**Secure Networking Hackathon**

**Overview**

**This 3-day Hackathon enables participants to** plan for and build networking and security configurations. This will be done using recommended Azure Networking and Azure Networking Security products and tools. You will be focusing on best practices while working through challenges inspired by real-world scenarios.

During the hack attendees will focus on designing and implementing Azure networking solutions. These solutions will address the demanding needs of today’s global enterprises. Your team will analyze the customers’ requirements and design a secure network infrastructure. Hackers will propose multiple design solutions and evaluate which solution is best in their scenario.

**By the end of the Hackathon**, participants will have knowledge on how to design and implement cloud networking and security solutions. Hackers will have identified solutions to improve workload performance, scalability, and security in Azure.

**Value Proposition**

* Networking is a critical component for any cloud or hybrid solution to ensure performance, resiliency, and security. Azure includes a robust networking infrastructure to support your application and service connectivity requirements.
* Azure networking and security solutions provide options for customers to connect to Microsoft in a secure and reliable manner. This establishes a foundational structure for building their hybrid cloud strategy.
* Azure networking built-in experiences across platforms provide for a friction-free experience. Enabling everyone to connect and work securely from anywhere, on any platform.
* Leverage Microsoft’s comprehensive suite of leading solutions unified across people, devices, apps, and data.

**Technical Scenarios**

* Achieving a global hybrid network that is secure, scalable, and resilient to failures
* Identify Azure Networking solutions that improve application delivery, security, and availability
* Managing and operationalizing a global hybrid network

**Audience**

* Target Audience:
  + Network Engineers, Solution Architects, Security architects, Application developers, DevOps engineers, Systems administrators, Systems integrators
* Target verticals:
  + Networking, Security, Infra, Apps, Data Architects, cross workload
  + Cross-industry, cross-solution
  + All

**Key Technologies**

Azure Virtual Network, Azure Virtual WAN, Azure ExpressRoute, Azure VPN Gateway, Azure Virtual Network NAT Gateway, Azure DNS, Azure Peering service, Azure Private Link, Azure Traffic Manager, Azure Front Door, Azure Application Gateway, Azure Load balancer, Azure Network Security Groups, Azure Web Application Firewall, Azure Virtual Network Endpoints, Azure Network Watcher

**Agenda**

**Note: Hackathons will run for three days (Tues – Thurs). Please plan to block your calendar as this course will require your full participation each day.**

**Agenda – Athens time zone**

|  |  |  |  |
| --- | --- | --- | --- |
| Timeslot /Day | Tuesday, 28 Nov | Wednesday, 29 Nov | Thursday, 30 Nov |
| 9:30 AM – 10:00 AM | Opening + Welcome | Team Hacking | Team Hacking |
| 10:00 AM - 1:00 PM | Team Hacking |
| 1:00 PM - 2:00 PM | Break | | |
| 2:00 PM – 5:00 PM | Team Hacking | Team Hacking | Team Hacking |
| 4:30 PM - 5:00 PM | Closing Remarks |

**Prerequisites**

**Knowledge Prerequisites**

To be successful and get the most out of this Hackathon, it is highly recommended that participants have previous experience with:

* Required knowledge of [Azure network administration](https://docs.microsoft.com/learn/paths/az-104-manage-virtual-networks/)
* Required knowledge of [Azure Fundamentals](https://docs.microsoft.com/learn/paths/az-900-describe-cloud-concepts/)
* Understanding of network configurations, including TCP/IP, Domain Name System (DNS), virtual private networks (VPNs), firewalls, and encryption technologies.
* Understanding of software defined networking.
* Understanding hybrid network connectivity methods, such as VPN
* Understanding resilience and disaster recovery, including high availability, and restore operations regarding networking.

Be prepared to roll up your sleeves, learn, and participate in an interactive team environment.

**Tooling Prerequisites**

To be successful and get the most out of this Hackathon and to avoid any delays with downloading or installing tooling, you are encouraged to have the following ready to go ahead of the Hackathon:

* A modern laptop running Windows 10 (1703 or higher), Mac OS X (10.13 or higher), or one of these [Ubuntu versions](https://github.com/Azure/azure-functions-core-tools#linux)
* Download and install the latest version of [PowerShell 7.x](https://docs.microsoft.com/en-gb/powershell/scripting/install/installing-powershell?view=powershell-7.1)
* Download and install the latest version of [Azure CLI](https://docs.microsoft.com/en-us/cli/azure/install-azure-cli?view=azure-cli-latest) and the [Azure PowerShell Module](https://docs.microsoft.com/en-us/powershell/azure/install-az-ps)
* Install your choice of Integrated Development Environment (IDE) software, such as [Visual Studio](https://visualstudio.microsoft.com/vs/community/) or [Visual Studio Code](https://code.visualstudio.com/download)

**Development Environment Configuration**

* The hack environment requires an Azure subscription with the setup deploy.ps1 script deployed
* PowerShell
* CLI
* ARM template

**Links & Resources**

* [AZ-700 Designing and Implementing Microsoft Azure Networking Solutions - Learn | Microsoft Docs](https://docs.microsoft.com/en-us/learn/paths/design-implement-microsoft-azure-networking-solutions-az-700/)
* [Azure Fundamentals part 4: Describe general security and network security features (AZ-900) - Learn | Microsoft Docs](https://docs.microsoft.com/en-us/learn/paths/az-900-describe-general-security-network-security-features/)
* [Configure and manage virtual networks for Azure administrators - Learn | Microsoft Docs](https://docs.microsoft.com/en-us/learn/paths/azure-administrator-manage-virtual-networks/)
* [Explore Azure networking services - Learn | Microsoft Docs](https://docs.microsoft.com/en-us/learn/modules/azure-networking-fundamentals/)
* [Networking architecture design - Azure Architecture Center | Microsoft Docs](https://docs.microsoft.com/en-us/azure/architecture/guide/networking/networking-start-here)

**Post Learning Recommendations**

* [AZ-700 Designing and Implementing Microsoft Azure Networking Solutions - Learn | Microsoft Docs](https://docs.microsoft.com/en-us/learn/paths/design-implement-microsoft-azure-networking-solutions-az-700/)
* [Networking architecture design - Azure Architecture Center | Microsoft Docs](https://docs.microsoft.com/en-us/azure/architecture/guide/networking/networking-start-here)
* [Hub-spoke network topology with Azure Virtual WAN - Azure Architecture Center | Microsoft Docs](https://docs.microsoft.com/en-us/azure/architecture/networking/hub-spoke-vwan-architecture)

**Challenges**

**Overview**

Contoso Mortgage Company (CMC) is in the process of expanding their cloud footprint and needs a secure global cloud network. They have tasked you and your team with designing and deploying their Azure network environment and gradually scaling up to meet the demands of their enterprise level security and network requirements. CMC is currently focused on leveraging a combination of PaaS and IaaS resources in Azure. It is up to you to present the best design based on their requirements.

**Challenge 1:** **Build the foundation**

Contoso Mortgage requires a strong foundation that they can leverage for development and future production workloads. They want to leverage a shared services model that is designed to scale to multiple regions in the future. In this challenge, your team is tasked with designing and deploying CMCs Azure network foundation.

Learning objectives:

* Design and implement Azure Virtual Networks
* Design and implement hybrid connectivity
* Validate hybrid connection
* Understand BGP configurations in Azure

**Challenge 2: Deploy the first application**

The application team has asked for their OHND App to be the first project deployed on Azure. Your task is to deploy the web and application tier reliably in Azure. This will be the first of many applications deployed. Be sure to plan your network design accordingly.

Learning objectives:

* Deploy and load balance a web application
* Ensure network design is scalable for future workloads
* Validate application is highly available and traffic is redirected in the case of an outage
* Enable secure access to manage VMs

**Challenge 3: Design and implement network security**

In this challenge, you will address the network security requirements presented by CMC. The Network Security team requires central control over the security aspects, such as Firewall, and requires granular management capabilities for each workload.

Learning objectives:

* Design and deploy subnet level network security
* Design and deploy a solution to inspect and filter inbound and outbound traffic from the Azure network
* Design and deploy a solution that provides a central security policy and route management
* Utilize cloud native network monitoring tools

**Challenge 4: Design and implement web application security**

CMC requires web application security that leverages layer 7 load balancing. In this challenge, you will design a solution that meets their requirements and integrates with your existing network design.

Learning objectives:

* Design and document the options considered and present the best solution
* Implement secure delivery of web applications
* Ensure all web applications are secure by default

**Challenge 5: CMC goes global**

CMC is ready to go global. In this challenge, you will expand the network architecture to multiple Azure regions and establish global connectivity between VNets in the Azure regions. Your network design must continue to evolve to meet the growing needs as the company expands.

Learning objectives:

* Design and deploy a muti region cloud network
* Design and implement global load balancing
* Design to optimize the application user experience including the case of a regional outage

**Challenge 6: Secure access to Azure PaaS services**

In this challenge, you will design a solution that provides private access to the PaaS database as well as a solution that ensures Azure services are automatically integrated with DNS.

Learning objectives:

* Design and implement a solution to keep database access on the internal network and not over public endpoints
* Understand the DNS solutions available in Azure
* Design and implement a DNS solution in Azure

**Challenge 7: Integrating name resolution between Azure and on prem**

In this challenge, you will learn advanced DNS techniques to manage and integrate your private DNS on-prem and in Azure.

Learning objectives:

* Resolving prem names in Azure
* Resolving azure names from on prem
* Enabling access to private endpoints from on-prem

**Challenge 8: Centrally manage Azure Virtual Networks at scale**

In this challenge, you will operationalize your network design by leveraging cloud native scaling and management tools.

Learning objectives:

* Vnet peering network management at scale
* Network security management at scale
* Hierarchal network security

**Challenge 9: Retrospective – Looking back**

Now that you have solved all of CMC’s challenges, as team take the time to reflect and answer the last set of questions. The objective of this challenge is to reflect on design decisions and analyze the pros and cons of your solutions.

Learning objectives:

* Communicate design decisions and tradeoffs
* Understand design limitations
* Reflect on a global scale

**Registration questions**

|  |  |
| --- | --- |
| Topic specific question | Response Options |
| What is your level of understanding using Azure today? | None Some understanding I have some pilot work on Azure I rely on Azure today for cloud |
| How much time have you spent using Azure Networking services | < 3 months  3-6 months  6 months - 1 year  > 1 year |
| How much time have you spent using enterprise networking services? | < 3 months  3-6 months  6 months - 1 year  > 1 year |
| What is your level of understanding of network security? | None Some understanding I implement network security solutions I design network security solutions |

**FAQ**

Q: Is there a suggested flow of Hackathons which participant should attend first, before going to yours?

A: No, but it is good to know general concepts around networking like hybrid connectivity and security.

Q: I already use Azure Virtual Networks, should I attend this Hackathon

A: Yes, even if you currently use Azure virtual networks or other Azure networking services there is an opportunity to learn more in a challenge-based learning environment.

Q: What tools will I need?

A: You will need a modern laptop running Windows 10 (1703 or higher), Mac OS X (10.13 or higher), or one of these Ubuntu versions, the latest version of PowerShell 7.x , the latest version of Azure CLI and the Azure PowerShell Module and your choice of Integrated Development Environment (IDE) software, such as Visual Studio or Visual Studio Code