AWS Certified Solutions Architect - Professional Cheat Sheet

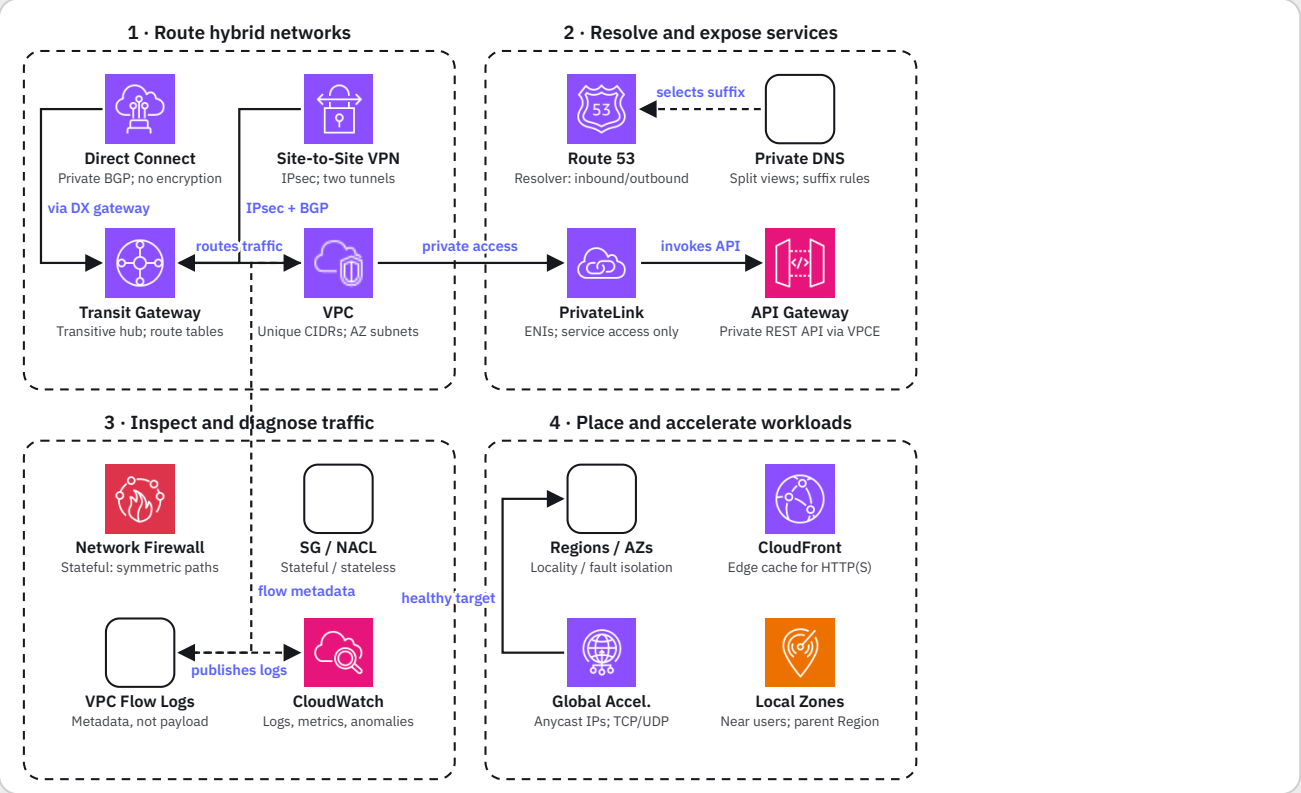
SAP-C02 · Domain 1 of 4

BlowStack

DOMAIN 1 · DESIGN SOLUTIONS FOR ORGANIZATIONAL COMPLEXITY · 26% OF THE EXAM · TASK STATEMENT 1.1

Architect network connectivity strategies

Connect, resolve, inspect, localize



1 Route hybrid networks

Choose **Transit Gateway** for many routed networks; separate route tables isolate spokes only when associations and propagation enforce it. Direct Connect reaches the hub through a Direct Connect gateway.

2 Resolve and expose services

Use **conditional forwarding**: inbound endpoints accept on-prem DNS queries; outbound endpoints forward VPC queries to on-prem DNS. PrivateLink exposes a service without opening network-wide connectivity.

3 Inspect and diagnose traffic

Preserve **symmetric routing** through stateful inspection; Transit Gateway appliance mode maintains AZ affinity. Check forward and return routes and filters. Traffic Mirroring copies packets from supported ENIs.

4 Place and accelerate workloads

Choose Regions for **data locality** and measured latency; AZs isolate failures. CloudFront caches content; Global Accelerator steers connections to healthy endpoints. Local Zones place supported compute nearer users.

Exam traps

- **Peering is nontransitive**: A–B and B–C do not connect A–C. Peering rejects overlapping CIDRs; Transit Gateway does not solve overlapping address spaces.
- **Direct Connect is not encrypted by default**. Use supported MACsec or IPsec when required. Two VPN tunnels do not replace diverse Direct Connect connections and locations.
- **PrivateLink is not peering**: it exposes services, not transit routes. Gateway endpoints serve S3/DynamoDB; endpoint policies do not replace IAM or resource-policy authorization.

Get practice exams and lessons for AWS Certified Solutions Architect - Professional

AWS Certified Solutions Architect - Professional Cheat Sheet

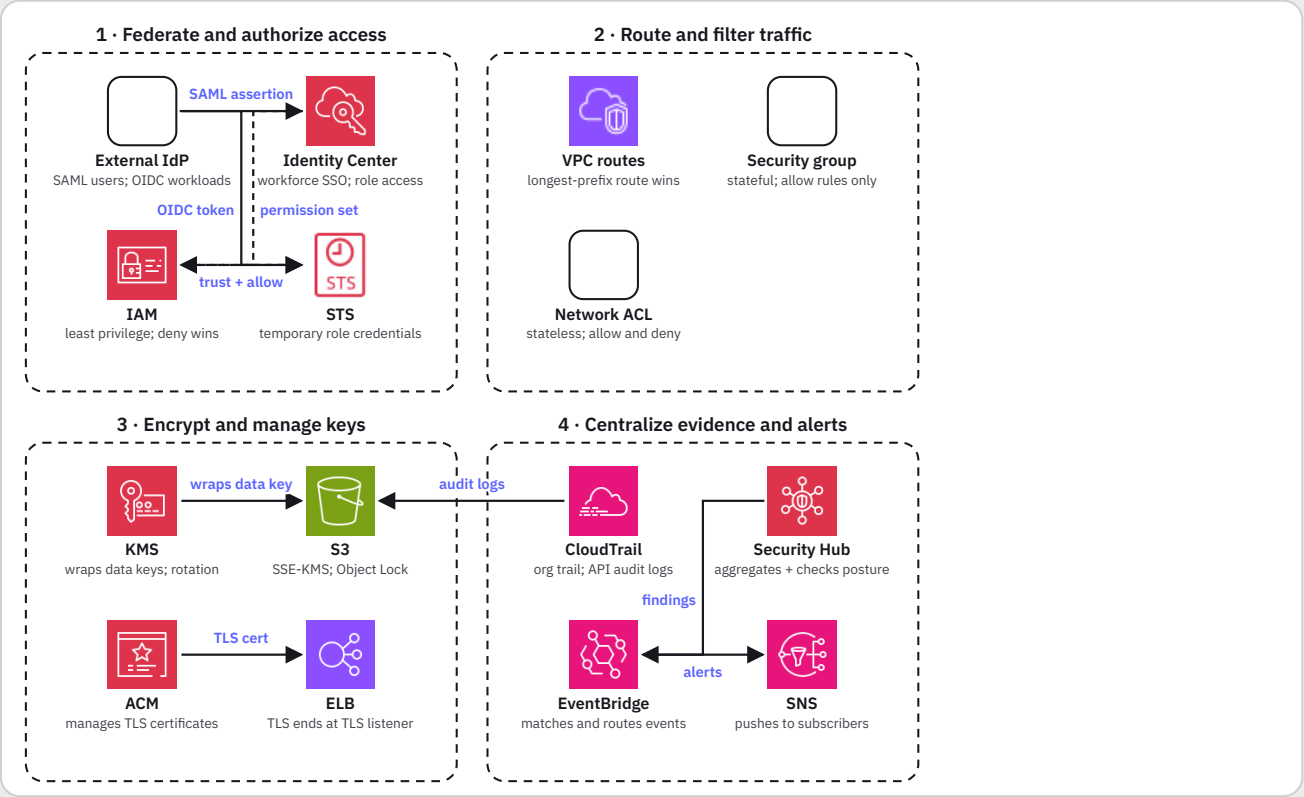
SAP-C02 · Domain 1 of 4

BlowStack

DOMAIN 1 · DESIGN SOLUTIONS FOR ORGANIZATIONAL COMPLEXITY · TASK STATEMENT 1.2

Prescribe security controls

Authorize, segment, encrypt, audit



1 Federate and authorize access

For **cross-account roles**, caller permission and role trust must allow; SCPs, boundaries and session policies limit permissions. Identity Center serves workforce access; Cognito serves application users.

2 Route and filter traffic

Use **security groups** for resource-level access; return traffic is automatic. Subnet NACLs need rules in both directions, including ephemeral ports. Routes select paths; separate subnets alone do not enforce isolation.

3 Encrypt and manage keys

Use **envelope encryption**: data keys encrypt data; KMS protects data keys. CloudHSM provides customer-controlled HSM keys; AWS Private Certificate Authority issues private certificates. Target TLS is separate from listener TLS.

4 Centralize evidence and alerts

Use **central auditing**: an organization trail delivers to a restricted S3 archive; log validation detects tampering, Object Lock enforces retention. GuardDuty detects threats; Inspector finds vulnerabilities; Hub aggregates.

Exam traps

- An **SCP grants nothing**: it limits available permissions. AWS RAM shares supported resources, not arbitrary IAM permissions; cross-account SSE-KMS access also needs authorization on the KMS key.
- Prevent the **confused deputy**: require a customer-specific ExternalId for third-party role assumption; use aws:SourceArn and aws:SourceAccount for supported AWS service-to-service requests.
- **KMS rotation does not re-encrypt existing data**; prior key material remains available for decryption. Automatic rotation applies only to eligible keys; deleting a needed key can make data unrecoverable.

Get practice exams and lessons for AWS Certified Solutions Architect - Professional

AWS Certified Solutions Architect - Professional Cheat Sheet

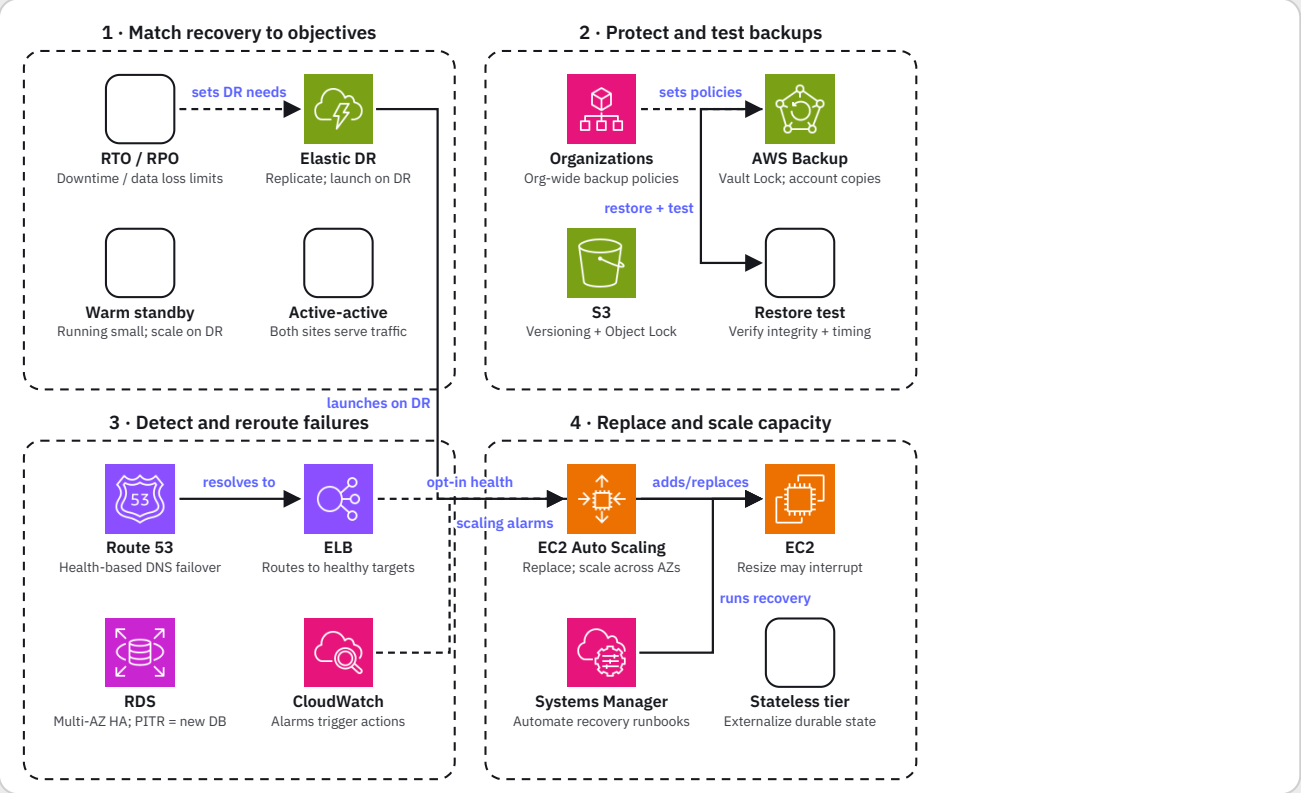
SAP-C02 · Domain 1 of 4

BlowStack

DOMAIN 1 · DESIGN SOLUTIONS FOR ORGANIZATIONAL COMPLEXITY · TASK STATEMENT 1.3

Design reliable and resilient architectures

Replicate, protect, fail over, scale



1 Match recovery to objectives

For tighter **RTO**, typically move from backup/restore to pilot light, warm standby, then active-active as cost rises. Pilot light launches servers; warm standby scales. RPO follows backup frequency or replication lag.

2 Protect and test backups

Use **isolated, immutable** recovery points against ransomware: cross-account copies, locked retention, and protected keys. Backup schedules constrain RPO; restore tests verify integrity and RTO, including application dependencies.

3 Detect and reroute failures

Use **Multi-AZ** for automatic database failover, not Regional DR. A standard RDS Multi-AZ DB instance standby cannot serve reads. Route 53 failover depends on health signals and DNS caching.

4 Replace and scale capacity

Scale out stateless tiers across AZs for capacity and fault isolation. Enable ELB health checks in Auto Scaling to replace app-unhealthy instances. Scale up has size limits and may interrupt service.

Exam traps

- **Asynchronous replication** does not guarantee zero RPO; lag can lose recent writes. Replication can also propagate corruption, so retained recovery points remain necessary.
- **RDS read replicas** scale reads; promotion is not the automatic standby failover of a standard Multi-AZ DB instance. PITR creates a new DB instance, not an in-place rewind.
- **Vault Lock compliance mode** cannot be removed after its grace period, even by root. Governance mode allows authorized removal; neither replaces protected keys and tested restores.

Get practice exams and lessons for AWS Certified Solutions Architect - Professional

AWS Certified Solutions Architect - Professional Cheat Sheet

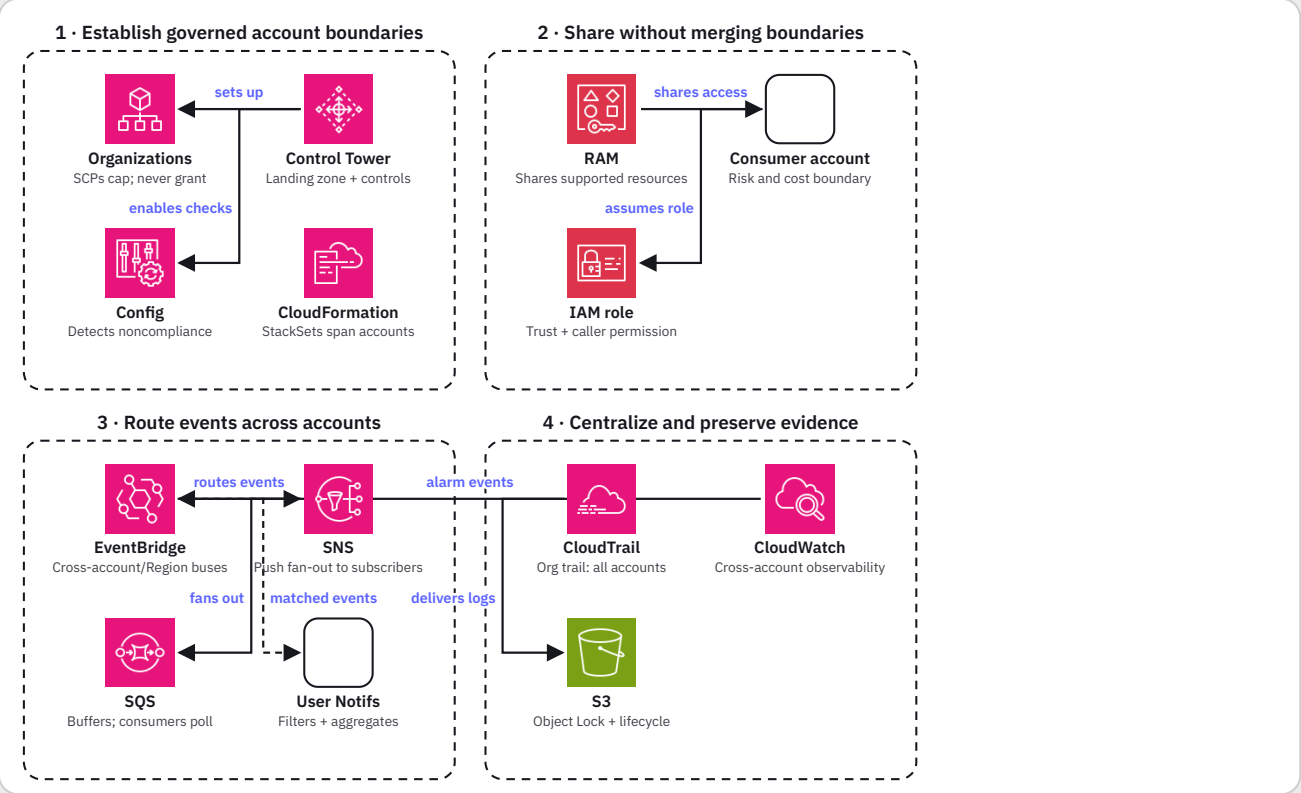
SAP-C02 · Domain 1 of 4

BlowStack

DOMAIN 1 · DESIGN SOLUTIONS FOR ORGANIZATIONAL COMPLEXITY · TASK STATEMENT 1.4

Design a multi-account AWS environment

Govern, share, route, preserve



1 Establish governed account boundaries

Control Tower automates landing-zone setup and controls. Group accounts into OUs by governance needs; separate production, nonproduction, security and logging for blast radius, separation of duties and cost allocation.

2 Share without merging boundaries

AWS RAM shares supported resources without copying; enabled organization sharing avoids invitations. Cross-account role assumption instead requires target trust and caller permission, both scoped to least privilege.

3 Route events across accounts

Cross-account events use a destination bus policy and sender role. EventBridge routes; SNS provides publish-subscribe fan-out; SQS buffers delivery. User Notifications aggregates human-facing operational alerts.

4 Centralize and preserve evidence

Audit evidence: a multi-Region organization trail delivers to central S3. Validate CloudTrail digests for tamper detection; Object Lock protects retention and lifecycle controls storage cost. Restrict log deletion.

Exam traps

- **SCP inheritance is a ceiling**: permissions must survive every hierarchy level; explicit deny wins. SCPs grant nothing and do not restrict the management account, but do restrict member-account root.
- **Detection is not prevention**: AWS Config detects deployed-resource violations; SCPs cap permissions. StackSets deploy baselines as code; AWS Service Catalog offers approved products, not OU guardrails.
- **Visibility is not storage**: CloudWatch cross-account observability does not copy logs. CloudTrail validation detects tampering; access and retention controls protect evidence against deletion.

Get practice exams and lessons for AWS Certified Solutions Architect - Professional

AWS Certified Solutions Architect - Professional Cheat Sheet

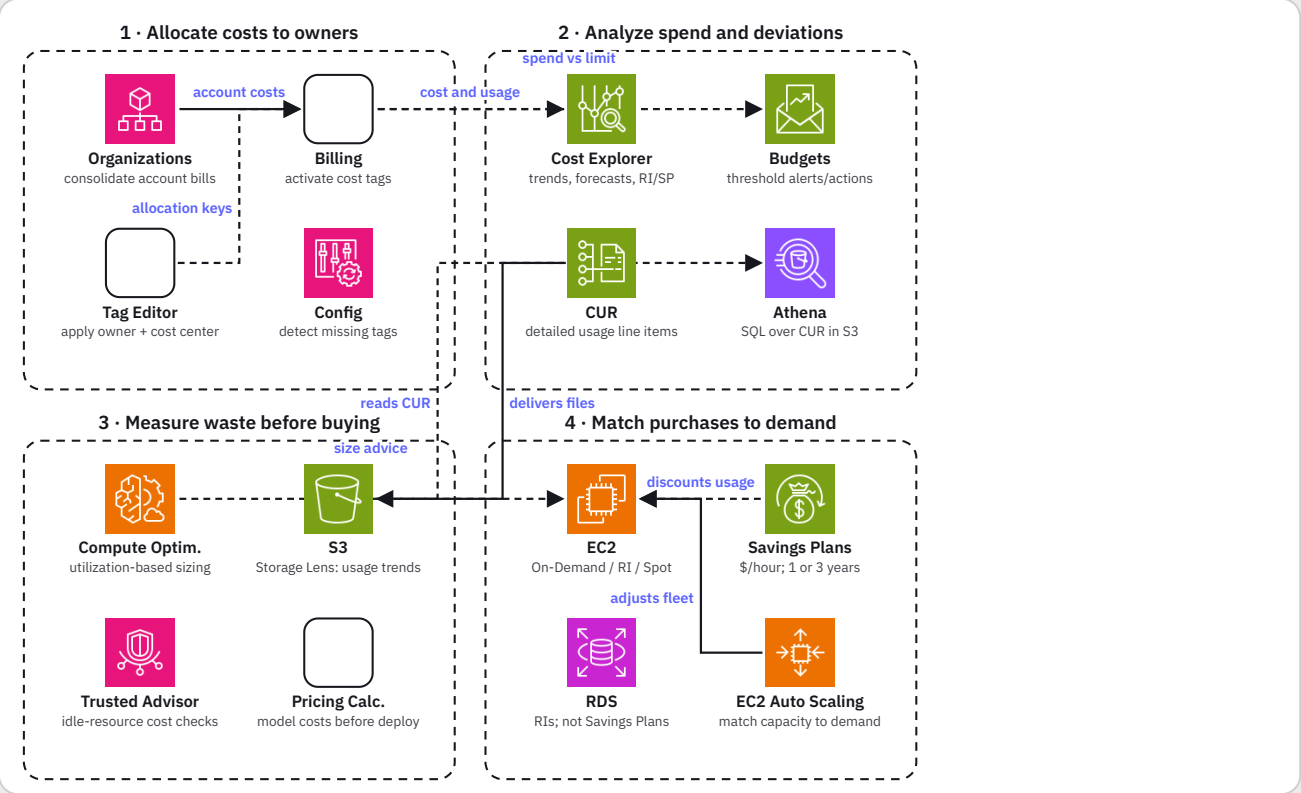
SAP-C02 · Domain 1 of 4

BlowStack

DOMAIN 1 · DESIGN SOLUTIONS FOR ORGANIZATIONAL COMPLEXITY · TASK STATEMENT 1.5

Determine cost optimization and visibility strategies

Allocate, monitor, rightsize, commit



1 **Allocate costs to owners**

Use accounts plus **activated cost allocation tags** for business-unit showback. Tag Editor applies tags; Config detects missing tags. Tag policies standardize values but do not require tags on every resource.

2 **Analyze spend and deviations**

Use **CUR + Athena** for detailed SQL analysis, Cost Explorer for trends/forecasts, and Budgets for thresholds/actions. Cost Anomaly Detection flags unexpected spend, not a fixed budget breach.

3 **Measure waste before buying**

Use **measured utilization** before commitments: Compute Optimizer recommends sizes, Trusted Advisor flags waste, Storage Lens exposes storage trends, and Pricing Calculator models alternatives. Advice does not resize.

4 **Match purchases to demand**

Commit only the **steady baseline**; use On-Demand for uncertain demand and Spot for interruption-tolerant work. Rightsize first; compare cost per useful work at required performance, not hourly price.

Exam traps

- **Budgets is not a hard spending cap**: alerts can lag, and actions require configuration. A threshold does not automatically stop all resources or prevent further charges.
- **Tags are not retroactive**: applying a tag alone does not allocate historical charges. Activate cost allocation tags for billing use; account boundaries still identify untagged account spend.
- **Discount is not capacity**: Savings Plans and regional EC2 RIs do not reserve capacity. Zonal EC2 RIs include capacity reservation; unused commitments still cost money.

Get practice exams and lessons for AWS Certified Solutions Architect - Professional

AWS Certified Solutions Architect - Professional Cheat Sheet

SAP-C02 · Domain 1 of 4

BlowStack

DOMAIN 1 · DESIGN SOLUTIONS FOR ORGANIZATIONAL COMPLEXITY · WHAT TO REMEMBER

Concepts and services of Design Solutions for Organizational Complexity

Concepts to know

Cross-Account Access

Account boundaries require explicit authorization. **Role assumption** requires the target role's trust policy and caller authorization; resource policies support direct access where the service permits it.

Transitive Routing

Connectivity from A to B and B to C does not imply A can reach C. **VPC peering is nontransitive**; many-to-many connectivity favors a transit hub with explicit routes and segmentation.

Policy Inheritance

Organizational policies apply through the root, OU, and account hierarchy. **SCPs limit permissions; they do not grant them**. Member-account access must remain within every applicable SCP boundary, including for root users.

Core services



AWS Organizations

Use **OUs and SCPs** for centrally governed account groups and permission ceilings. Consolidated billing combines charges; account boundaries separate workload ownership and blast radius.



AWS Transit Gateway

Choose a **regional transit hub** for many VPCs and hybrid networks. Separate route tables isolate spokes; associations and propagation determine connectivity, not attachment alone.



AWS Identity and Access Management (IAM)

Choose **cross-account roles** for delegated access without shared long-term credentials. Trust policies identify who can assume a role; permissions policies define what its sessions can do.

Get practice exams and lessons for AWS Certified Solutions Architect - Professional