solliance

SECURING LINUX WORKLOADS IN AZURE

White Paper

Sponsored by Microsoft Azure and AMD

Written by Reid Patrick

Microsoft Azure AMD

About Solliance

Solliance delivers expert led end-to-end technology solutions—from strategic planning to architecture design and implementation—for a diverse range of customers, including Fortune 500 companies and start-ups. Our global team of more than 300 top tier industry experts spans 18 countries, features 30 Microsoft MVPs and averages 20 years of experience in Cloud, AI & Data, Infrastructure & DevOps, Security, Applications, Microservices, Advanced Computing, and Training.

Recognized as one of Microsoft's top global partners, Solliance was awarded the exclusive Advanced Specialization in AI and Machine Learning on Microsoft Azure. Our team also regularly leads advanced 300 & 400 level trainings for the Microsoft field.

Our fast growing AI & Data practice brings unparalleled expertise in Artificial Intelligence, Cloud Analytics, Machine Learning, Natural Language Processing and Large Language Models. Years before the excitement around OpenAI, Solliance was using generative AI technologies to build real-world, innovative applications.

About the Author

Reid Patrick is a 15-year veteran at Microsoft and a nine-time Microsoft Azure MVP for Networking. He has extensive DevOps experience using Terraform, Bicep, PowerShell, and Bash, and is highly skilled in Cloud Architecture, Microservices, DevOps, Automation, Hybrid Networking, Infrastructure Modernization, Migrations, and Disaster Recovery.

With a career spanning over three decades, Reid has worked with at-scale internet deployments using Linux since 1995, building some of the largest websites in the world. He is also highly experienced in leveraging Kubernetes for deployments on Azure, solidifying his expertise in modern cloud-native practices. Currently, Reid is focused on DevOps for AI solutions using Azure OpenAI and FoundationaLLM (https://foundationallm.ai).

Reid is the Chief Infrastructure Architect at Solliance. He has a distinguished background in IT Infrastructure and Operations, having architected and led teams supporting some of the largest service providers in North America, managing environments with as many as 15,000 Windows Servers and 120 million endpoints.

As a published author, Reid contributed to the Networking, Azure Active Directory, and Containers sections of the 70-533 Exam Reference for Microsoft Press. Additionally, he has written nearly 250 pages of the Cloud Adoption Framework for Microsoft Azure, further solidifying his thought leadership in the field.

Contents

Executive Summary

Microsoft Azure offers a comprehensive suite of cloud services, enabling developers and IT professionals to build, deploy, and manage applications efficiently across a global network of data centers. This platform also provides extensive support for running Linux workloads, allowing users to leverage the scalability, reliability, and flexibility of Linux within Azure's secure and high-performance environment.

The adoption of Linux on Azure has grown significantly, driven by the platform's robust features and flexibility. Linux is fundamental to cloud-native environments due to its scalability, reliability, and compatibility with modern cloud applications. Every day, Azure deploys thousands of Linux virtual machines, reflecting the platform's growing adoption of Linux workloads. Azure's support for various Linux distributions, including commercial options such as Ubuntu Pro, Red Hat Enterprise Linux, and SUSE Linux Enterprise Server, and community-supported distros such as Rocky and AlmaLinux, supports this surge. With more than 60% of all customer cores on Azure running Linux, Microsoft's significant investments and commitment to optimizing Linux performance and security on their cloud infrastructure are evident.

Azure's commitment to Linux is demonstrated through continuous investments in infrastructure, comprehensive support for various distributions, and strategic partnerships to enhance and optimize Linux solutions on the Azure platform.

In collaboration with AMD, Microsoft Azure offers high-performance virtual machines powered by AMD EPYC™ processors, improving performance and cost-efficiency for various workloads on the Azure cloud platform. Additionally, Azure supports confidential computing using AMD processors, ensuring that data remains encrypted for data in use and providing an extra layer of security for sensitive workloads.

By accelerating the deployment of Linux workloads on Azure and improving its perception as a proven platform for running Linux and open-source workloads, Azure and AMD demonstrate their thought leadership in the Linux and open-source ecosystem.

When designing and deploying Linux-based solutions on Azure, Platform engineers must address critical areas of concern, including **data in use, data at rest, data in transit,** and **data access,** each requiring specific protective measures provided by Azure, as seen in Table 1 – Security areas of concern.

Area of Concern	Details
Data in use	Data actively being processed by applications, including in-memory data. Techniques like confidential computing, which ensure data is encrypted even during processing, help protect data in use from unauthorized access or tampering.
Data at rest	Refers to inactive data stored physically in any digital form (e.g., databases, data warehouses). Encryption and access controls are essential to protect this data from unauthorized access or breaches.
Data in transit	Data actively moving from one location to another, such as across the internet or through a private network. It is crucial to secure this data using encryption protocols like TLS to prevent interception and ensure data integrity.
Data access	Involves controlling who has the right to access and manipulate data. This includes implementing authentication, authorization, and auditing mechanisms to ensure only authorized users can access sensitive data.

Table 1 – Security areas of concern

The following sections will detail how Microsoft Azure and AMD address these concerns while providing robust scalability and security from deployment to ongoing operations.

Azure Platform Security Features for Linux

Azure provides a robust platform with comprehensive security features designed to protect Linux workloads at every stage. Amongst the various services, some of the most important measures include:

- **Azure Confidential Computing:** AMD Secure Encrypted Virtualization-Secure Nested Paging (SEV-SNP) enabled VMs and hardware and full-disk encryption with secure-key release leveraging virtual TPM (vTPM), ensuring that data remains encrypted during processing and storage.
- **Microsoft Defender for Cloud:** Advanced threat protection and endpoint security
- **Microsoft Sentinel:** Scalable cloud-native security information and event management (SIEM) solution tailored for Linux environments

Azure Confidential Computing

Confidential computing is an industry term established by the Confidential Computing Consortium (CCC), part of the Linux Foundation.

These secure and isolated environments help prevent unauthorized access or modification of applications and data while in use, thereby increasing the security level of organizations that manage sensitive and regulated data.

Microsoft and AMD are members of the governing body, which was formed in 2019, and have members serving on its governing body and the Technical Advisory Council (TAC).

Confidential computing secures sensitive and regulated data while being processed in the cloud. It encrypts data in memory in hardware-based and attested trusted execution environments. It processes it only after the cloud environment is verified, helping prevent data access by cloud providers, administrators, and unauthorized third parties.

Confidential VMs using AMD Processors

Azure leverages AMD EPYC™ processors with Secure Encrypted Virtualization-Secure Nested Paging (SEV-SNP) to ensure data remains encrypted in memory. This technology creates isolated encrypted environments that protect sensitive workloads from unauthorized access or tampering. Existing VMs can be moved to Azure and secured without additional code changes. Running confidential VMs in Azure using AMD processors provides the following benefits:

- Robust hardware-based isolation between virtual machines, hypervisor, and host management code.
- Customizable attestation policies to ensure the host’s compliance before deployment.
- Cloud-based Confidential OS disk encryption before the first boot.
- VM encryption keys that the platform or the customer (optionally) owns and manages.

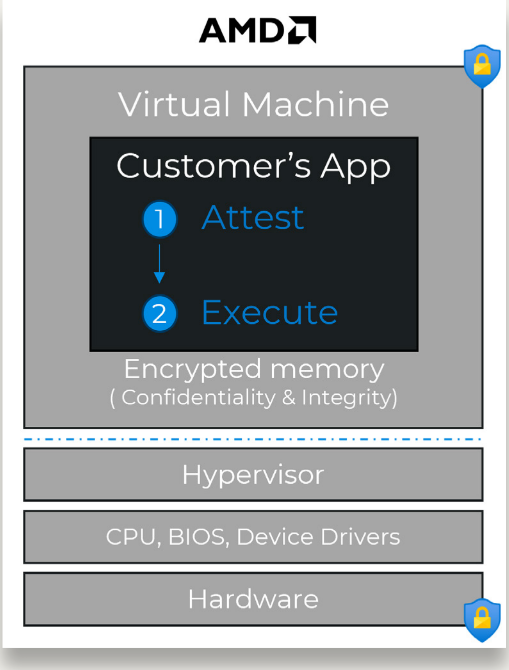


Figure 1 – AMD Confidential Computing on Azure

Figure 1 – AMD Confidential Computing on Azure shows how AMD's SEV-SNP Trusted Execution Environment (TEE) technology offers multiple protections: memory encryption, unique CPU keys, encryption for the processor register state, integrity protection, firmware rollback prevention, side-channel hardening, and restrictions on interrupt and exception behavior.

Collectively, AMD SEV technologies harden guest protections to deny hypervisor and other host management code access to VM memory and state. Confidential VMs leverage AMD SEV-SNP with Azure technologies such as full-disk encryption and Azure Key Vault Managed HSM. Data can be encrypted in use, in transit, and at rest with keys under user control. Built-in Azure Attestation capabilities allow independent establishment of trust in the security, health, and underlying infrastructure of confidential VMs.

Azure confidential VMs on AMD SEV-SNP undergo attestation as part of their boot phase. This process is opaque to the user and occurs in the cloud operating system with the Microsoft Azure Attestation and Azure Key Vault services. Confidential VMs also allow users to perform independent attestation for their confidential VMs. This attestation uses Azure Confidential VM (CVM), enabling customers to attest that their confidential VMs are running on AMD processors with SEV-SNP enabled.

Additionally, Azure employs full-disk encryption with Secure Key Release to enhance data protection by ensuring that encryption keys are securely managed and released only to authorized entities. Virtual TPM (vTPM) provides hardware-based encryption key management, further enhancing critical data security. These combined technologies offer robust protection for sensitive information, making Azure an ideal platform for securely handling and processing critical workloads.

Microsoft Defender for Cloud

This platform security system is pivotal in securing Linux workloads on Azure by providing advanced threat protection tailored for Linux environments. It continuously monitors, analyzes, and responds to potential security threats, integrating seamlessly with the Azure platform. This integration allows for unified security management and threat protection across hybrid cloud workloads, ensuring comprehensive security coverage. Microsoft Defender for Cloud helps maintain security baselines and applies best practices, offering robust protection against an evolving threat landscape.

Microsoft Defender for Cloud is a cloud-native application protection platform (CNAPP) comprising security measures and practices designed to protect cloud-based applications from various cyber threats and vulnerabilities. Defender for Cloud combines the capabilities of:

- A development security operations (DevSecOps) solution that unifies security management at the code level across multi-cloud and multiple-pipeline environments
- A cloud security posture management (CSPM) solution that surfaces actions that you can take to prevent breaches
- A cloud workload protection platform (CWPP) with specific protections for servers, containers, storage, databases, and other workloads

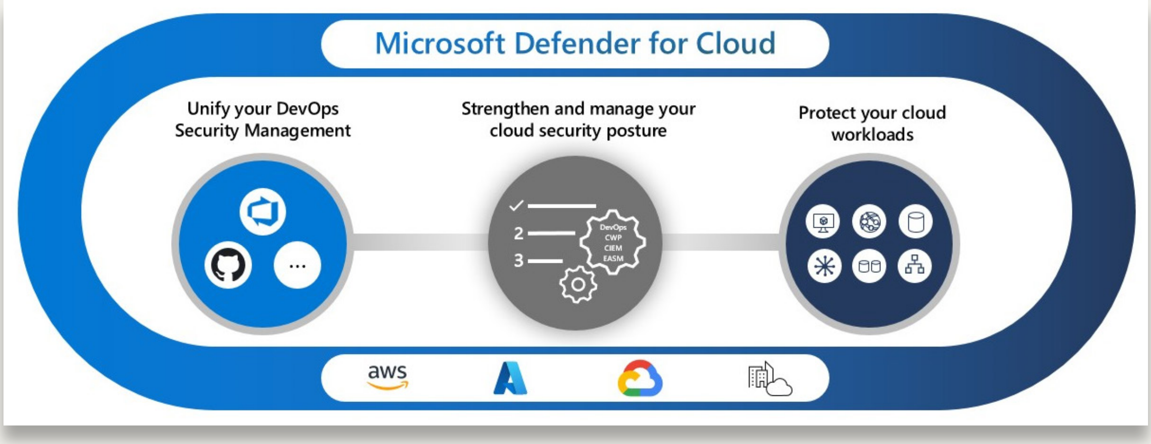

Microsoft Defender for Cloud
Unify your DevOps Security Management
Strengthen and manage your cloud security posture
Protect your cloud workloads
2
3
DevOps
CWP
CIEM
EASM
...
aws

Figure 2 – Microsoft Defender for Cloud

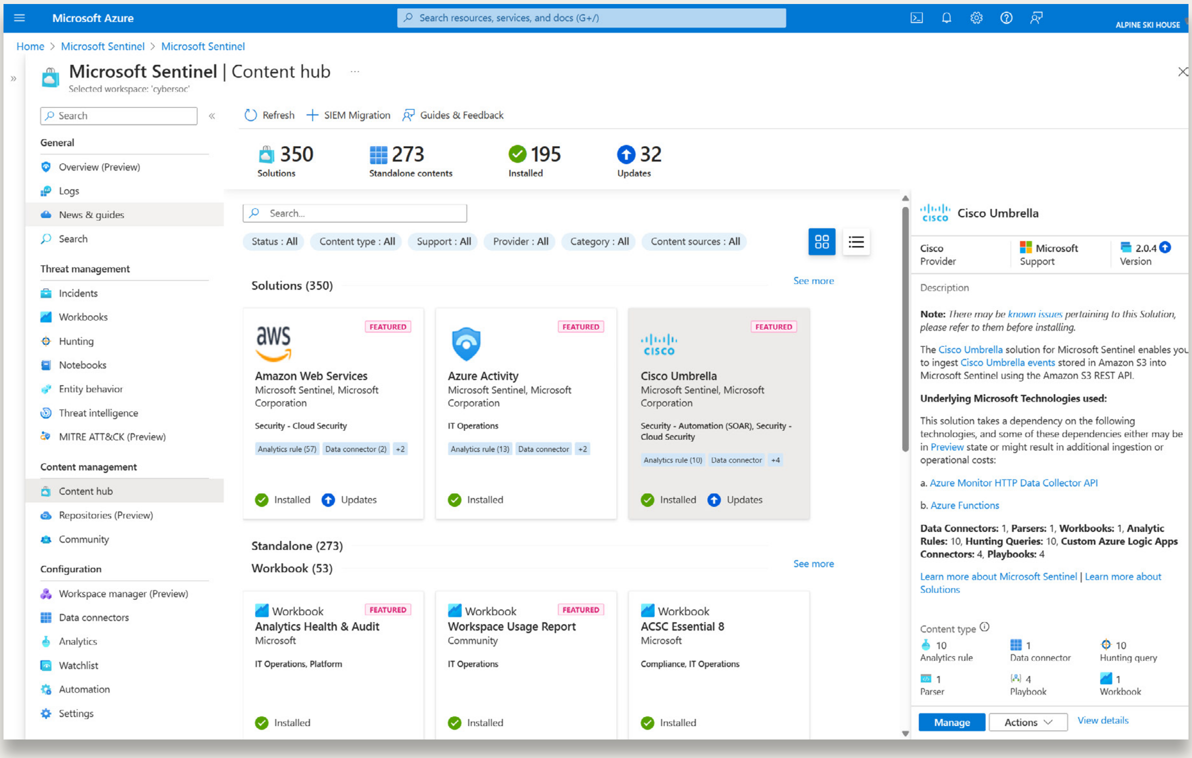
Microsoft Defender for Cloud extends its capabilities with robust endpoint management for Linux, ensuring comprehensive security across all devices and systems within the Azure environment. By integrating advanced threat detection and response functionalities, Microsoft Defender for Cloud monitors endpoint activities continuously, identifying and mitigating potential security risks in real time. This endpoint management system enforces security baselines, ensuring Linux workloads adhere to best practices and compliance requirements. It also facilitates automated responses to detected threats, minimizing the risk of breaches and reducing the workload on IT security teams. With these features, Microsoft Defender for Cloud provides a cohesive security strategy, safeguarding Linux environments against an evolving threat landscape.

Microsoft Sentinel

Microsoft Sentinel is a scalable, cloud-native Security Information and Event Management (SIEM) solution that delivers an intelligent and comprehensive approach to SIEM and Security Orchestration, Automation, and Response (SOAR). It provides cyber threat detection, investigation, response, and proactive hunting, offering a panoramic view across the enterprise.

Microsoft Sentinel natively incorporates proven Azure services such as Log Analytics and Logic Apps, enriching investigations, and detection with artificial intelligence. It leverages Microsoft's threat intelligence stream and allows the integration of custom threat intelligence.

Deploying Microsoft Sentinel helps mitigate the stress of increasingly sophisticated attacks, the growing volume of alerts, and prolonged resolution time frames. Figure 3 – Microsoft Sentinel Content Hub shows a heads-up display of security issues in all environments.



Note: *There may be known issues pertaining to this Solution, please refer to them before installing.*

The Cisco Umbrella solution for Microsoft Sentinel enables you to ingest Cisco Umbrella events stored in Amazon S3 into Microsoft Sentinel using the Amazon S3 REST API.

Underlying Microsoft Technologies used:

This solution takes a dependency on the following technologies, and some of these dependencies either may be in Preview state or might result in additional ingestion or operational costs:

a. Azure Monitor HTTP Data Collector API

b. Azure Functions

Data Connectors: 1, **Parsers:** 1, **Workbooks:** 1, **Analytic Rules:** 10, **Hunting Queries:** 10, **Custom Azure Logic Apps Connectors:** 4, **Playbooks:** 4

Learn more about Microsoft Sentinel | Learn more about Solutions

Figure 3 – Microsoft Sentinel Content Hub

Microsoft Sentinel complements Microsoft Defender for Cloud as a scalable, cloud-native security information and event management (SIEM) solution. Designed to provide intelligent security analytics and threat intelligence, Microsoft Sentinel leverages built-in AI capabilities to detect, investigate, and respond to security threats swiftly. It integrates seamlessly with other Azure services, enabling comprehensive threat visibility and mitigation. By providing real-time security analytics and threat intelligence, Azure Sentinel ensures that Linux workloads on Azure are well-protected and can swiftly adapt to emerging security challenges.

Architecting Linux solutions for Azure

Several vital considerations ensure secure and efficient architecture when deploying Linux on Azure. The architecture should be designed with security best practices for IaaS and for networking of Linux deployments, including minimizing attack surfaces and securing data to address the items in Table 1 – Security areas of concern. Each component must be meticulously configured to maintain the integrity and security of the Linux environment within Azure:

- **Compute Resources:** Using confidential computing, selecting the proper VM generation and Azure VM family type based on the workload profile, and implementing Secure Boot with vTPM. Select the appropriate Linux distro, select or create VM image, and apply DevOps deployment techniques.
- **Storage Solutions:** Determining how to configure Azure's durable and highly available storage, ensuring at-rest and transit encryption, leveraging Azure's Platform Based Host Encryption and Azure Key Vault with Hardware Security Module (HSM).
- **Networking Considerations:** Implementing strict firewall rules and load balancing with a web application firewall (WAF) and secure virtual networks, segmented subnets, and virtual network interface cards with Network Security Groups (NSGs). An extensive set of VM SKUs provide support for encrypted network traffic.
- **Identity Management:** Integrating with Microsoft Entra ID to implement role-based access controls (RBAC) and multi-factor authentication (MFA). Leverage Azure Managed Identities to allow RBAC to be applied to Linux VMs.

Compute

When deploying Linux on Azure, selecting the appropriate computing resources is crucial for ensuring performance and security. Key considerations include using confidential computing, choosing the proper VM generation and Azure VM family type based on the workload profile, and implementing Secure Boot and Trusted Launch VMs. This section will explore how to make informed decisions regarding Linux OS distribution selections, VM image selection and creation, and proper deployment techniques within a DevOps framework. By addressing these aspects, organizations can optimize their computing environment for efficiency and security.

Confidential Computing: Several crucial aspects must be considered to ensure secure and effective deployment when implementing Azure VMs using confidential computing. These include selecting Generation 2 virtual machines, configuring Secure Boot, enabling the virtual Trusted Platform Module (vTPM) service, and using a Linux OS distribution image enabled for confidential computing.

Generation 2 Virtual Machines: Generation 2 VMs offer advanced features essential for confidential computing, such as improved security, increased performance, and support for larger VM sizes. When selecting VMs for confidential computing, it is critical to choose Generation 2 VMs as they support Secure Boot and vTPM, which are necessary for creating a secure execution environment.

Secure Boot: Secure Boot is a security standard developed to ensure that a device boots using only software trusted by the Original Equipment Manufacturer (OEM). Enabling Secure Boot is vital when configuring confidential VMs in Azure, as it helps prevent unauthorized software and malware from loading during the boot process. Secure Boot checks the digital signatures of all boot components, ensuring that only approved software is executed.

Virtual Trusted Platform Module (vTPM): The vTPM service is essential for confidential computing, providing hardware-based security functions. A TPM chip stores cryptographic keys securely and performs cryptographic operations. Enabling vTPM on Azure VMs enhances security by ensuring that sensitive data, such as encryption keys, is stored securely and can only be accessed by authorized software. This adds an extra layer of protection against attacks and unauthorized access.

Supported Operating Systems: When deploying VMs for confidential computing, it is crucial to use an OS distribution that supports these advanced security features. Not all Linux distributions are compatible with confidential computing, so selecting a supported OS is essential. Commonly supported distributions include specific versions of Ubuntu, SUSE, and Red Hat Enterprise Linux (RHEL) enabled for confidential computing. These distributions are optimized to work seamlessly with Generation 2 VMs, Secure Boot, and vTPM security features.

Trusted Launch: Trusted Launch is an Azure feature that enhances the security of VMs by providing continuous monitoring and assessment of the VM's security posture. It ensures that VMs are not tampered with by validating the boot process, performing integrity checks, and enforcing security policies. Trusted Launch leverages both Secure Boot and vTPM to offer a comprehensive security solution, ensuring the confidential computing environment remains secure throughout its lifecycle.

AMD EPYC™-based Azure Virtual Machines

The AMD EPYC™ series supports confidential computing in Azure, offering advanced security features and high-performance capabilities tailored to meet the needs of modern cloud environments. Azure confidential VMs leverage these processors to provide a secure enclave where data can be processed while remaining encrypted. This is a significant advancement over virtual machines (VMs), which do not inherently offer the same level of protection for data in use.

AMD-based confidential VMs, such as the DCasv5 and ECasv5-series, are specifically designed to utilize AMD Secure Encrypted Virtualization-Secure Nested Paging (SEV-SNP) technology. These VM sizes come with additional security features like virtual Trusted Platform Module (vTPM) and Secure Boot, which ensure that data is protected from unauthorized access even during processing. This level of security is critical for organizations handling sensitive information and needing to comply with stringent security and regulatory requirements.

In contrast, while still offering robust security measures, Azure VM sizes do not provide the same guarantees for data confidentiality during computation. They are designed for general-purpose workloads and do not include the specialized hardware-based security features that confidential computing VMs offer. This makes them less suitable for workloads requiring high data protection during processing.

The differences between confidential computing VM sizes and regular VM sizes can be summarized as follows:

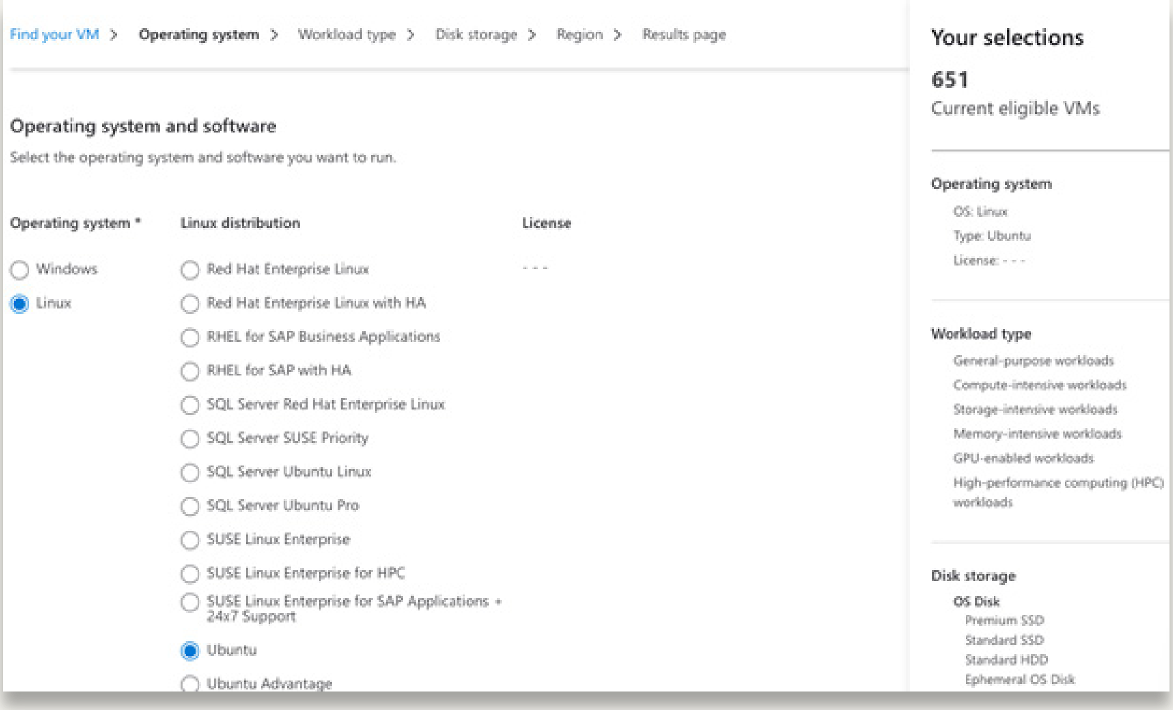
- **Security Features:** Azure Confidential VMs include SEV-SNP, vTPM, and Secure Boot, while Azure VMs do not.
- **Use Cases:** Confidential VMs are ideal for workloads involving sensitive data and requiring high levels of data protection, while Azure VMs are suitable for general-purpose computing.
- **Performance:** Azure VM types leverage the high performance of AMD EPYC™ processors, but confidential VMs are optimized for security alongside performance.

Azure Virtual Machine types: Azure offers a diverse range of VM types tailored to meet the unique demands of various workloads. Each VM type has specific features and performance characteristics, making it suitable for different use cases, from entry-level applications to high-performance computing and confidential data processing.
Table 2 – Azure Virtual Machine types, highlight key features and example use cases to guide you in selecting the best VM type for your specific requirements.

Type	Description
General purpose	Balanced CPU-to-memory ratio. Ideal for testing and development, burstable workloads, small to medium databases, and low to medium traffic web servers.
Compute optimized	High CPU-to-memory ratio. Good for medium traffic web servers, network appliances, batch processes, and application servers.
Memory optimized	High memory-to-CPU ratio. Great for relational database servers, medium to large caches, and in-memory analytics.
Storage optimized	High disk throughput and IO ideal for Big Data, SQL, NoSQL databases, data warehousing and large transactional databases.
GPU	Specialized virtual machines targeted for heavy graphic rendering and video editing, as well as AI model training and inferencing (ND) with deep learning. Available with single or multiple GPUs.
High performance computing	Fastest and most powerful CPU virtual machines with optional high-throughput network interfaces (RDMA).

Table 2 – Azure Virtual Machine types

Microsoft provides a Virtual Machine selector tool to help customers determine which family of VMs is best for their use case. Figure 4 – Virtual Machine selector tool, shows the tool with the endorsed Linux distributions found in the Azure Marketplace.



Find your VM > Operating system > Workload type > Disk storage > Region > Results page

Operating system and software

Select the operating system and software you want to run.

Operating system *

○ Windows
● Linux

Linux distribution

○ Red Hat Enterprise Linux
○ Red Hat Enterprise Linux with HA
○ RHEL for SAP Business Applications
○ RHEL for SAP with HA
○ SQL Server Red Hat Enterprise Linux
○ SQL Server SUSE Priority
○ SQL Server Ubuntu Linux
○ SQL Server Ubuntu Pro
○ SUSE Linux Enterprise
○ SUSE Linux Enterprise for HPC
○ SUSE Linux Enterprise for SAP Applications + 24x7 Support
● Ubuntu
○ Ubuntu Advantage

License

- - -

Your selections

651
Current eligible VMs

Operating system
OS: Linux
Type: Ubuntu
License: - - -

Workload type
General-purpose workloads
Compute-intensive workloads
Storage-intensive workloads
Memory-intensive workloads
GPU-enabled workloads
High-performance computing (HPC) workloads

Disk storage
OS Disk
Premium SSD
Standard SSD
Standard HDD
Ephemeral OS Disk

Figure 4 – Virtual Machine selector tool

AMD EPYC™ confidential computing VM options: These AMD EPYC™ processors are specifically designed to meet the demanding security and performance requirements of confidential computing workloads in Azure.

Azure VM Name	Processor Name	Workload Types
DCasv5-series	3rd Gen AMD EPYC™ 7763v	General purpose CVM with remote storage. No local temporary disk.
DCadsv5-series	3rd Gen AMD EPYC™ 7763v	General purpose CVM with local temporary disk.
ECasv5-series	3rd Gen AMD EPYC™ 7763v	Memory-optimized CVM with remote storage. No local temporary disk.
ECadsv5-series	3rd Gen AMD EPYC™ 7763v	Memory-optimized CVM with local temporary disk.

Table 3 – AMD EPYC™ Confidential Computing VM Sizes

AMD EPYC™ VM options: Table 4 – AMD EPYC™ VM Sizes are some options designed to meet Azure workloads' demanding security and performance requirements. All these configurations support Linux. All VM sizes are compatible with Azure VM security features except those specifically designed for confidential computing.

VM Series	Processor Name	Workload Types	Details
Basv2-series	3rd Gen AMD EPYC™ 7763v	Burstable	Burstable general-purpose workloads with long periods of idle time utilizing a CPU credit model.
Dasv6 and Dadsv6-series	4th Gen EPYC™ 9004v	General Purpose	General-purpose, enterprise applications. General computing workloads, such as e-commerce systems, web front ends, desktop virtualization solutions, customer relationship management applications, entry-level and mid-range databases, and application servers.
Dalsv6 and Daldsv6-series	4th Gen EPYC™ 9004v	General Purpose	General-purpose, enterprise applications. Optimized for workloads that require less RAM per vCPU than standard VM sizes. Best for running non-memory intensive applications, including web servers, gaming, video encoding, AI/ML, and batch processing. OS images that are tagged with NVMe support.
Falsv6, Fasv6, and Famsv6-series	4th Gen EPYC™ 9004v	Compute Optimized	Optimized for scientific simulations, financial and risk analysis, gaming, rendering and other workloads able to take advantage of the exceptional performance Configured without Simultaneous Multithreading (SMT), meaning a vCPU is mapped to a full physical core, allowing software processes to run on dedicated and uncontested resources.
NCads H100 v5-series	4th Gen AMD EPYC™ 9V33X	GPU-Accelerated	Designed for real-world Azure Applied AI training and batch inference workloads. Powered by 4th-generation AMD EPYC™ 9V33X processors with NVIDIA H100 NVL GPUs. Ideal for Applied AI workloads, such as: GPU-accelerated analytics and databases, Batch inferencing with heavy pre-and post-processing, Autonomy model training, Oil and gas reservoir simulation, Machine learning (ML) development, Video processing, and AI/ML web services.
NC A100 v4-series	AMD EPYC™ 7763v Series	GPU-Accelerated	Designed for real-world Azure Applied AI training and batch inference workloads. Powered by AMD EPYC™ 7763v processors using NVIDIA A100 PCIe GPU. Ideal for real-world Applied AI workloads, such as: GPU-accelerated analytics and databases, Batch inferencing with heavy pre- and post-processing, Autonomy model training, Oil and gas reservoir simulation, Machine learning (ML) development, Video processing, and AI/ML web services.
HX-series	AMD EPYC™ 9V33X	High Performance Compute	HX-series VMs are optimized for workloads that require significant memory capacity with twice the memory capacity as HBv4. For example, workloads such as silicon design can use HX-series VMs to enable EDA customers targeting the most advanced manufacturing processes to run their most memory-intensive workloads.

Table 4 – AMD EPYC™ VM Sizes

Linux distributions supported on Azure

All Linux distributions (distros) are welcome in Azure. There are several different Linux VM images available for Azure. Each source provides a different expectation for quality, utility, and support. Image support comes from **Marketplace, Platform,** and **Community gallery images.**

Azure requires that the publishers of the endorsed Linux distributions regularly update their platform images in Azure Marketplace with the latest patches and security fixes at a quarterly or faster cadence. Updated images in the Marketplace are available automatically to customers as new versions of an image SKU. Learn how to find Linux images using the Azure CLI in the Azure Marketplace.

The Azure Linux Agent is already preinstalled on Azure Marketplace images and is typically available from the distribution package repository. Customers can integrate the Linux agent into custom images; the source code can be found on GitHub. The Linux Integration Services (LIS) drivers for Hyper-V and Azure also contribute directly to the upstream Linux kernel.

Marketplace images: Images published and maintained by either Microsoft or partners. Multiple publishers offer images for various use cases (security-hardened, full database/ application stack, etc.). They can be free, pay-as-you-go, or BYOL (bring your own license/ subscription).

Linux distributions such as Rocky, AlmaLinux, Kali, and others are available in Azure Marketplace. Microsoft assists with these distributions but may require customers to engage with vendors to allow collaboration between organizations. Vendors must provide distribution-specific fixes. For more information about support from Microsoft Azure on using Linux, see this article.

Platform Images: Platform images are Marketplace images for which Microsoft has partnered with several mainstream publishers (see table below about Partners) to create a set of "platform images" that undergo additional testing and receive predictable updates. These platform images can be used to build custom images and solution stacks. They are published by the endorsed Linux distribution partners Canonical (Ubuntu), Red Hat (RHEL), and Credativ (Debian). Some of the images have Azure-tuned Kernels.

Microsoft provides commercially reasonable customer support for these images. Red Hat, Canonical, and SUSE offer integrated vendor support capabilities for their platform images.

AMD Azure Confidential Computing VM

Platform images have been published for use with Confidential Computing VMs. Table 5 - AMD Confidential VM Linux OS lists the distros available for seamless deployment and support.

Linux Distribution	OS Version
Ubuntu	20.04 LTS | 22.04 LTS | 24.04 LTS
RedHat Enterprise Linux	9.3
SUSE Enterprise Linux	15 SP5 and 15 SP5 for SAP (Tech Preview)

Table 5 – AMD Confidential VM Linux OS

Community gallery images: Opensource projects, communities, and teams create and provide these images. They are provided using licensing terms set out by the publisher, often under an open source license. They do not appear as traditional marketplace listings. However, they do appear on the portal and via command-line tools. More information on community galleries can be found here: Azure Compute Gallery.

Microsoft provides commercially reasonable support for Community Gallery images.

Custom Images: Azure also supports uploading your own images for use on the platform. The customer creates and maintains these images, often based on platform images. These images can also be made from scratch and uploaded to Azure—learn how to create custom images. Customers can host these images in Azure Compute Gallery and share them with others in their organization. Microsoft provides commercially reasonable customer support for custom images.

When deploying Linux VMs, tools like Packer and Azure Images streamline the creation and management of VM images, ensuring consistency and repeatability across deployments. Integrating image scanning and secure supply chain repositories into your DevOps processes helps identify vulnerabilities and maintain the integrity of your images, ensuring that only secure and compliant images are deployed.

Azure now has a service called Azure Image Builder for defining and creating custom images. Azure Image Builder is built on Packer, allowing existing Packer shell provisioner scripts to be used. To start with Azure Image Builder, see Create a Linux VM with Azure Image Builder.

Deploying Linux VMs using Infrastructure as Code (IaC)

Deploying Linux virtual machines (VMs) in Azure can be efficiently managed using DevOps tools such as Azure Bicep, Terraform, Azure CLI, and PowerShell. Infrastructure as Code (IaC) tools are critical for secure deployments in Azure because they enable consistent, repeatable, and automated resource provisioning. They ensure that security best practices, such as role-based access control, encryption, and network configurations, are applied uniformly across all environments, reducing the risk of misconfigurations and human error.

These tools enable the automation of deployment processes, ensuring consistency, repeatability, and efficiency in managing Linux VMs in Azure. By integrating these DevOps tools into your CI/CD pipelines, customers can achieve continuous deployment and infrastructure management, significantly enhancing operational agility and minimizing manual intervention.

Bicep: Bicep, a domain-specific language (DSL) that uses declarative syntax to deploy Azure resources. In a Bicep file, the desired infrastructure is defined, and the file is used throughout the development lifecycle to deploy infrastructure repeatedly. Resources are deployed consistently.

Bicep provides concise syntax, reliable type safety, and support for code reuse, offering a first-class authoring experience for infrastructure-as-code solutions in Azure.

One advantage of Bicep is that it immediately supports all resource types and API versions. This includes all preview and GA versions for Azure services. When a resource provider introduces new resource types and API versions, they can be used in a Bicep file without waiting for tools to be updated before utilizing the new services.

Terraform using the Azure providers: Terraform, an IaC tool by HashiCorp, provides a consistent CLI workflow for managing and provisioning infrastructure using configuration files. This makes it possible to version control and automate deployments across different Azure deployments, environments, or subscriptions. Terraform has providers for Azure Resource Manager (ARM), AzureAD (Entra ID), and directly to the Azure ARM API. DevOps configurations can also be maintained using Azure DevOps and GitHub Providers.

Azure Command Line Tools: The Azure CLI is a command-line tool that allows for seamless scripting and automation of Azure resources. At the same time, Azure PowerShell, with its extensive cmdlet library, provides a robust scripting environment for managing and deploying Azure infrastructure. Both tools are cross-platform, bringing advanced scripting capabilities for provisioning and managing Azure resources on Windows, macOS, and Linux.

Cloud-init for Linux VMs: Cloud-init is a widely used approach to customize Linux VM as it boots for the first time. Cloud-init can be used to install packages and write files or to configure users and security. As cloud-init runs during the initial boot process, there are no additional steps or required agents to apply your configuration.

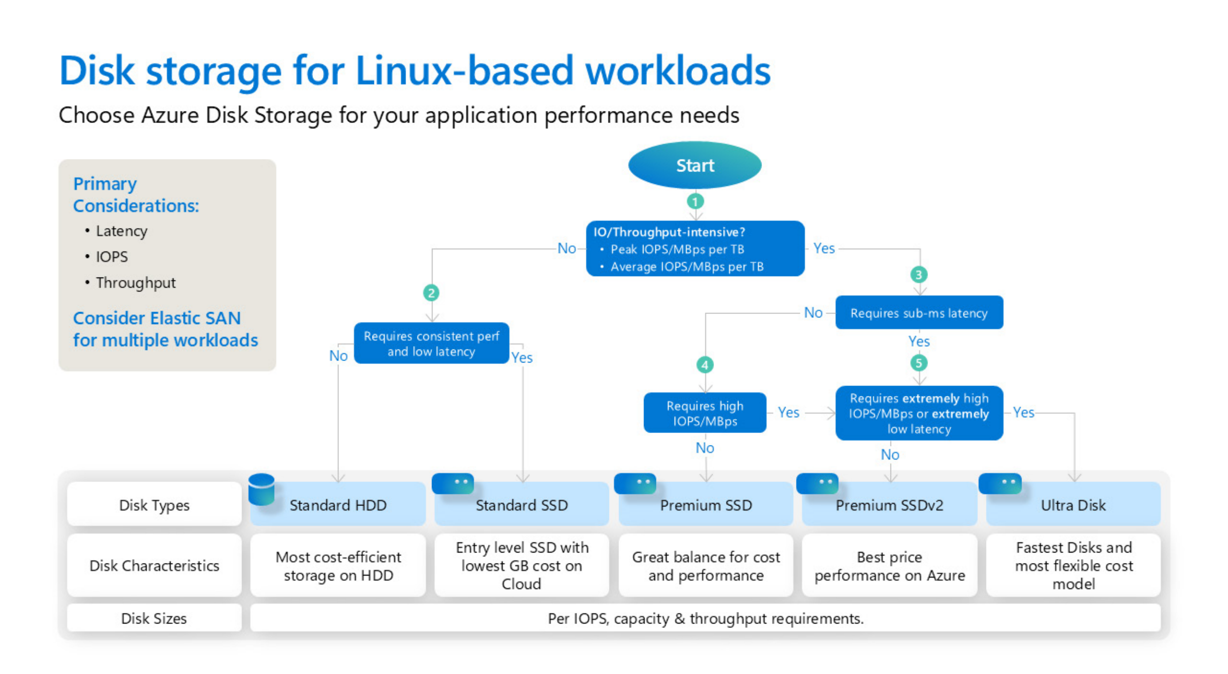
Cloud-init also works across distributions. For example, there's no need to use apt-get install or yum install to install a package. Instead, a list of packages can be defined for installation. Cloud-init automatically uses the native package management tool for the distro you select. Review this article for more information about using cloud-init with Linux VMs on Azure.

Storage

Using Azure Disk Storage with Linux VMs involves several vital practices to ensure security, efficiency, and reliability. Managed disks in Azure provide a scalable and secure storage solution, abstracting the complexities of storage management while offering high availability and durability. Securing access to these disks and encryption are practical tools for building secure Linux VMs. Together, these practices form a comprehensive approach to managing Azure Disk Storage with Linux VMs, enhancing security and operational efficiency.

Azure Disk Storage

Azure Disk Storage are block-level storage volumes managed by Azure and used with Azure Virtual Machines. They are like physical disks in an on-premises server but virtualized. With managed disks, only the disk size and type are required to be provisioned. Once the disk is provisioned, Azure handles the rest. The available disks are Ultra Disks, Premium SSDs, standard SSDs, and Standard HDDs. Figure 5 – Selecting Azure Manage Disks Storage shows a selection process that can be used to select the proper types of disks for Linux deployments on Azure. Additionally, this article provides information about each disk type.



Disk storage for Linux-based workloads

Choose Azure Disk Storage for your application performance needs

Primary Considerations:

- Latency
- IOPS
- Throughput

Consider Elastic SAN for multiple workloads

Start

1 IO/Throughput-intensive?
- Peak IOPS/MBps per TB
- Average IOPS/MBps per TB

No → 2 Requires consistent perf and low latency (No → Standard HDD; Yes → Standard SSD)

Yes → 3 Requires sub-ms latency

No → 4 Requires high IOPS/MBps (No → Premium SSD; Yes → Premium SSDv2)

Yes → 5 Requires **extremely** high IOPS/MBps or **extremely** low latency (No → Premium SSDv2; Yes → Ultra Disk)

Disk Types	Standard HDD	Standard SSD	Premium SSD	Premium SSDv2	Ultra Disk
Disk Characteristics	Most cost-efficient storage on HDD	Entry level SSD with lowest GB cost on Cloud	Great balance for cost and performance	Best price performance on Azure	Fastest Disks and most flexible cost model
Disk Sizes	Per IOPS, capacity & throughput requirements.				

Figure 5 – Selecting Azure Manage Disks

Securing access to Azure Disk Storage

Securing access to these disks is crucial; implementing Azure role-based access control (Azure RBAC) and leveraging Entra ID ensures that only authorized users and services can interact with the storage resources—specific permissions for a managed disk to one or more users. Managed disks expose various operations, including reading, writing (create/updating), deleting, and retrieving a shared access signature (SAS) URI for the disk. Access can be granted only to the operations required for a person to perform their job. For example, if the intent is to prevent a person from copying a managed disk to a storage account, access to the export action for that managed disk can be withheld. Similarly, if copying a managed disk using a SAS URI should be restricted, that permission can be omitted from the managed disk access.

Private Links: Private Links support for managed disks can be used to import or export a managed disk internal to the network. This restricts the export and import of managed disks only within an Azure virtual network. Private Links allows you to ensure your data only travels within the secure Microsoft backbone network.

Private Links allow for generating a time-bound Shared Access Signature (SAS) URI for unattached managed disks and snapshots. This URI can export the data to other regions for regional expansion, disaster recovery, and forensic analysis. The SAS URI can also be used to directly upload a VHD to an empty disk from on-premises.

To enable private links to import or export a managed disk, see the CLI or Portal articles.

Disk Encryption

Encryption is another vital aspect. Azure offers server-side encryption with platform-managed keys and customer-managed keys, ensuring data at rest is protected against unauthorized access. Managed disks offer two different kinds of encryption. The first is server-side encryption (SSE), which is performed by the storage service. The second is Azure Disk Encryption (ADE), which you can enable on the OS and data disks for your VMs.

Server-side encryption: Server-side encryption provides encryption-at-rest and safeguards data to meet organizational security and compliance commitments. It is enabled by default for all managed disks, snapshots, and images in all the Azure regions where managed disks are available. On the other hand, temporary disks are not encrypted by server-side encryption unless you enable encryption at the host.

Azure can manage keys automatically, which are platform-managed keys, or manually manage the keys, which are customer-managed. Visit the Server-side encryption of Azure Disk Storage article for details.

Azure Disk Encryption: Azure Disk Encryption encrypts the OS and data disks that an IaaS Virtual Machine uses. This encryption includes managed disks. For Linux, the disks are encrypted using the DM-Crypt technology. The encryption process is integrated with Azure Key Vault to allow you to control and manage the disk encryption keys. For more information, see Azure Disk Encryption for Linux VMs.

Networking

Securing Linux VMs in Azure involves implementing a comprehensive virtual network (VNet) security strategy using various Azure services and tools. Key components include Azure Bastion, Azure Firewall, Azure DDoS Protection, Azure Private Link, Azure Front Door with Web Application Firewall (WAF), and Network Security Groups (NSGs). Additionally, the internal firewall on the Linux OS should be configured as part of the defense-in-depth strategy.

These networking technologies collectively enhance the security posture of Linux VMs in Azure by providing robust controls and protections against various network-based threats and vulnerabilities. Table 6 – Azure Networking Security for Linux provides a consolidated view of the networking security features available to Platform engineers.

Name	Deployment	Purpose
Azure Bastion	Regional, VNet	Provides secure and seamless RDP and SSH access to VMs without exposing them to the public internet.
Azure DDoS Protection	Global	Protects Azure resources from Distributed Denial of Service (DDoS) attacks with automatic network traffic monitoring and mitigation.
Azure Firewall	Global, Regional	Provides a managed, cloud-based network security service to protect Azure Virtual Network resources with high availability and scalability.
Third-party Network Virtual Appliance Firewalls	Regional	Deployed as VMs into virtual network or into Azure Virtual WAN. These devices provide firewall services that match on-premises firewall deployments and management software. These are deployed using the Azure Marketplace.
Azure Front Door with Web Application Firewall (WAF)	Global	Provides global load balancing and web application acceleration, with built-in security features like Web Application Firewall (WAF) to protect against web vulnerabilities.
Azure Private Link	Regional, VNet	Enables private connectivity from a virtual network to Azure services, eliminating data exposure to the public internet.
Network Security Groups (NSG)	Regional, VNet	Filters network traffic to and from Azure resources, controlling inbound and outbound traffic based on security rules.

Table 6 – Azure Networking Security for Linux

Azure Bastion

Azure Bastion is a fully managed PaaS service that is provisioned to connect to VMs securely via a private IP address. It provides secure and seamless RDP/SSH connectivity to VMs directly over TLS from the Azure portal or via the native SSH or RDP client installed on a local computer. When connecting via Azure Bastion, VMs don’t need a public IP address, agent, or special client software.

Bastion provides secure RDP and SSH connectivity to all the VMs in the virtual network for which it’s provisioned. Azure Bastion protects VMs from exposing RDP/SSH ports to the outside world while providing secure access using RDP/SSH.

Azure DDoS Protection

Azure DDoS Protection safeguards resources from Distributed Denial of Service (DDoS) attacks through automatic traffic monitoring and mitigation. Distributed denial of service (DDoS) attacks are some of the most extensive availability and security concerns facing companies moving their applications to the cloud. A DDoS attack attempts to exhaust an application’s resources, making the application unavailable to legitimate users. DDoS attacks can be targeted at any publicly reachable endpoint through the internet.

These mitigation features defend against DDoS attacks and are automatically tuned to help protect specific Azure resources in a VNet. Protection is simple to enable on any new or existing virtual network and requires no application or resource changes.

Azure Firewall

Azure Firewall offers a managed, cloud-based security service that protects VNet resources with high availability and scalability. It is a cloud-native and intelligent network firewall security service that provides best-of-breed threat protection for VMs and cloud workloads running in Azure. It’s a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability. It provides both east-west and north-south traffic inspection.

Azure Private Link

Azure Private Link enables private connectivity from a VNet to Azure services, eliminating exposure to the public internet. It allows access to Azure PaaS Services such as Azure Storage and Azure PostgreSQL Database, as well as Azure-hosted customer-owned/partner services over a private endpoint connected to a subnet within the VNet.

A private endpoint is a network interface that uses a private IP address from the VNet. This network interface connects privately and securely to a service powered by Azure Private Link, allowing you to bring the service into your virtual network through the private endpoint. By leveraging Azure Private Link, communication occurs entirely within the Azure network, ensuring the traffic stays private and secure without exposing the service to the public internet.

Azure Front Door

Azure Front Door is Microsoft's modern cloud Content Delivery Network (CDN) that provides fast, reliable, and secure access to users' and applications' static and dynamic web content worldwide. Azure Front Door delivers content using Microsoft's global edge network, which has hundreds of global and local points of presence (PoPs) distributed to enterprise and consumer end users.

Azure Web Application Firewall (WAF) on Azure Front Door provides centralized protection for web applications. WAF defends web services against common exploits and vulnerabilities, ensuring high availability for users and helping meet compliance requirements.

Azure Web Application Firewall on Azure Front Door is a global and centralized solution. It's deployed on Azure network edge locations around the globe. WAF-enabled web applications inspect every incoming request delivered by Azure Front Door at the network edge.

A WAF prevents malicious attacks close to the attack sources before they enter a VNet. This means customers get global protection at scale without sacrificing performance. A WAF policy links to any Azure Front Door profile in a subscription. New rules can be deployed within minutes, enabling the ability to respond quickly to changing threat patterns.

WAF on Azure Front Door is based on the Core Rule Set (CRS) from the Open Web Application Security Project (OWASP).

Network Security Groups (NSGs)

NSGs control network traffic to and from Azure resources at regional and virtual network levels, enforcing inbound and outbound traffic rules based on SRE-defined security rules. Each rule can specify five critical pieces of information: source IP address, source port, destination IP address, destination port, and protocol (TCP or UDP). Rules are ordered by priority, from 100 to 65500, which dictates the sequence in which Azure evaluates packets. The lower the priority number, the higher the priority, meaning a rule with a priority of 150 would be assessed before a rule with a priority of 250. Three default rules are automatically applied: allowing all virtual network traffic, allowing Azure load balancer traffic, and denying all traffic in that order.

NSGs are stateful, meaning a flow record is created for existing connections, allowing or denying communication based on the connection state. For instance, if an outbound rule permits traffic over port 443 to any address, there's no need to create an inbound rule for the return traffic. Similarly, an outbound rule isn't required for responses if inbound traffic is allowed.

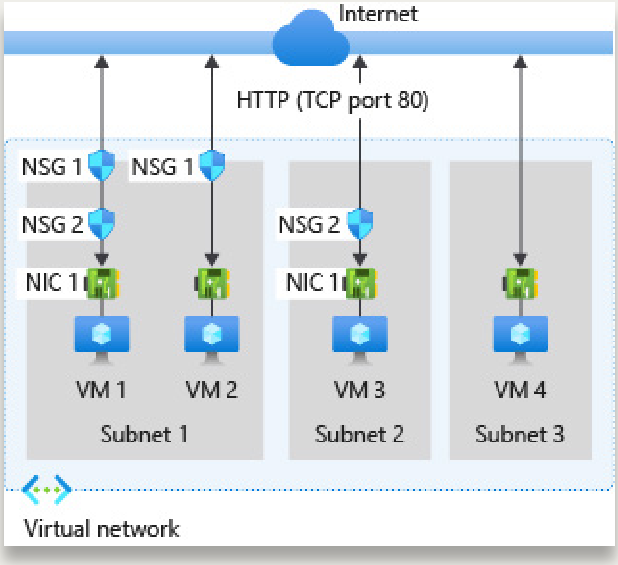


Figure 6 – NSG Rule Associations

Figure 6 – NSG Rule Associations shows how rules can be applied at either the subnet level within a VNet or the virtual NIC level. Subnet-based NSGs are evaluated when traffic enters or exits the VNet, while NIC-based NSGs are evaluated as packets arrive at or leave the VM NIC. The evaluation order depends on the traffic's origin. For example, traffic from the internet to a VM is first evaluated at the subnet level as it enters the VNet before being checked against the NIC-level NSG. However, traffic between two VMs on the same subnet is only evaluated at the NIC level since it doesn't cross a subnet boundary.

Linux OS Firewall

Securing the internal firewall on Linux VMs in Azure involves configuring the operating system's firewall to enforce strict inbound and outbound traffic rules, allowing only necessary ports and services while blocking all other traffic by default. Layering this protection with Azure's network security features, such as Network Security Groups (NSGs), provides a defense-in-depth approach.

Identity

A common challenge for Platform engineers is managing the secrets, credentials, certificates, and keys used to secure communication between services. Managed Identities eliminate the need to manage these credentials.

While Platform engineers can securely store the secrets in Azure Key Vault, services need a way to access them. Managed identities provide an automatic identity in Microsoft Entra ID for Linux VMs to use when connecting to resources that support Microsoft Entra authentication. Linux VMs can use managed identities to obtain Microsoft Entra tokens without having to manage any credentials.

Thus, each Linux VM deployed can be configured to have a unique Managed Identity, which can be assigned RBAC rights to these credentials. The Entra ID and Key Vault integration enhances security by managing identities and encrypting keys and secrets. Aligning with regulatory standards, Azure's strategic investments in infrastructure and partnerships showcase its commitment to optimizing and securing Linux solutions on its cloud platform.

SSH Authentication with Microsoft Entra ID: The Secure Shell (SSH) protocol encrypts networking services on an unsecured network. SSH replaces the Telnet protocol, which doesn't provide encryption in an unsecured network.

Microsoft Entra ID provides a VM extension for Linux-based systems that run on Azure and a client extension that integrates with the Azure CLI and the OpenSSH client.

You can use SSH authentication with Entra ID when:

- Working with Linux-based VMs that require remote command-line sign-in.
- Running remote commands in Linux-based systems.
- Securely transferring files in an unsecured network.

Using SSH with Entra ID allows for multi-factor authentication and the application of conditional access policies. This removes the need to use passwords when connecting to Linux VMs in Azure and enforces the best practice of having centrally stored credentials. Review this article to learn more about using Entra ID for SSH.

Using Entra ID with PostgreSQL Authentication: Integrating Entra ID with PostgreSQL offers a highly secure and manageable authentication mechanism. This approach removes the need to manage individual PostgreSQL user credentials by allowing users to authenticate with their Entra ID credentials. This integration provides several key benefits:

- **Centralized Identity Management:** Entra ID provides a centralized platform for managing users, roles, and access permissions across your organization. When used with PostgreSQL, database access is governed through the same directory service used for other applications, ensuring consistent security policies.
- **Enhanced Security:** Entra ID authentication supports advanced features such as Multi-Factor Authentication (MFA), Conditional Access policies, and identity protection. These features help mitigate risks like password breaches by ensuring that only authorized users can access the database through secure, multi-layered protection mechanisms.
- Simplified User Management: Entra ID enables Role-Based Access Control (RBAC) to PostgreSQL, allowing administrators to manage permissions at scale. User roles and access can be assigned based on their organizational group or job function, reducing the overhead of managing individual database accounts.
- Eliminating Password Management: Entra ID removes the need for database-specific passwords, which can be challenging to manage and prone to security risks. Entra ID authentication ensures access is controlled and monitored by your directory service, enforcing password complexity, expiration, and other security policies.

Organizations can streamline their identity management practices, enforce robust security protocols, and reduce the risks associated with traditional database authentication methods by adopting Entra ID for PostgreSQL authentication.

Security Operations Management support for Linux on Azure

Once Platform engineers have configured and deployed Linux VMs into a VNet, they must operate and maintain a secure and compliant environment. Azure Monitor Agent, VM Insights, Update Management, Azure Policy, and Log Management are advanced tools that facilitate efficient operations and ensure systems remain secure and compliant.

Azure Monitor Agent

Azure Monitor Agent (AMA) collects monitoring data from the guest operating system of Azure and hybrid virtual machines and delivers it to Azure Monitor for use by features, insights, and other services, such as Microsoft Sentinel and Microsoft Defender for Cloud. The monitor agent is supported on Linux VMs and appliances that run Linux, such as routers and third-party firewalls.

Running as an Azure VM extension on Linux, the agent is simple to install and configure.

VM Insights

VM Insights provides a quick and easy method to monitor workloads on Linux VMs. It displays an inventory of your existing VMs and provides a guided experience to enable base monitoring for them. It also monitors VMs' performance by collecting data on their running processes and dependencies on other resources.

Update Management

Azure Update Manager is a unified service that helps manage and govern updates for all VMs. From a single dashboard, Linux update compliance across deployments in Azure, on-premises, and other cloud platforms can be managed. Update Manager can be used to make real-time updates or schedule them within a defined maintenance window.

With Azure Update Manager Platform engineers can perform the following actions on Linux VMs in Azure:

- Oversee update compliance for your entire fleet of machines in Azure, on-premises, and in other cloud environments.
- Instantly deploy critical updates to help secure your machines.
- Use flexible patching options such as automatic virtual machine (VM) guest patching in Azure, and customer-defined maintenance schedules.

Azure Policy

Azure Policy helps enforce organizational standards and assess compliance at scale. Through its compliance dashboard, it provides an aggregated view to evaluate the overall state of the environment, with the ability to drill down to the per-resource, per-policy granularity. It also helps bring resources to compliance through bulk remediation for existing resources and automatic remediation for new resources.

Azure Policy is essential for enforcing organizational standards and assessing compliance at scale, particularly when managing Linux virtual machines (VMs) in Azure. By leveraging Azure Policy, administrators can define and apply policies to ensure that Linux VMs adhere to best practices and security guidelines. These policies can include rules for resource configuration, security settings, and operational practices, such as ensuring that all VMs have up-to-date antivirus protection or are encrypted.

Azure Policy provides built-in policies for common scenarios, and custom policies can be created to meet specific organizational needs. The policy compliance dashboard in Azure allows administrators to monitor the compliance status of their Linux VMs in real time, providing insights and remediation steps for non-compliant resources. This proactive approach helps maintain a secure and well-governed cloud environment, reducing the risk of misconfigurations and ensuring that all Linux VMs consistently meet defined standards.

Azure Policy guest configuration extension

The Azure Policy guest configuration extension audits the configuration settings in a virtual machine. The guest configuration supports Azure VMs natively and non-Azure physical and virtual servers through Azure Arc-enabled servers.

Compliance frameworks and benchmarks

Azure Policy can be effectively utilized to enforce Federal Information Processing Standards (FIPS) and Center for Internet Security (CIS) benchmarks on Linux virtual machines (VMs) in Azure, ensuring high security and compliance levels.

FIPS provides a set of standards for cryptographic modules, while CIS benchmarks offer comprehensive guidelines for securing IT systems. By implementing Azure Policy, administrators can apply these standards and benchmarks to Linux VMs to ensure they meet stringent security requirements.

Azure Policy’s built-in definitions include policies for both FIPS and CIS benchmarks, enabling automated compliance checks and enforcement. These policies can audit settings like encryption protocols, secure configuration parameters, and system integrity. The compliance state of Linux VMs can be monitored through Azure Policy’s compliance dashboard, which provides detailed reports and remediation steps for non-compliant resources. This automation and continuous monitoring facilitate maintaining a secure environment, reducing the risk of vulnerabilities, and ensuring that Linux VMs comply with industry-standard security practices.

Log Management

Log management for Linux virtual machines (VMs) in Azure is critical to maintaining security, performance, and compliance. Azure provides various tools and services to manage and analyze logs from Linux VMs efficiently. The primary service for this purpose is Azure Monitor, which integrates seamlessly with Linux systems to collect, aggregate, and analyze log data. Azure supports shipping syslogs from Linux VMs to Log Analytics, enabling centralized analysis and correlation of system events. Through Azure Log Analytics, administrators can create custom queries, set up alerts, and visualize log data for better insights into system performance and security events. Microsoft Sentinel also offers advanced threat detection and recommendations by analyzing real-time log data.

Implementing robust log management practices ensures that all activities within the Linux VMs are monitored. This aids in quickly identifying and resolving issues, thus enhancing the cloud environment’s overall security posture and operational efficiency.

Customer Scenario – Contoso Mortgage Application

This section explores a real-world application of running Linux on Azure through the lens of a customer scenario. Contoso Mortgage, a large lending institution in the United States, recently undertook a modernization project for its Mortgage application. The project involved migrating from an on-premises three-tier architecture to a cloud-based Microsoft Azure solution.

On-premises Deployment

Figure 7 – On-premises Mortgage architecture documents the application's legacy setup in a data center. Running as a mix of hardware devices and VMs following a traditional three-tier architecture with file storage on a Network-Attached Storage (NAS) device.

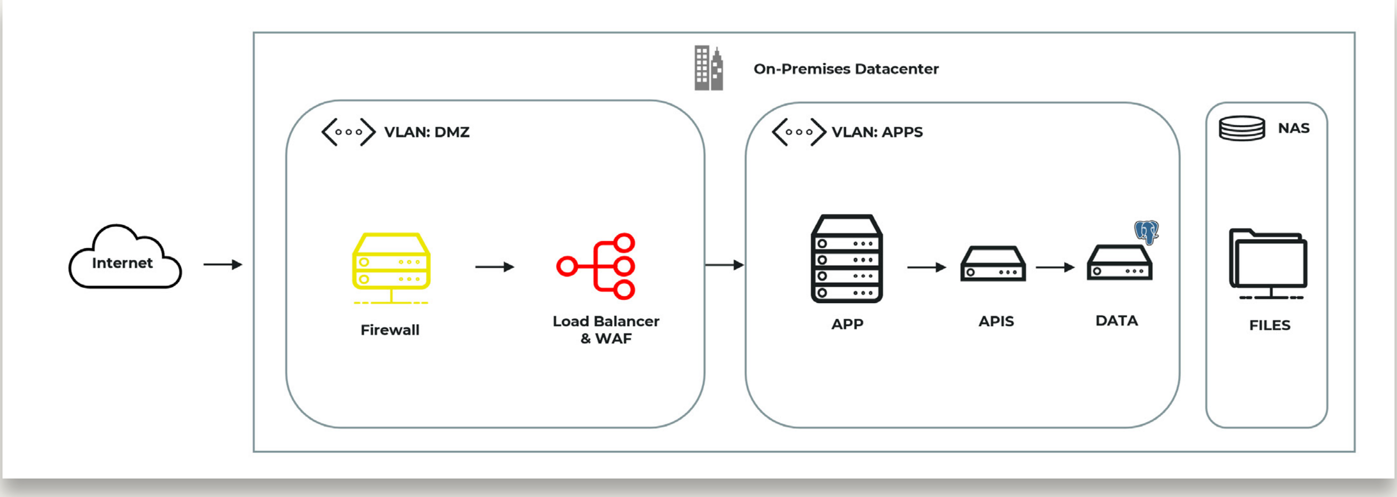


Figure 7 – On-premises Mortgage architecture

External traffic from the internet first passes through a hardware-based next-generation firewall (NGFW) located in a VLAN dedicated to the DMZ, followed by a hardware load balancer. Once the traffic is filtered, it reaches the application layer hosted within a separate VLAN. With all VMs running Linux, the application tier interacts with backend APIs, which connect to a data tier hosting a PostgreSQL database. Additionally, the application has access to a network-attached storage (NAS) system for file storage using Network File System (NFS) 3.0.

Deployment challenges

The on-premises deployment of the application faced numerous challenges that impacted both security and scalability, ultimately leading to performance inefficiencies and operational risks. Table 7 – Deployment Challenges highlights these limitations:

Area		Description
Compute	Lack of confidential computing	VMs without confidential computing are vulnerable because data processed in memory remains unencrypted, leaving it exposed to potential attacks from malicious insiders, compromised hypervisors, or other unauthorized access during execution.
Compute	Linux VM images are not secured by default	Linux VMs were deployed without hardened security configurations, leaving them exposed to vulnerabilities and threats.
Compute	Single API VM	Relying on a single VM to host the API made the system highly vulnerable to failures, with no redundancy for continuous operation.
Compute	Single database VM	The database was hosted on a single VM, posing availability risks and limiting scalability to meet demand.
Compute	No scalability	The infrastructure did not provide mechanisms for scaling application workloads, making it difficult to handle increased traffic or demands.
Compute	No endpoint security	The Linux VMs don't have endpoint security configured leaving the system vulnerable to malware, unauthorized access, and exploitation.
Identity	Connection Strings on local VMs	Connection strings are used on the local VMs to connect to the API tier and the database tier of the application. These are insecure and have passwords in clear text.
Identity	Local accounts with elevated privileges on Linux	Local accounts with elevated privileges were used on Linux, increasing the risk of privilege escalation.
Identity	Local accounts on PostgreSQL database	Local accounts with elevated privileges were used on PostgreSQL DBMS, increasing the risk of privilege escalation.
Identity	Row-level security not implemented on PostgreSQL	The PostgreSQL database lacked row-level security, leaving sensitive data vulnerable to unauthorized access.
Identity	Certificates are imported into local VMs	Certificates were manually imported into VMs, increasing the risk of misconfiguration or outdated certificates.
Networking	No DDoS protection	The infrastructure lacked Distributed Denial of Service (DDoS) protection, making it vulnerable to traffic overloads or attacks.
Networking	Firewall and load balancer management issues	The firewall and load balancer could not be managed with the same tools as the rest of the infrastructure, complicating operations.
Networking	All VMs are on the same VLAN without traffic management	All traffic flowed unfiltered between VMs, increasing the risk of internal threats and making it harder to isolate services for security.
Networking	No web acceleration or SSL offload	The system lacked web acceleration techniques like SSL offloading, reducing performance optimization.
Networking	Lack of SSL/TLS between API & PostgreSQL	SSL/TLS was not configured between the API tier VMs and the PostgreSQL database VM. This allows sensitive information such as login credentials, to be transmitted in plaintext, making it vulnerable to interception and unauthorized access by attackers during transit.
Storage	Files on the NAS are not encrypted	Files stored on the NAS were left unencrypted, exposing potentially sensitive data to unauthorized access.
Storage	Lack of encrypted drives on VMs	Sensitive data on virtual machines was stored without encryption, increasing the risk of data exposure in the event of unauthorized access.

Table 7 – Deployment Challenges

Azure Deployment

Contoso Mortgage has implemented a new cloud-based architecture by migrating the on-premises application to Azure, leveraging cloud-native technologies for scalability, security, and high availability.

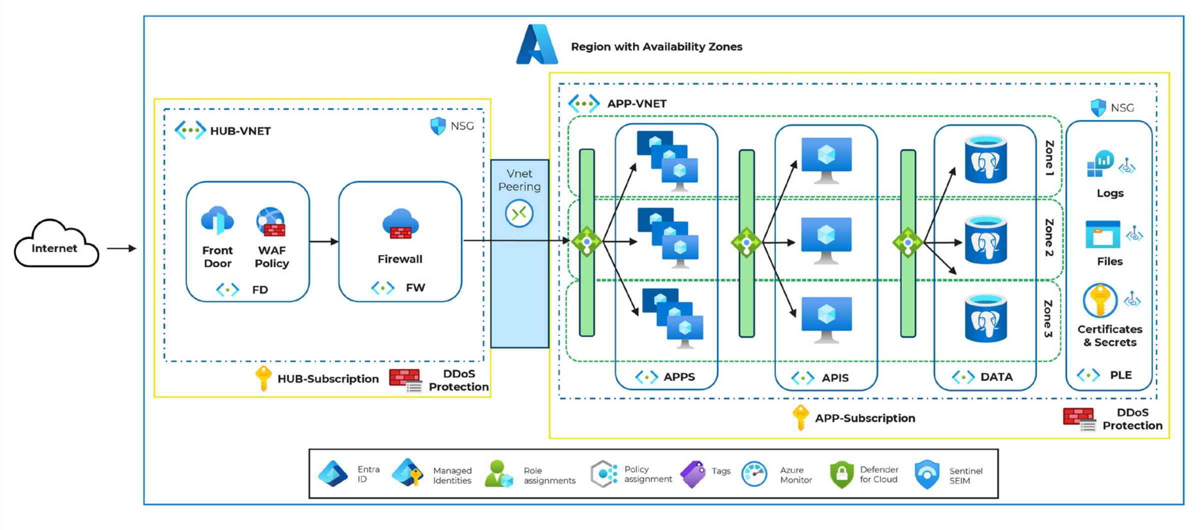


Figure 8 – Azure Linux architecture

Figure 8 – Azure Linux architecture, shows the newly deployed Contoso Mortgage application. The implementation leverages all Azure services and features for running a secured Linux deployments on Azure.

This Azure design introduces significant improvements in scalability and management, with components like PostgreSQL databases spread across zones for better performance and availability. The architecture fully uses Azure's platform-level services, such as private link endpoints (PLE), for secure connectivity and enhanced security. The move to this cloud-based model allows for more flexible scaling and streamlined security and management through centralized policies and monitoring tools.

Azure Monitor provides comprehensive visibility and monitoring of the infrastructure, ensuring performance and security metrics are tracked in real time. Logs from all tiers are centralized in Azure Log Analytics, providing detailed insights into system activity and enabling advanced threat detection and troubleshooting. Microsoft Defender for Cloud is implemented to provide unified security management and advanced threat protection for workloads, continuously assessing security posture.

Additionally, Microsoft Sentinel offers intelligent security analytics and threat intelligence across the environment, enabling rapid detection and response to threats. Microsoft Defender for Endpoint Security adds another layer of defense, offering advanced threat protection across all virtual machines. Furthermore, Azure Update Management automates patching and updates, ensuring that all systems remain up-to-date and secure.

In addition to the security architecture outlined, Contoso Mortgage utilized Bicep to define and deploy the entire infrastructure, including virtual networks, subnets, and virtual machines (VMs), ensuring consistent and secure configuration of all resources. To further automate the configuration of the VMs, Contoso Mortgage employed GitHub Actions in conjunction with cloud-init, which handled tasks such as installing required packages, applying security patches, and setting up monitoring agents directly upon VM boot. This combination of tools enabled rapid, repeatable deployments while minimizing manual errors. By leveraging Bicep for infrastructure as code, GitHub Actions for automation, and cloud-init for VM initialization, Contoso Mortgage ensured its infrastructure remained scalable, secure, and aligned with the project's operational requirements.

The following subsections will detail the critical components of this architecture, covering Compute, Storage, Networking, and Identity considerations focused on improving the security of the application platform.

Compute

A multi-tier architecture was adopted to deploy Contoso Mortgage's Azure-based solution, leveraging advanced security features to safeguard data across the application, API, and database tiers. The application and API tiers are powered by Virtual Machine Scale Sets (VMSS) and dedicated Virtual Machines (VMs), respectively, utilizing AMD EPYC™ processors with Azure Confidential Computing capabilities and hardened Linux images. These pre-configured images are optimized for security, ensuring that the VMs start with enhanced protection against vulnerabilities. The VMs are Generation 2 and use vTPM with Secure boot, leveraging all the security features available for IaaS workloads in Azure.

The database tier is secured with Azure Database for PostgreSQL – Flexible Server, offering robust encryption, firewall protection, and automated backup features. This architecture enhances scalability and performance while embedding security at every infrastructure level.

Web Tier: Virtual Machine Scale Sets (VMSS) with AMD Processors

Previously managed by four on-premises VMs, the web tier was transitioned to a VMSS in Azure. This change allowed for better scalability, with the ability to adjust the number of VMs based on demand dynamically.

Virtual Machine Scale Sets (VMSS) are utilized to ensure scalability, resilience, and security. The VMs in the scale set are powered by AMD EPYC™ processors with Azure Confidential Computing capabilities, ensuring the application data is encrypted at rest, in transit, and in use. Confidential VMs provide an additional layer of data protection by encrypting memory, helping to prevent unauthorized access from privileged system users and processes. The VMs are further secured with Azure's network security groups (NSGs) to restrict traffic, and Azure Disk Encryption is used to protect data at rest. Updated images will be used as new nodes are provisioned using the VMSS's automatic OS image update capability.

Logic Tier: Virtual Machines with AMD Processors

The API tier runs on dedicated virtual machines powered by AMD EPYC™ processors with Confidential Computing technology. This ensures that the API VMs provide high performance and enhanced security for sensitive backend services. Confidential VMs encrypt the data in use, adding additional protection against unauthorized access, even from Azure administrators. Network Security Groups (NSGs) are implemented to manage and control inbound and outbound traffic. Regular patches and updates are automated using Azure patch management, ensuring the VMs remain secure. Additionally, TLS encryption is employed for all communication between the API and database tiers to secure data in transit.

Database Tier: Azure Database for PostgreSQL – Flexible Server with VNet integration

The database tier is powered by Azure Database for PostgreSQL – Flexible Server, which offers advanced configuration options for high availability and security. Database for PostgreSQL – Flexible Server is protected by built-in firewall rules restricting access to specific trusted IP addresses and Azure services. All data is encrypted at rest using Azure Storage Service Encryption, and Transparent Data Encryption (TDE) is applied to protect sensitive information. Database for PostgreSQL – Flexible Server also supports role-based access control (RBAC) and managed identities to secure database access, ensuring that only authorized services and users can access the database. Automated backups and point-in-time recovery are configured to ensure data integrity and protection from accidental data loss. Row-level security was also implemented to ensure data accessed is only shown if the user has the proper authority.

Storage

Security is critical in the Contoso Mortgage architecture deployed on Azure, particularly in data storage and management. The architecture leverages Azure's built-in security features to protect both file storage and virtual machine disks, safeguarding sensitive data against unauthorized access, data loss, and other vulnerabilities.

Azure Files with NFS 4.1

Contoso Mortgage needed fast, secure file storage for its mortgage application. To modernize its file infrastructure, Contoso replaced the legacy on-premises NAS system with Azure Files using NFS 4.1, which provided the flexibility and performance needed to handle its growing data demands while ensuring a high level of security.

Contoso Mortgage migrated its entire file storage environment to an Azure Files storage account configured with NFS 4.1. This shift allowed them to leverage encryption at rest using Azure Storage Service Encryption (SSE), with the option to manage their encryption keys through Azure Key Vault with HSM. By using customer-managed keys (CMKs), the company ensured complete control over encryption, key rotation, and compliance with strict security requirements.

To further protect their data, Contoso Mortgage implemented TLS encryption for all data in transit, safeguarding it against potential interception or tampering as it moves between users, services, or applications. This was especially important for handling sensitive financial information.

Performance was a critical factor for Contoso Mortgage. NFS 4.1 was delivered with support for session trunking and parallel I/O, significantly improving the company's high-throughput, large-scale data processing performance. These performance enhancements were combined with availability zone redundancy to ensure the file system remained accessible and resilient, even during hardware or zone failures.

Security was further enhanced by integrating Azure Private Link, which allowed Contoso Mortgage to ensure that all file access stayed within their virtual networks. This eliminated exposure to the public internet, reducing the attack surface and ensuring that only authorized users and applications within the VNet had access to the files.

Additionally, Network Security Groups (NSGs) were configured to control file share access tightly. NSGs enabled the company to define rules restricting which applications or services could interact with the file shares, using IP addresses, subnets, and other network conditions to guard against unauthorized access or malicious traffic. The primary access NSG allowed was the API subnet, which manages the application's file access requirements.

By adopting Azure Files with NFS 4.1, Contoso Mortgage achieved a modern, cloud-based storage solution that was secure, scalable, and capable of handling its demanding performance requirements. The company now benefits from enhanced security, simplified management, and a storage platform that supports current and future business needs.

Azure Disk Storage

Contoso Mortgage implemented Azure Disk Storage throughout its architecture to store data for the virtual machines (VMs) in the Application and API tiers. These managed disks offer advanced security features and provide secure and reliable storage for the company's VMs.

Contoso Mortgage uses Azure Disk Encryption to ensure data protection. This service leverages dm-crypt for Linux VMs to encrypt data at the operating system level, safeguarding data from unauthorized access. The encryption keys are managed via Azure Key Vault, giving the company complete control over key management and lifecycle, ensuring that encryption is handled securely.

Contoso Mortgage uses customer-managed keys (CMKs) stored in Azure Key Vault to encrypt managed disks for additional security. This approach allows the company to retain complete control over key rotation, revocation, and audibility, meeting strict security and compliance requirements.

Role-Based Access Control (RBAC) is also used to manage and modify Azure Disk Storage. Only authorized users or services can create, attach, or delete disks, minimizing the risk of unauthorized access and reducing the likelihood of data breaches or misconfigurations.

To ensure data recoverability, Contoso Mortgage uses incremental snapshots and encrypted backups. These features provide quick restoration of VMs in case of failure while ensuring that backup data remains protected from unauthorized access.

Contoso Mortgage uses Zone-Redundant Managed Disks for its mission-critical workload, replicating data across availability zones. This replication ensures that if a disk failure occurs in one zone, the data remains available in other zones, adding a critical layer of security against data loss and ensuring business continuity.

By leveraging Azure Disk Storage, Contoso Mortgage guarantees that all VM data is securely stored and protected from unauthorized access or malicious threats. This comprehensive approach ensures sensitive information is encrypted, controlled, and monitored, fully utilizing Azure's integrated security capabilities to meet the company's operational and security requirements.

Networking

In Figure 8 – Azure Linux architecture, the newly deployed Contoso Mortgage application shows internet traffic first entering through the Azure Front Door, which handles global load balancing and integrates with a Web Application Firewall (WAF) policy for enhanced security using OWASP rules. AFD also simplifies SSL certificate management and custom domain integration, ensuring streamlined configuration and maintenance. In this architecture, traffic is secured with end-to-end TLS, meaning it is re-encrypted before reaching the web servers, ensuring data confidentiality throughout the traffic flow.

After passing through AFD, traffic routes through a firewall in the HUB-VNET, which provides centralized security controls across all connected environments. The HUB-VNET also includes DDoS protection to mitigate distributed denial-of-service attacks. The application workloads are hosted in the APP-VNET, peered with the HUB-VNET, allowing secure communication between the two virtual networks. The application tier is deployed across availability zones to ensure redundancy and fault tolerance.

This setup ensures that the apps, APIs, and data tiers are distributed across multiple zones, enhancing the overall resilience of the architecture. Each tier is protected by network security groups (NSGs) to regulate traffic flow, and Azure services such as logs, files, and certificates & secrets are integrated for monitoring, storage, and security management using secure private link endpoints. Additionally, DDoS protection is extended to this application subscription, further strengthening its defenses.

Supporting services leverage private links within the virtual network to ensure all traffic remains secure and confined to the VNet, eliminating exposure to the public internet. This configuration enhances data privacy and security while maintaining efficient, low-latency communication between services.

Networking was a critical component of Contoso Mortgage's cloud architecture, ensuring that the various application tiers could communicate securely and efficiently.

Identity

Identity management played a critical role in Contoso Mortgage's migration to Azure. The company focused on securing access to the application, infrastructure, and data and adopted a series of Azure-native identity solutions to strengthen security across the entire architecture.

Managed Identities were extensively used to handle access to resources like Azure Storage, Key Vault, and the VMs. This approach eliminated the need for hardcoded credentials, allowing the VMs to authenticate to Azure resources using system-assigned Managed Identities securely. The VMs retrieved certificates and connection strings securely from Azure Key Vault, ensuring these sensitive items were managed and accessed without exposing secrets in the application code.

In a critical security enhancement, local identities on the VMs were removed to enforce centralized identity management through Entra ID. Using SSH authentication with Entra ID, Contoso Mortgage secured remote access to its VMs, reducing the risks associated with local user accounts and passwords. This approach allowed centralized management of VM access through Entra ID, ensuring tighter control and auditing of user actions.

The PostgreSQL database was also a focus of identity-based security. Contoso Mortgage used Managed Identity for its VMs to connect securely to Azure Key Vaults to retrieve connection strings for the PostgreSQL database without exposing credentials. Additionally, the use of Row-Level Security (RLS) in conjunction with Entra ID Role-Based Access Control (RBAC) allowed the company to enforce granular access controls within the database itself. This setup ensured that only authorized users or services could view or modify specific rows of data, securing sensitive customer information based on predefined roles.

The integration of Entra ID also extended to the entire application, with RBAC used to manage access to both application-level resources and infrastructure components. This ensured that users and services had only the permissions necessary to perform their jobs, significantly reducing the risk of privilege escalation.

Key Vault played a central role in managing secrets and certificates, with Private Link ensuring that these sensitive items could only be accessed from within the virtual network. This private network integration further protected the certificates and connection strings accessed by Managed Identities, adding another layer of security to the architecture.

Through these identity management practices, Contoso Mortgage ensured that all aspects of access control—across VMs, data, and resources—were centralized, secure, and compliant with stringent security standards. The comprehensive use of Managed Identities, Entra ID, and advanced access control measures, such as RBAC and Row-Level Security, ensured that the company's infrastructure was well-protected from unauthorized access and data breaches.

Governance, Operations, and Security

Governance, operations, and security are essential to Contoso Mortgage's Azure architecture, ensuring compliance, efficient management, and strong defense against threats. This combination of governance, monitoring, and security practices supports Contoso Mortgage's Azure-based architecture's integrity, compliance, and reliability.

Governance

The organization uses Azure Policy to enforce compliance with organizational standards, ensuring resource configurations align with best practices, such as encryption requirements or limiting public-facing endpoints. Tags are used extensively to classify and manage resources, providing better visibility into usage and facilitating cost management. These governance measures maintain an organized, efficient, and compliant Azure environment.

Operations

Contoso Mortgage uses Azure Monitor to track its infrastructure's health, performance, and usage. Logs from all application tiers are centralized in Azure Log Analytics, allowing for custom queries, visualizations, and proactive alerts to detect and resolve issues quickly. Automated tools like Azure Update Management ensure systems are consistently patched and updated, reducing vulnerabilities and streamlining maintenance.

Security

Contoso Mortgage leverages Microsoft Defender for Cloud for unified security management and threat protection. The service continuously assesses workloads and provides actionable recommendations to address vulnerabilities. Microsoft Sentinel enhances security with advanced threat detection, hunting, and incident response capabilities. Sensitive services like Azure Key Vault and Log Analytics use private links to ensure all traffic remains within the virtual network, protecting data from exposure.

Summary

In conclusion, deploying Linux on Azure, particularly with AMD processors, offers a robust and secure environment for modern workloads. Azure's comprehensive suite of security features, including confidential computing, ensures that data remains protected throughout its lifecycle, from processing to storage and transit. The collaboration between Microsoft and AMD exemplifies a commitment to providing high-performance, cost-efficient, and secure solutions for diverse workloads. By leveraging Azure's advanced security measures, extensive support for various Linux distributions, and seamless integration with management tools, organizations can confidently deploy and manage their Linux-based applications in the cloud, ensuring compliance with stringent security standards and optimizing operational efficiency.