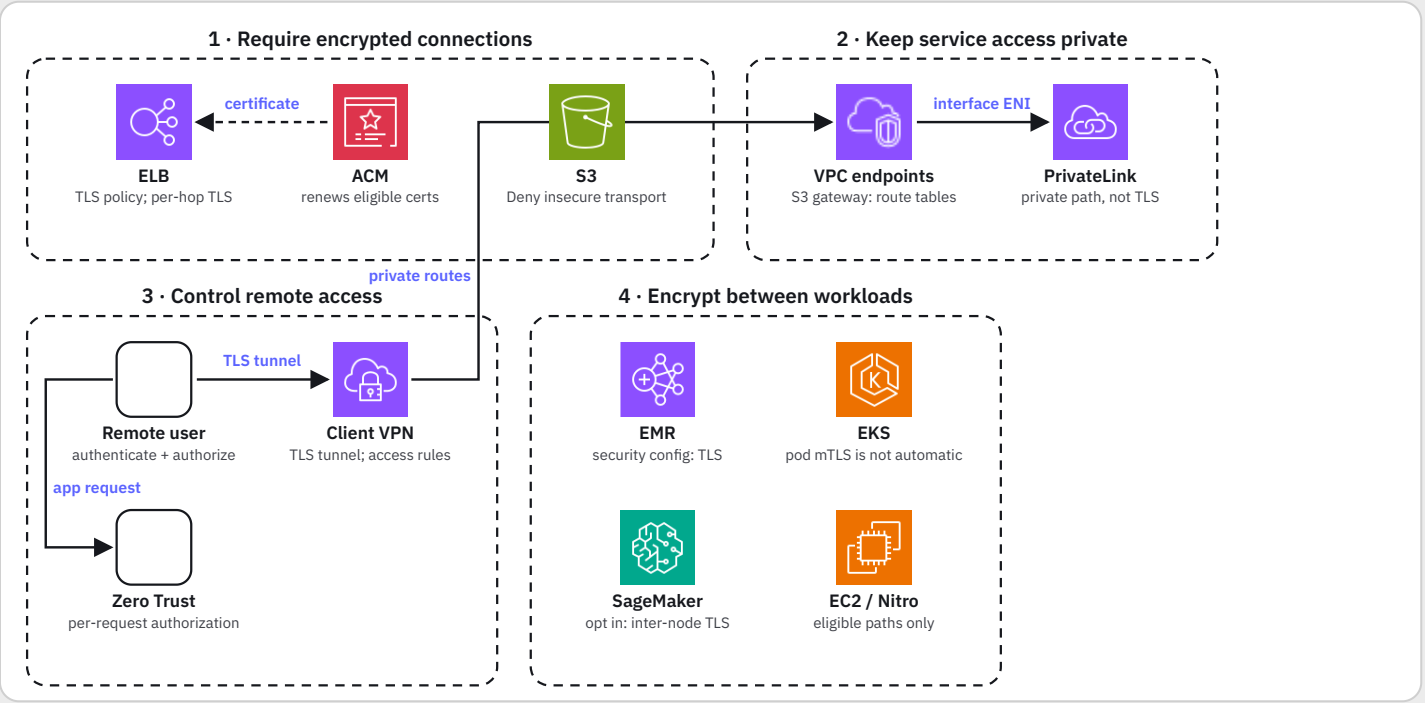
DOMAIN 5 · DATA PROTECTION · 18% OF THE EXAM · TASK STATEMENT 5.1

Design and implement controls for data in transit

Enforce TLS, privatize, authenticate, encrypt



1 Require encrypted connections

Require **TLS** with listener security policies and S3 explicit Deny conditions. Encrypt the target hop separately. ACM renews eligible issued certificates; imported certificates require external renewal.

2 Keep service access private

Choose **interface endpoints** for PrivateLink; S3 also supports gateway endpoints. Private routing does not enforce encryption. Endpoint policies restrict resource access, not TLS versions.

3 Control remote access

Choose Client VPN for **network access**; routes and authorization rules are both required. AWS Verified Access provides application access without a VPN, using identity and device context.

4 Encrypt between workloads

Configure **inter-node encryption** through EMR security configurations, SageMaker job settings, and EKS workload TLS/mTLS. Nitro automatically encrypts supported instance-to-instance paths, not every network hop.

Exam traps

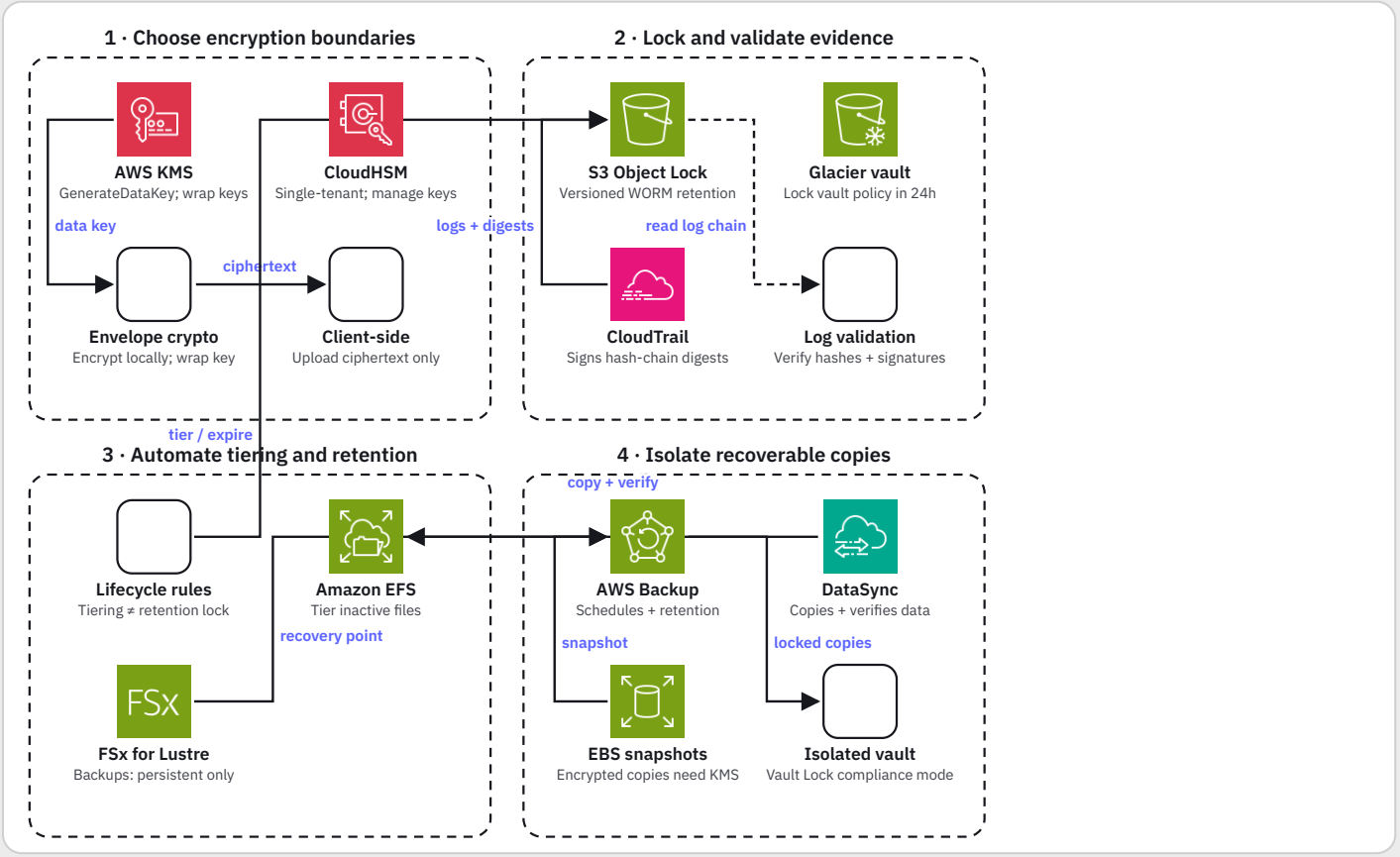
- **HTTPS at the load balancer** does not encrypt the backend hop. Configure HTTPS/TLS to targets separately; frontend security policies govern client connections.
- **aws:SecureTransport=false** denies HTTP to S3; it does not set a minimum TLS version. Use s3:TlsVersion for version restrictions, with appropriate AWS service-principal exceptions.
- **mTLS authenticates both peers**, not their permissions. Certificate trust, expiry, and rotation still matter; authorization remains a separate control.

Get practice exams and lessons for AWS Certified Security - Specialty

DOMAIN 5 · DATA PROTECTION · TASK STATEMENT 5.2

Design and implement controls for data at rest

Encrypt, preserve, tier, isolate



1 Choose encryption boundaries

Choose **client-side encryption** when the storage service must not receive plaintext; server-side encryption operates inside the service. KMS manages key access; CloudHSM provides customer-controlled, single-tenant HSMs.

2 Lock and validate evidence

Choose **compliance mode** for retention that even root cannot bypass; governance permits authorized bypass. Legal holds have no expiry and require explicit removal. Finalized Glacier Vault Lock policies cannot change.

3 Automate tiering and retention

Use **lifecycle policies** to transition/expire S3 objects or tier EFS files; they do not enforce immutable retention. AWS Backup schedules supported FSx for Lustre persistent file-system backups; scratch has no backups.

4 Isolate recoverable copies

For **ransomware recovery**, copy backups across accounts/Regions, isolate administrators and keys, and apply Backup Vault Lock compliance mode. Test restores; DataSync replication alone is not a retained recovery point.

Exam traps

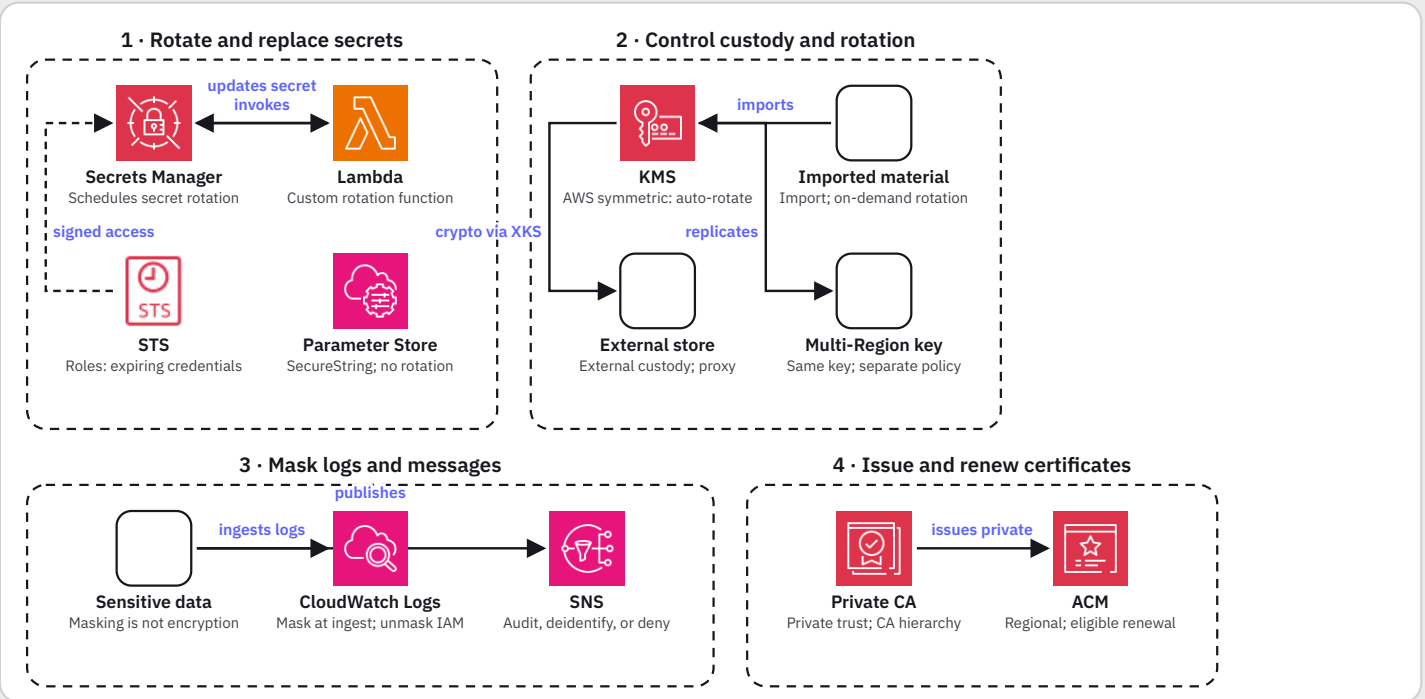
- **Glacier Vault Lock** applies to Glacier vaults, not S3 Glacier storage classes; S3 objects need Object Lock. Versioning alone is not WORM.
- CloudTrail **log file integrity validation** delivers signed digest files; checking them is not automatic. Validation detects tampering but does not prevent deletion.
- **Backup Vault Lock compliance mode** becomes immutable only after its grace period. Immutable backups still become unrecoverable if their required encryption keys are deleted.

Get practice exams and lessons for AWS Certified Security - Specialty

DOMAIN 5 · DATA PROTECTION · TASK STATEMENT 5.3

Design and implement controls to protect confidential data, credentials, secrets, and cryptographic key materials

Rotate, isolate, mask, certify



1 Rotate and replace secrets

Prefer **temporary credentials** through roles over access keys. Secrets Manager coordinates stored-secret rotation with the target; Lambda handles custom rotation. SecureString has no native secret rotation.

2 Control custody and rotation

BYOK imports material into KMS; XKS keeps material external and adds an availability dependency. Imported symmetric keys support on-demand, not automatic, rotation. Replicas require importing the same material in each Region.

3 Mask logs and messages

Use **data protection policies** to limit exposure. CloudWatch Logs masks newly ingested events; logs:Unmask reveals originals. SNS Standard topics can audit, de-identify, or deny messages at inbound and outbound boundaries.

4 Issue and renew certificates

Managed renewal applies to eligible ACM certificates, including ACM-requested private certificates. Certificates issued directly by Private CA need separate renewal automation. Private CA does not create public trust.

Exam traps

- **Rotation is not re-encryption**: KMS uses fresh material for new encryption and retains older material for decryption. Secret rotation must also update the target credential and accommodate consumers.
- **Imported is not external**: BYOK material resides in KMS. Expired or deleted imported material makes dependent ciphertext unusable until the original material is reimported; a new key cannot replace it.
- **Multi-Region is not global**: KMS replicas share material, not policies or grants. ACM certificates are regional; CloudFront requires its ACM certificate in us-east-1.

Get practice exams and lessons for AWS Certified Security - Specialty

DOMAIN 5 · DATA PROTECTION · WHAT TO REMEMBER

Concepts and services of Data Protection

Concepts to know

Key Management

Key management governs key generation, access, rotation, and recovery. **Custody and availability requirements** determine whether AWS-generated material, imported material, or an external key store fits; losing required key material can make data unrecoverable.

Transport Layer Security

TLS encrypts connections and authenticates peers through certificates. **Protect every required hop**: load balancer termination does not encrypt backend traffic, and private connectivity does not itself enforce TLS.

Write Once, Read Many (WORM) Storage

WORM prevents retained records from being overwritten or deleted. **Bypass requirements determine the retention mode**: governance permits authorized bypass; compliance prevents early deletion even by root. Legal holds have no fixed expiration.

Core services



AWS Key Management Service (AWS KMS)

Choose **customer managed keys** for control over key policies, grants, and lifecycle. Multi-Region keys support cross-Region cryptographic use; policies and grants remain independently managed.



Amazon S3

Use **Object Lock** for immutable object versions, not lifecycle rules or versioning alone. Bucket policies can deny non-TLS requests; SSE-KMS adds KMS authorization to object access.



AWS Secrets Manager

Choose **managed secret rotation** for supported credentials; Lambda handles custom rotation workflows. Use role-based temporary credentials instead of storing long-lived AWS access keys.

Get practice exams and lessons for AWS Certified Security - Specialty