3.6

Saturday, September 23, 2023 6:41 PM

Cloud vulnerable to remote access

auto services will use APIs

- assign secret keys for prog access
- 3rd party pword manager to store secret keys

external takeover and remote access

IAM apparently won't help

Zone-redundant storage - replicates data across mult data centers in 1 or 2 regions

regional replication

High availability

Geo redundant storage GRS - replicates data to secondary region far from primary

NGSWG - content filters, threat anal, DLP

Dynamic resource allocation - on-demand service capabilities that CSP provides can create virtual instance and containers

Security groups - stateful inbound/out

Filtering at layer 4

allow established and related traffic if a new connection has been accepted

CASB - monitors network traffic between org and CSP

- control over mobile access to org apps

- SSO
- support for multi device

Container namespaces - prevent one container from reading or writing processes in another

using multiple VPCs allows for greater degree of segmentation between instances rather than subnets

VPC endpoint - publish service accessible by instances in other VPCs using AWS internal network and Private IP

PrivateLink for private access

instance awareness - tracking all instances so keep management

Storage policy permission in JSON

* for action and principle

all users read/write

gives all users read/write