUTVIRTUAL 004005-TOUTVIRTUAL 004016; TOUTVIRTUAL 005751-TOUTVIRTUAL 005765; TOUTVIRTUAL 005766-TOUTVIRTUAL 005796; TOUTVIRTUAL 005797-TOUTVIRTUAL 005801. Azure Logic Apps provides users with an interface for submitting virtual asset provisioning requests. TOUTVIRTUAL 005058-TOUTVIRTUAL 005088;

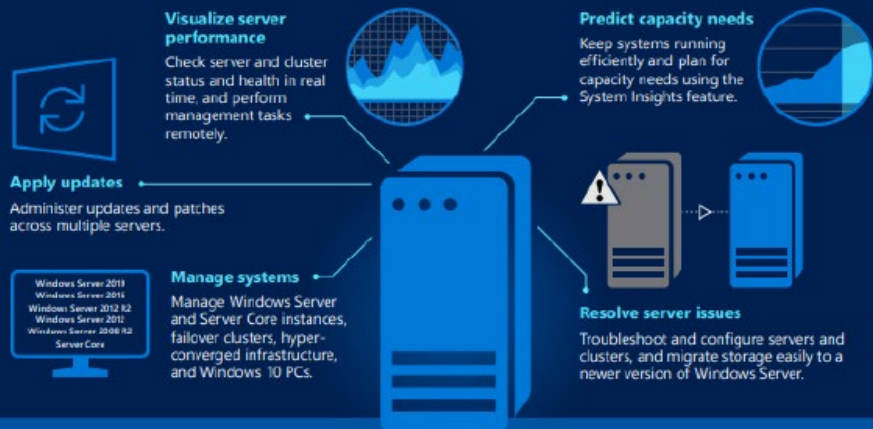


TOUTVIRTUAL 002509-TOUTVIRTUAL 002511; TOUTVIRTUAL 002124-TOUTVIRTUAL 002129; TOUTVIRTUAL 002503-TOUTVIRTUAL 002508.

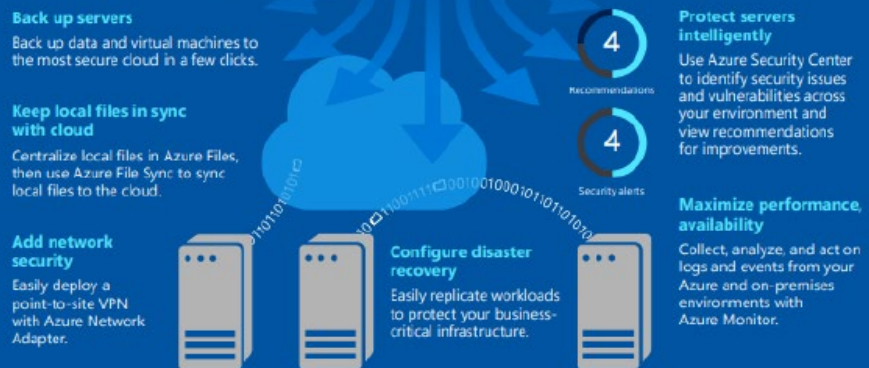
The Accused Instrumentality provides WAC, which extends functionalities like Azure Logic Apps to on-premises infrastructure. WAC's local deployment provides users with an interface for submitting virtual asset provisioning requests without needing to connect to the cloud.

TOUTVIRTUAL 002571-TOUTVIRTUAL 002575; TOUTVIRTUAL 002130-TOUTVIRTUAL 002133;

Streamline management tasks



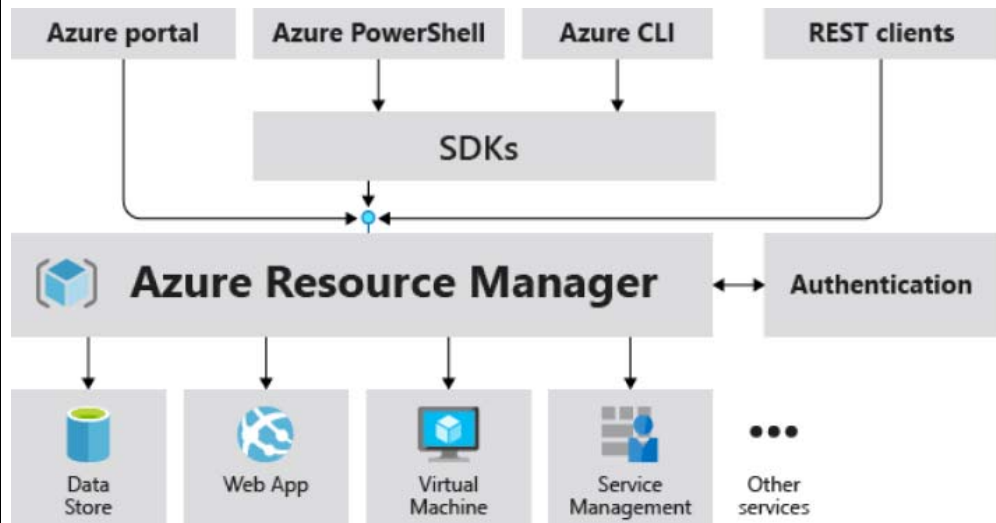
Extend your on-premises environment with Azure integrations

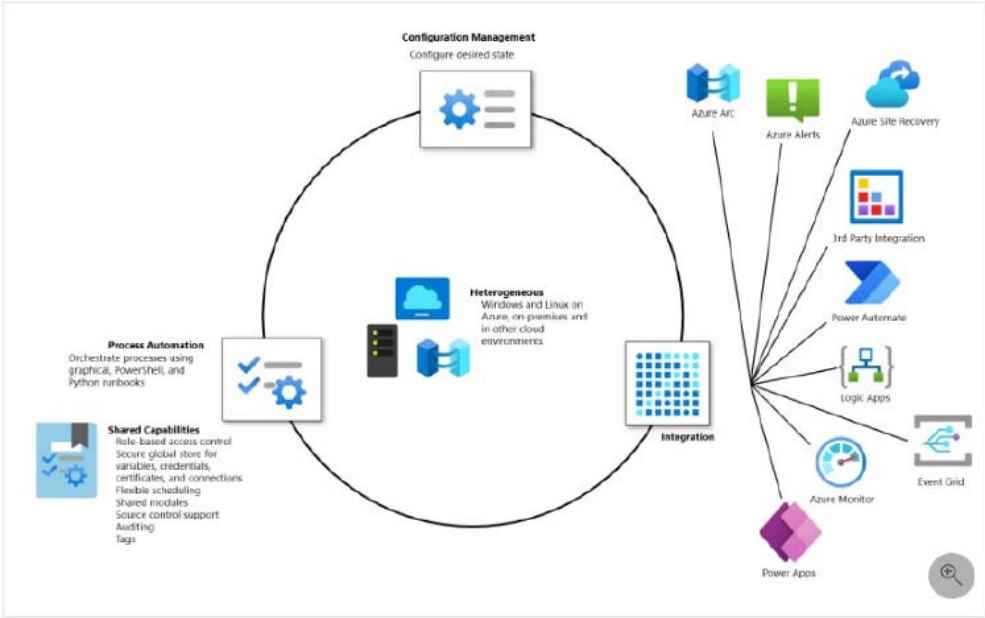


TOUTVIRTUAL 002596-TOUTVIRTUAL 002597.

The Accused Instrumentality provides Azure Logic Apps, which provides users with the ability to create and operate automated workflows. Users access Azure Logic Apps through the Azure Controllers and can create low-code-no-code solutions through templates that can operate with systems hosted in the cloud, on-premises, or in a hybrid environment. Azure Logic Apps also allows users to submit requests for workflows based on complex structured code through Azure Functions. TOUTVIRTUAL 005676-TOUTVIRTUAL 005697; TOUTVIRTUAL 005698-TOUTVIRTUAL 005716; TOUTVIRTUAL 005717-TOUTVIRTUAL 005750. Once the user submits a virtual asset provisioning request through the interface provided by Azure Logic Apps hosted within the Azure Controllers, Azure Resource Manager will begin to validate and execute the request. TOUTVIRTUAL 004005-TOUTVIRTUAL 004016; TOUTVIRTUAL 005058-TOUTVIRTUAL 005088.

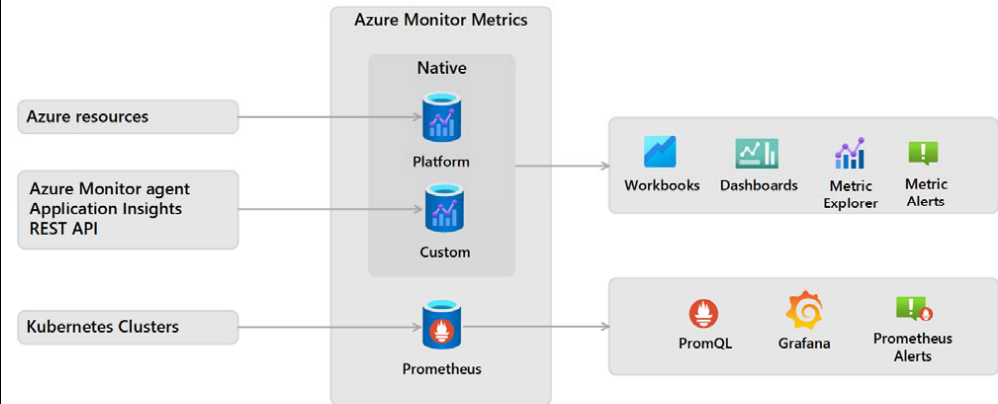
The Accused Instrumentality provides ARM, which provides a user with an interface via the Azure Controllers, which allows the user to submit virtual asset provisioning requests. When users submit virtual asset provisioning requests via the Azure Controllers, ARM may validate and execute the request. TOUTVIRTUAL 002150-TOUTVIRTUAL 002151;



	TOUTVIRTUAL 002143-TOUTVIRTUAL 002149. The Accused Instrumentality provides Azure Automation, which supports the Azure Controllers by executing runbooks and scripts that automatically manage and reconfigure virtual resources through network-based APIs across the virtualization environment.  The diagram illustrates the Azure Automation architecture. At the center is a circle labeled 'Heterogeneous Windows and Linux on Azure, on premises and in other cloud environments'. Surrounding this circle are four main components: 'Configuration Management' (top) with a gear icon and the text 'Configure desired state'; 'Process Automation' (left) with a checkmark and gear icon and the text 'Orchestrate processes using graphical, PowerShell, and Python runbooks'; 'Shared Capabilities' (bottom-left) with a gear icon and a list of features: 'Role-based access control', 'Secure global store for variables, credentials, certificates, and connections', 'Flexible scheduling', 'Shared modules', 'Source control support', 'Auditing', and 'Tags'; and 'Integration' (right) with a grid icon. To the right of the Integration component, a central hub connects to various Azure services: 'Azure ARC', 'Azure Alerts', 'Azure Site Recovery', '3rd Party Integration', 'Power Automate', 'Logic Apps', 'Event Grid', 'Azure Monitor', and 'Power Apps'. TOUTVIRTUAL 002166-TOUTVIRTUAL 002171; TOUTVIRTUAL 002760-TOUTVIRTUAL 002770; TOUTVIRTUAL 002771-TOUTVIRTUAL 002780.
Claim 13	
13.	See Claim 10.
The apparatus of <i>claim 10</i> , wherein the virtualization environment determines one	The Accused Instrumentality meets the recited claim language because each Azure Controller determines one or more performance metrics which further comprise determining one or more real time performance metrics.

or more real time performance metrics.

The Accused Instrumentality provides Azure Portal, which determines real time performance metrics of the virtual assets because it tracks the operational state and configuration of all provisioned virtual assets. Through Azure Portal's integration of Azure Monitor and Azure Service Health which includes Azure Status, Service Health, and Resource Health, Azure Portal collects real time telemetry such as CPU utilization, network throughput, disk I/O, and availability for each virtual asset at regular intervals. These measurements are continuously reported through the Azure Portal, ARM APIs, and the Azure Metrics Explorer interface. Azure Portal's telemetry data is also made available to automation workflows and alerting mechanisms for performance-based management.



TOUTVIRTUAL 003163-TOUTVIRTUAL 003168.

The Accused Instrumentality provides WAC, which determines real time performance metrics of the provisioned virtual asset because WAC continuously collects real time telemetry from host servers, server clusters, and VMs running within or outside of the Azure infrastructure, including on-premises datacenters and other cloud platforms, displaying metrics such as CPU, memory, disk, and network usage. When integrated with Azure Arc (TOUTVIRTUAL 002134-TOUTVIRTUAL 002137), WAC forwards this measurement data from these non-Azure systems to the Azure Portal for aggregation of the data and reporting of the real time performance metrics. Users may view detailed performance dashboards, generate usage reports, and receive notification of performance degradation through the WAC interface which is continuously collecting real time telemetry. This enables consistent performance measurement and reporting across both cloud-based and on-

premises virtual assets and physical resources. TOUTVIRTUAL 002543-TOUTVIRTUAL 002552; TOUTVIRTUAL 002553-TOUTVIRTUAL 002570; TOUTVIRTUAL 002576-TOUTVIRTUAL 002595.

The Accused Instrumentality provides Azure Service Health, which keeps users informed in real time about the health of its cloud resources, including current and upcoming issues, such as service impacting events, planned maintenance, and other changes that might affect network availability. As provided above, Azure Service Health Service includes (1) Azure Status, which informs users of service outages in the Azure virtualization environment globally; (2) Service Health, which provides users a personalized view of the health of the user’s Azure virtualization environment and notification through a preferred communication channel about issues or changes that may affect the user’s resources and assets; and (3) Resource Health, which provides information about the health of the user’s individual cloud resources, such as a specific virtual machine instance.

Microsoft Azure

My accountPortal

Welcome to the new Azure status page. Don't forget to update this page in your bookmarks. [Learn More](#)

Azure status

RSS

This page is only used for widespread incidents.

Sign in to view incidents that may be affecting your services

[Go to Azure Service Health >](#)

HELPFUL LINKS

[Azure status history](#)
[Learn when we use this page](#)
[Get notified of outages that impact you](#)
[Building reliable applications on Azure](#)

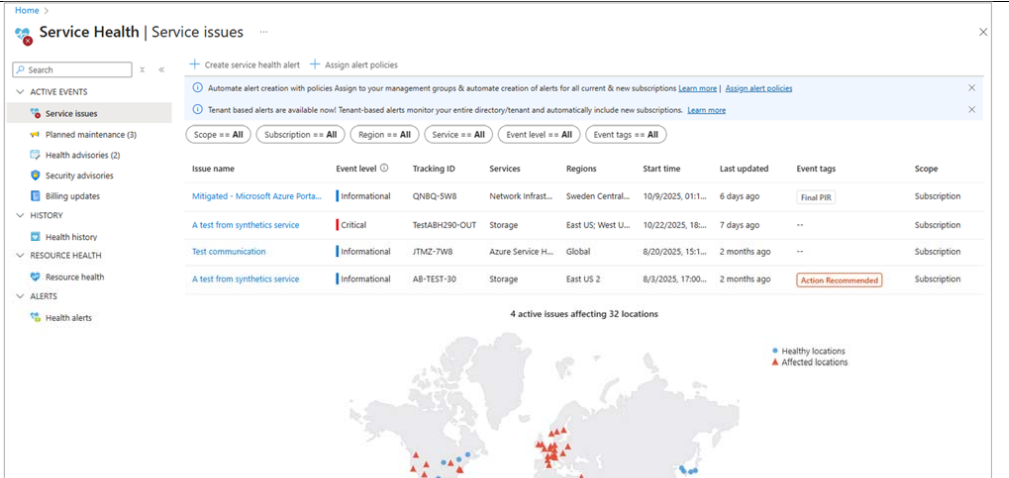
Updated 34 seconds ago | Refresh every 2 minutes

GoodInformationWarningCriticalN/A

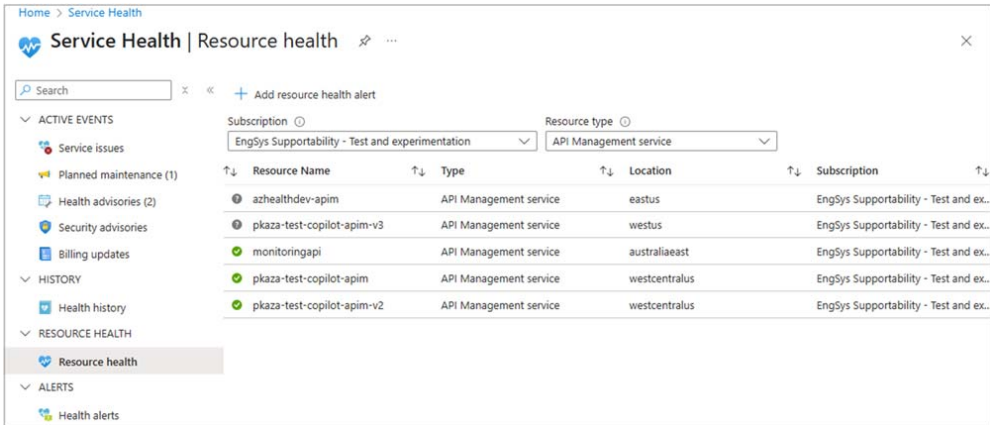
Current ImpactAmericasEuropeAsia PacificMiddle East and AfricaAzure GovernmentAzure ChinaJio¹

Products And Services	*Non-Regional ⓘ	East US	East US 2	Central US	North Central US	South Central US	West Central US	West US	West US 2	*West US 3	Canada East	Canada Central	Brazil South	Brazil Southeast	Mexico Central	Chile Central
COMPUTE																
Azure Compute Fleet	---	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure VMware Solution	---	✓	✓	✓	✓	✓	---	✓	✓	✓	✓	✓	✓	---	---	---
Azure VMware Solution by CloudSimple	---	✓	---	---	---	✓	---	✓	---	---	---	---	---	---	---	---
Batch	---	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	---	✓

TOUTVIRTUAL 003244-TOUTVIRTUAL 003247;

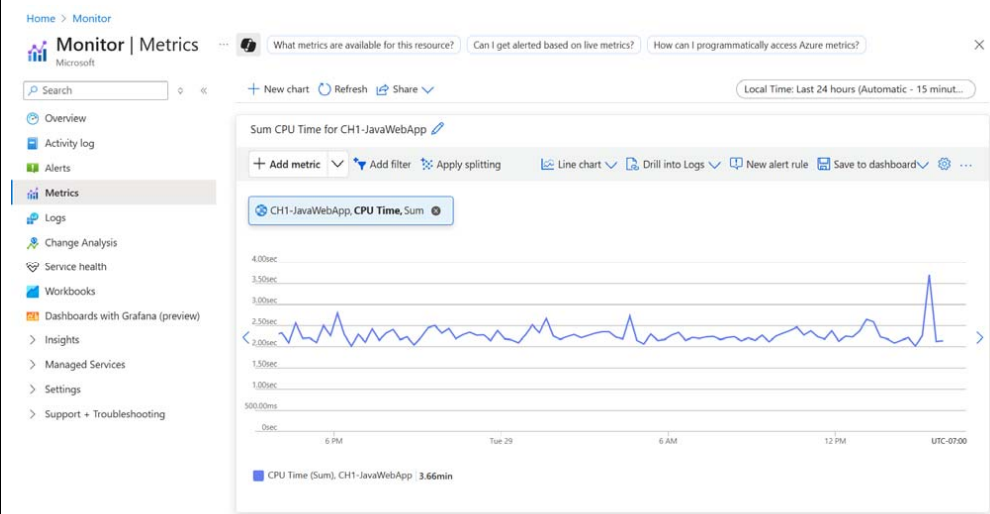


TOUTVIRTUAL 003242-TOUTVIRTUAL 003243;



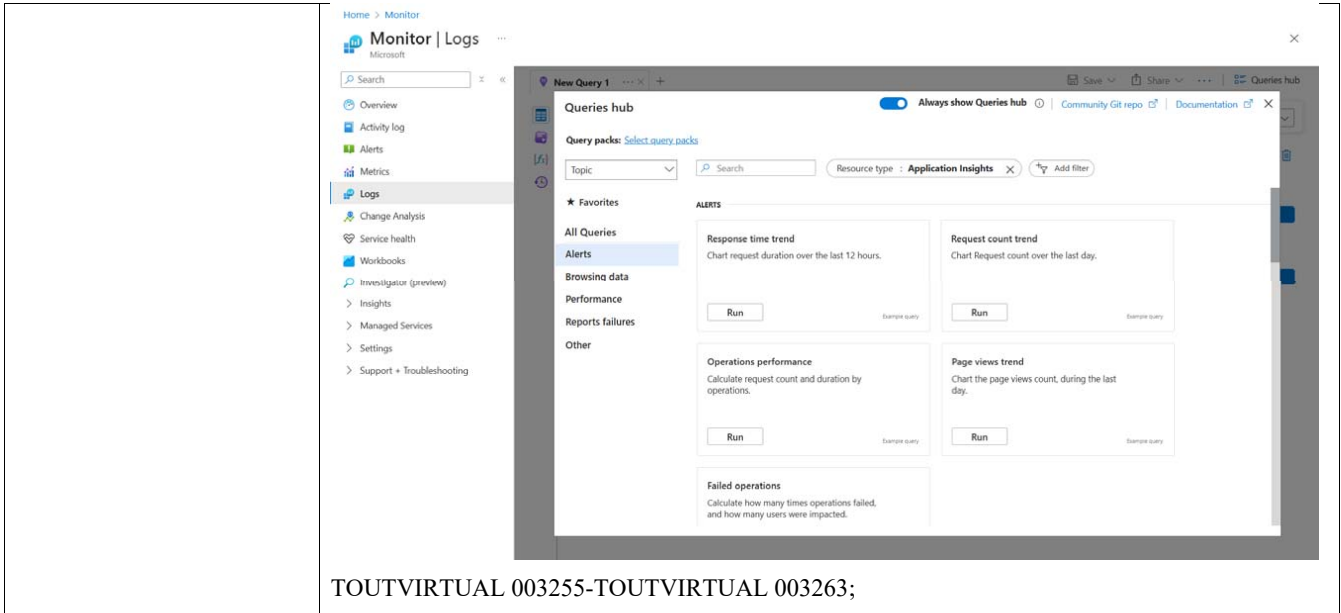
TOUTVIRTUAL 003248-TOUTVIRTUAL 003254.

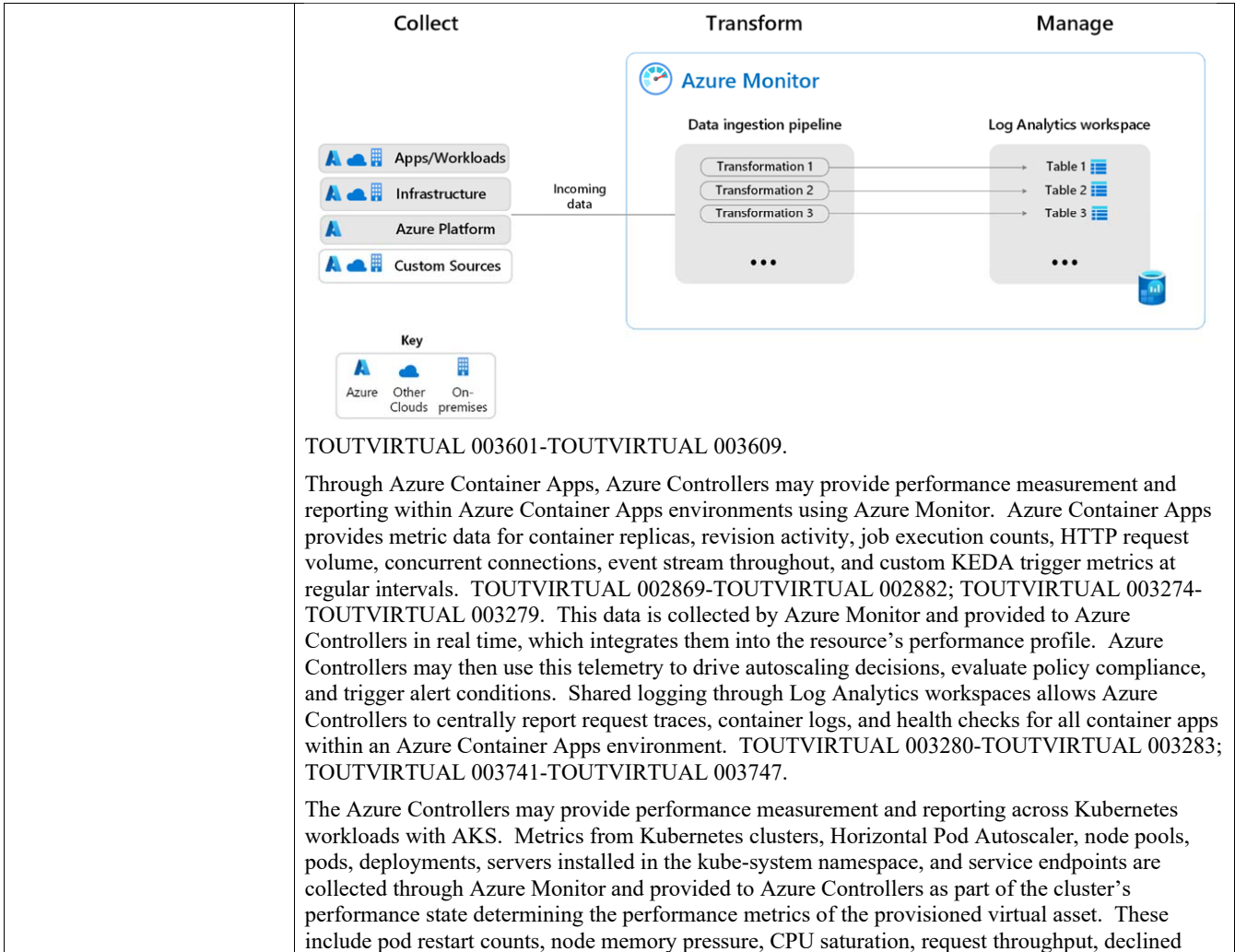
The Accused Instrumentality provides Azure Monitor, which includes Metrics Explorer, which helps users plot charts, visually correlate trends, and investigate spikes and dips in metrics values. Metrics Explorer enables users to investigate the health and utilization of the user's resources and assets in real time.



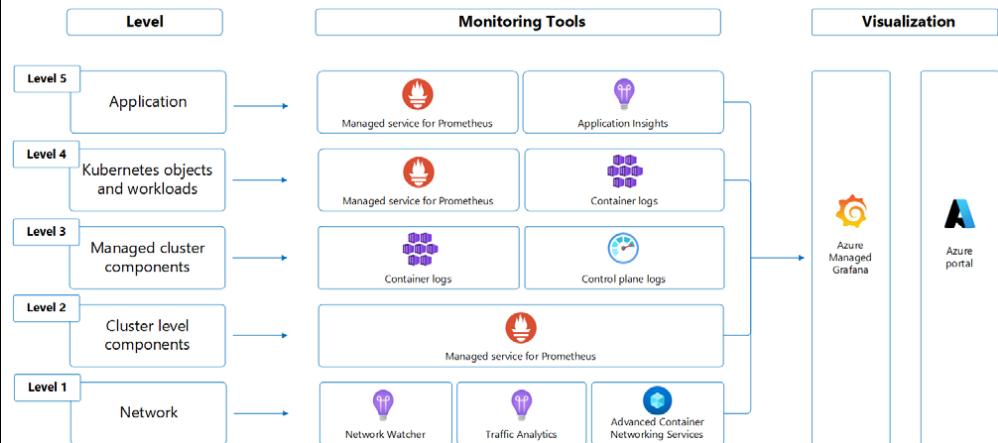
TOUTVIRTUAL 002281-TOUTVIRTUAL 002312.

Azure Monitor further includes Log Analytics that allows users to explore and analyze data collected by Azure Monitor Logs. A user may edit and run log queries to filter records, uncover trends, analyze patterns, and gain meaningful insights into the user's Azure virtualization environment in real time.



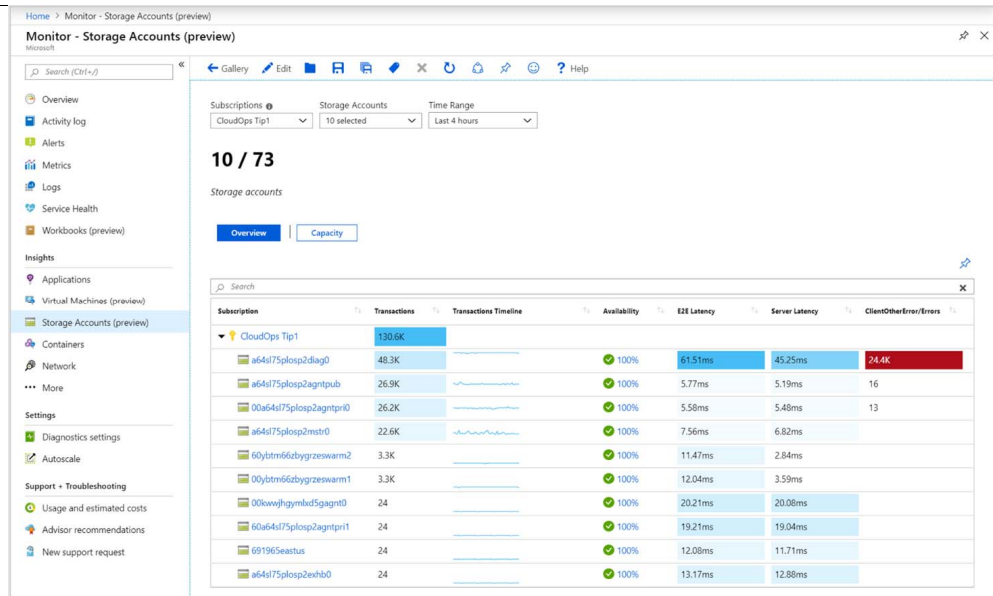


scheduling attempts, and container-level health signals. Azure Controllers use this performance data to generate reports, drive autoscaling logic, trigger alerts, and support automatic remediation in an AKS environment.



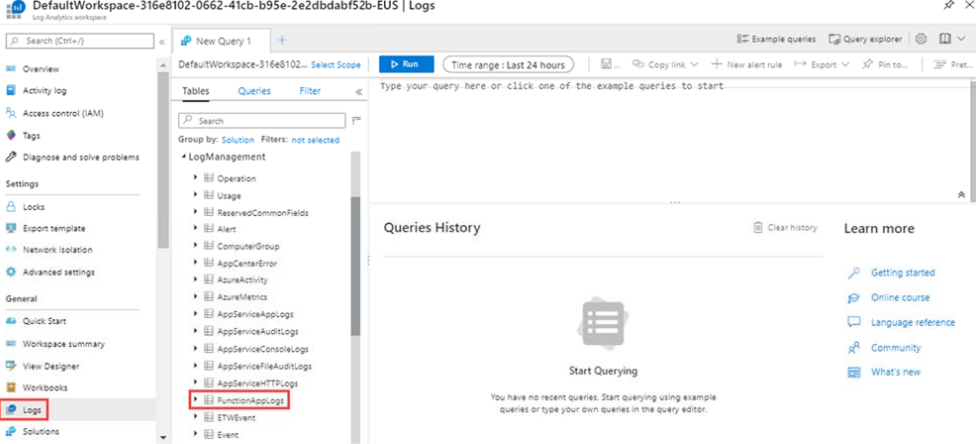
TOUTVIRTUAL 003284-TOUTVIRTUAL 003287.

The Azure Controllers may receive real time performance measurements and reports for storage-virtualized assets from Azure Monitor in real time. From Azure Blob Storage, Azure Monitor automatically collects metrics related to latency, throughput, throttling events, replication health, and capacity usage. From Azure Files, Azure Monitor automatically collects metrics related to SMB and NFS latency, IOPS, quota usage, and share health. From Azure Disk Storage, Azure Monitor automatically collects metrics related to IOPS, throughput, queue depth, read and write latency, and disk health signals. From Azure Elastic SAN, Azure Monitor automatically collects metrics related to volume throughput, SAN controller health, redundancy status, and capacity utilization. Azure Monitor collects these metrics automatically and provides these metrics to Azure Controllers, so that Azure Controllers may aggregate these metrics, provide continuous reporting, and support reallocation or deployment decisions.



TOUTVIRTUAL 003288-TOUTVIRTUAL 003303; TOUTVIRTUAL 003388-TOUTVIRTUAL 003397; TOUTVIRTUAL 003398-TOUTVIRTUAL 003405; TOUTVIRTUAL 003406-TOUTVIRTUAL 003413; TOUTVIRTUAL 003414-TOUTVIRTUAL 003416.

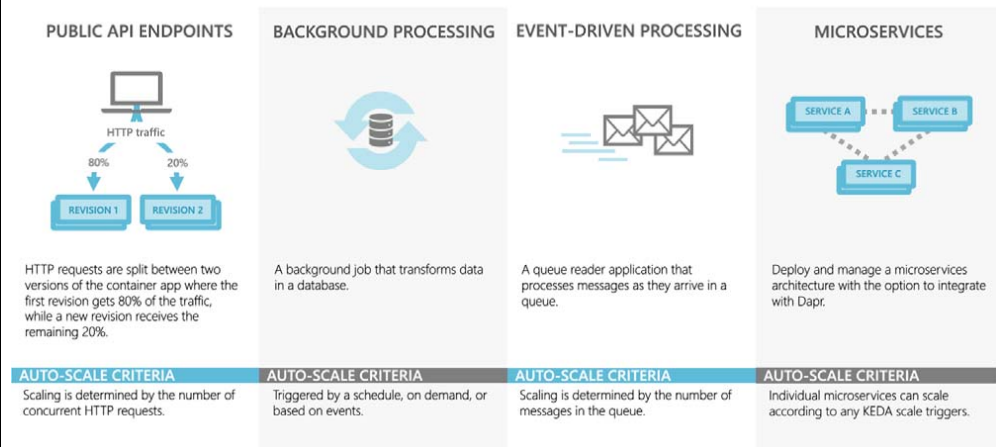
The Azure Controllers will also, in real time, determine performance metrics of the provisioned virtual asset through Azure Functions. Real time performance metrics will be measured and reported, along with other available resources, via Azure Functions based on different demand loads and over certain time periods that Azure Functions has been operating.

	 TOUTVIRTUAL 003304-TOUTVIRTUAL 003313.
Claim 14 14. The apparatus of <i>claim 9</i>, wherein the inventory further comprises one or more application programs.	See Claim 9[b][i]. The Accused Instrumentality meets the recited claim language because the virtualization environment's inventory comprises one or more application programs. The Accused Instrumentality's inventory includes but is not limited to application programs, such as Azure App Service, Azure Container Apps, Azure Kubernetes Service, Arc-enabled Kubernetes, and Azure Functions, that operate as virtual assets within the virtualization environment. TOUTVIRTUAL 002225-TOUTVIRTUAL 002226; TOUTVIRTUAL 002989-TOUTVIRTUAL 002991; TOUTVIRTUAL 002260-TOUTVIRTUAL 002264; TOUTVIRTUAL 002649-TOUTVIRTUAL 002650; TOUTVIRTUAL 002804-TOUTVIRTUAL 002806. These application programs allow the user to build, deploy, and manage tasks and solutions without regard to underlying infrastructure because the application programs are operating on a virtual asset. The Accused Instrumentality provides Azure App Service, which is a platform that manages infrastructure which allows the operation of web applications, mobile backends, and other APIs. TOUTVIRTUAL 002225-TOUTVIRTUAL 002226; TOUTVIRTUAL 002900-TOUTVIRTUAL 002908.

The Accused Instrumentality provides Azure Container Apps, which is a container platform that runs microservices, event-driven applications, Application Programming Interfaces (“APIs”), and background jobs without requiring a user to manage the underlying Kubernetes clusters directly. Azure Container Apps leverages Kubernetes, Kubernetes Event-driven Autoscaling (“KEDA”), Distributed Application Runtime (“Dapr”), and Microsoft-managed scale controllers to automatically scale containers based on events, HTTP load, or resource metrics. TOUTVIRTUAL 003095-TOUTVIRTUAL 003103. Container workloads from Azure Container Apps are executed inside managed Kubernetes clusters that run on Azure compute infrastructure. These Azure Container Apps compute hosts are implemented as Azure virtual machines, which run on physical servers controlled by the virtualization layer.



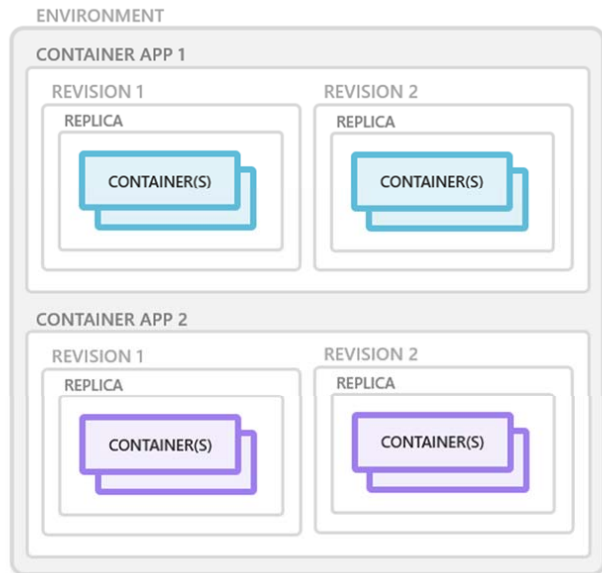
Azure Container Apps: Example scenarios



TOUTVIRTUAL 002989-TOUTVIRTUAL 002991;



Containers in an Azure Container Apps environment are grouped together in pods inside revision snapshots.



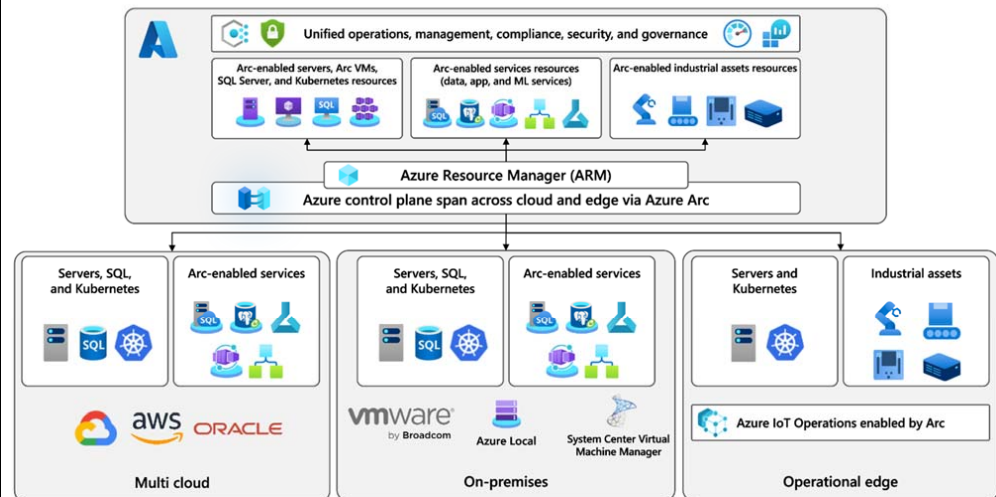
TOUTVIRTUAL 002992-TOUTVIRTUAL 002999; TOUTVIRTUAL 003000-TOUTVIRTUAL 003002; TOUTVIRTUAL 003003-TOUTVIRTUAL 003008.

The Accused Instrumentality provides AKS, which is a Kubernetes management service that allows users to deploy, scale, and manage containerized applications. AKS provides automated upgrades, node health monitoring, workload scheduling, and integration with Azure networking, storage, and security services. AKS relies on Azure virtual machines to serve as Kubernetes worker nodes. TOUTVIRTUAL 002260-TOUTVIRTUAL 002264; TOUTVIRTUAL 002614-TOUTVIRTUAL 002620, TOUTVIRTUAL 002640-TOUTVIRTUAL 002645; TOUTVIRTUAL 002646-TOUTVIRTUAL 002648; TOUTVIRTUAL 002649-TOUTVIRTUAL 002650.

The Accused Instrumentality provides Azure Arc, which extends management, governance, and Kubernetes orchestration capabilities to infrastructure running outside of the Azure environment, including on-premises servers, edge devices, and other cloud environments. TOUTVIRTUAL 002134-TOUTVIRTUAL 002137. Azure Arc also includes Azure Arc Resource Bridge, which is

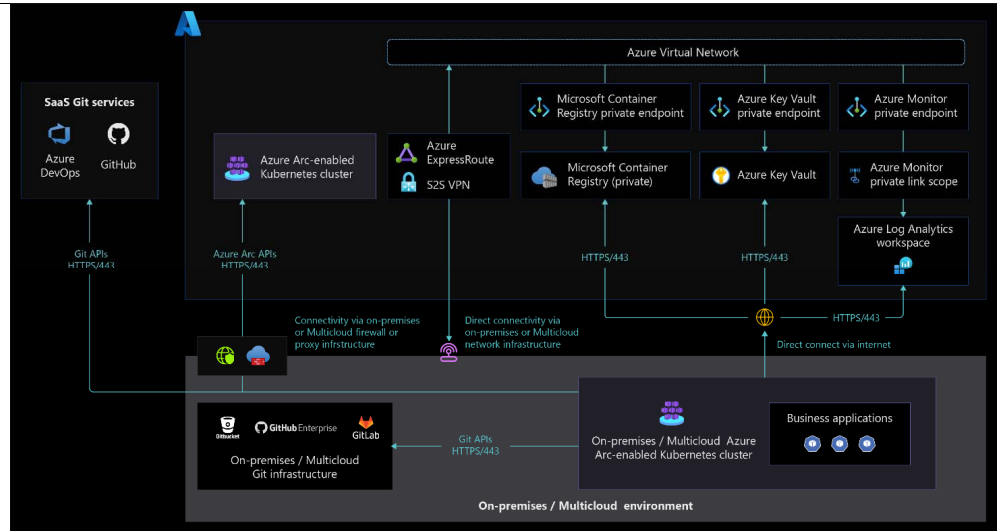
an appliance that runs in on-premises or edge environments and projects physical resources, such as servers, storage, and Kubernetes infrastructure, into the Azure Controllers as Azure resources. TOUTVIRTUAL 003039-TOUTVIRTUAL 003045. Azure Arc further projects these external systems into the Azure Portal or Windows Admin Center, allowing them to be managed through the same control plane as Azure physical resources and virtual assets.

Azure Arc solution overview architecture



TOUTVIRTUAL 002138-TOUTVIRTUAL 002142; TOUTVIRTUAL 002553-TOUTVIRTUAL 002570.

Azure Arc-enabled Kubernetes integrates external Kubernetes clusters within Azure's control plane. These clusters may run on different environments, such as Hyper-V in on-premises environments, VMware ESXi, bare-metal hardware, or cloud virtual machines in Amazon Web Services, Google Cloud Platform, etc. Regardless of the underlying environment, Azure Arc views these systems as Azure-managed virtual assets. TOUTVIRTUAL 002646-TOUTVIRTUAL 002648; TOUTVIRTUAL 002649-TOUTVIRTUAL 002650; TOUTVIRTUAL 002810-TOUTVIRTUAL 002816;



TOUTVIRTUAL 003211-TOUTVIRTUAL 003213; TOUTVIRTUAL 003217-TOUTVIRTUAL 003219; TOUTVIRTUAL 003220-TOUTVIRTUAL 003224.

The Accused Instrumentality provides Azure Functions, which extend Azure App Service's functionality such that code may be implemented based on a trigger event. This functionality leverages Azure App Service such that code may be initiated automatically once a trigger event occurs so that the virtual environment may respond to changes instantaneously. TOUTVIRTUAL 002225-TOUTVIRTUAL 002226; TOUTVIRTUAL 002804-TOUTVIRTUAL 002806; TOUTVIRTUAL 005107-TOUTVIRTUAL 005114.