**1. Intro to AWS Security Architecture**

**Topics**

* Overview of AWS architecture principles with a focus on security (Security by Design, Shared Responsibility Model)
* Key AWS security services: IAM, KMS, CloudTrail, GuardDuty, AWS Config, Security Hub

**Required Infrastructure & Components**

* AWS account with administrative access
* IAM setup (users, roles, policies)
* AWS Console and CLI access
* Multi-region setup for geographic redundancy

**To-Dos & Steps**

1. Prepare AWS account (enable MFA, secure root user)
2. Create IAM roles for admins and auditors
3. Introduce identity-based and resource-based policies
4. Enable security services: CloudTrail, GuardDuty, AWS Config
5. Demo: S3 bucket with fine-grained IAM policy access control

**Webinars**:

* AWS Security Fundamentals (Webinar Series) - <https://www.aws.training/Details/Video?id=15853>
* [AWS – Shared Responsibility Model Explained](https://www.youtube.com/watch?v=iODPCcQEPto)

**YouTube**:

* [AWS Security Services Overview](https://www.youtube.com/watch?v=fkHHONc8v6g)
* [AWS Identity and Access Management (IAM) Basics](https://www.youtube.com/watch?v=Dt_7qGDxVgE)

**Reading Material**:

* AWS Security Best Practices Whitepaper - [AWS Security Best Practices - AWS Whitepaper](https://docs.aws.amazon.com/pdfs/whitepapers/latest/aws-security-best-practices/aws-security-best-practices.pdf)
* [AWS Well-Architected Framework: Security Pillar](https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/welcome.html)
* [AWS Shared Responsibility Model](https://aws.amazon.com/compliance/shared-responsibility-model/)

**2. VPC Basics**

**Topics**

* Virtual Private Cloud (VPC) design
* CIDR planning, IP ranges, and subnetting
* Default vs. custom VPCs

**Required Infrastructure & Components**

* A custom VPC including:
  + At least two subnets (public and private)
  + Internet Gateway (IGW)
  + NAT Gateway (for outbound access from private subnets)
  + Route tables for traffic control

**To-Dos & Steps**

1. Create a custom VPC (e.g., 10.0.0.0/16)
2. Set up two subnets:
   * Public (e.g., 10.0.1.0/24)
   * Private (e.g., 10.0.2.0/24)
3. Attach an Internet Gateway to the VPC
4. Deploy a NAT Gateway in the public subnet
5. Configure route tables for each subnet
6. Example setup: Web server in the public subnet, database in the private subnet

**Webinars**:

* AWS Networking Fundamentals Webinar - [PowerPoint Presentation](https://d1.awsstatic.com/events/Summits/AMER2020/Sept29/NET201_AWS_networking_fundamentals.pdf)

**YouTube**:

* [AWS VPC Basics](https://www.youtube.com/watch?v=7_NNlnH7sAg)
* [AWS VPC Cloud Tutorial](https://www.youtube.com/watch?v=g2JOHLHh4rI)

**Reading Material**:

* [VPC Documentation](https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html)
* VPC Best Practices Whitepaper - [Design and Configuration Guide: Best Practices for Virtual Port Channels (vPC) on Cisco Nexus Series Switches](https://www.cisco.com/c/dam/en/us/td/docs/switches/datacenter/sw/design/vpc_design/vpc_best_practices_design_guide.pdf)

**3. Subnet Types**

**Topics**

* **Public Subnet**: Internet accessible via IGW
* **Private Subnet**: Internal use only, uses NAT for outbound traffic
* **Isolated Subnet**: No internet access (ideal for sensitive workloads)

**Required Infrastructure & Components**

* At least one of each subnet type
* Security Groups and Network ACLs for traffic control
* VPC Flow Logs for monitoring traffic

**To-Dos & Steps**

1. Set up one public, one private, and one isolated subnet
2. Launch EC2 instances in each to demonstrate behavior
3. Configure Security Groups:
   * Allow HTTP/HTTPS on public instance
   * Restrict database access to private subnet
4. Add Network ACLs for extra control
5. Enable VPC Flow Logs to CloudWatch for visibility

**Webinars**:

* AWS Advanced VPC Design Webinar - [(216) AWS re:Invent 2023 - Advanced VPC designs and new capabilities (NET306) - YouTube](https://www.youtube.com/watch?v=cRdDCkbE4es)

**YouTube**:

* [AWS VPC & Subnet Basics](https://www.youtube.com/watch?v=TUTqYEZZUdc)
* [Public vs Private VPC Subnets in AWS](https://www.youtube.com/watch?v=ApGz8tpNLgo)

**Reading Material**:

* [Subnet Basics in VPC](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Subnets.html)
* [Security Best Practices for Subnets](https://www.hyperglance.com/blog/aws-vpc-security-best-practices/)

**4. Route Tables**

**Topics**

* Directing network traffic between subnets
* Dependency on subnet type and associated gateways

**Required Infrastructure & Components**

* At least two route tables:
  + One with default route to IGW (for public)
  + One with default route to NAT Gateway (for private)
* Optional blackhole route for troubleshooting

**To-Dos & Steps**

1. Configure route table for public subnet: 0.0.0.0/0 → IGW
2. Configure route table for private subnet: 0.0.0.0/0 → NAT Gateway
3. Ensure internal routing between subnets
4. Test with traceroute from private instance to the internet

**Webinars**:

* AWS Networking Core Concepts Webinar - <https://aws.amazon.com/de/awstv/watch/c37546e1558/>

**YouTube**:

* [AWS Route Tables Simplified](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Route_Tables.html)

**Reading Material**:

* [VPC Route Tables](https://www.geeksforgeeks.org/aws-vpc-route-table/)
* [Routing Best Practices in AWS](https://medium.com/@nagarjun_nagesh/aws-route-53-routing-strategies-and-best-practices-abc23c226af1)

**Compliance Landscape Overview**

**5. GDPR vs. SOC 2 vs. ISO 27001 – Key Differences**

**Topics**

* **GDPR**: EU data protection law – personal data rights, accountability, erasure
* **SOC 2**: US-based framework focused on Trust Principles (security, availability, confidentiality, etc.)
* **ISO 27001**: Global standard for Information Security Management Systems (ISMS)

**Required Infrastructure & Components**

* AWS Config with compliance rules
* AWS Artifact for audit reports
* AWS Security Hub for compliance posture

**To-Dos & Steps**

1. Perform compliance mapping using AWS Well-Architected Tool
2. Review control mappings between AWS services and GDPR/SOC2/ISO 27001
3. Use AWS Artifact to access reports and certifications
4. Show practical GDPR-related features:
   * Data encryption (KMS)
   * Audit logging (CloudTrail)
   * Access control (IAM)
5. Use ISO 27001 Annex A controls for a risk management example

**Webinars**:

* AWS Compliance and Security Webinar - <https://www.youtube.com/watch?v=OnQ4bV7aQG0>

**YouTube**:

* [AWS Compliance Programs Overview](https://www.youtube.com/watch?v=ymijS4GWxsI)
* [GDPR Compliance on AWS](https://www.youtube.com/watch?v=Ts3xvgSrEaM)

**Reading Material**:

* [AWS Compliance Center](https://aws.amazon.com/financial-services/security-compliance/compliance-center/)
* [Mapping of GDPR to AWS Services](https://aws.amazon.com/compliance/gdpr-center/)
* [ISO 27001 on AWS](https://aws.amazon.com/compliance/iso-27001-faqs/)

**Understanding the AWS Security Ecosystem & High-Level Compliance Goals**

**6. AWS Security Ecosystem**

**Topics**

* Key security services overview:
  + IAM, KMS, CloudTrail, Config, Security Hub, GuardDuty
* Security best practices:
  + Principle of Least Privilege
  + Defense in Depth
  + Encryption Everywhere
  + Zero Trust Networking

**Required Infrastructure & Components**

* Security service configurations in a demo environment
* Trusted Advisor for security best practices
* AWS Security Hub for central findings aggregation

**To-Dos & Steps**

1. Deep dive into IAM roles and policies
2. Create and apply KMS keys for data encryption (e.g., S3)
3. Enable CloudTrail in all regions
4. Set up AWS Config rules for compliance enforcement
5. Enable GuardDuty and review findings
6. Use Security Hub to view combined security posture

**Webinars**:

* AWS Security Services Deep Dive Webinar - <https://www.youtube.com/watch?v=78qFK-r7WBI>
* [AWS re:Inforce – Security Foundations](https://docs.aws.amazon.com/prescriptive-guidance/latest/security-reference-architecture/foundations.html)

**YouTube**:

* [Top AWS Security Services Explained](https://www.youtube.com/watch?v=swfT1ZY8E9A)
* [AWS GuardDuty Tutorial](https://www.youtube.com/watch?v=WXl4gW0znVc)

**Reading Material**:

* [AWS Security Hub User Guide](https://docs.aws.amazon.com/securityhub/latest/userguide/what-is-securityhub.html)
* [IAM Best Practices](https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html)
* [AWS CloudTrail User Guide](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html)

**🎯 End-of-Day Goal**

Participants should be able to:

* Understand and configure basic AWS networking and security principles
* Differentiate between major compliance frameworks
* Recognize how AWS services support high-level compliance and security goals
* Build a secure, functional network architecture using best practices