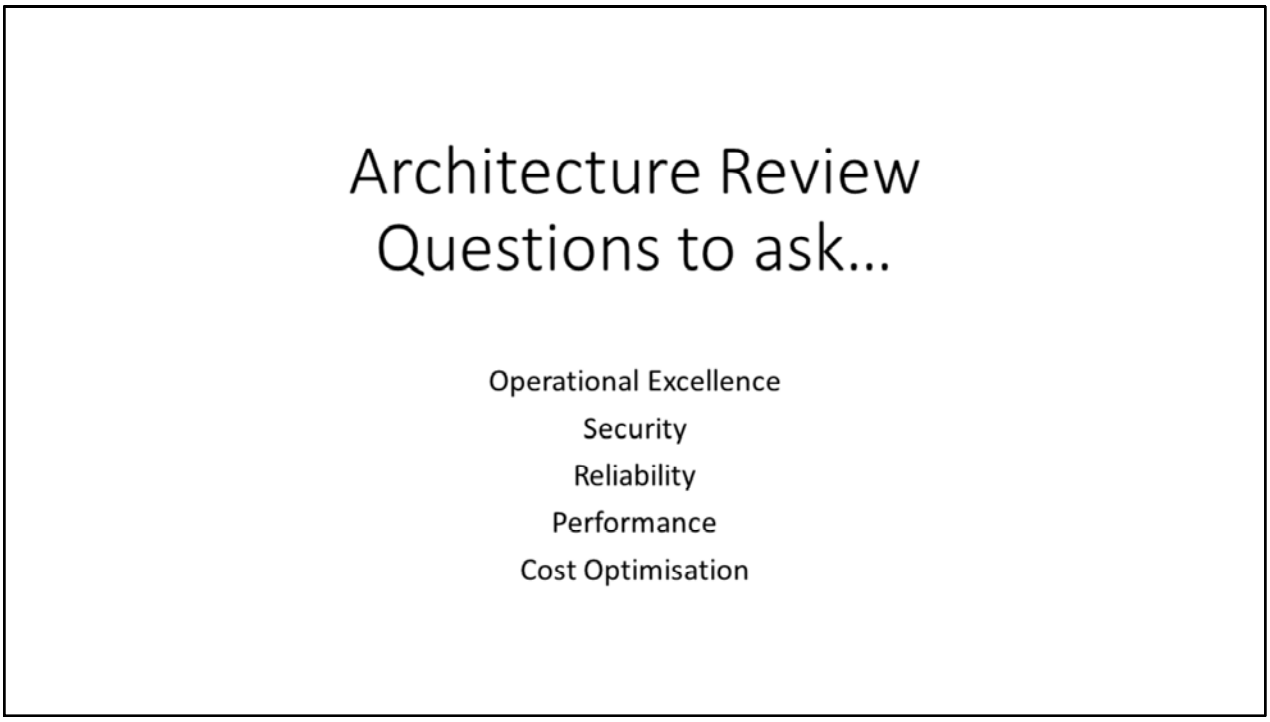
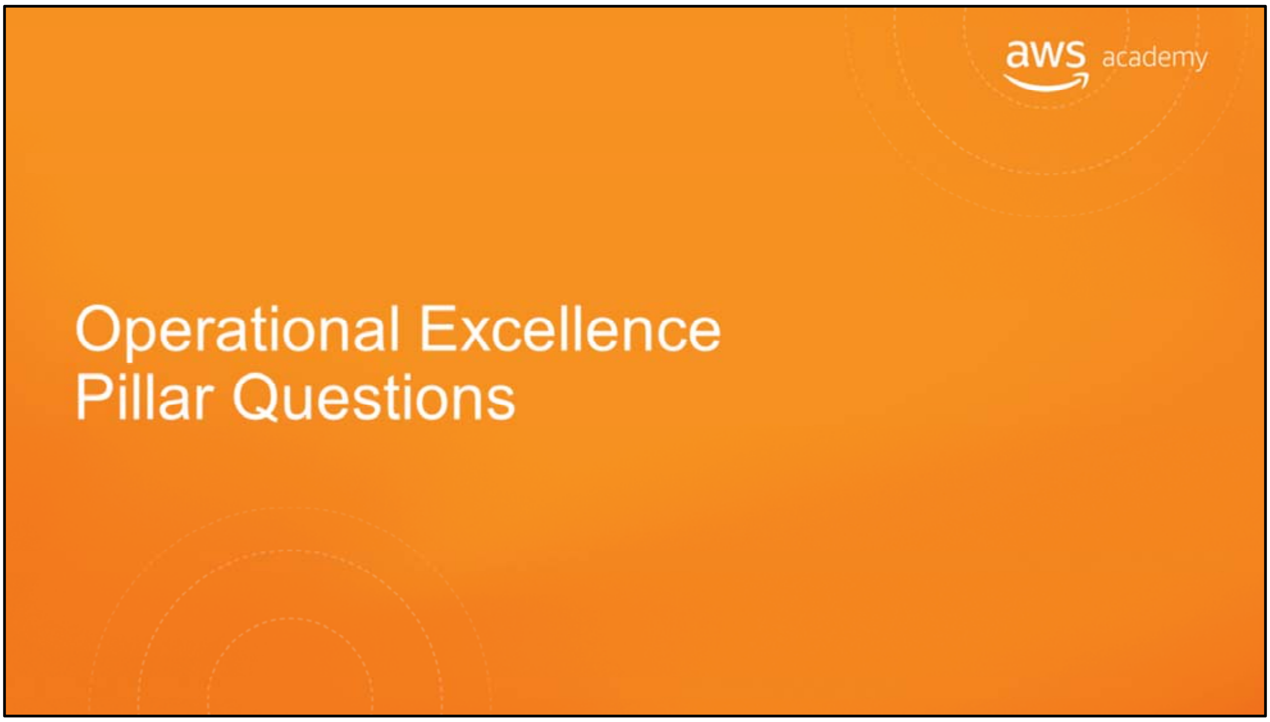


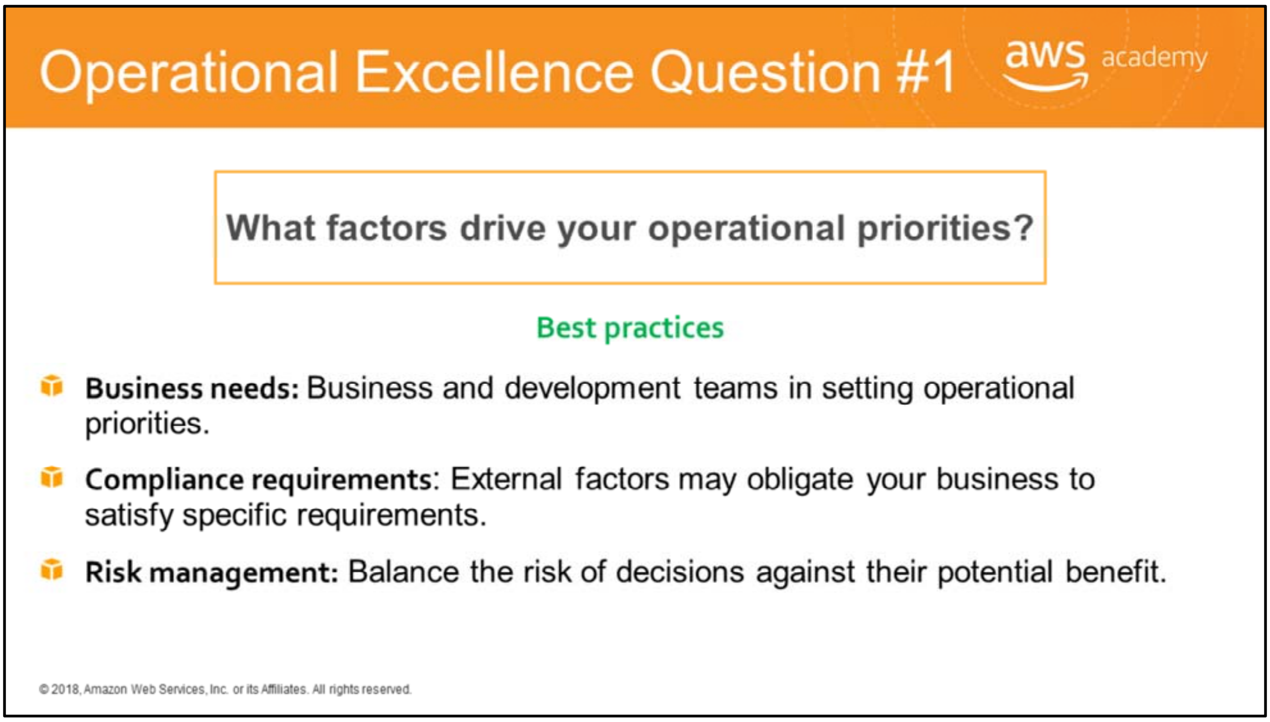
Architecture Review
Questions to ask…

Operational Excellence
Security
Reliability
Performance
Cost Optimisation



Operational Excellence Pillar Questions

In this final section, we'll ask a question that relates to operational excellence, and then reveal some best practices.



Operational Excellence Question #1

aws academy

What factors drive your operational priorities?

Best practices

- **Business needs:** Business and development teams in setting operational priorities.
- **Compliance requirements**: External factors may obligate your business to satisfy specific requirements.
- **Risk management:** Balance the risk of decisions against their potential benefit.

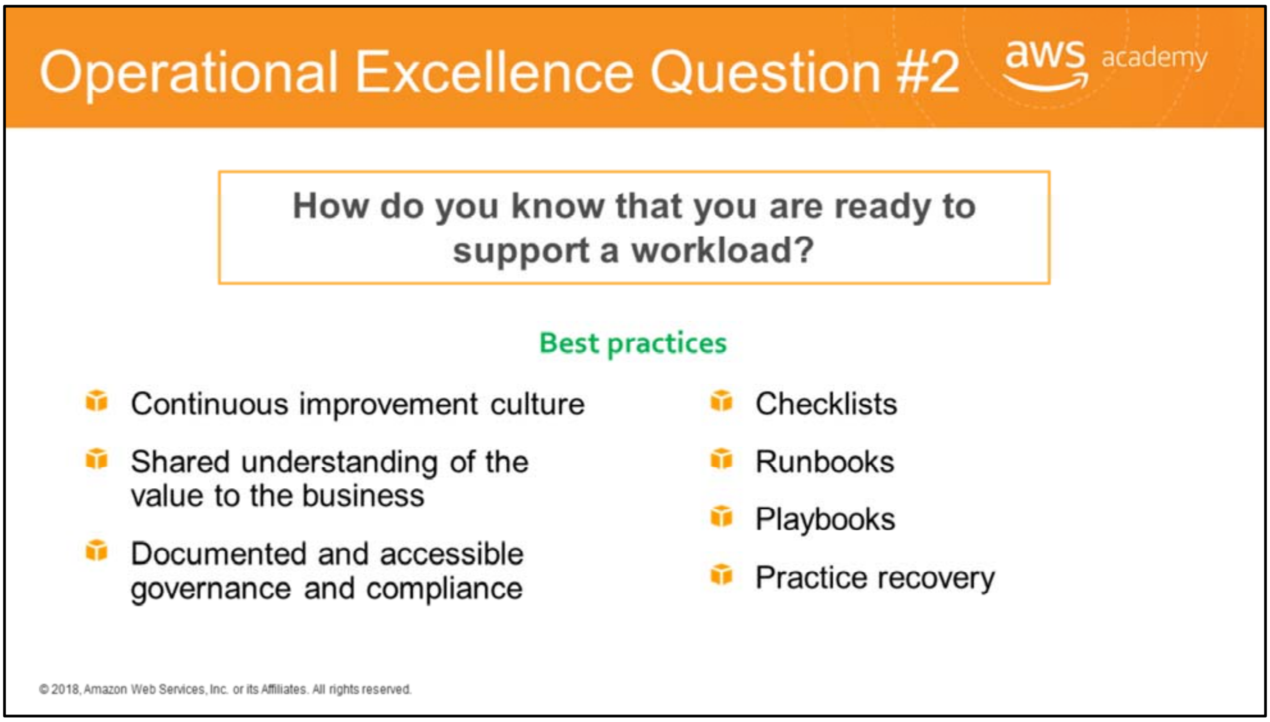
What factors drive your operational priorities?

Best practices for understanding these factors include:

- Involving the business and development teams when you set operational priorities.

- Following compliance requirements. External factors—such as regulatory standards or industry standards—might obligate your business to satisfy specific requirements. An example of a requirement is considering Sarbanes-Oxley—or SOX—regulatory compliance requirements versus payment card industry —or PCI—best practices.

- Engaging in risk management to balance the risk of decisions against their potential benefit.



Operational Excellence Question #2

How do you know that you are ready to support a workload?

Best practices

- Continuous improvement culture
- Shared understanding of the value to the business
- Documented and accessible governance and compliance
- Checklists
- Runbooks
- Playbooks
- Practice recovery

How do you know that you are ready to support a workload?

Best practices for determining whether you are ready to support a workload include:

- Continuously improving your culture. This best practice governs the way you operate. You must recognize that change is constant, and that you need to continue to experiment and evolve by acting on opportunities to improve.

- Having a shared understanding of the value to the business. Make sure that you have cross-team consensus on the value of the workload to the business, and that you have procedures that you can use to engage additional teams for support.

- Ensuring that you have enough personnel so that you can have an appropriate number of trained personnel to support the needs of your workload. Perform regular reviews of workload demands, and train existing personnel or adjust personnel capacity as needed.

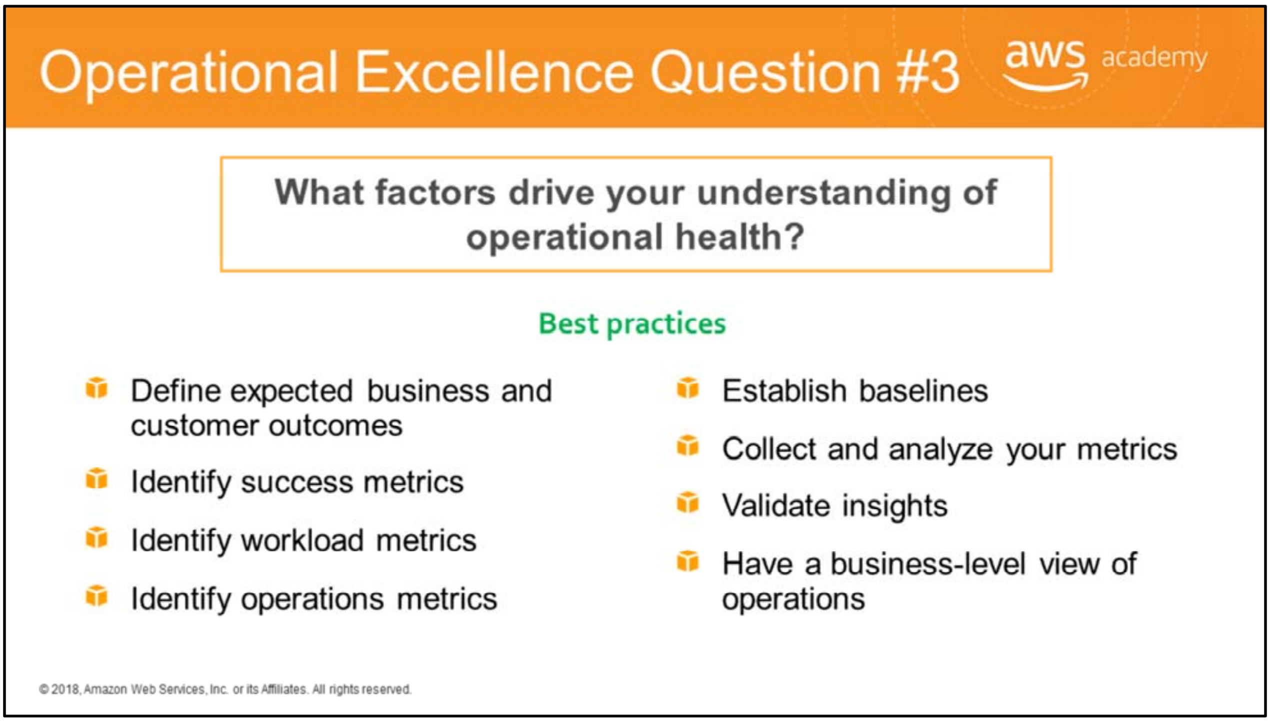
- Making sure that governance and guidance are documented and accessible.: Ensure that standards are accessible, readily understood, and measurable for compliance. Make sure that you have a way to propose changes to standards, and request exceptions.

- Using checklists to evaluate whether you are ready to operate workloads. These checklists include operational readiness checklists and security checklists.

- Having runbooks for events and procedures that you understand well.

- Having a playbook for failure scenarios.

- Practicing recovery so that you can identify potential failure scenarios and test your responses—for example, game days, and failure injection.



Operational Excellence Question #3

What factors drive your understanding of operational health?

Best practices

- Define expected business and customer outcomes
- Identify success metrics
- Identify workload metrics
- Identify operations metrics
- Establish baselines
- Collect and analyze your metrics
- Validate insights
- Have a business-level view of operations

What factors drive your understanding of operational health?

Best practices for understanding operational health include:

- Defining expected business and customer outcomes. Make sure that you have a documented definition of what success looks like for the workload, from business and customer perspectives.

- Identifying success metrics. Define metrics that can be used to measure the behavior of the workload against the expectations of the business and of customers.

- Identifying workload metrics. Define metrics that can be used to measure the status—and the success—of the workload and its components.

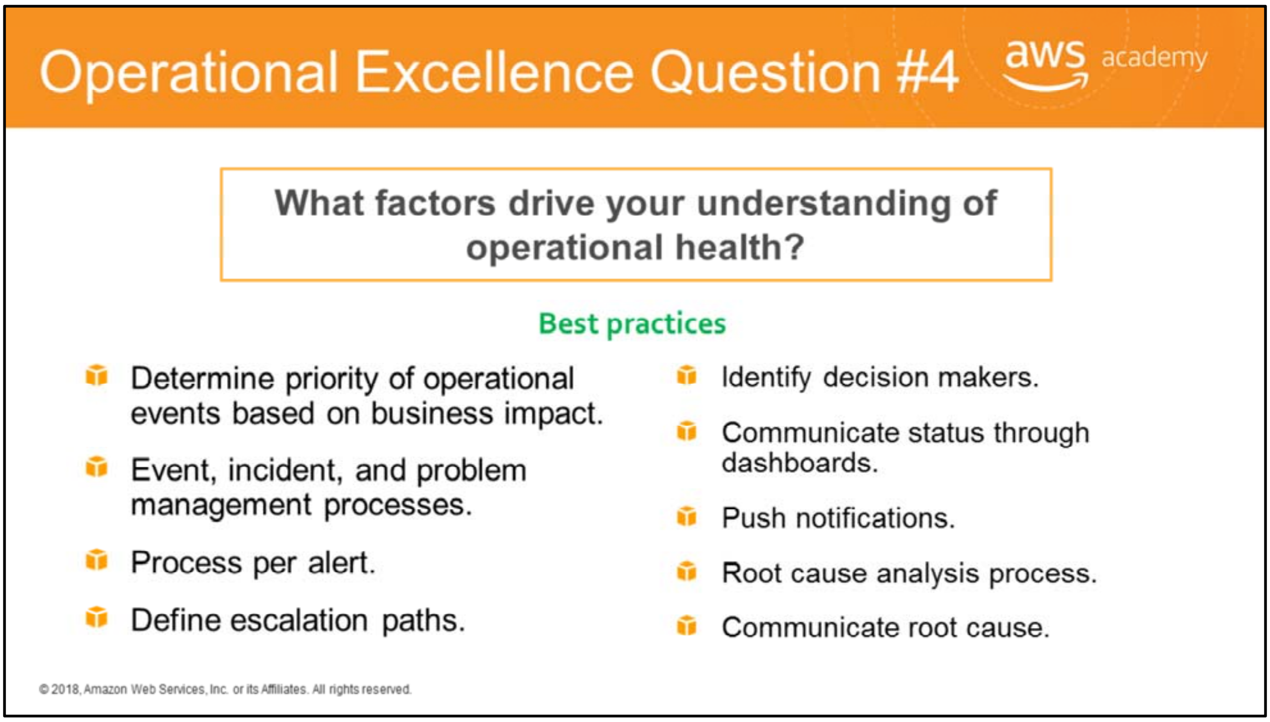
- Identifying operations metrics. Define metrics that can be used to measure the execution of operations activities, such as runbooks and playbooks.

- Establishing baselines for metrics so that they provide expected values as the basis for comparison.

- Collecting and analyzing your metrics. Perform regular, proactive reviews to identify trends and determine responses.

- Validating insights. Review the results of your analysis and responses with cross-functional teams and business owners. Adjust the responses as appropriate.

- Taking a business-level view of your operations. Determine whether you are satisfying customer needs, and identify areas that need improvement so that you can reach your business goals.



Operational Excellence Question #4

aws academy

What factors drive your understanding of operational health?

Best practices

- Determine priority of operational events based on business impact.
- Event, incident, and problem management processes.
- Process per alert.
- Define escalation paths.
- Identify decision makers.
- Communicate status through dashboards.
- Push notifications.
- Root cause analysis process.
- Communicate root cause.

What factors drive your understanding of operational health?

Best practices for understanding operational health include:

- Determining the priority of operational events based on their impact on the business. When multiple events require intervention, priority is based on the business impact.

- Putting processes in place to handle event, incident, and problem management. Establish processes to address observed events, events that require intervention—such as incidents)—and events that require intervention but cannot currently be resolved, such as problems.

- Processing each alert. Any event for which you raise an alert should have a well-defined response, such as a runbook or playbook. The event should also have a specifically identified owner, such as an individual, a team, or a role.

- Defining escalation paths. Runbooks and playbooks should have a definition for what triggers an escalation, a process for escalation, and specifically identify the owners for each action. Escalations might include third parties, such as for example, vendors, AWS Support, and others.

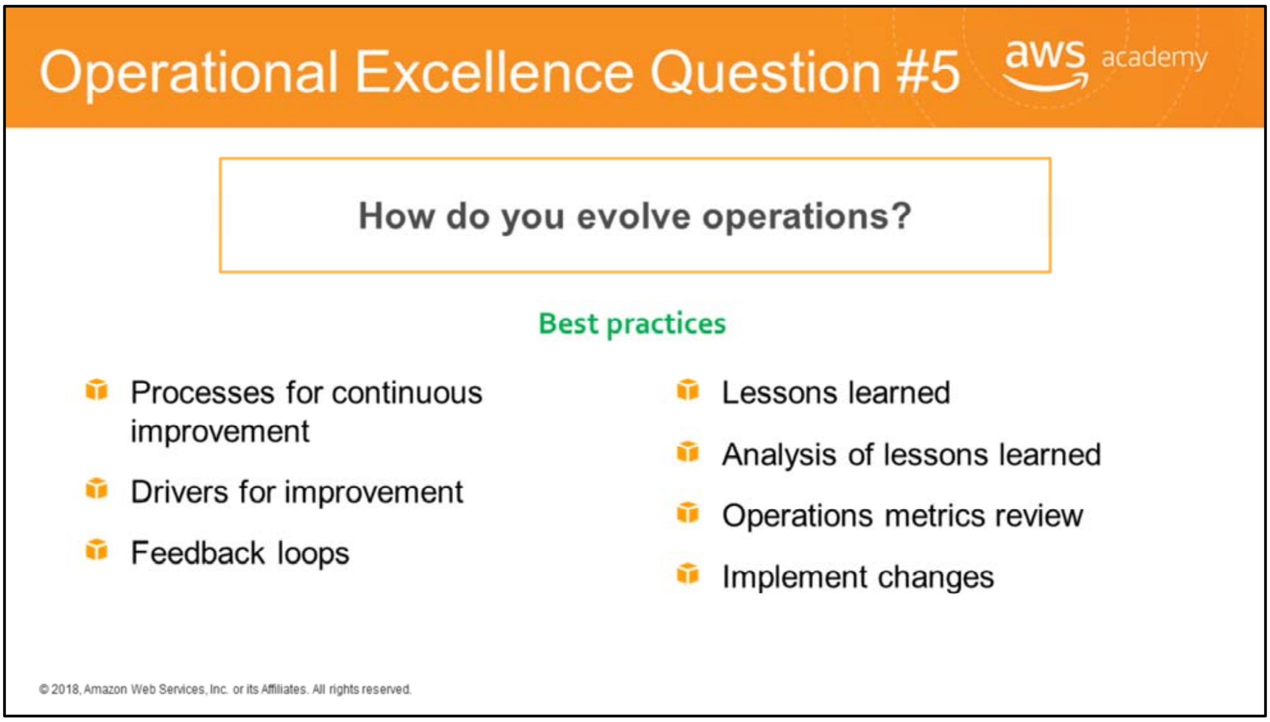
- Identifying decision makers. When actions have a potential impact on business outcomes, you must identify decision makers who are empowered to make decisions regarding a course of action on the behalf of the organization.

- Communicating operating status through dashboards. Create dashboards that communicate the current operating status of the business. Dashboards should be tailored to the target audiences, such as internal technical teams, leaders, and customers. Examples include the CloudWatch dashboard, Personal Health Dashboard, and Service Health Dashboard.

- Pushing notifications to communicate with your users when the services they consume are being impacted, and when the services return to normal operating conditions, such as via email or SMS.

- Establishing a root cause analysis process that identifies and documents the root cause of an event.

- Communicating the root cause of an issue or event. Make sure that you understand the root causes of events and their impact, and communicate them as appropriate. Also make sure that you tailor your communications to the target audiences.



Operational Excellence Question #5

How do you evolve operations?

Best practices

- Processes for continuous improvement
- Drivers for improvement
- Feedback loops
- Lessons learned
- Analysis of lessons learned
- Operations metrics review
- Implement changes

How do you evolve operations?

Best practices for evolving operations include:

- Putting processes in place to support continuous improvement. Your operations processes include dedicated work cycles to make continuous incremental improvements possible. Opportunities can then be evaluated and prioritized for action.

- Integrating drivers for improvement. Consider the features, capabilities, and improvements that you want. Also consider which issues, bugs, and vulnerabilities cannot be accepted. Finally, also consider which updates are required to maintain compliance with your policies, or to maintain support from a vendor.

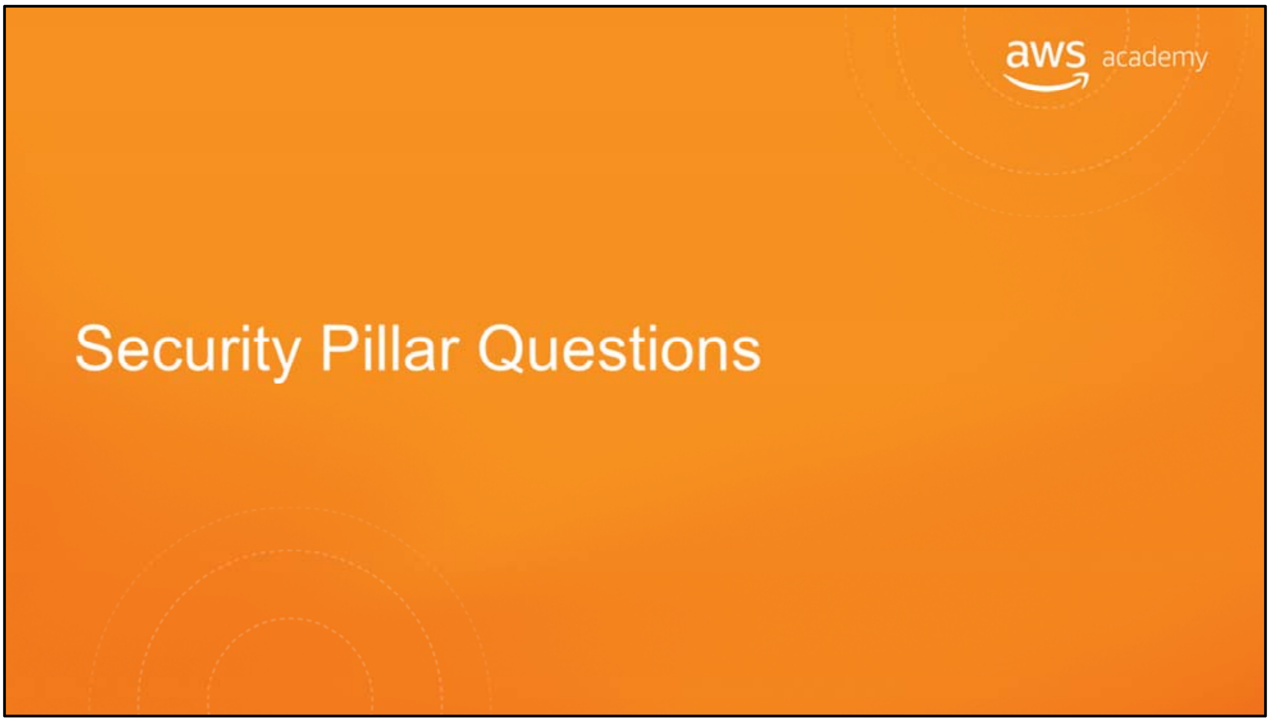
- Including feedback loops for procedures so that you can identify areas for improvement.

- Having procedures in place to capture and document lessons learned from the execution of operations activities, which means that they can be used by other teams.

- Analyzing lessons learned along with procedures so that you can identify trends in what you learned, and identify areas to investigate for improvement opportunities.

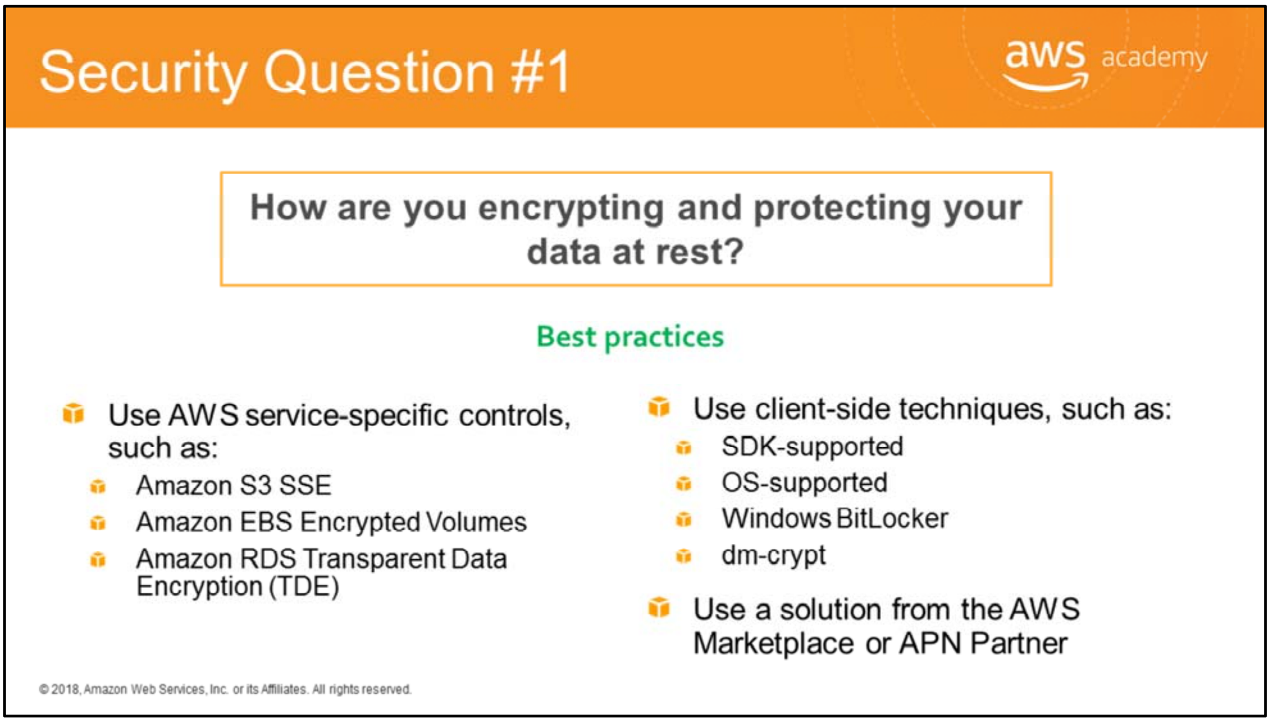
- Performing retrospective analysis of operations metrics with participants spanning the business to determine opportunities and methods for improvement.

- Implementing changes to facilitate improvement, and evaluating the results to determine whether the changes are successful.



Security Pillar Questions

Before we finalize this module, let’s review some questions and best practices regarding the Security pillar.



Security Question #1

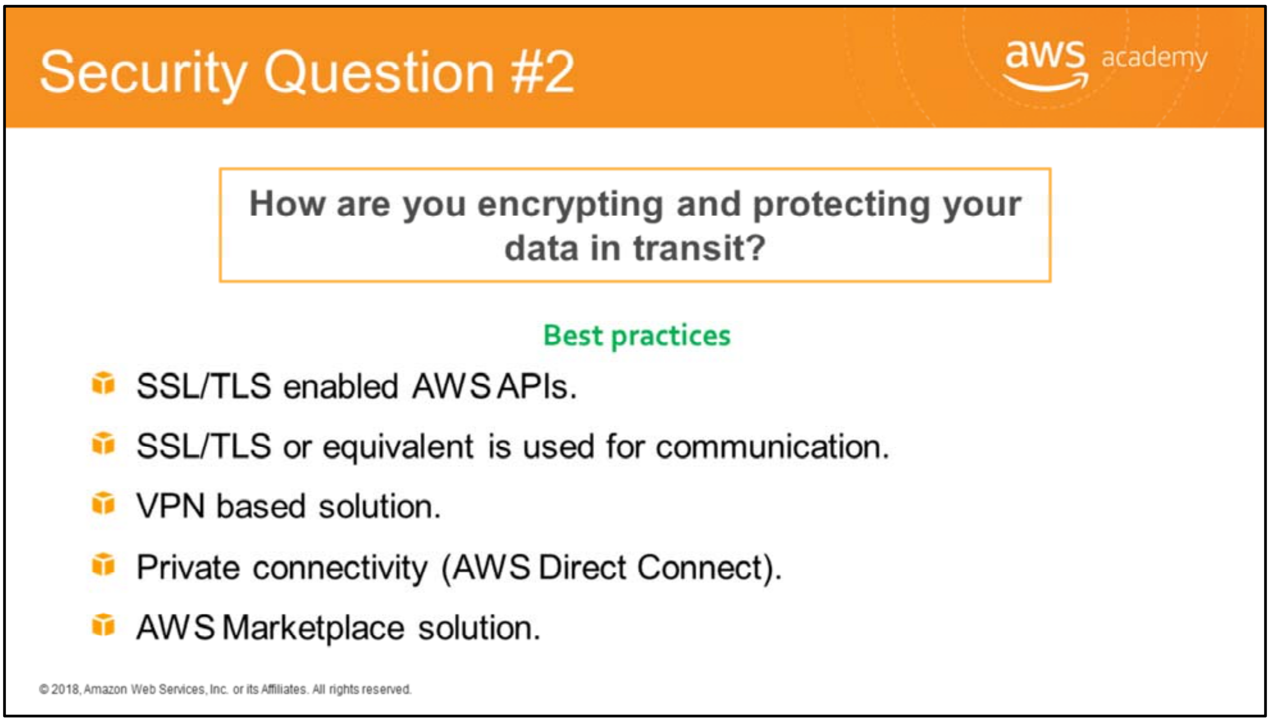
How are you encrypting and protecting your data at rest?

Best practices

- Use AWS service-specific controls, such as:
  - Amazon S3 SSE
  - Amazon EBS Encrypted Volumes
  - Amazon RDS Transparent Data Encryption (TDE)
- Use client-side techniques, such as:
  - SDK-supported
  - OS-supported
  - Windows BitLocker
  - dm-crypt
- Use a solution from the AWS Marketplace or APN Partner

How are you encrypting and protecting your data at rest?

Take a moment to review some best practices.



Security Question #2

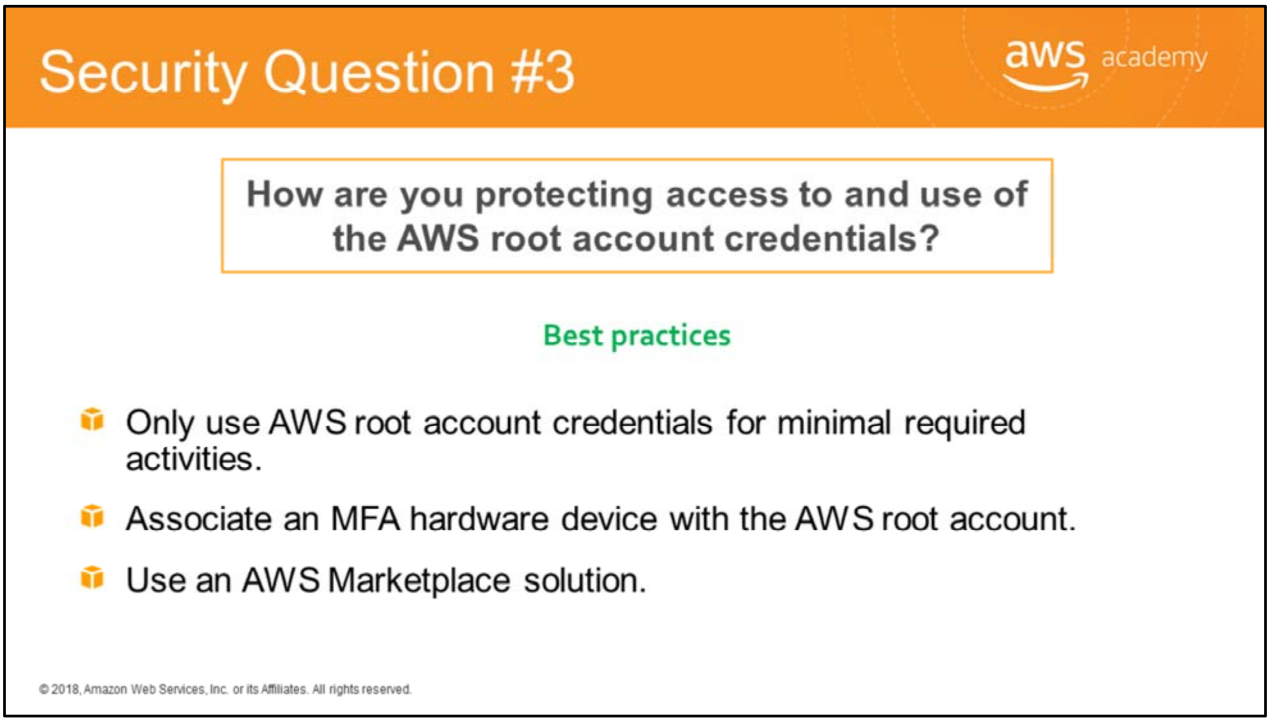
How are you encrypting and protecting your data in transit?

Best practices

- SSL/TLS enabled AWS APIs.
- SSL/TLS or equivalent is used for communication.
- VPN based solution.
- Private connectivity (AWS Direct Connect).
- AWS Marketplace solution.

How are you encrypting and protecting your data in transit?

Take a moment to review some best practices.



Security Question #3

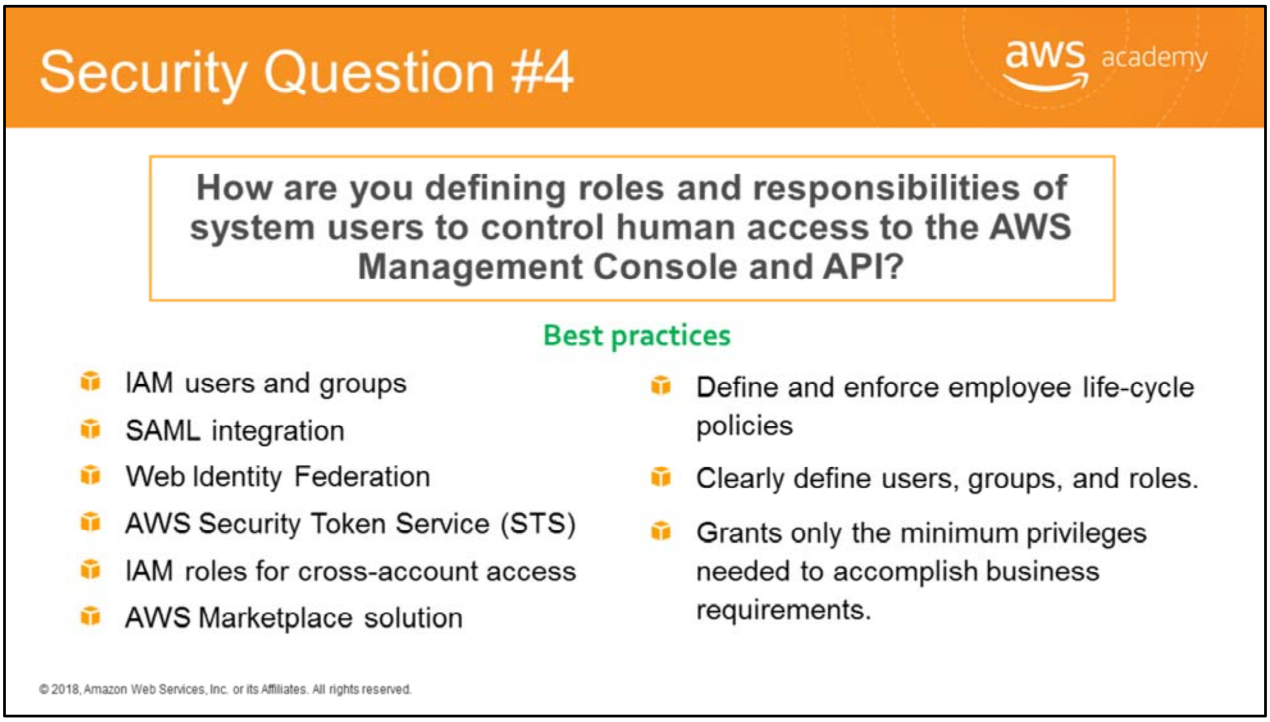
How are you protecting access to and use of the AWS root account credentials?

Best practices

- Only use AWS root account credentials for minimal required activities.
- Associate an MFA hardware device with the AWS root account.
- Use an AWS Marketplace solution.

How do you protect access to the AWS root account credentials, and how they are used?

Take a moment to review some best practices.



Security Question #4

aws academy

How are you defining roles and responsibilities of system users to control human access to the AWS Management Console and API?

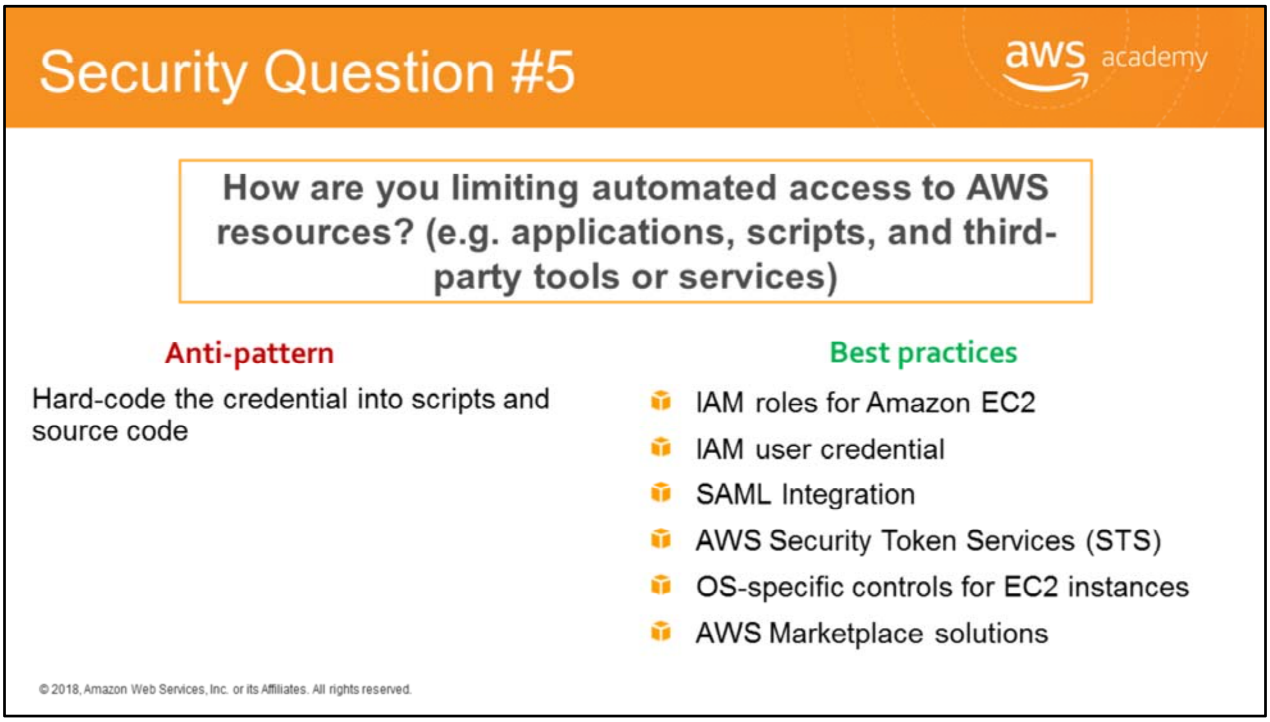
Best practices

- IAM users and groups
- SAML integration
- Web Identity Federation
- AWS Security Token Service (STS)
- IAM roles for cross-account access
- AWS Marketplace solution

- Define and enforce employee life-cycle policies
- Clearly define users, groups, and roles.
- Grants only the minimum privileges needed to accomplish business requirements.

How do you define the roles and responsibilities of system users so that you can control human access to the AWS Management Console and the API?

Take a moment to review some best practices.



Security Question #5

How are you limiting automated access to AWS resources? (e.g. applications, scripts, and third-party tools or services)

Anti-pattern

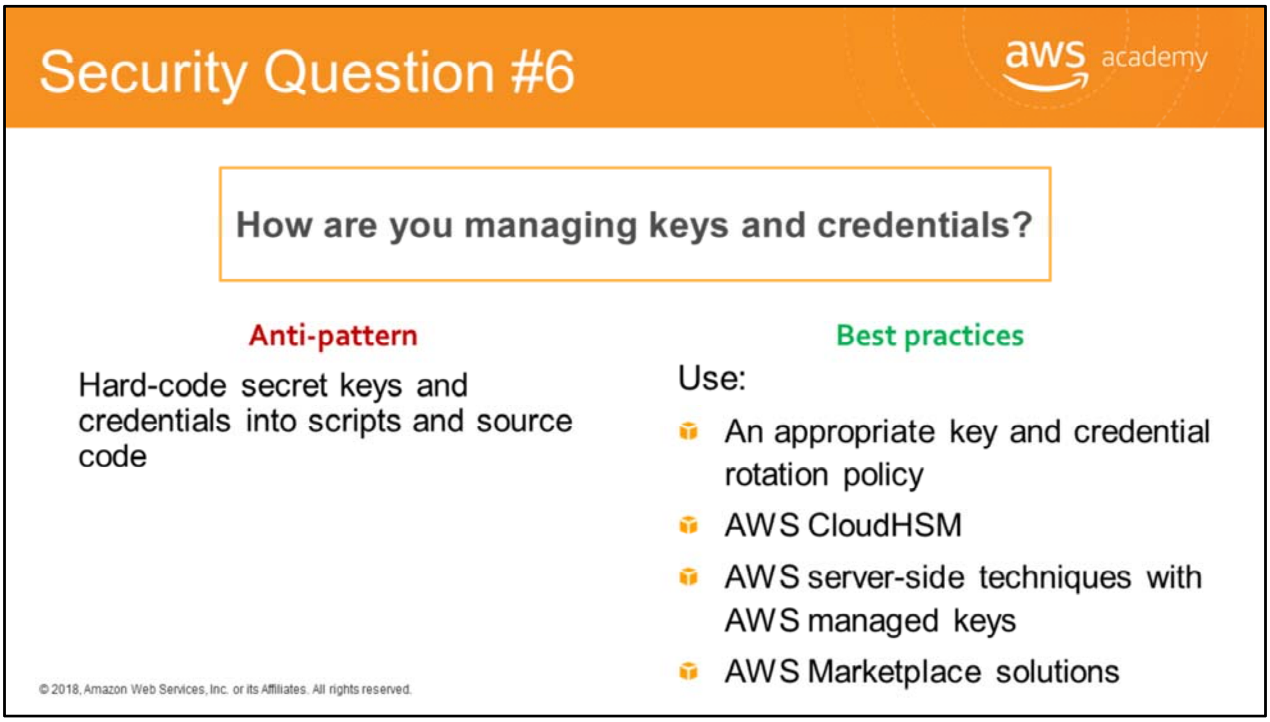
Hard-code the credential into scripts and source code

Best practices

- IAM roles for Amazon EC2
- IAM user credential
- SAML Integration
- AWS Security Token Services (STS)
- OS-specific controls for EC2 instances
- AWS Marketplace solutions

How are you limiting automated access to AWS resources, such as applications, scripts, and third-party tools or services?

Take a moment to review the anti-pattern and some best practices.



Security Question #6

How are you managing keys and credentials?

Anti-pattern

Hard-code secret keys and credentials into scripts and source code

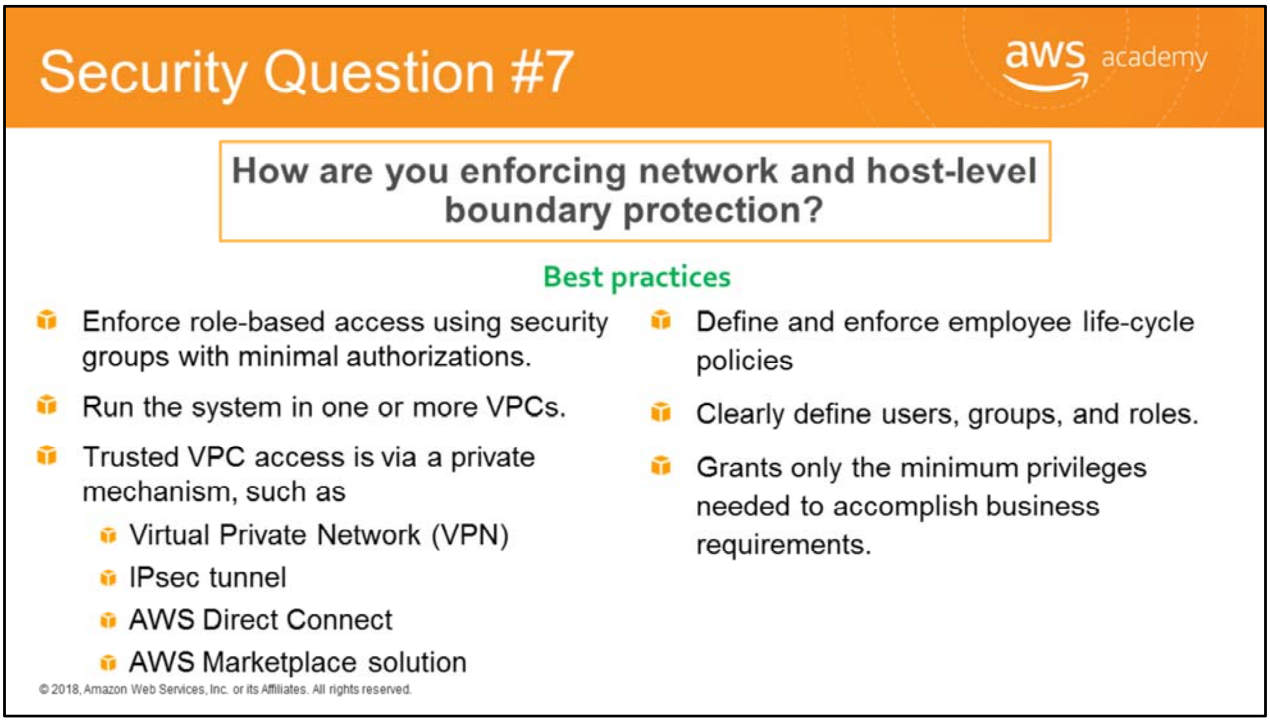
Best practices

Use:

- An appropriate key and credential rotation policy
- AWS CloudHSM
- AWS server-side techniques with AWS managed keys
- AWS Marketplace solutions

How are you managing keys and credentials?

Take a moment to review the anti-pattern and some best practices.



Security Question #7

aws academy

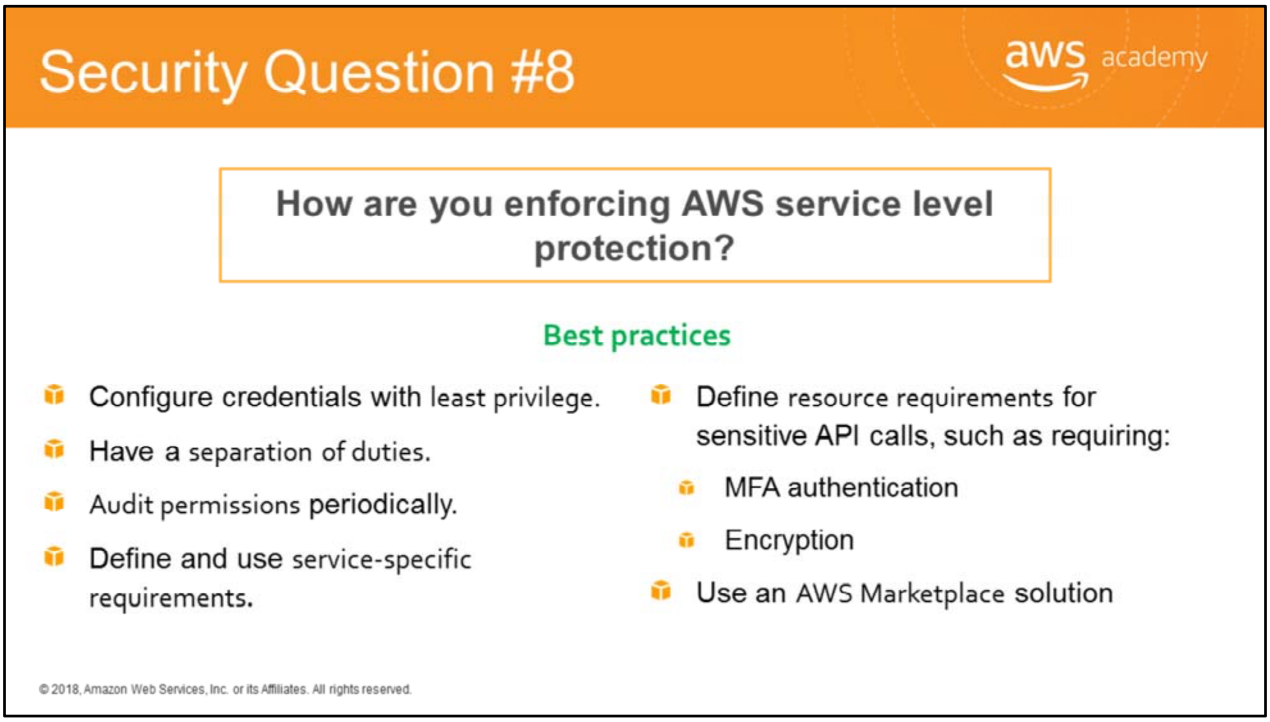
How are you enforcing network and host-level boundary protection?

Best practices

- Enforce role-based access using security groups with minimal authorizations.
- Run the system in one or more VPCs.
- Trusted VPC access is via a private mechanism, such as
  - Virtual Private Network (VPN)
  - IPsec tunnel
  - AWS Direct Connect
  - AWS Marketplace solution
- Define and enforce employee life-cycle policies
- Clearly define users, groups, and roles.
- Grants only the minimum privileges needed to accomplish business requirements.

How are you enforcing network and host-level boundary protection?

Take a moment to review some best practices.



Security Question #8

aws academy

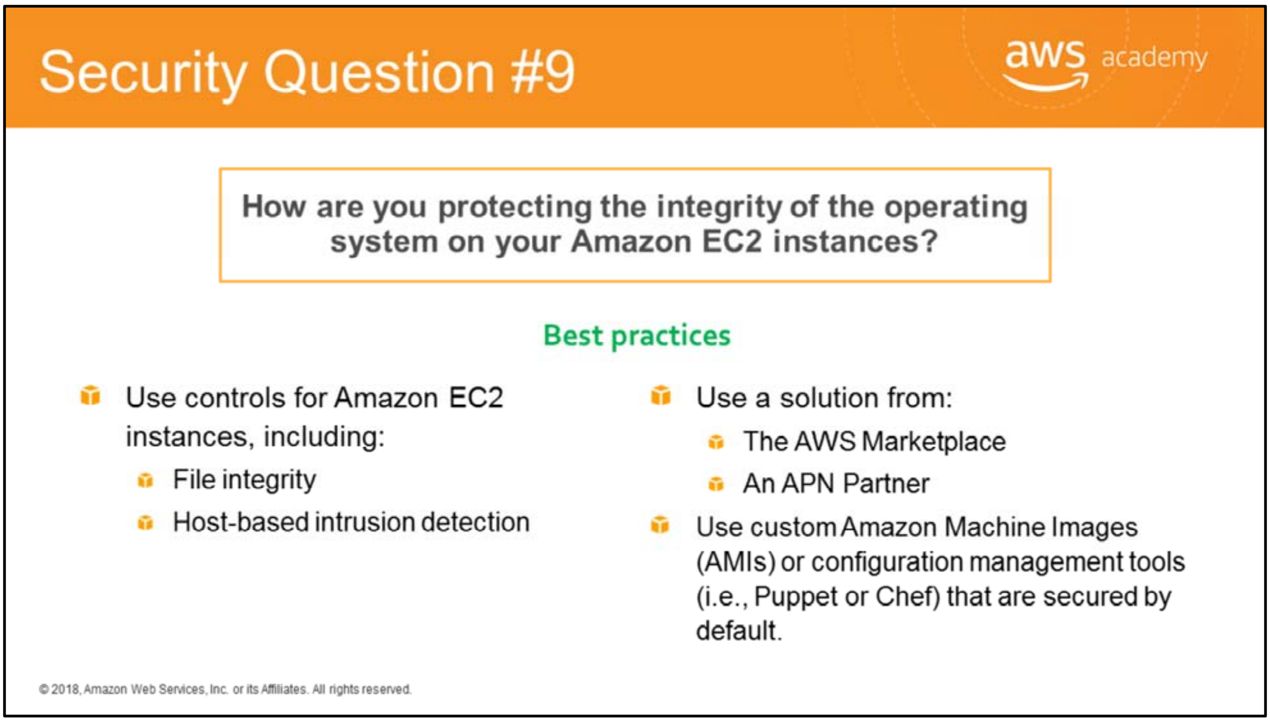
How are you enforcing AWS service level protection?

Best practices

- Configure credentials with least privilege.
- Have a separation of duties.
- Audit permissions periodically.
- Define and use service-specific requirements.
- Define resource requirements for sensitive API calls, such as requiring:
  - MFA authentication
  - Encryption
- Use an AWS Marketplace solution

How are you enforcing AWS service-level protection?

Take a moment to review some best practices.



Security Question #9

aws academy

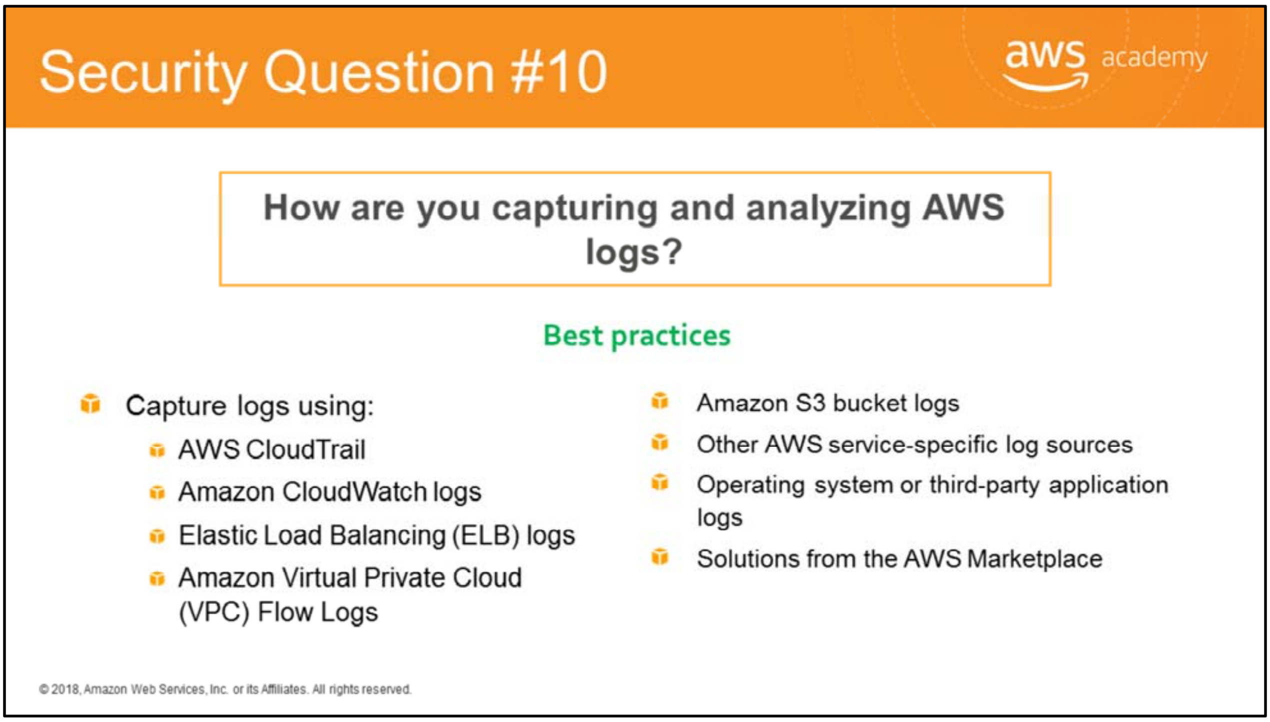
How are you protecting the integrity of the operating system on your Amazon EC2 instances?

Best practices

- Use controls for Amazon EC2 instances, including:
  - File integrity
  - Host-based intrusion detection
- Use a solution from:
  - The AWS Marketplace
  - An APN Partner
- Use custom Amazon Machine Images (AMIs) or configuration management tools (i.e., Puppet or Chef) that are secured by default.

How are you protecting the integrity of the operating system on your Amazon EC2 instances?

Take a moment to review some best practices.



Security Question #10

aws academy

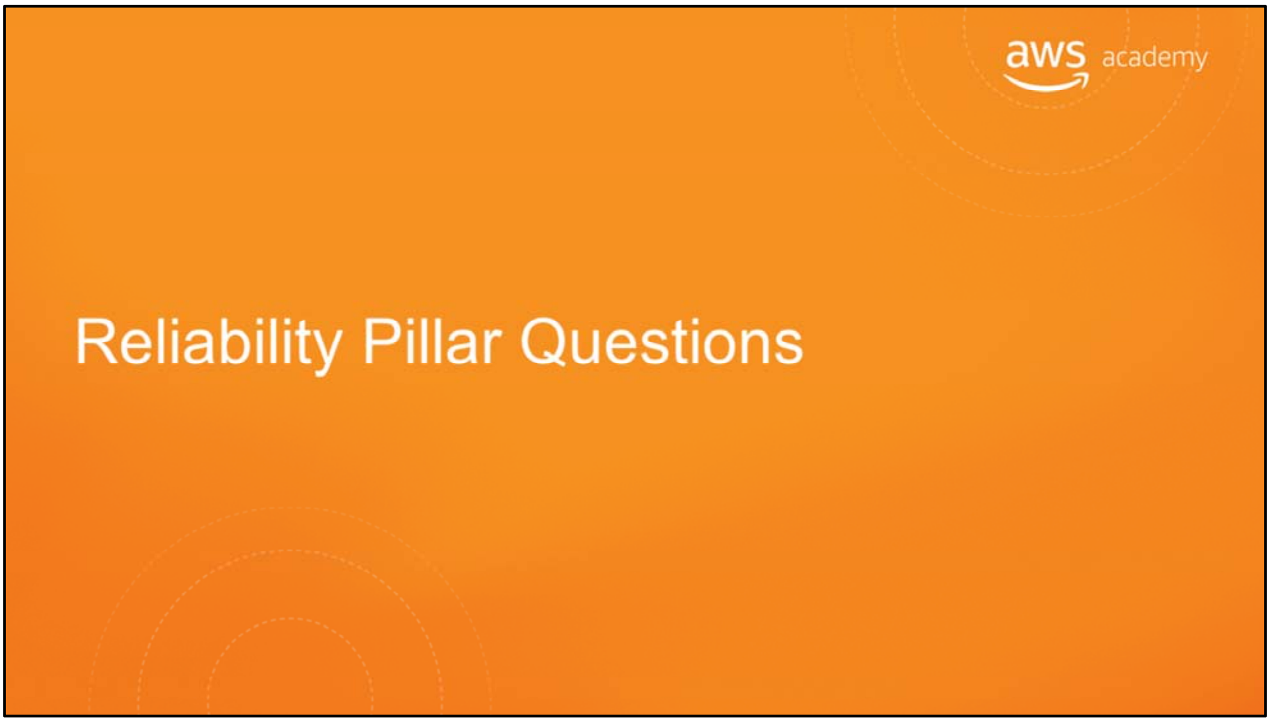
How are you capturing and analyzing AWS logs?

Best practices

- Capture logs using:
  - AWS CloudTrail
  - Amazon CloudWatch logs
  - Elastic Load Balancing (ELB) logs
  - Amazon Virtual Private Cloud (VPC) Flow Logs
- Amazon S3 bucket logs
- Other AWS service-specific log sources
- Operating system or third-party application logs
- Solutions from the AWS Marketplace

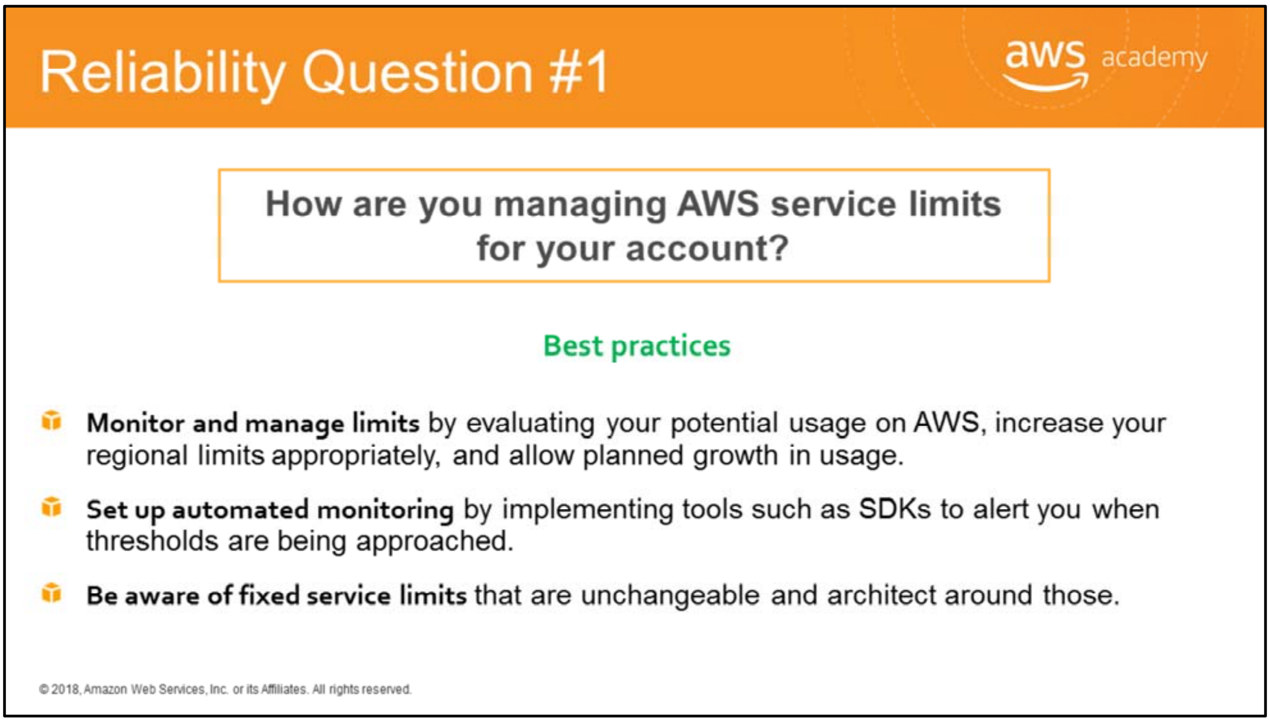
How are you capturing and analyzing AWS logs?

Take a moment to review some best practices.



Reliability Pillar Questions

In this next section, we will ask a question for you to consider, and provide some best practices.



Reliability Question #1

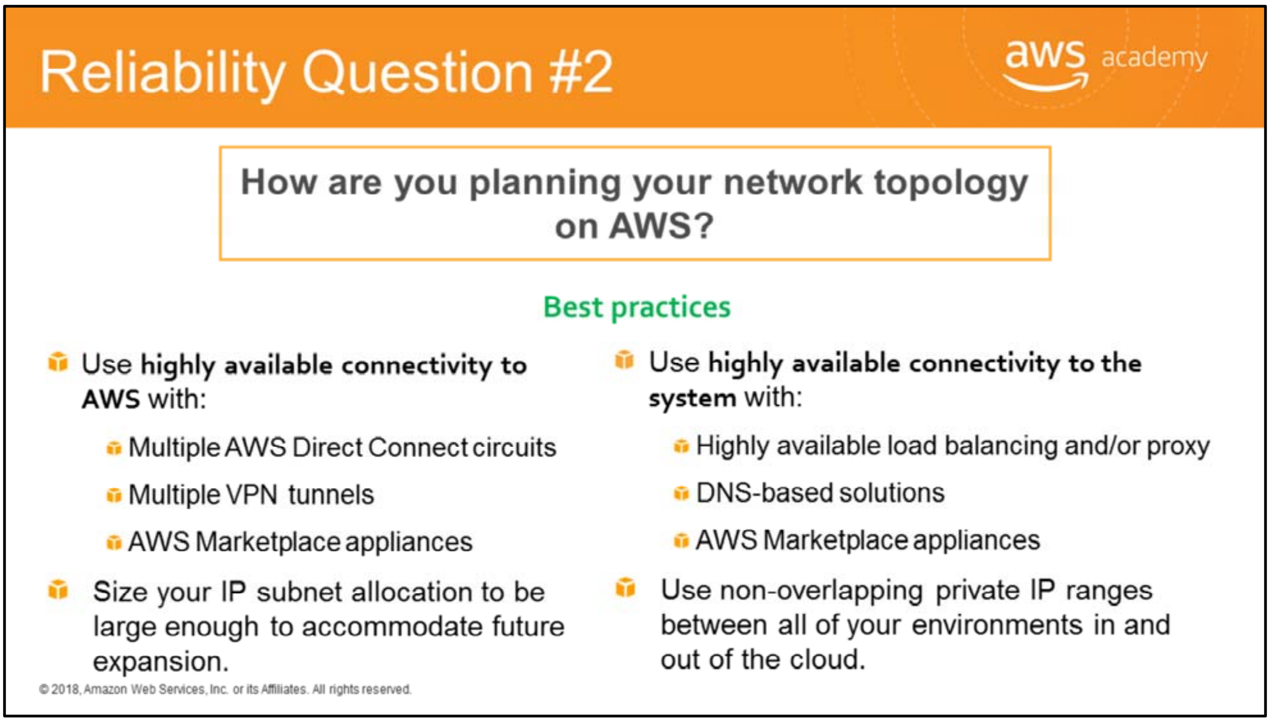
How are you managing AWS service limits for your account?

Best practices

- **Monitor and manage limits** by evaluating your potential usage on AWS, increase your regional limits appropriately, and allow planned growth in usage.
- **Set up automated monitoring** by implementing tools such as SDKs to alert you when thresholds are being approached.
- **Be aware of fixed service limits** that are unchangeable and architect around those.

How are you managing AWS service limits for your account?

Take a moment to review some best practices.



Reliability Question #2

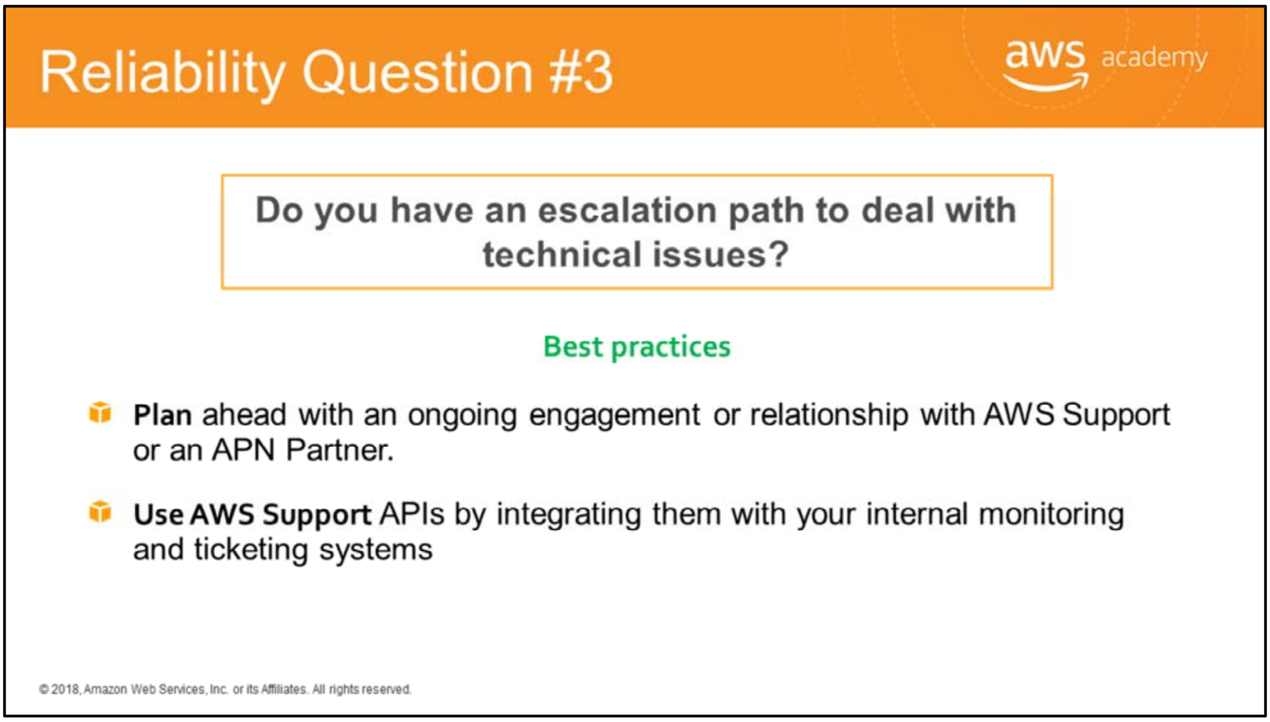
How are you planning your network topology on AWS?

Best practices

- Use **highly available connectivity to AWS** with:
  - Multiple AWS Direct Connect circuits
  - Multiple VPN tunnels
  - AWS Marketplace appliances
- Size your IP subnet allocation to be large enough to accommodate future expansion.
- Use **highly available connectivity to the system** with:
  - Highly available load balancing and/or proxy
  - DNS-based solutions
  - AWS Marketplace appliances
- Use non-overlapping private IP ranges between all of your environments in and out of the cloud.

How are you planning your network topology on AWS?

Take a moment to review some best practices.



Reliability Question #3

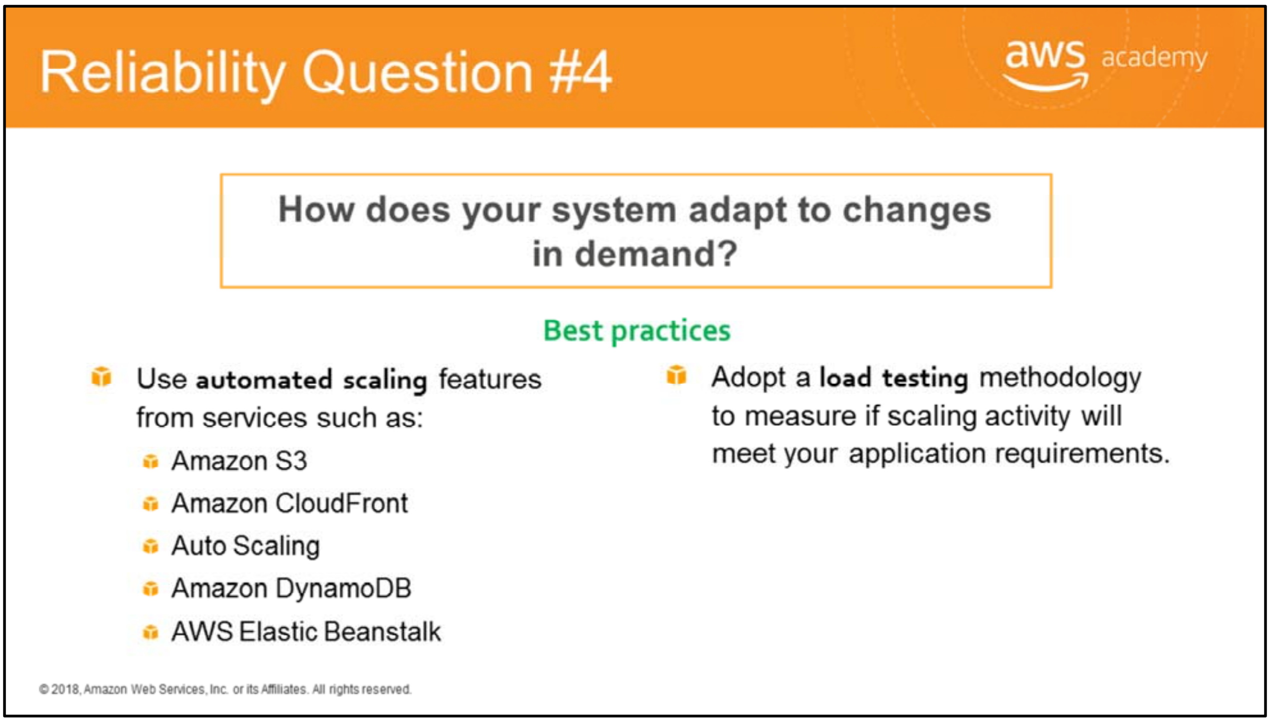
Do you have an escalation path to deal with technical issues?

Best practices

- **Plan** ahead with an ongoing engagement or relationship with AWS Support or an APN Partner.
- **Use AWS Support** APIs by integrating them with your internal monitoring and ticketing systems

Do you have an escalation path to deal with technical issues?

Take a moment to review some best practices.



Reliability Question #4

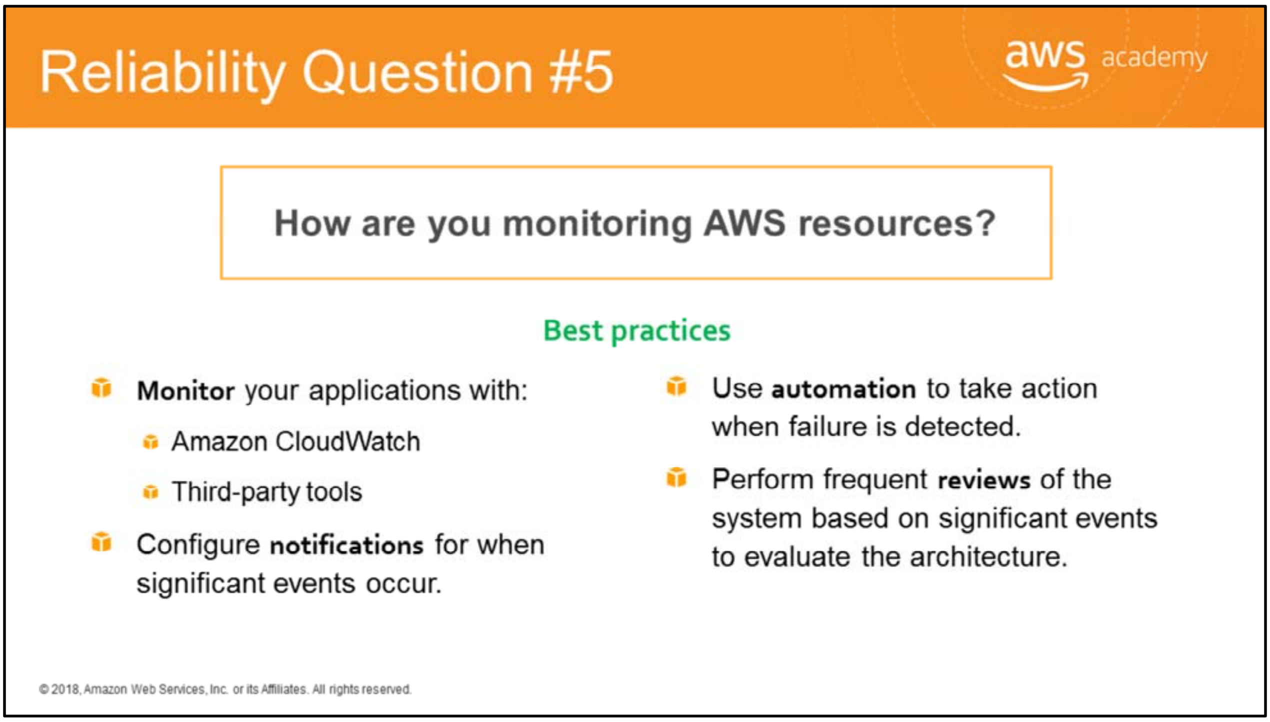
How does your system adapt to changes in demand?

Best practices

- Use **automated scaling** features from services such as:
  - Amazon S3
  - Amazon CloudFront
  - Auto Scaling
  - Amazon DynamoDB
  - AWS Elastic Beanstalk
- Adopt a **load testing** methodology to measure if scaling activity will meet your application requirements.

How does your system adapt to changes in demand?

Take a moment to review some best practices.



Reliability Question #5

aws academy

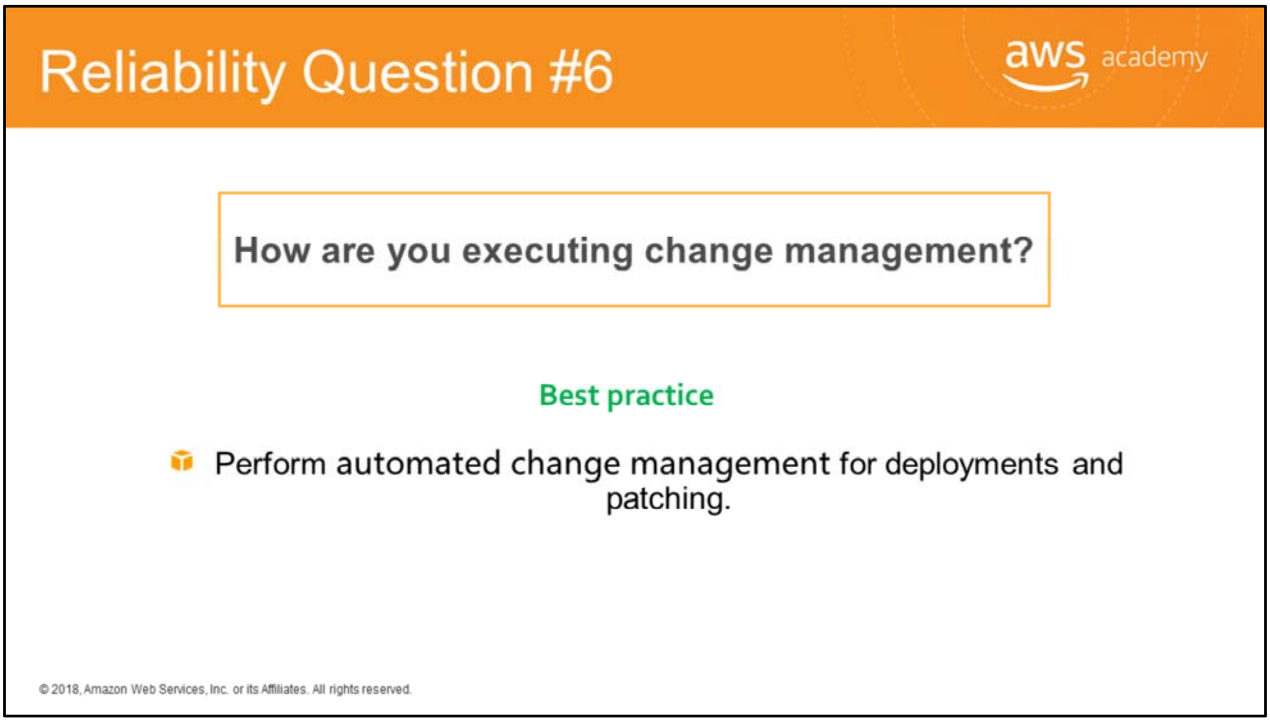
How are you monitoring AWS resources?

Best practices

- **Monitor** your applications with:
  - Amazon CloudWatch
  - Third-party tools
- Configure **notifications** for when significant events occur.
- Use **automation** to take action when failure is detected.
- Perform frequent **reviews** of the system based on significant events to evaluate the architecture.

How are you monitoring AWS resources?

Take a moment to review some best practices.



Reliability Question #6

aws academy

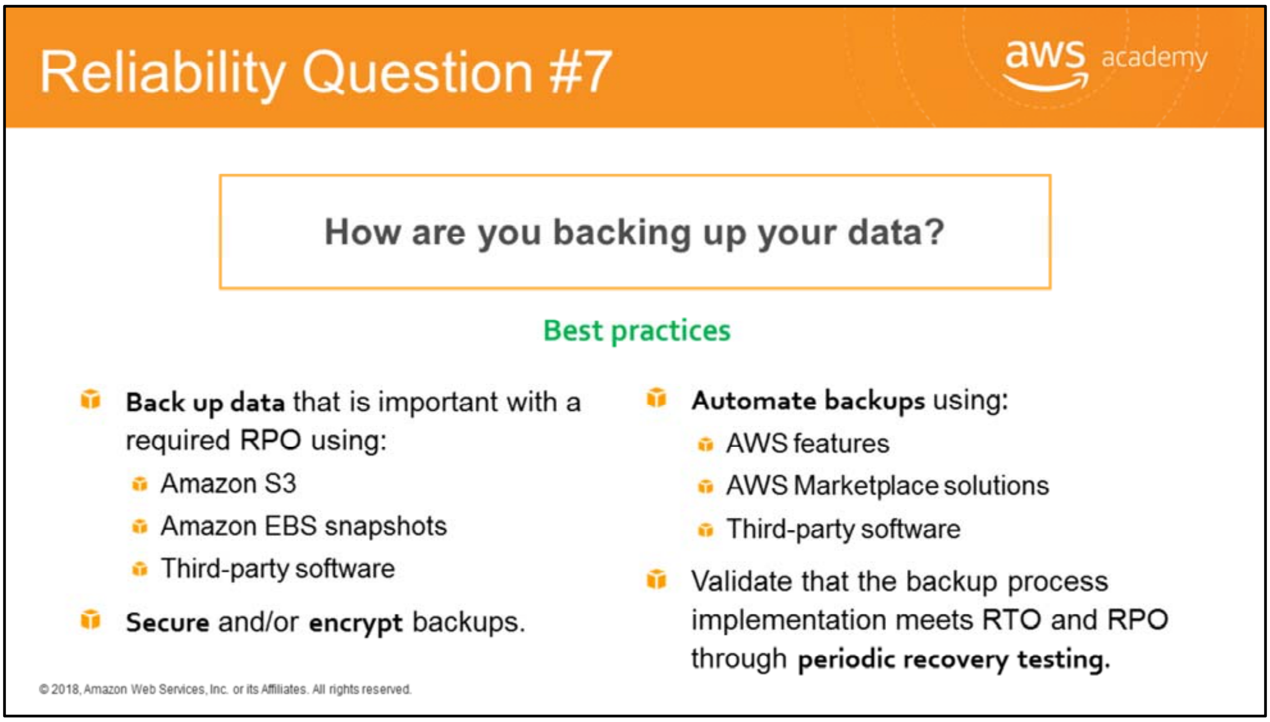
How are you executing change management?

Best practice

- Perform automated change management for deployments and patching.

How are you executing change management?

Take a moment to review a best practice.



Reliability Question #7

aws academy

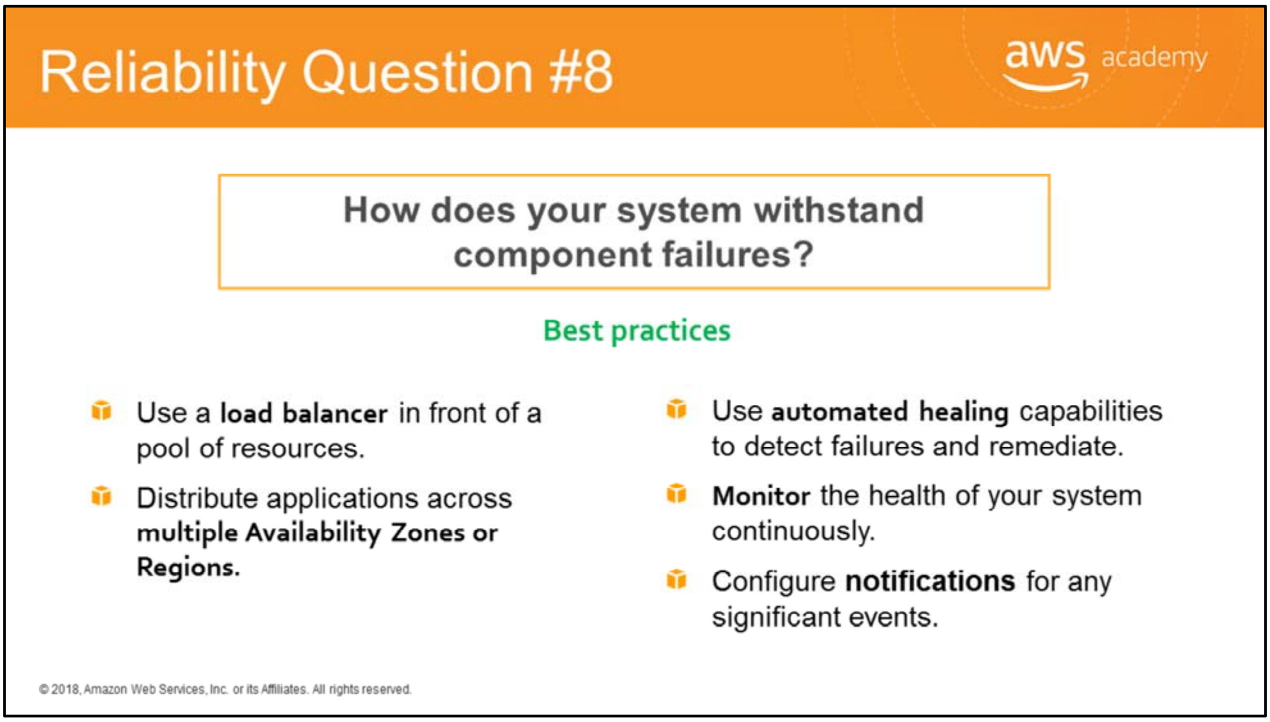
How are you backing up your data?

Best practices

- **Back up data** that is important with a required RPO using:
  - Amazon S3
  - Amazon EBS snapshots
  - Third-party software
- **Secure** and/or **encrypt** backups.
- **Automate backups** using:
  - AWS features
  - AWS Marketplace solutions
  - Third-party software
- Validate that the backup process implementation meets RTO and RPO through **periodic recovery testing.**

How are you backing up your data?

Take a moment to review some best practices.



Reliability Question #8

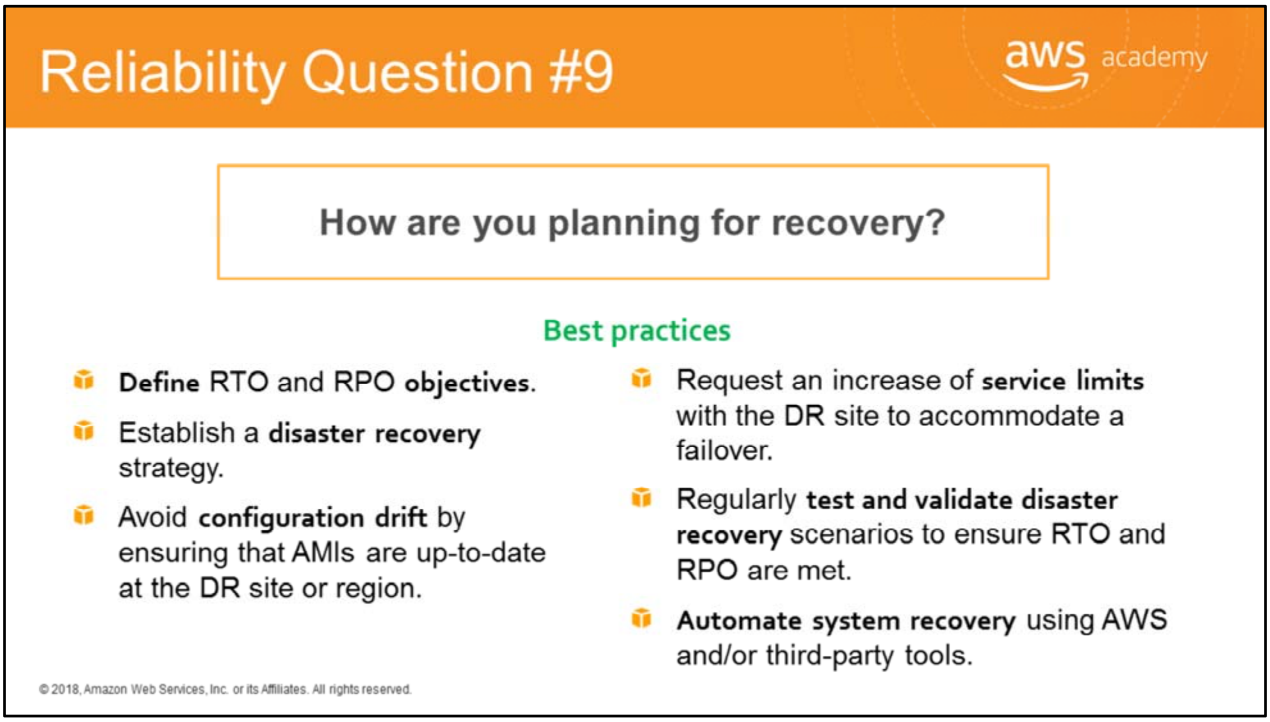
How does your system withstand component failures?

Best practices

- Use a **load balancer** in front of a pool of resources.
- Distribute applications across **multiple Availability Zones or Regions.**
- Use **automated healing** capabilities to detect failures and remediate.
- **Monitor** the health of your system continuously.
- Configure **notifications** for any significant events.

How does your system withstand component failures?

Take a moment to review some best practices.



Reliability Question #9

aws academy

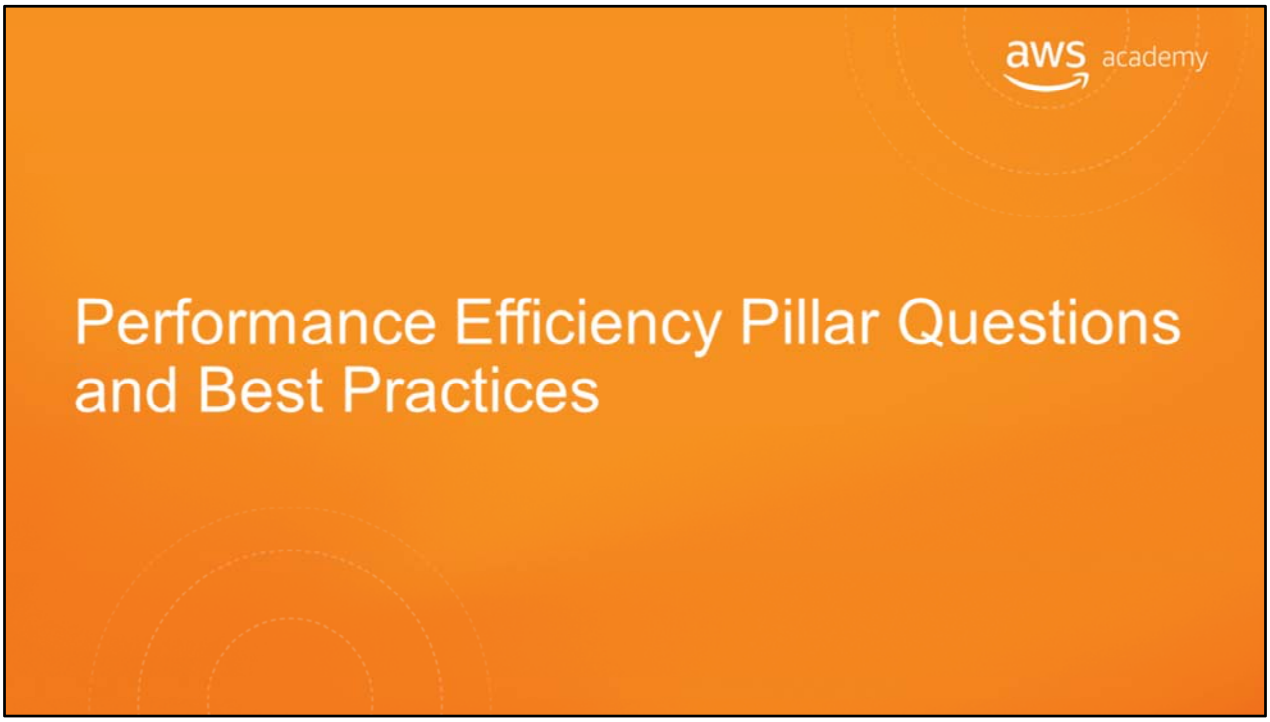
How are you planning for recovery?

Best practices

- **Define** RTO and RPO **objectives**.
- Establish a **disaster recovery** strategy.
- Avoid **configuration drift** by ensuring that AMIs are up-to-date at the DR site or region.
- Request an increase of **service limits** with the DR site to accommodate a failover.
- Regularly **test and validate disaster recovery** scenarios to ensure RTO and RPO are met.
- **Automate system recovery** using AWS and/or third-party tools.

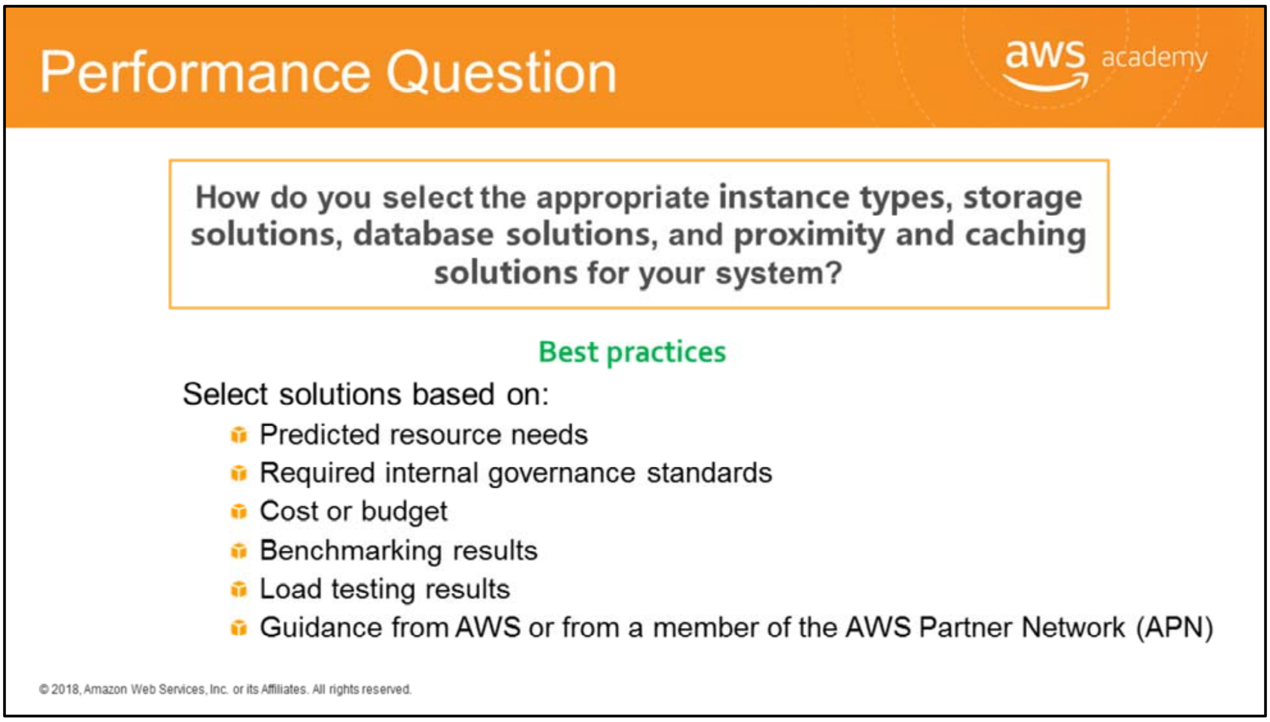
How are you planning for recovery?

Take a moment to review some best practices.



Performance Efficiency Pillar Questions and Best Practices

Before wrapping up this module, let’s review some performance efficiency questions and best practices.



Performance Question

How do you select the appropriate instance types, storage solutions, database solutions, and proximity and caching solutions for your system?

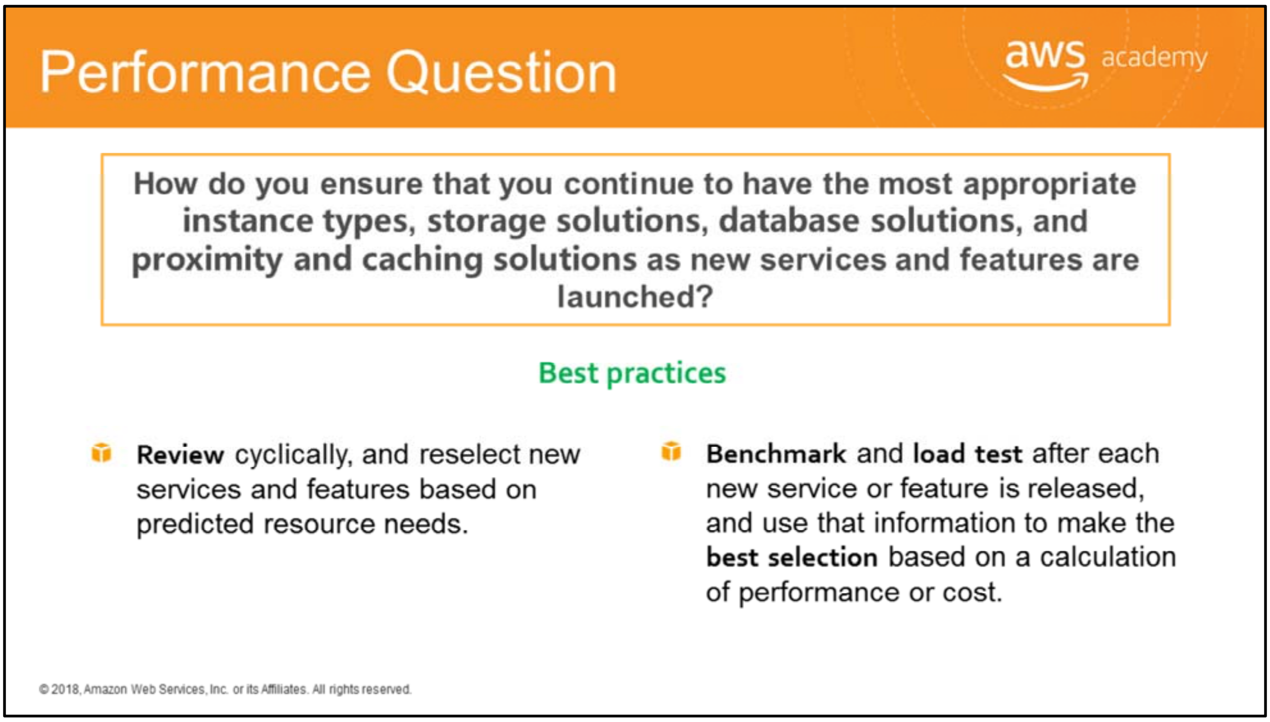
Best practices

Select solutions based on:

- Predicted resource needs
- Required internal governance standards
- Cost or budget
- Benchmarking results
- Load testing results
- Guidance from AWS or from a member of the AWS Partner Network (APN)

How do you select the appropriate instance types, storage solutions, database solutions, and proximity and caching solutions for your system?

Take a moment to review the best practices.



Performance Question

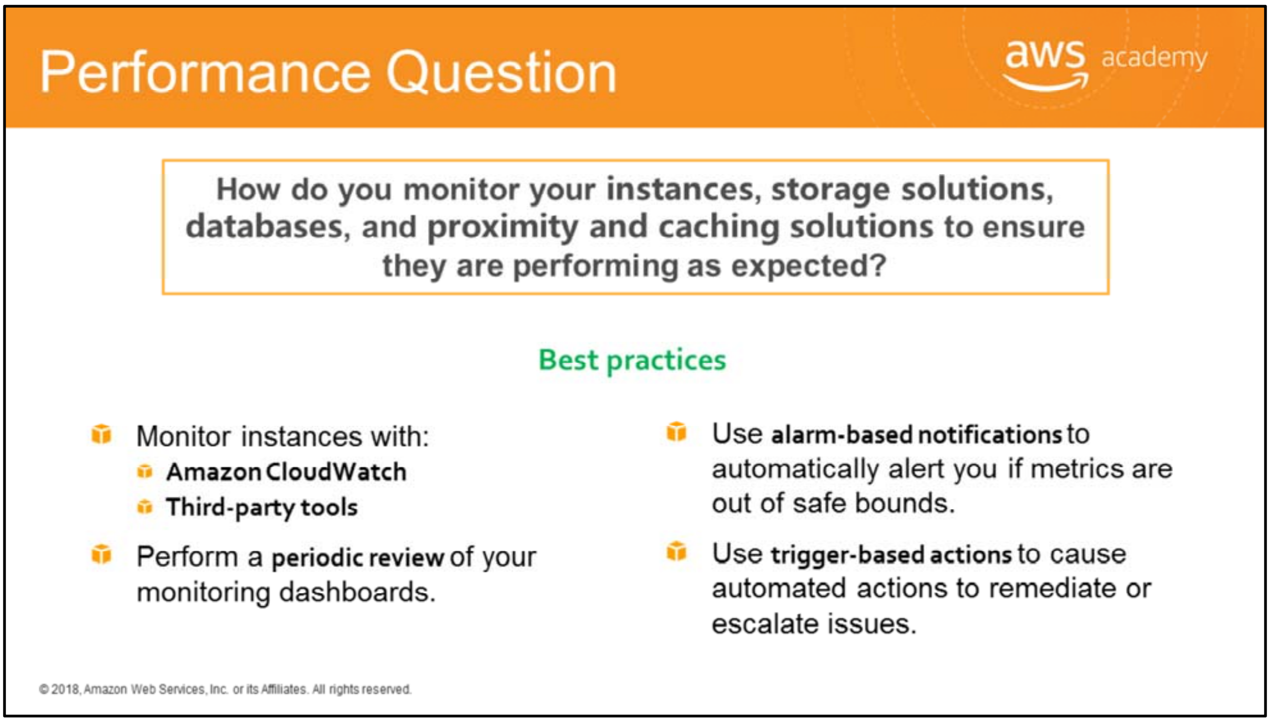
How do you ensure that you continue to have the most appropriate instance types, storage solutions, database solutions, and proximity and caching solutions as new services and features are launched?

Best practices

- **Review** cyclically, and reselect new services and features based on predicted resource needs.
- **Benchmark** and **load test** after each new service or feature is released, and use that information to make the **best selection** based on a calculation of performance or cost.

How do you ensure that you continue to have the most appropriate instance types, storage solutions, database solutions, and proximity and caching solutions as new services and features are launched?

Take a moment to review the best practices.



Performance Question

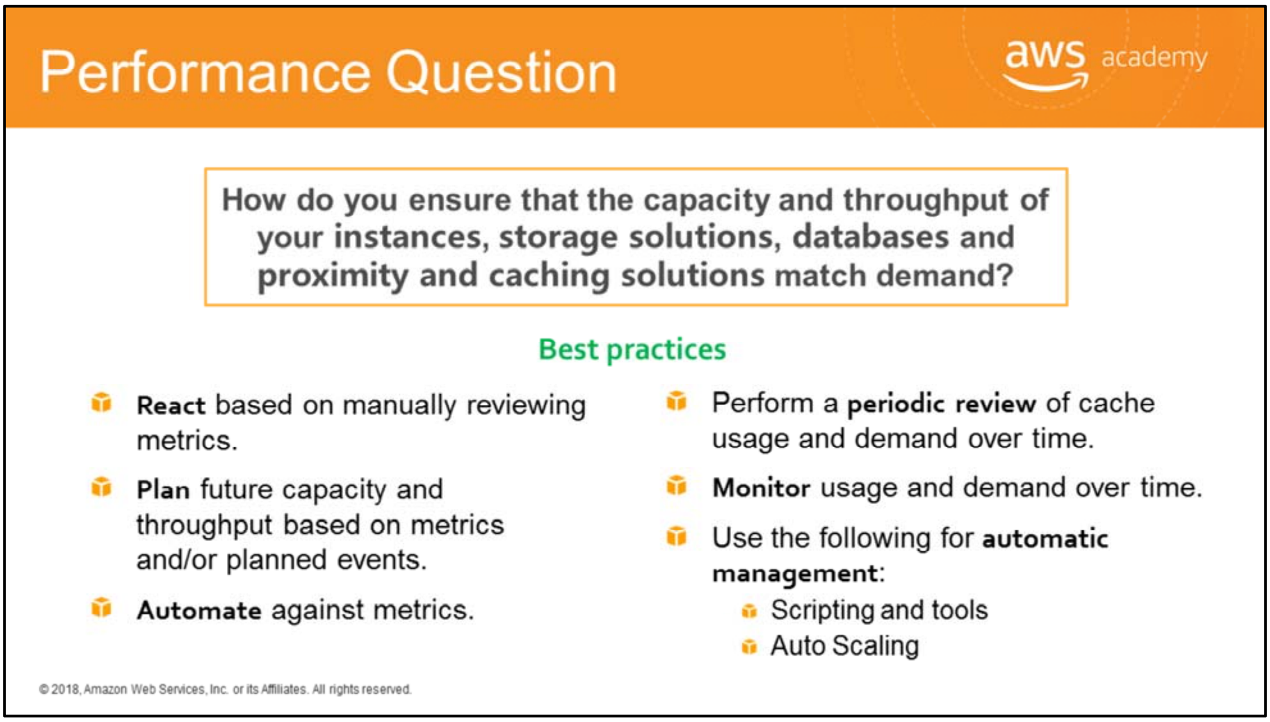
How do you monitor your instances, storage solutions, databases, and proximity and caching solutions to ensure they are performing as expected?

Best practices

- Monitor instances with:
  - **Amazon CloudWatch**
  - **Third-party tools**
- Perform a **periodic review** of your monitoring dashboards.
- Use **alarm-based notifications** to automatically alert you if metrics are out of safe bounds.
- Use **trigger-based actions** to cause automated actions to remediate or escalate issues.

How do you monitor your instances, storage solutions, databases, and proximity and caching solutions to ensure they are performing as expected?

Take a moment to review the best practices.



Performance Question

How do you ensure that the capacity and throughput of your instances, storage solutions, databases and proximity and caching solutions match demand?

Best practices

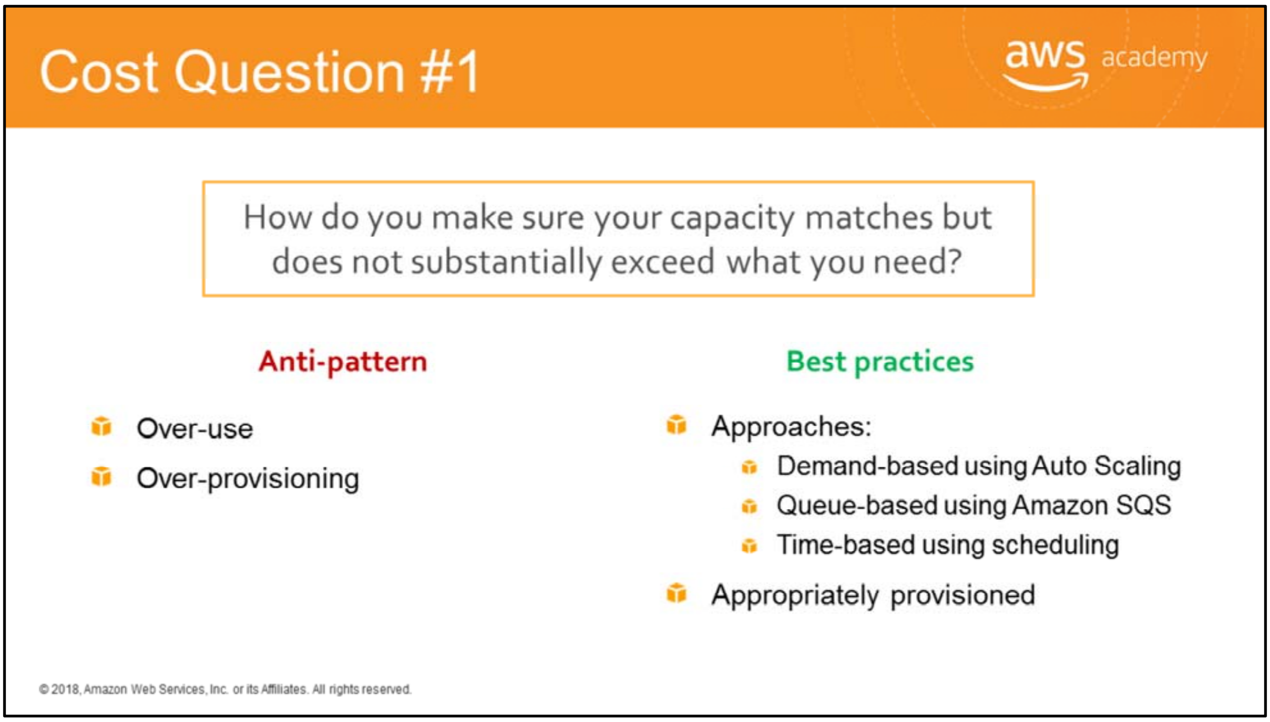
- **React** based on manually reviewing metrics.
- **Plan** future capacity and throughput based on metrics and/or planned events.
- **Automate** against metrics.
- Perform a **periodic review** of cache usage and demand over time.
- **Monitor** usage and demand over time.
- Use the following for **automatic management**:
  - Scripting and tools
  - Auto Scaling

How do you ensure that the capacity and throughput of your instances, storage solutions, databases, and proximity and caching solutions match demand?

Take a moment to review the best practices.

Cost Optimization Pillar Questions and Best Practices

Now, let’s consider questions about cost optimization, and provide some best practices.



Cost Question #1

How do you make sure your capacity matches but does not substantially exceed what you need?

Anti-pattern

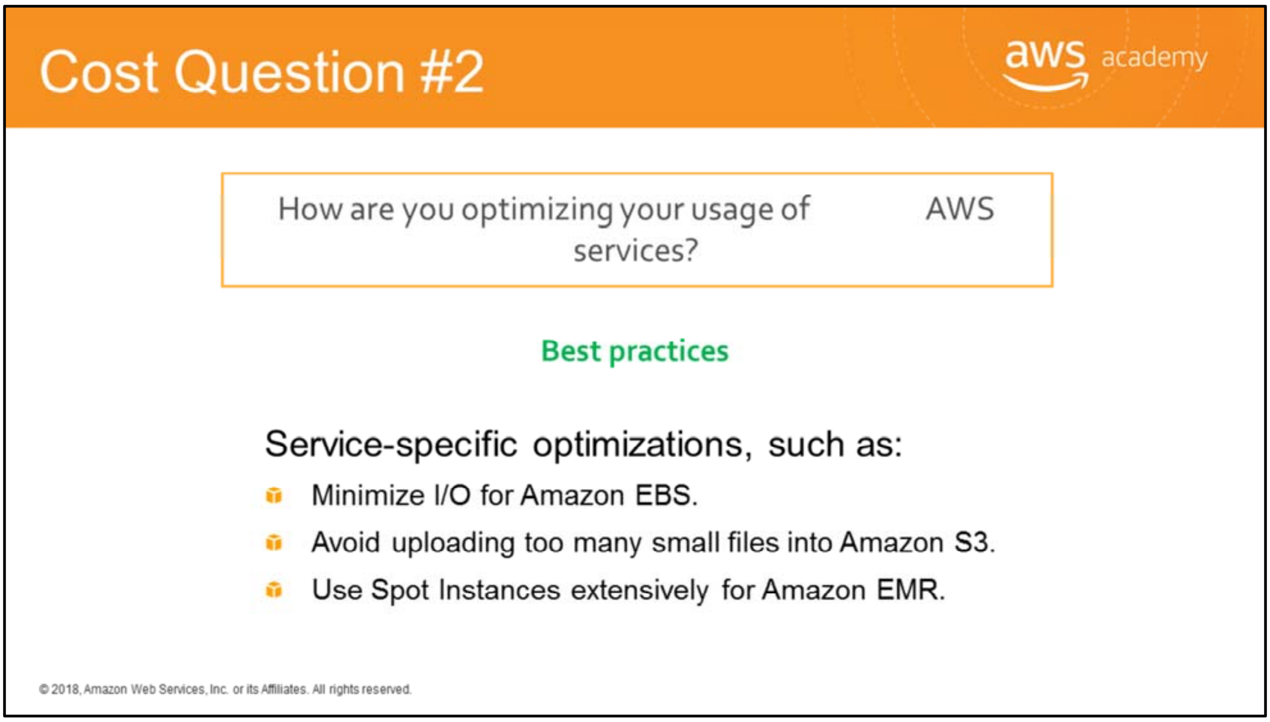
- Over-use
- Over-provisioning

Best practices

- Approaches:
  - Demand-based using Auto Scaling
  - Queue-based using Amazon SQS
  - Time-based using scheduling
- Appropriately provisioned

How do you make sure that your capacity matches—but does not substantially exceed—what you need?

Take a moment to review the anti-pattern and some best practices.



Cost Question #2

How are you optimizing your usage of AWS services?

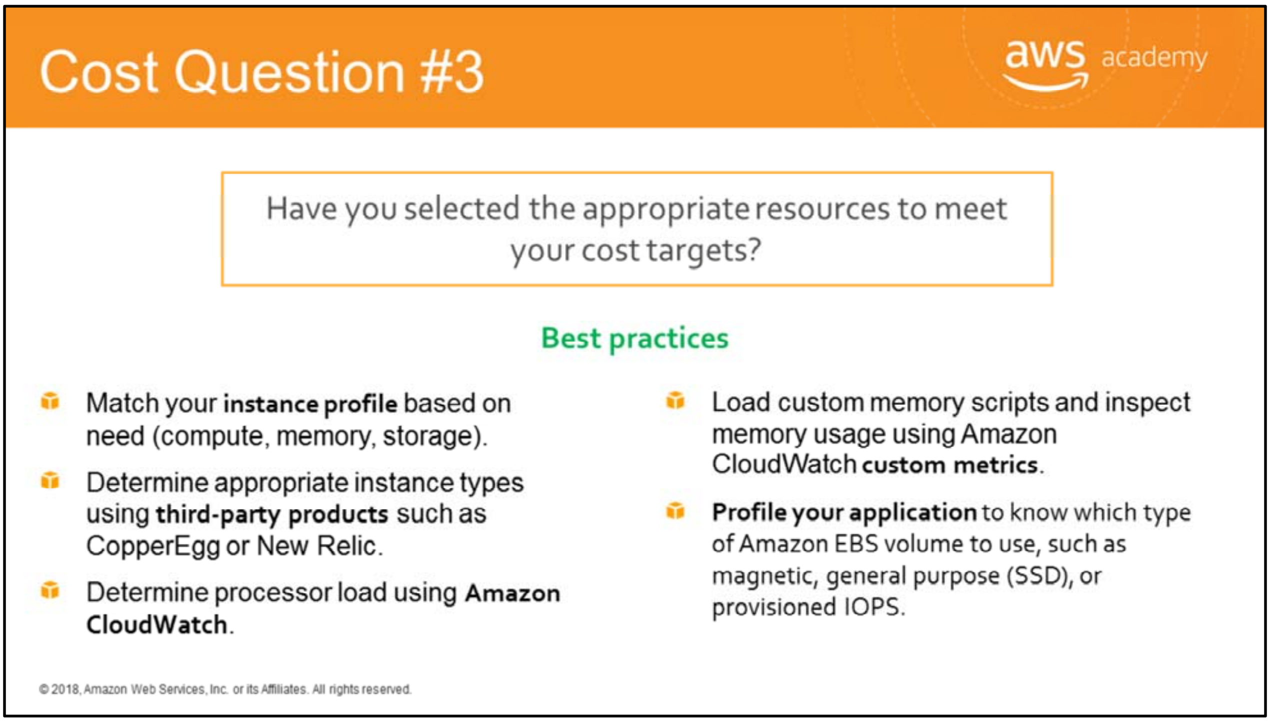
Best practices

Service-specific optimizations, such as:

- Minimize I/O for Amazon EBS.
- Avoid uploading too many small files into Amazon S3.
- Use Spot Instances extensively for Amazon EMR.

How are you optimizing your usage of AWS services?

Take a moment to review some best practices.



Cost Question #3

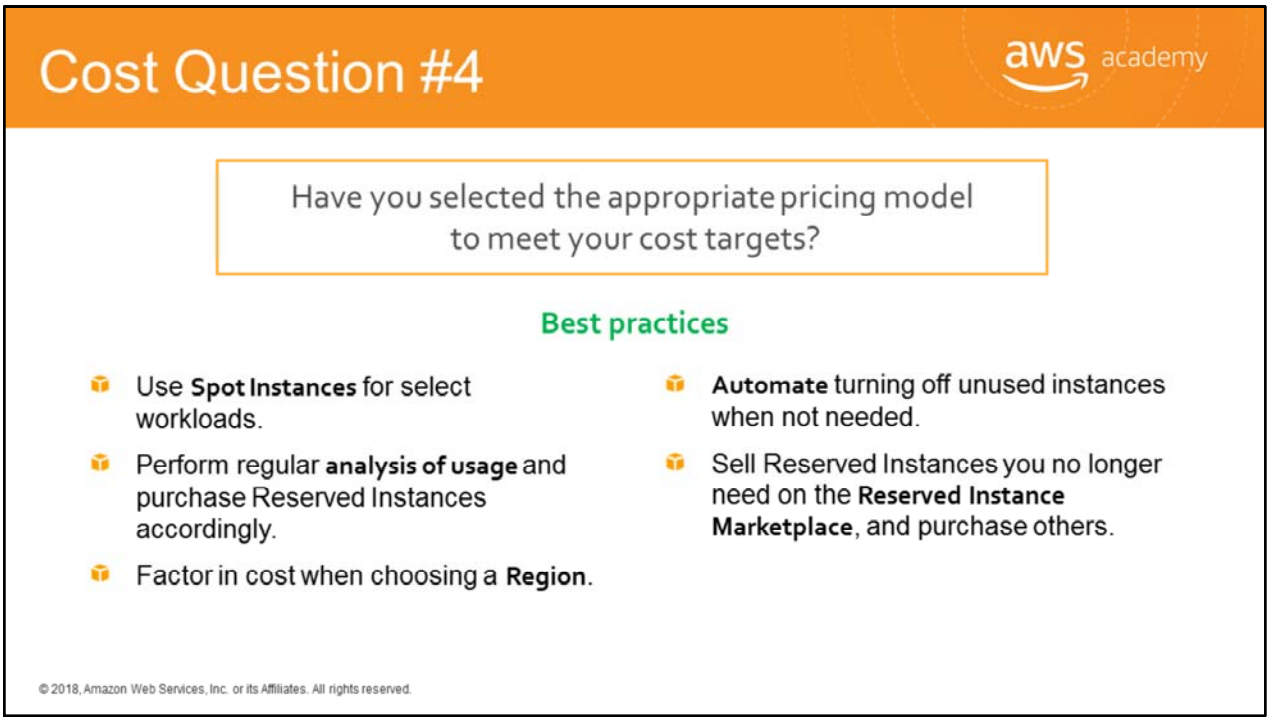
Have you selected the appropriate resources to meet your cost targets?

Best practices

- Match your **instance profile** based on need (compute, memory, storage).
- Determine appropriate instance types using **third-party products** such as CopperEgg or New Relic.
- Determine processor load using **Amazon CloudWatch**.
- Load custom memory scripts and inspect memory usage using Amazon CloudWatch **custom metrics**.
- **Profile your application** to know which type of Amazon EBS volume to use, such as magnetic, general purpose (SSD), or provisioned IOPS.

Have you selected the appropriate resources to meet your cost targets?

Take a moment to review some best practices.



Cost Question #4

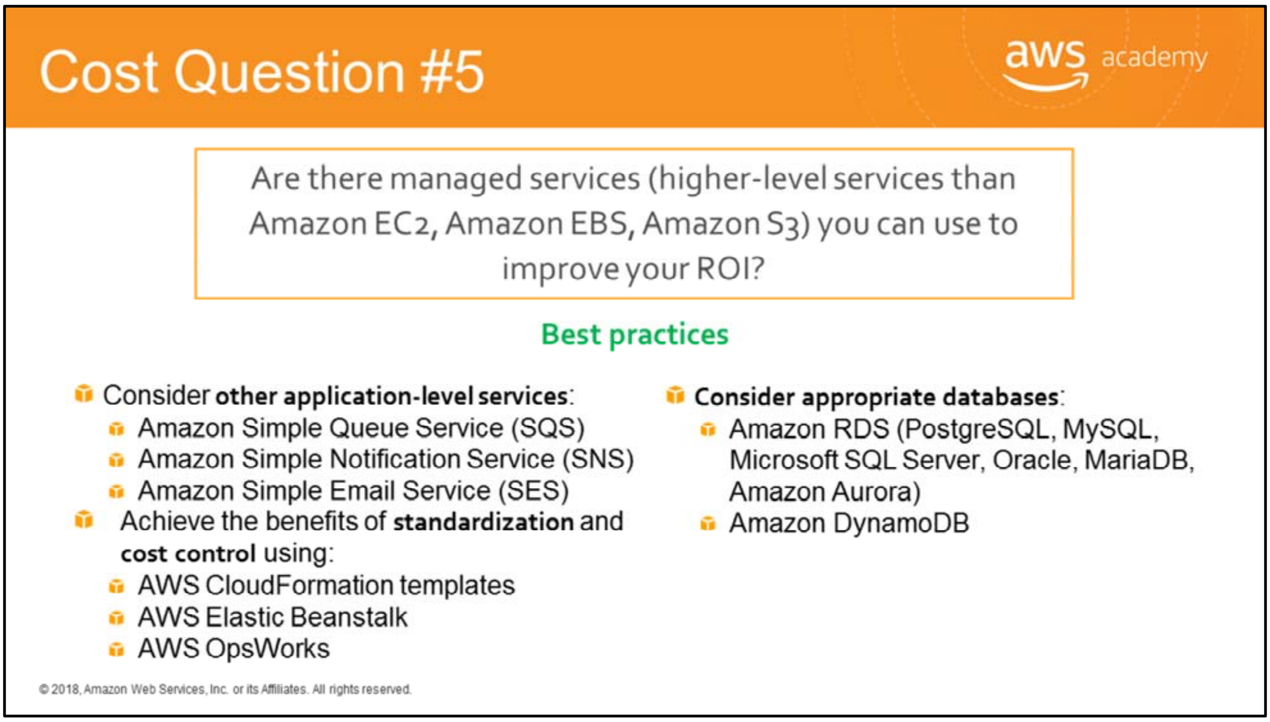
Have you selected the appropriate pricing model to meet your cost targets?

Best practices

- Use **Spot Instances** for select workloads.
- Perform regular **analysis of usage** and purchase Reserved Instances accordingly.
- Factor in cost when choosing a **Region**.
- **Automate** turning off unused instances when not needed.
- Sell Reserved Instances you no longer need on the **Reserved Instance Marketplace**, and purchase others.

Have you selected the appropriate pricing model to meet your cost targets?

Take a moment to review some best practices.



Cost Question #5

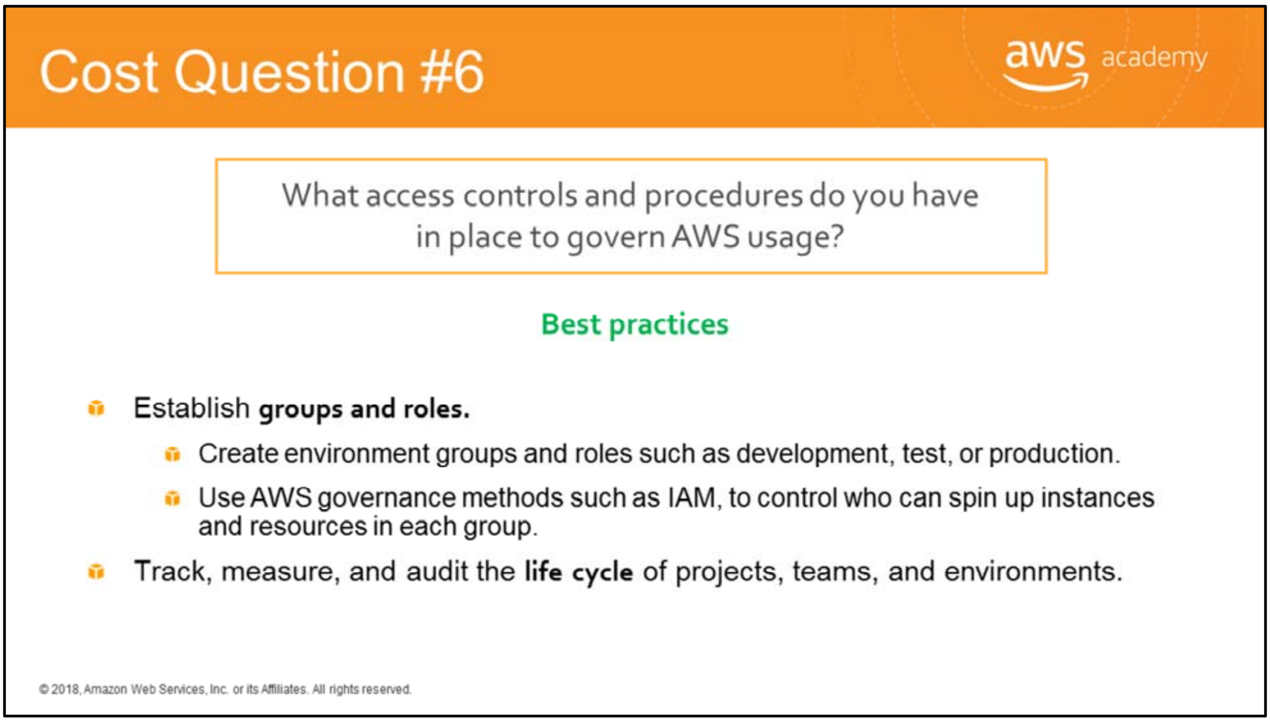
Are there managed services (higher-level services than Amazon EC2, Amazon EBS, Amazon S3) you can use to improve your ROI?

Best practices

- Consider **other application-level services**:
  - Amazon Simple Queue Service (SQS)
  - Amazon Simple Notification Service (SNS)
  - Amazon Simple Email Service (SES)
- Achieve the benefits of **standardization** and **cost control** using:
  - AWS CloudFormation templates
  - AWS Elastic Beanstalk
  - AWS OpsWorks
- **Consider appropriate databases**:
  - Amazon RDS (PostgreSQL, MySQL, Microsoft SQL Server, Oracle, MariaDB, Amazon Aurora)
  - Amazon DynamoDB

Can you use managed services—that is, services that run at a higher level than Amazon EC2, Amazon EBS, and Amazon S3—to improve your ROI?

Take a moment to review some best practices.



Cost Question #6

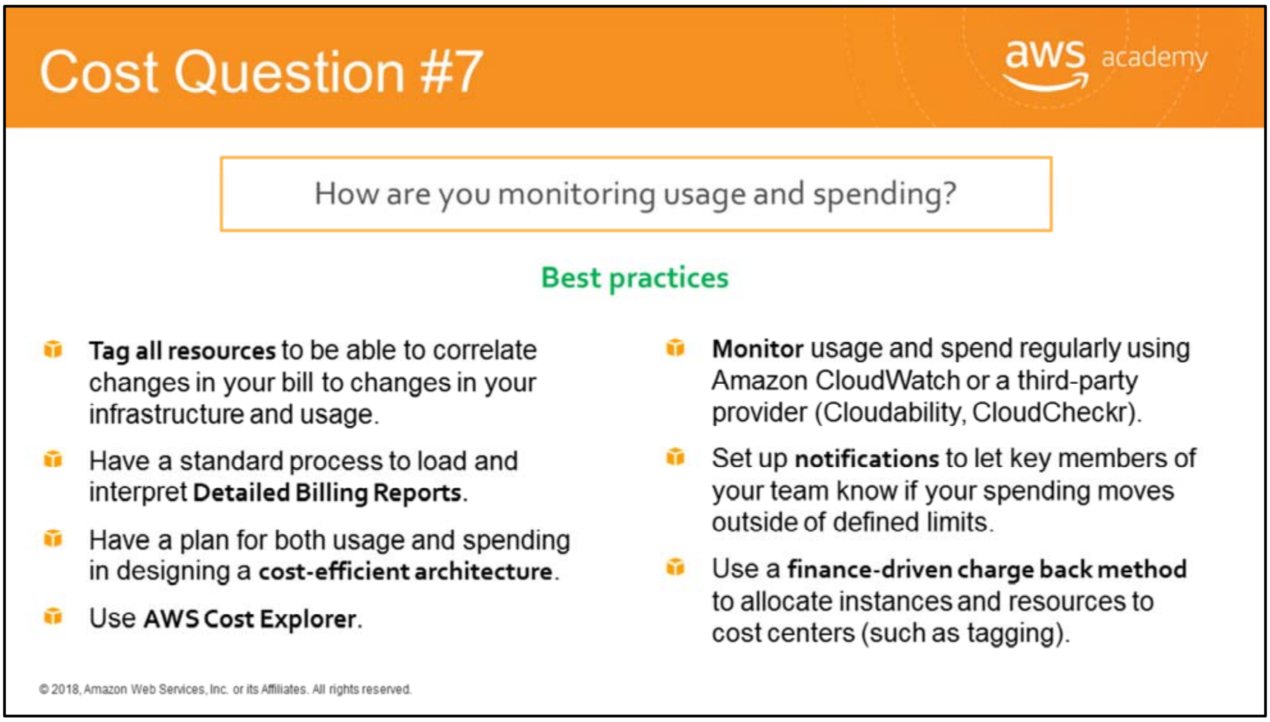
What access controls and procedures do you have in place to govern AWS usage?

Best practices

- Establish **groups and roles.**
  - Create environment groups and roles such as development, test, or production.
  - Use AWS governance methods such as IAM, to control who can spin up instances and resources in each group.
- Track, measure, and audit the **life cycle** of projects, teams, and environments.

What access controls and procedures do you have in place to govern AWS usage?

Take a moment to review some best practices.



Cost Question #7

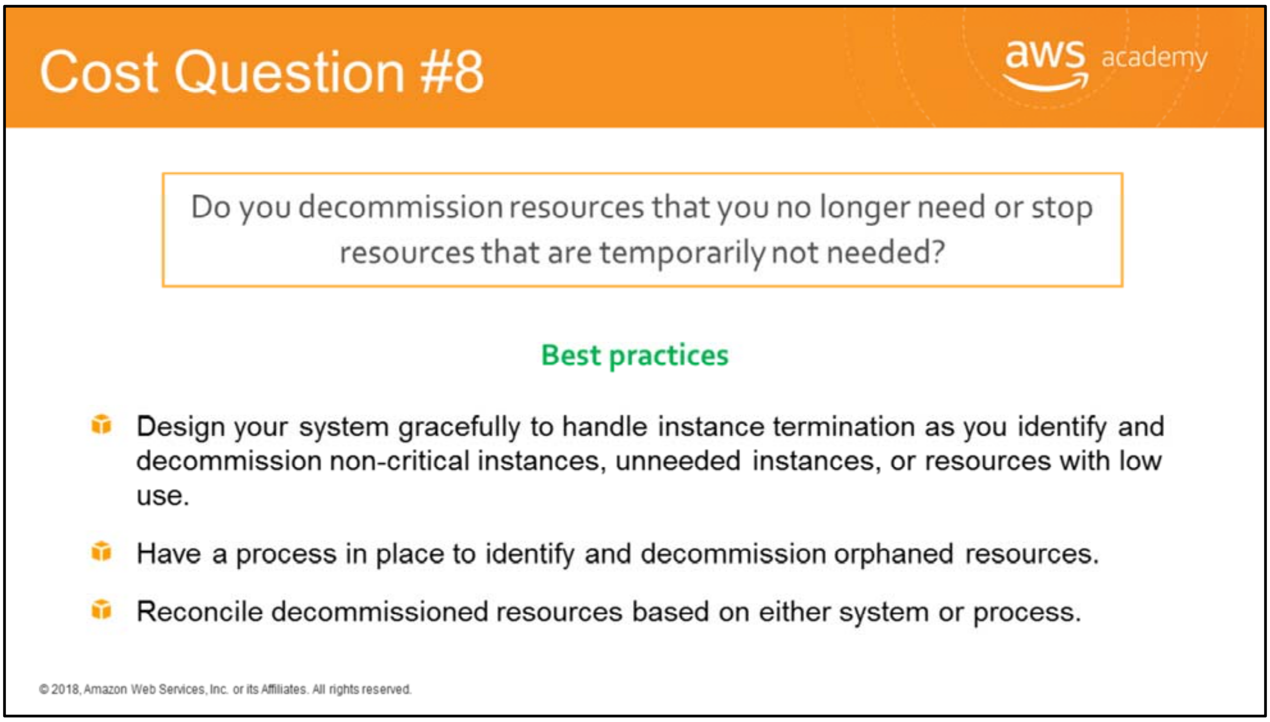
How are you monitoring usage and spending?

Best practices

- **Tag all resources** to be able to correlate changes in your bill to changes in your infrastructure and usage.
- Have a standard process to load and interpret **Detailed Billing Reports**.
- Have a plan for both usage and spending in designing a **cost-efficient architecture**.
- Use **AWS Cost Explorer**.
- **Monitor** usage and spend regularly using Amazon CloudWatch or a third-party provider (Cloudability, CloudCheckr).
- Set up **notifications** to let key members of your team know if your spending moves outside of defined limits.
- Use a **finance-driven charge back method** to allocate instances and resources to cost centers (such as tagging).

How are you monitoring usage and spending?

Take a moment to review some best practices.



Cost Question #8

aws academy

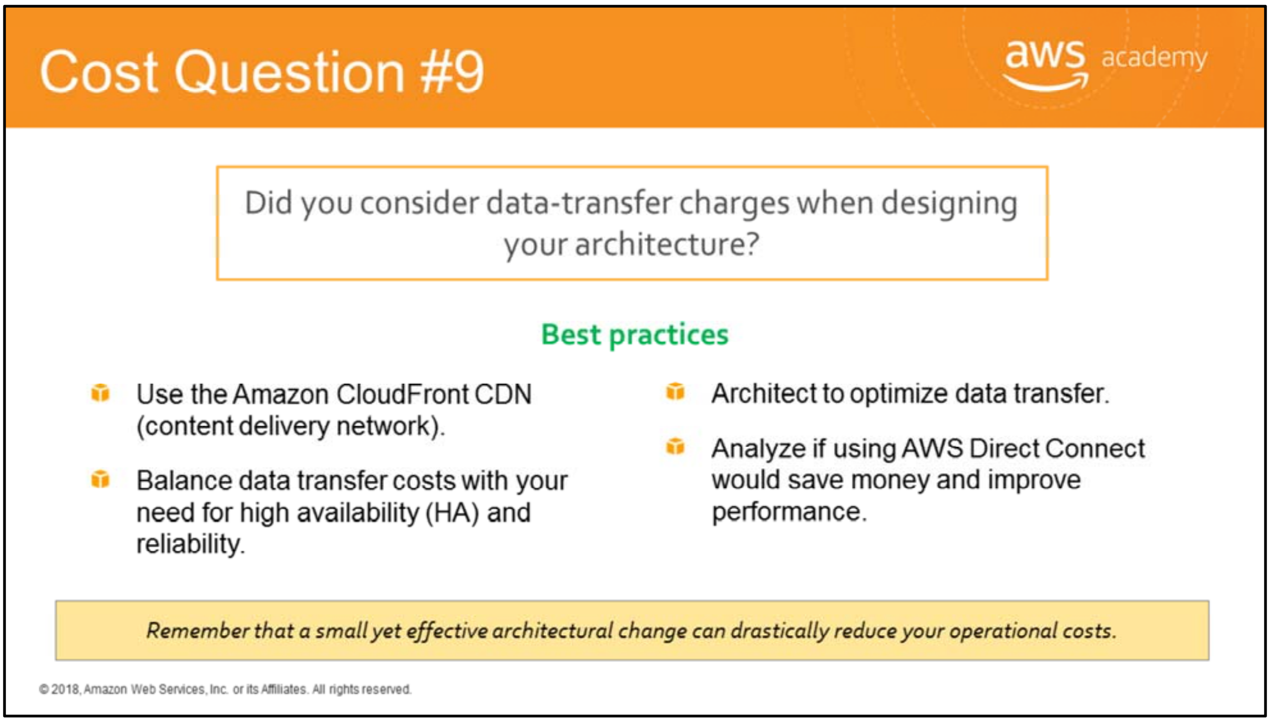
Do you decommission resources that you no longer need or stop resources that are temporarily not needed?

Best practices

- Design your system gracefully to handle instance termination as you identify and decommission non-critical instances, unneeded instances, or resources with low use.
- Have a process in place to identify and decommission orphaned resources.
- Reconcile decommissioned resources based on either system or process.

Do you decommission resources that you no longer need, or stop resources that are temporarily not needed?

Take a moment to review some best practices.



Cost Question #9

Did you consider data-transfer charges when designing your architecture?

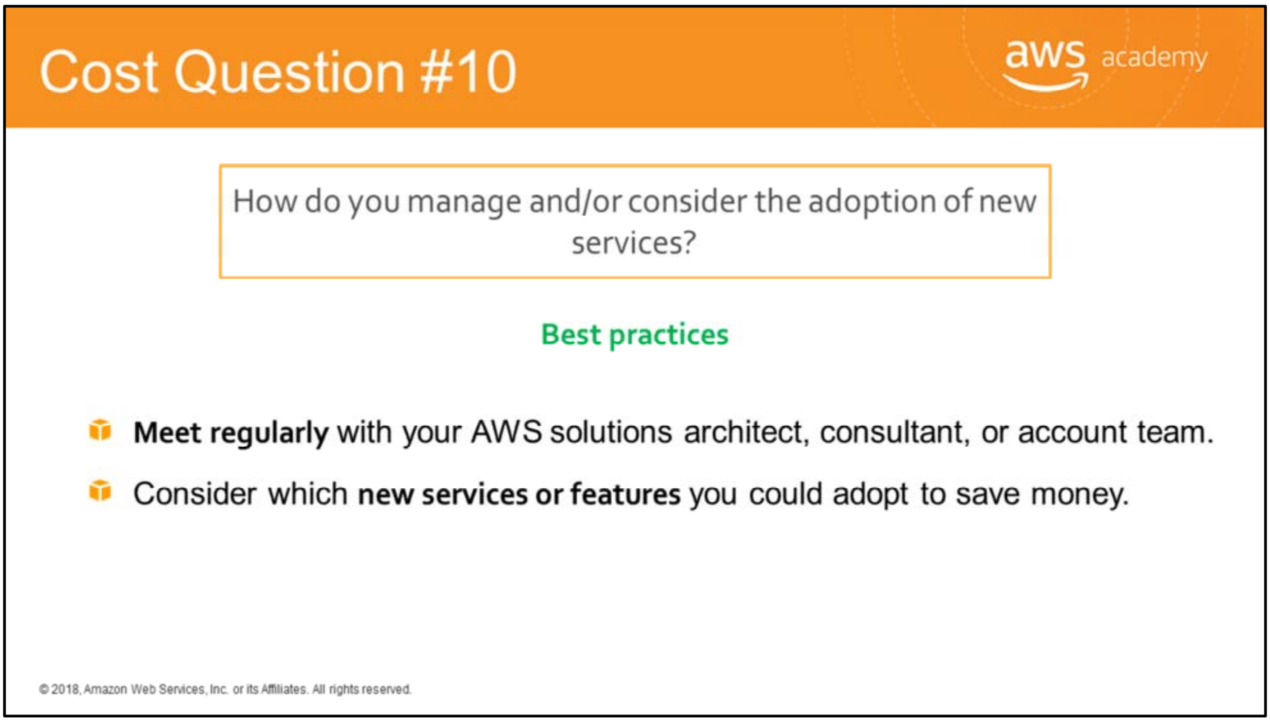
Best practices

- Use the Amazon CloudFront CDN (content delivery network).
- Balance data transfer costs with your need for high availability (HA) and reliability.
- Architect to optimize data transfer.
- Analyze if using AWS Direct Connect would save money and improve performance.

Remember that a small yet effective architectural change can drastically reduce your operational costs.

Did you consider data-transfer charges when you design your architecture?

Take a moment to review some best practices.



Cost Question #10

aws academy

How do you manage and/or consider the adoption of new services?

Best practices

- **Meet regularly** with your AWS solutions architect, consultant, or account team.
- Consider which **new services or features** you could adopt to save money.

How do you manage or consider the adoption of new services?

Take a moment to review some best practices.