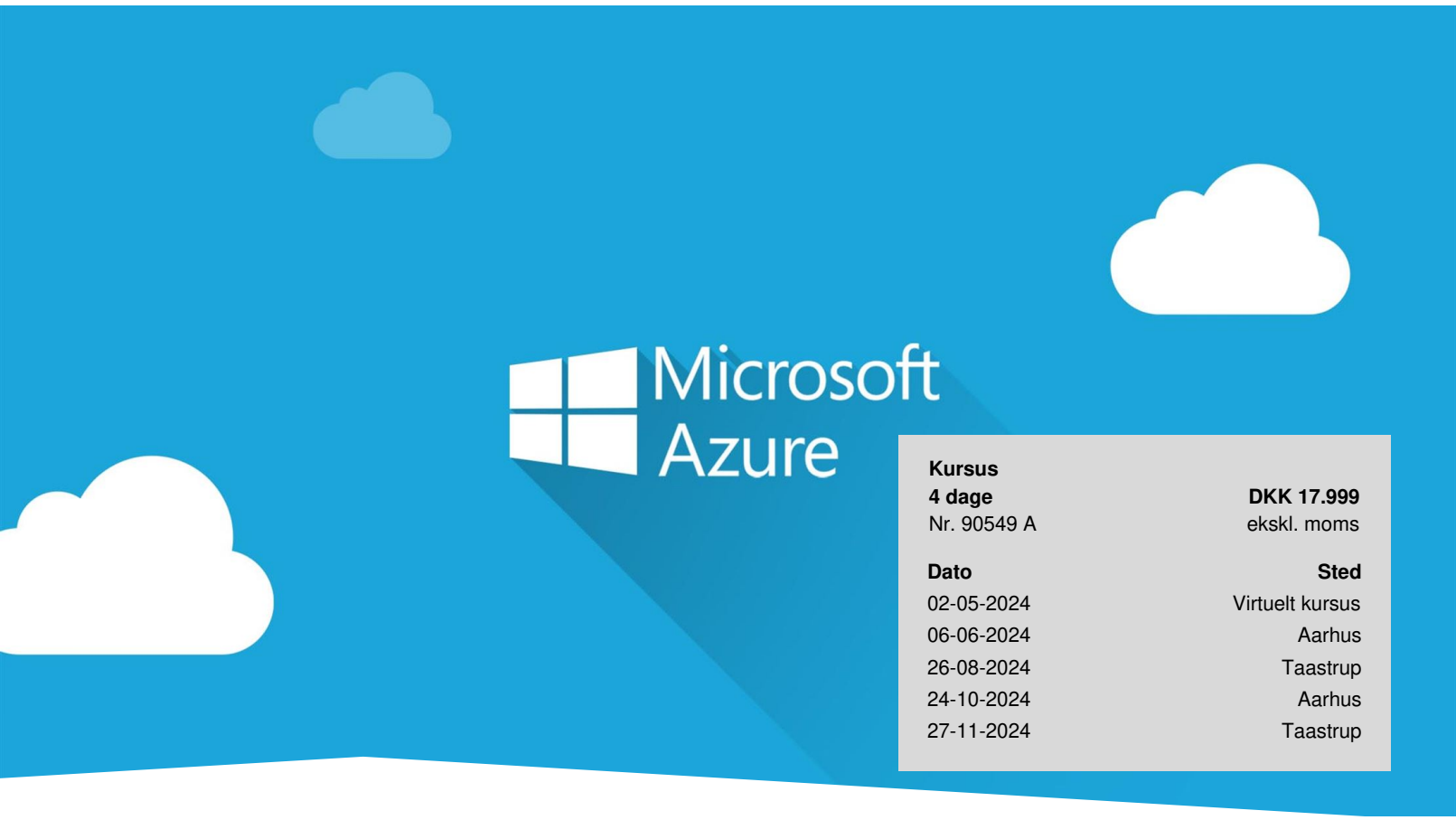

Kursus
4 dage **DKK 17.999**
Nr. 90549 A ekskl. moms

Dato	Sted
02-05-2024	Virtuelt kursus
06-06-2024	Aarhus
26-08-2024	Taastrup
24-10-2024	Aarhus
27-11-2024	Taastrup

Microsoft Azure Security Technologies [AZ-500T00]

Lær om sikkerhed i Microsoft Azure. På kurset får du den nødvendige viden og færdigheder til at implementere sikkerhedskontroller, vedligeholde sikkerhedsindstillingerne samt identificere og afhjælpe sårbarheder ved hjælp af en række sikkerhedsværktøjer i Azure.

Vi har samlet alt til din læringsrejse

For at du får størst muligt udbytte af dit kursus, får du adgang til en læringsportal, der samler alt omkring dit kursus. Læs mere under Form.

Deltagerprofil

Kurset er for dig, som skal implementere og vedligeholde sikkerhedskontroller i Azure.

Forudsætninger

Vi anbefaler, at du har deltaget på Azure Administrator AZ-104T00 eller har tilsvarende viden. Du forventes at have praktisk erfaring med sikkerhed af Azure workloads og sikkerhedskontroller i Azure.

Udbytte

- Lær at beskrive specialiserede dataklassifikationer i Azure
- Få metoder til at identicifere Azure databeskyttelse
- Lær at implementere datakryptering i Azure
- Lær at sikre internet protokoller og forstå, hvordan du implementerer dem på Azure
- Lær at beskrive Azure sikkerhedstjenester og funktioner

Det får du på arrangementet

- Øvelser og inddragelse
- Kursusbevis
- Erfaren underviser
- Fuld forplejning
- Gratis parkering
- Materiale på engelsk
- Undervisning på dansk
- Certificeret underviser

Indhold

Module 1: Manage Identity and Access

- This module equips you with the ability to secure users, groups, and external identities in Microsoft Entra ID while implementing advanced identity protection measures.
  - Secure Azure solutions with Microsoft Entra ID
  - Implement Hybrid identity
  - Deploy Microsoft Entra ID Protection
  - Configure Microsoft Entra Privileged Identity Management
  - Design an enterprise governance strategy

Module 2: Implement Platform Protection

- Learn how to plan and implement robust security measures for virtual networks, private access, and public-facing resources, ensuring the utmost protection for your network infrastructure.
  - Implement perimeter Security
  - Configure Network Security
  - Configure and manage Host Security
  - Enable Containers Security

Module 3: Secure your data and Application Security

- In this module you will learn how to protect your keys, certificates, and secrets in Azure Key Vault, and configure key vault for the most secure deployment. You will also learn how to register your company applications then use Azure security features to configure and monitor secure access to the application, and ensure your data is stored, transferred, and accessed in a secure way using Azure storage and file security features. Finally, you will learn how to configure and lock down your SQL database on Azure to protect your corporate data while it is stored.
  - Deploy and secure Azure Key Vault
  - Configure application security features
  - Implement Storage Security
  - Configure and manage SQL database security

Module 4: Manage security operations

- In this module you will learn how to use Azure Monitor, Log Analytics, and other Azure tools to monitor the secure operation of your Azure solutions. You will also learn how to use Azure Security Center, Azure Defender, and Secure Score to track and improve your security posture in Azure. Finally, you will learn how to use Azure Sentinel to discover, track, and respond to security breaches within your Azure environment.
  - Configure and manage Azure Monitor
  - Enable and manage Microsoft Defender for Cloud

- Configure and monitor Microsoft Sentinel

Form

For at du får størst muligt udbytte af dit kursus, får du adgang til en læringsportal, der samler alt omkring dit kursus. Her får du et godt overblik over emnerne på kursusdagene, direkte adgang til kursusmaterialet opdelt efter emner, og koder til online labs, så du kan løse opgaver undervejs. Du får desuden adgang til udvalgt ekstra materiale. Du kan bruge platformen fra en browser, lige når det passer dig, og du har adgang i 180 dage efter dit kursus.

Certificering

Kurset er rettet mod eksamen AZ-500 Microsoft Azure Security Technologies og ved bestået opnår du certificeringen **Microsoft Certified: Azure Security Engineer Associate**. Du skal bestille og betale din eksamen særskilt.

Microsoft skriver følgende om denne eksamen:

- This exam measures your ability to accomplish the following technical tasks: manage identity and access; implement platform protection; manage security operations; and secure data and applications.
- Candidates for this exam are Microsoft Azure security engineers who implement security controls, maintain the security posture, manages identity and access, and protects data, applications, and networks.
- Candidates identify and remediate vulnerabilities by using a variety of security tools, implements threat protection, and responds to security incident escalations. As a Microsoft Azure security engineer, candidates often serve as part of a larger team dedicated to cloud-based management and security and may also secure hybrid environments as part of an end-to-end infrastructure.
- Candidates for this exam should have strong skills in scripting and automation, a deep understanding of networking, virtualization, and cloud N-tier architecture, and a strong familiarity with cloud capabilities, Microsoft Azure products and services, and other Microsoft products and services.

Læs mere om IT-certificering.

UNDERVISER

Nis Gabriel

Nis har mere end 20 års erfaring med undervisning inden for Microsoft Servere, klienter og cloud-services. Nis er Microsoft Certified Trainer (MCT) og har en lang række certificeringer (MCSA, MCSE etc.) inden for Windows Server (fra Windows NT til Server 2016) og Windows Client (Windows NT til Windows 10) samt Microsoft Azure og Microsoft 365. I sin undervisning fokuserer han på, at IT-drift skal være effektiv, fleksibel, sikker og ikke mindst veldokumenteret.

Har du faglige spørgsmål så kontakt

Charlotte Heimann
+45 72203147
chhn@teknologisk.dk