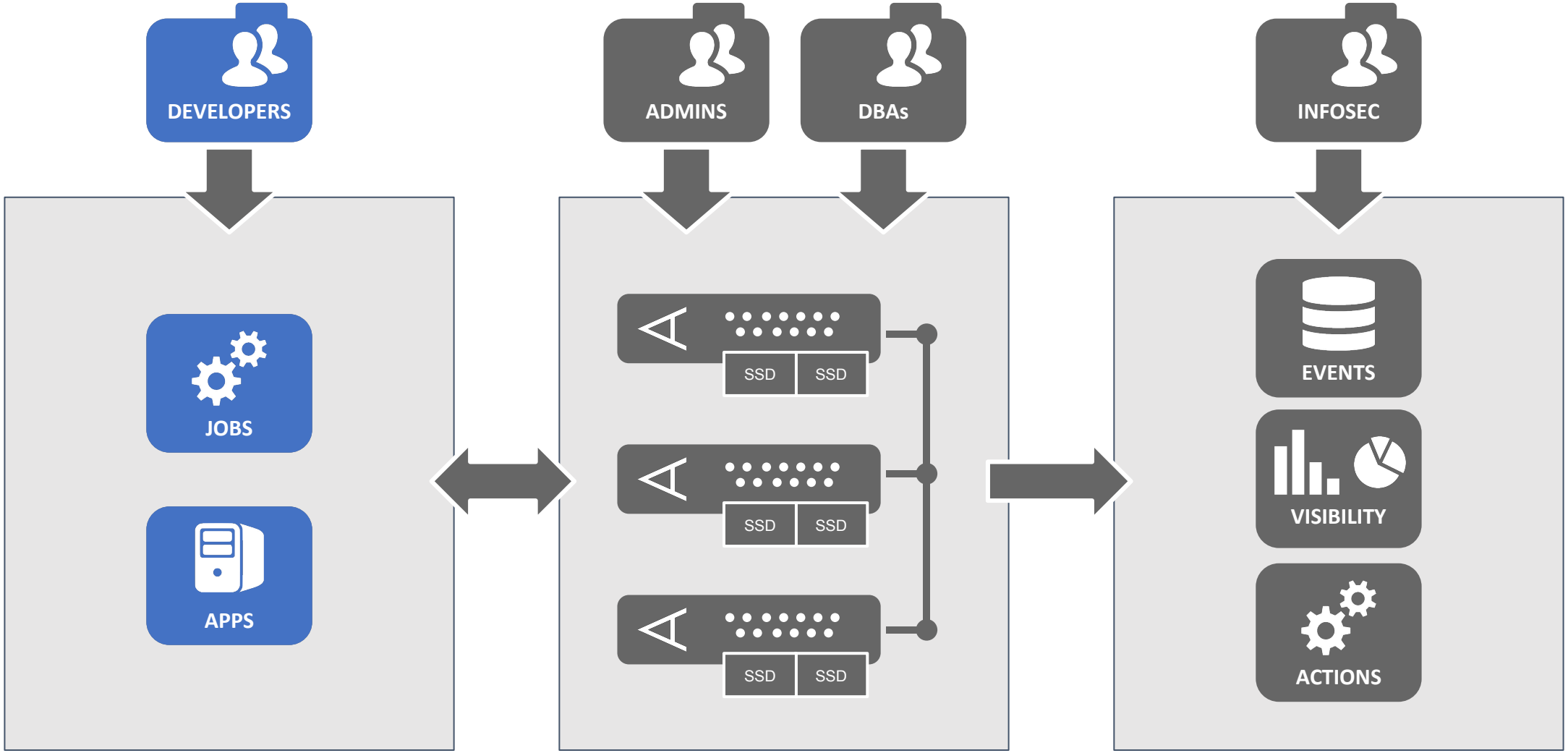
AEROSPIKE

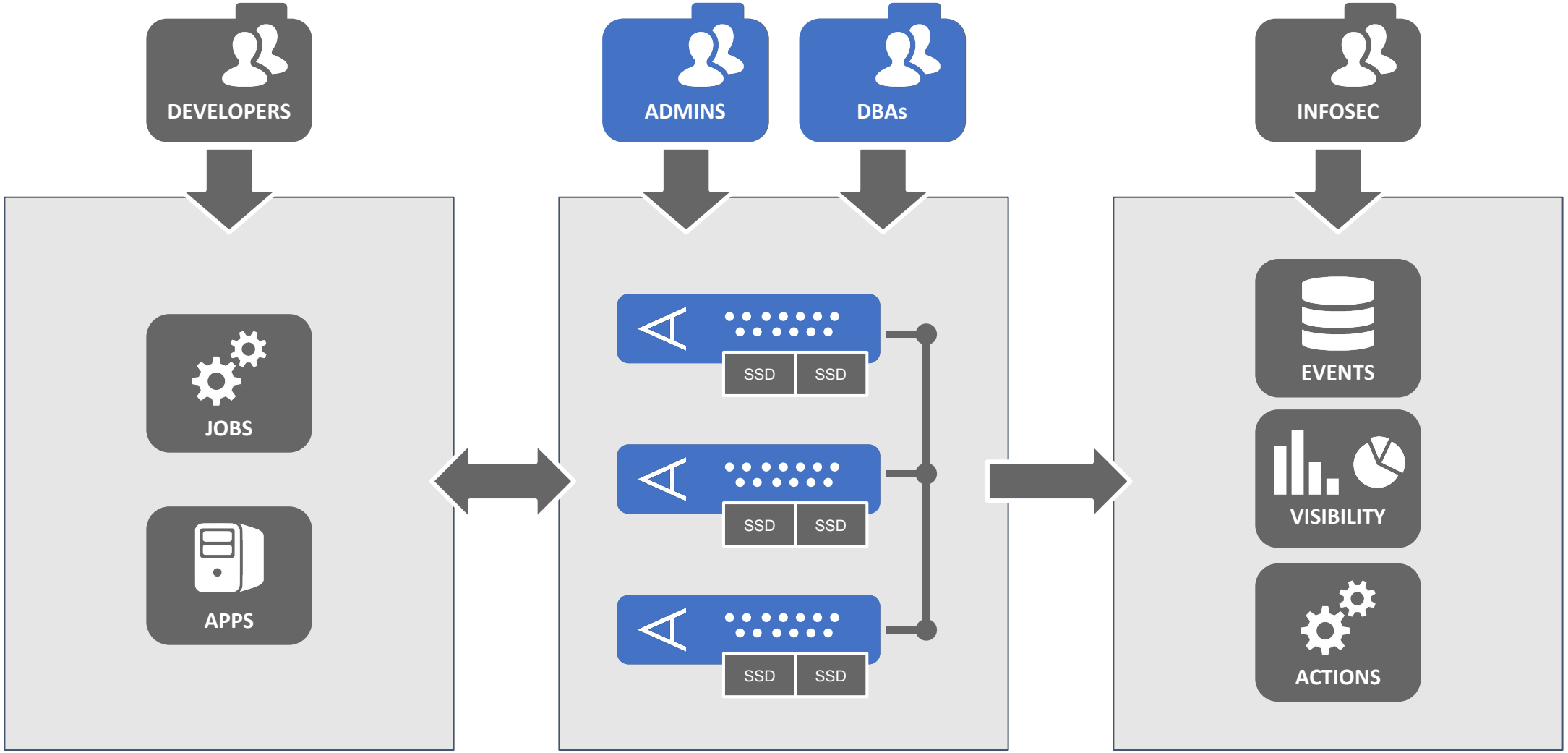
NEXTGEN NOW SUMMIT '20

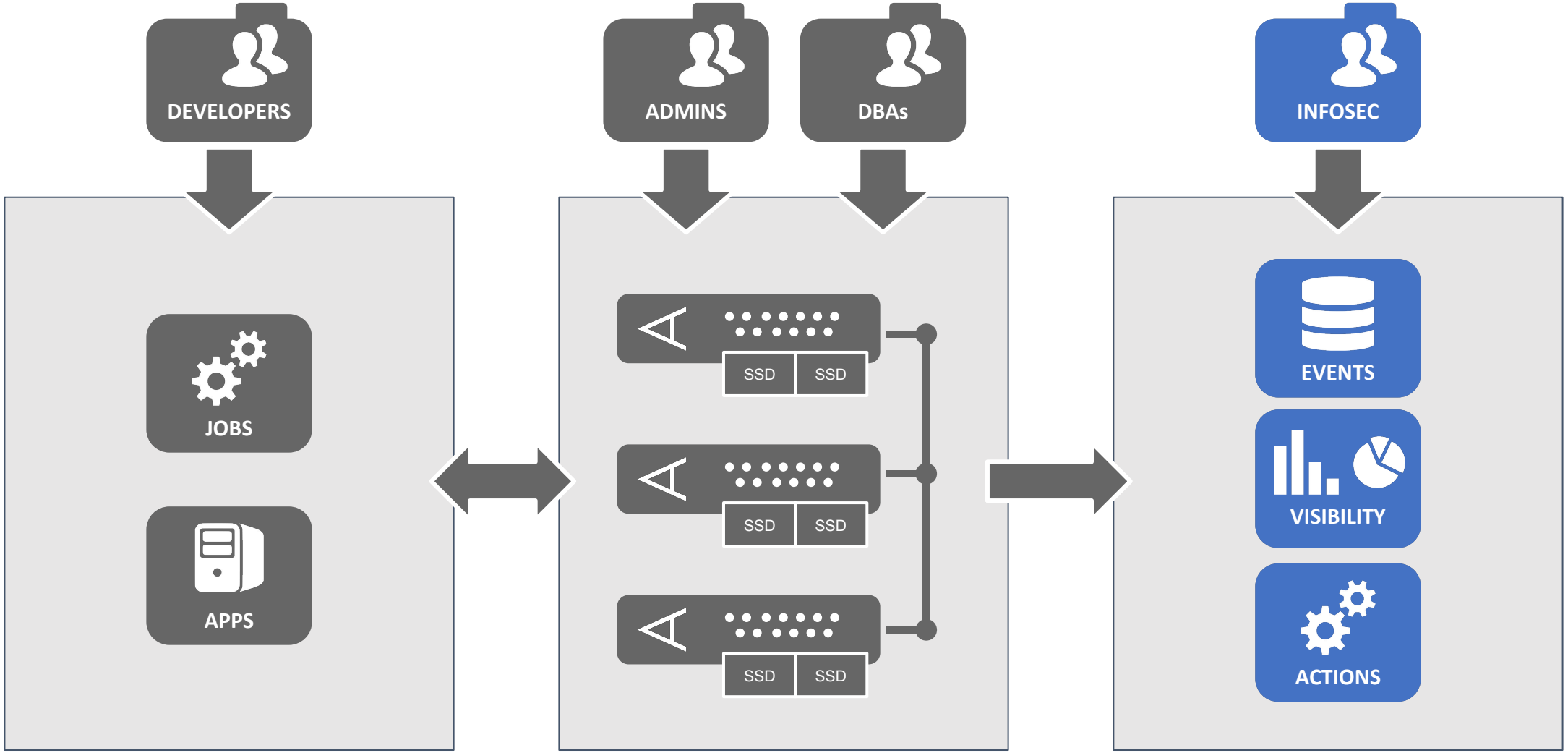
Enterprise Database Security

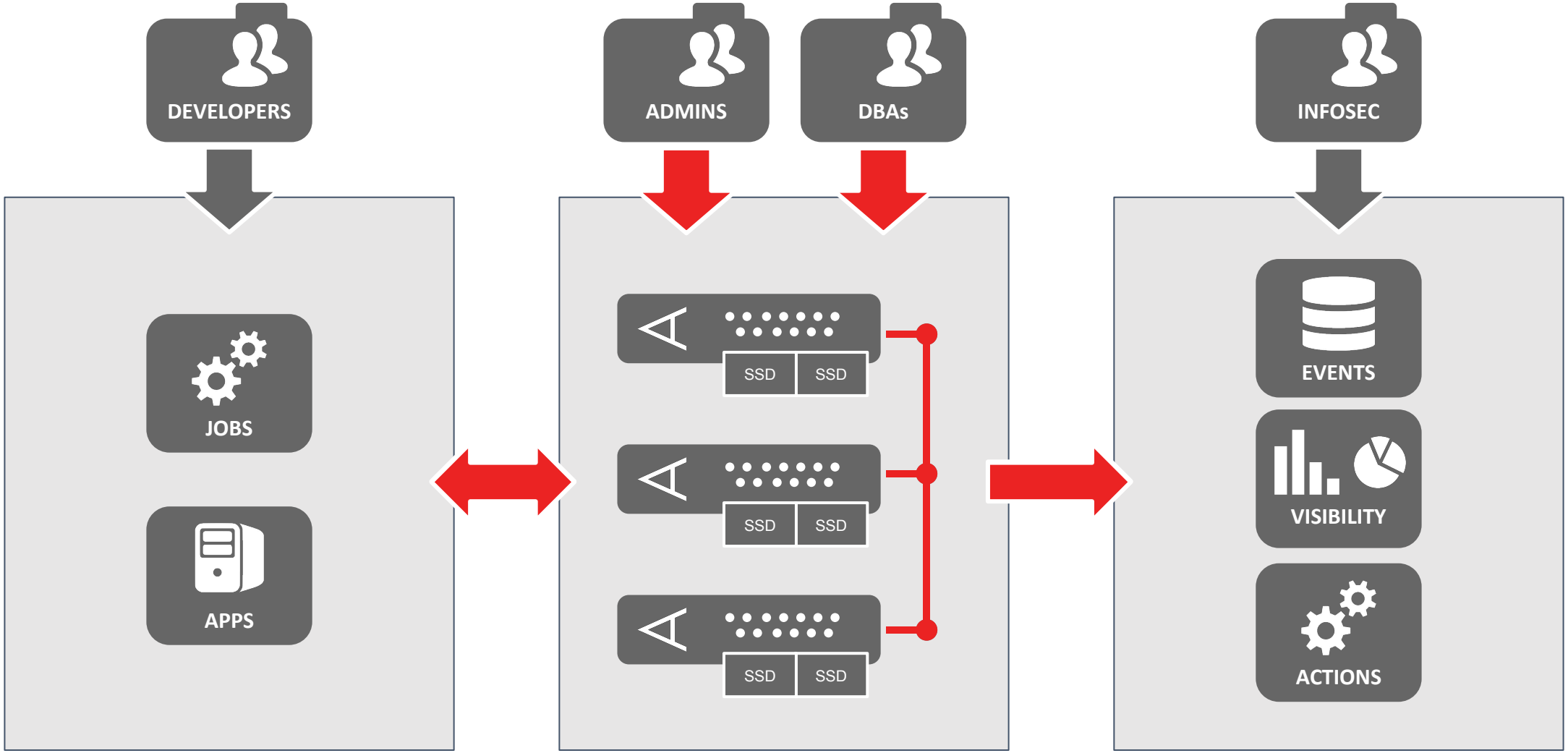
AEROSPIKE

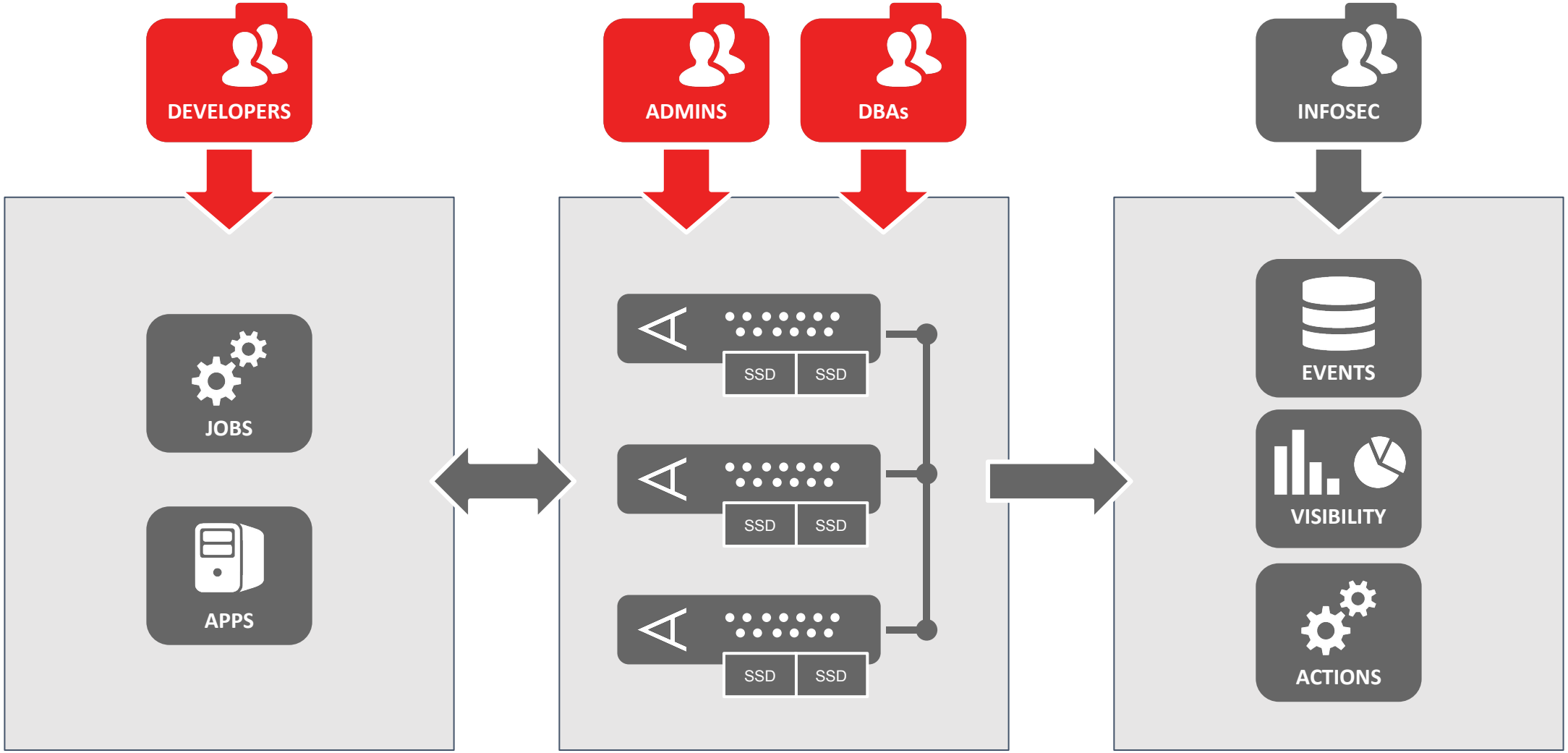
Micah Carrick
Consulting Director
AEROSPIKE

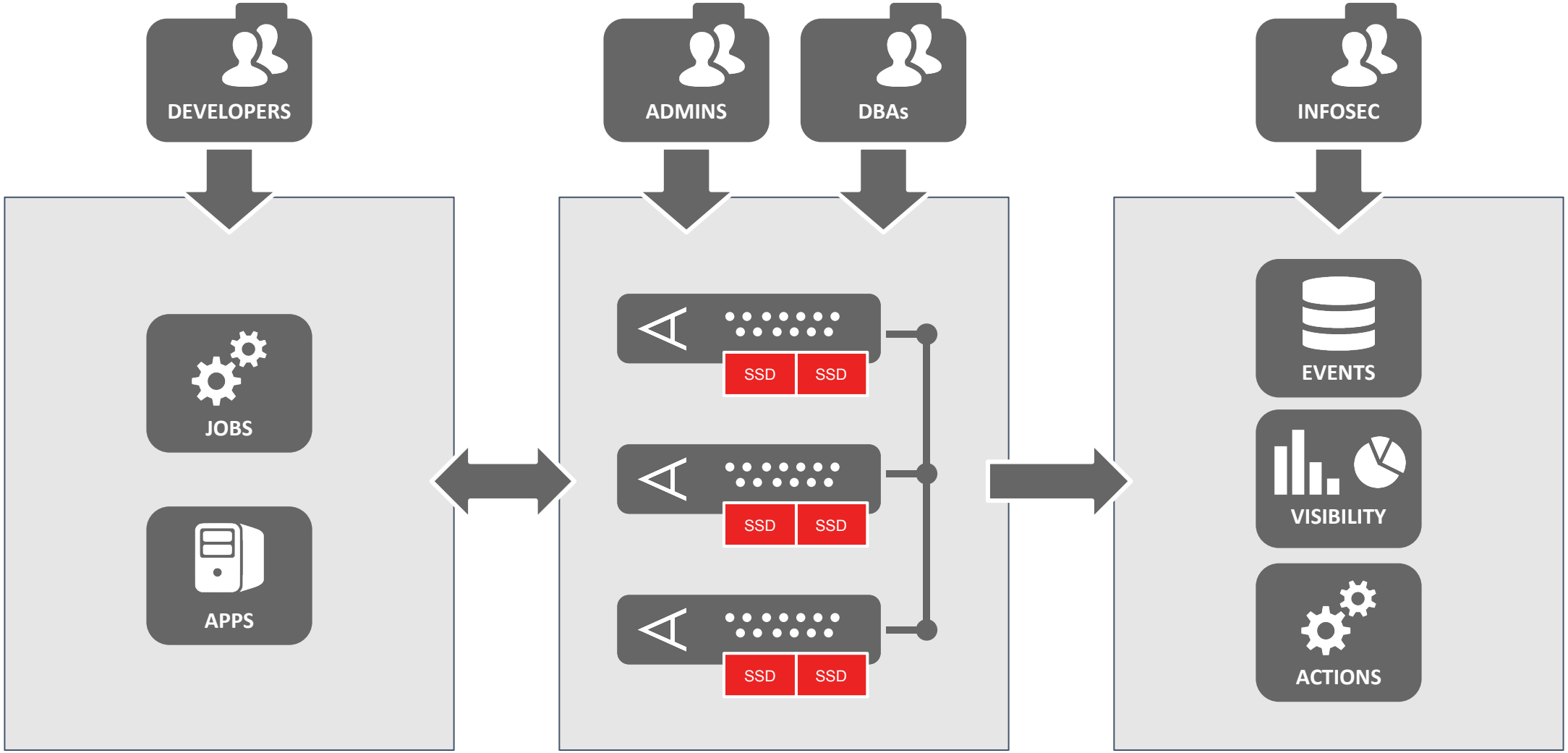

DEVELOPERS
ADMINS
DBAs
INFOSEC
JOBS
APPS
SSD
SSD
SSD
SSD
SSD
SSD
EVENTS
VISIBILITY
ACTIONS

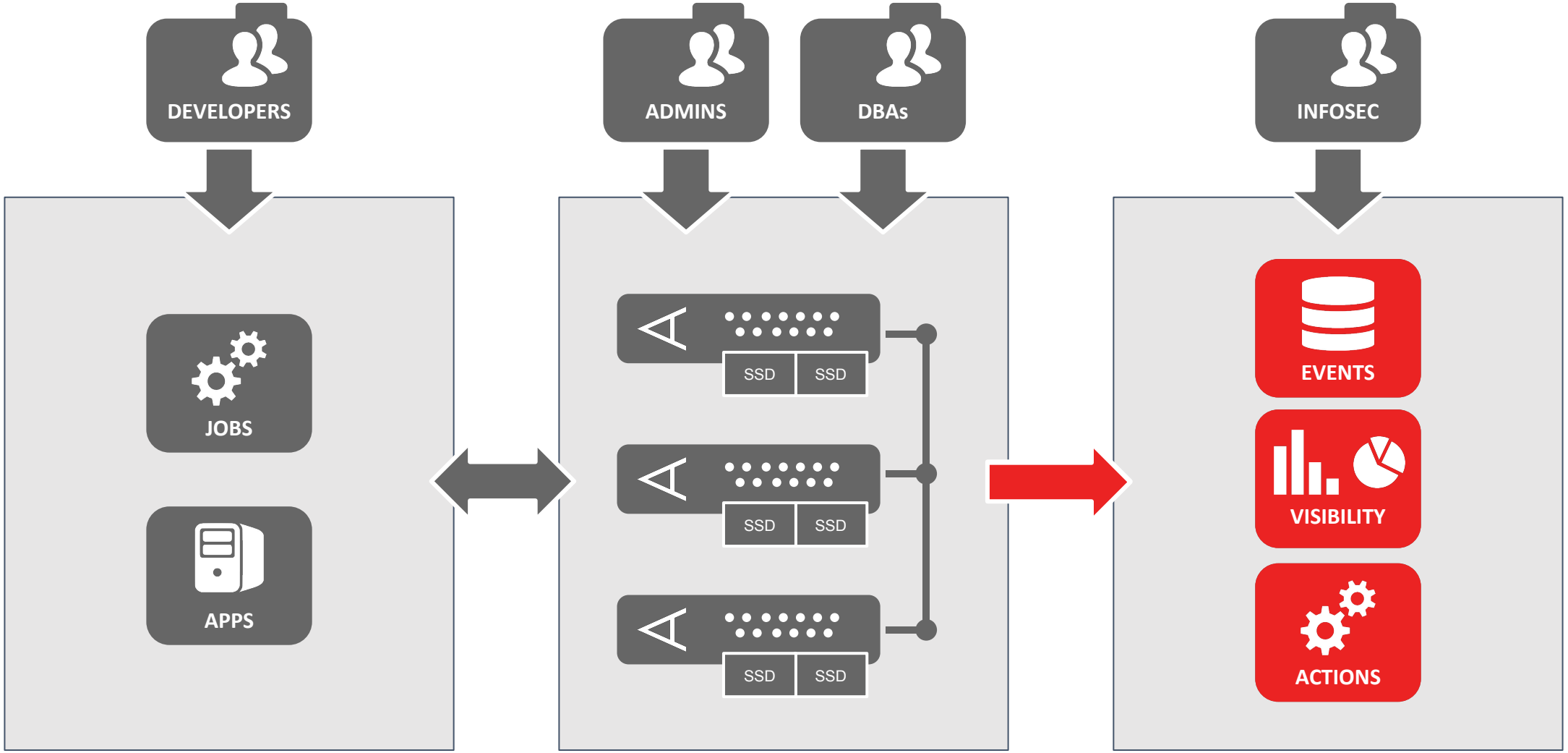

DEVELOPERS
ADMINS
DBAs
INFOSEC
JOBS
APPS
SSD
SSD
SSD
SSD
SSD
SSD
EVENTS
VISIBILITY
ACTIONS


DEVELOPERS
ADMINS
DBAs
INFOSEC
JOBS
APPS
SSD
SSD
SSD
SSD
SSD
SSD
EVENTS
VISIBILITY
ACTIONS

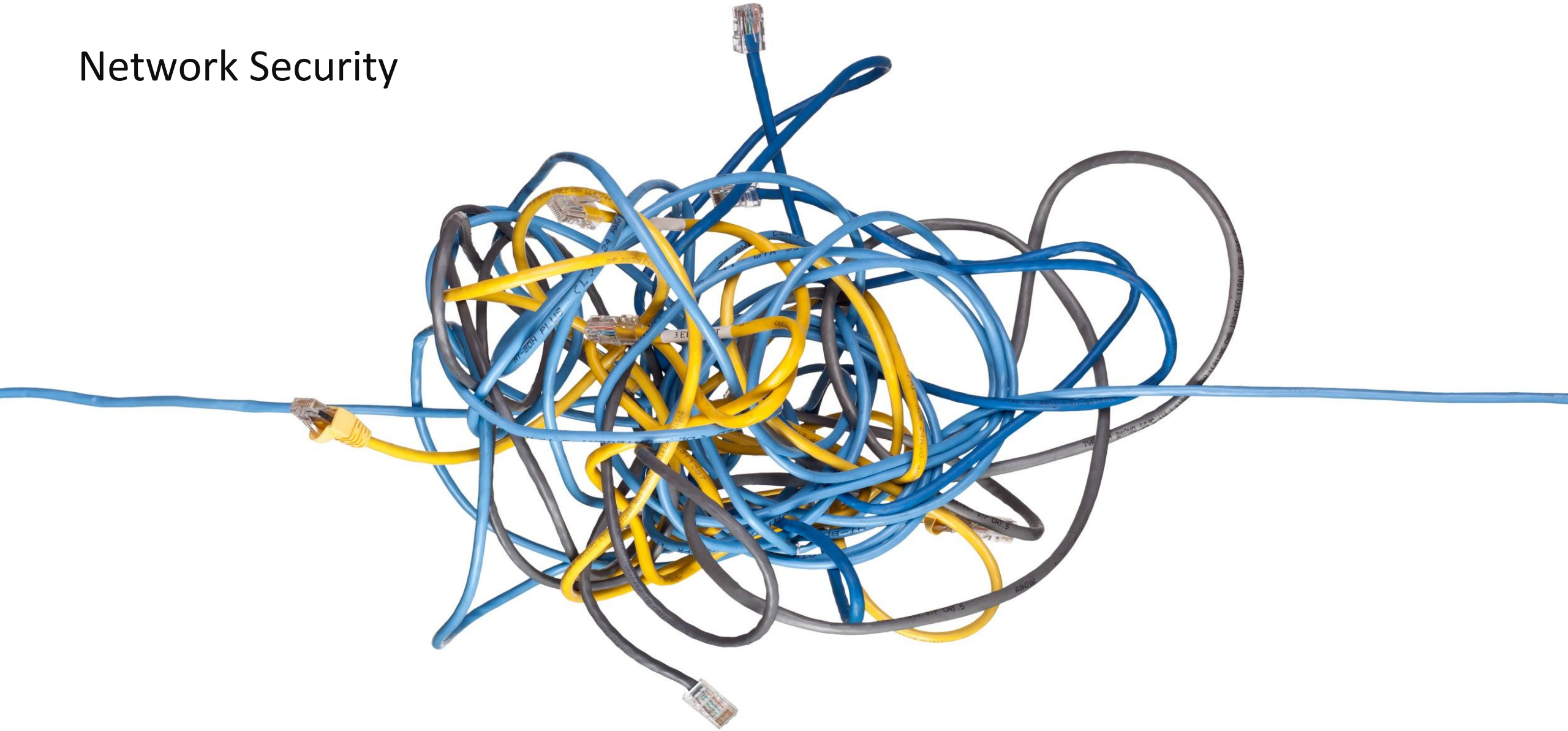

DEVELOPERS
ADMINS
DBAs
INFOSEC
JOBS
APPS
SSD
SSD
SSD
SSD
SSD
SSD
EVENTS
VISIBILITY
ACTIONS


DEVELOPERS
ADMINS
DBAs
INFOSEC
JOBS
APPS
SSD
SSD
SSD
SSD
SSD
SSD
EVENTS
VISIBILITY
ACTIONS

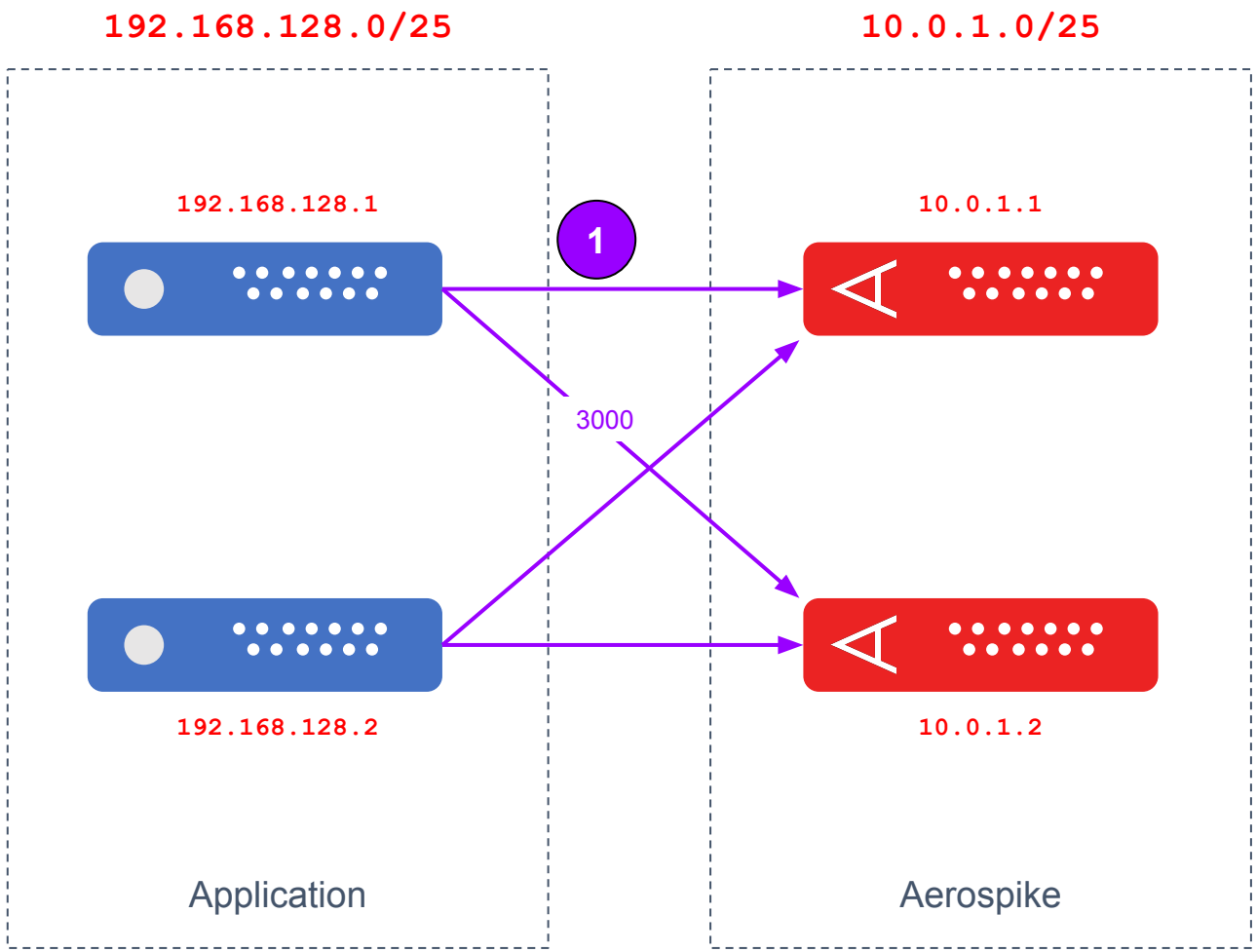

DEVELOPERS
ADMINS
DBAs
INFOSEC
JOBS
APPS
SSD
SSD
SSD
SSD
SSD
SSD
EVENTS
VISIBILITY
ACTIONS


DEVELOPERS
ADMINS
DBAs
INFOSEC
JOBS
APPS
SSD
SSD
SSD
SSD
SSD
SSD
EVENTS
VISIBILITY
ACTIONS

Network Security

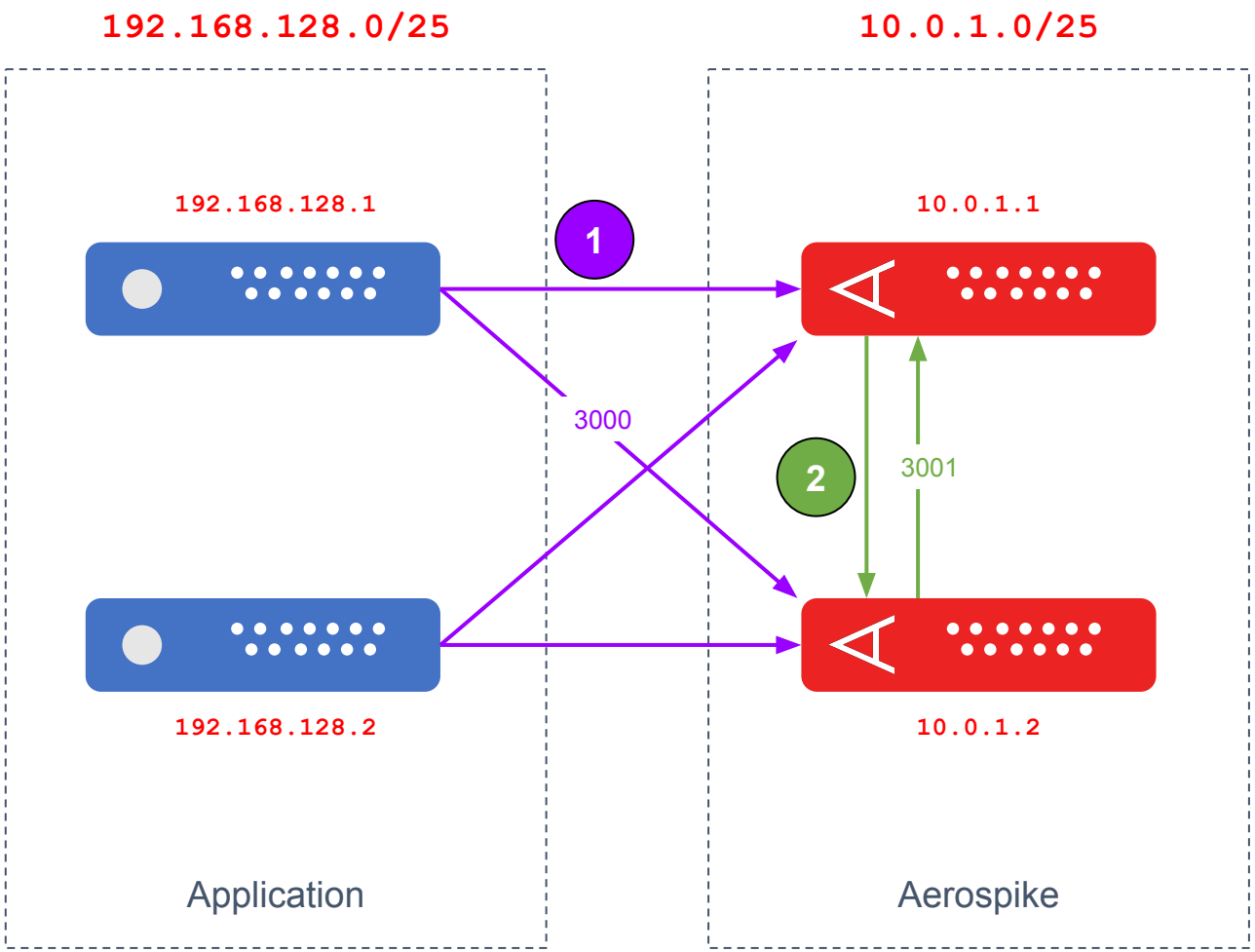


1 Allow TCP on **service** port



1 Allow TCP on **service** port

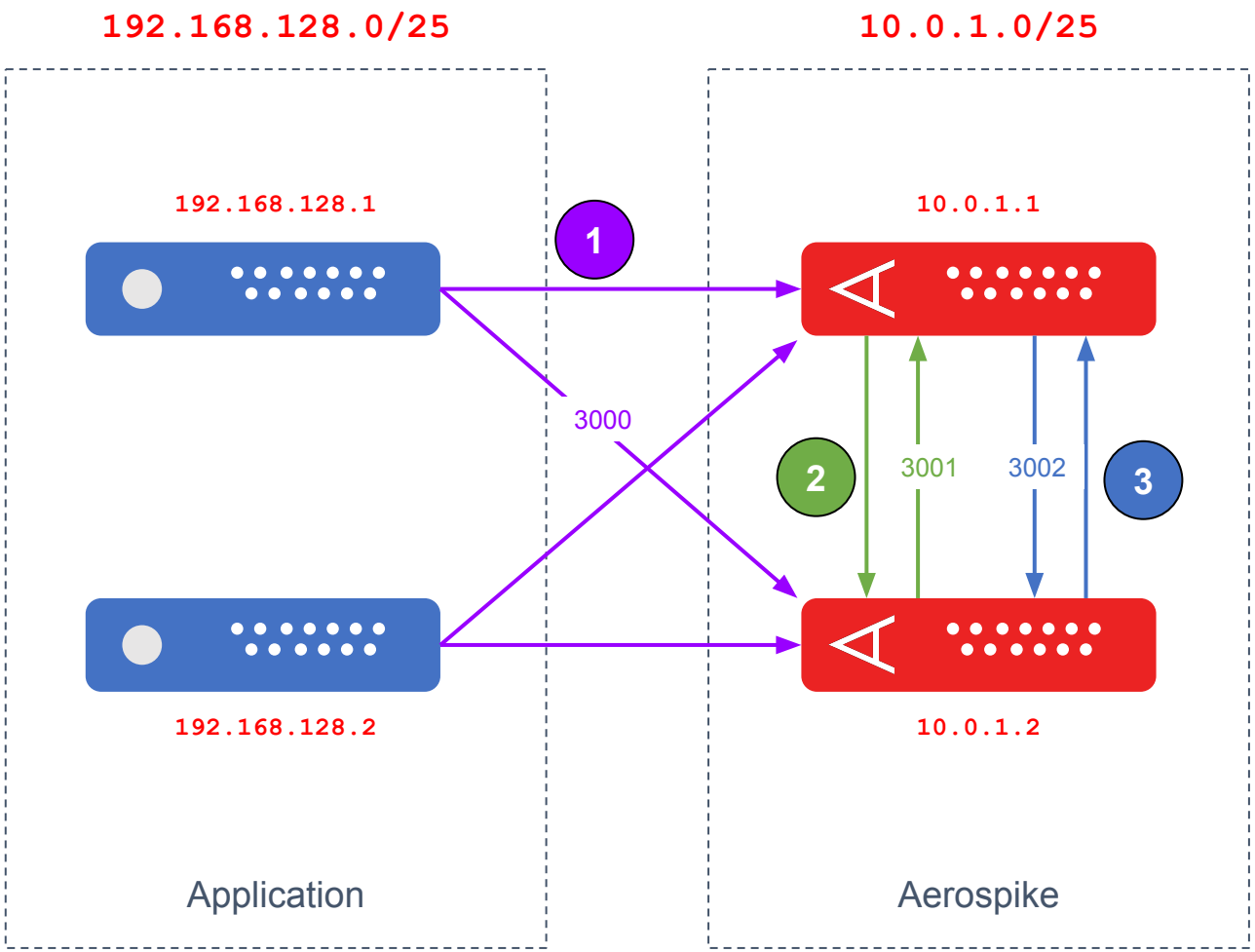
2 Allow TCP on **heartbeat** port



1 Allow TCP on **service** port

2 Allow TCP on **heartbeat** port

3 Allow TCP on **fabric** port

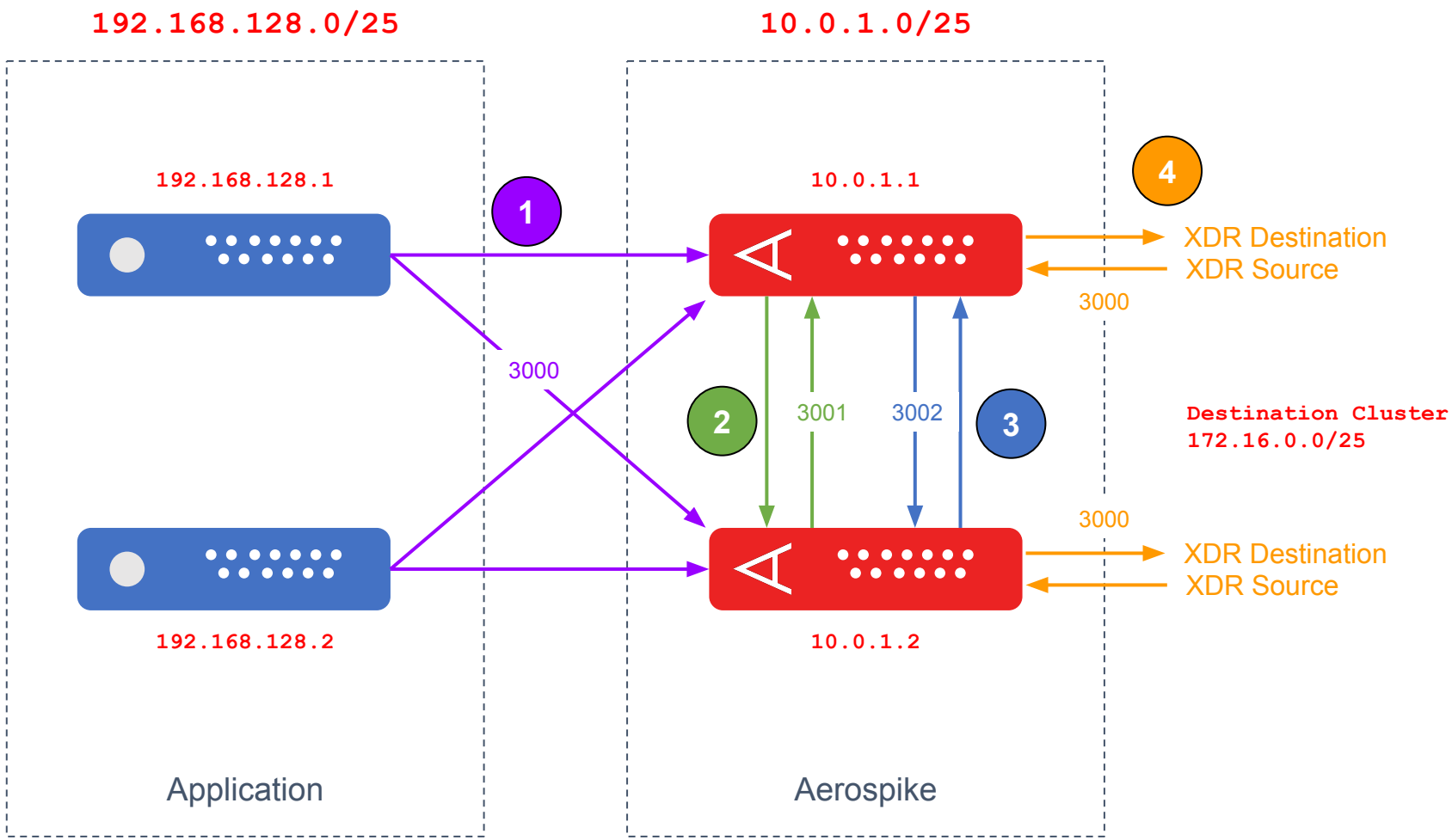


1 Allow TCP on **service** port

2 Allow TCP on **heartbeat** port

3 Allow TCP on **fabric** port

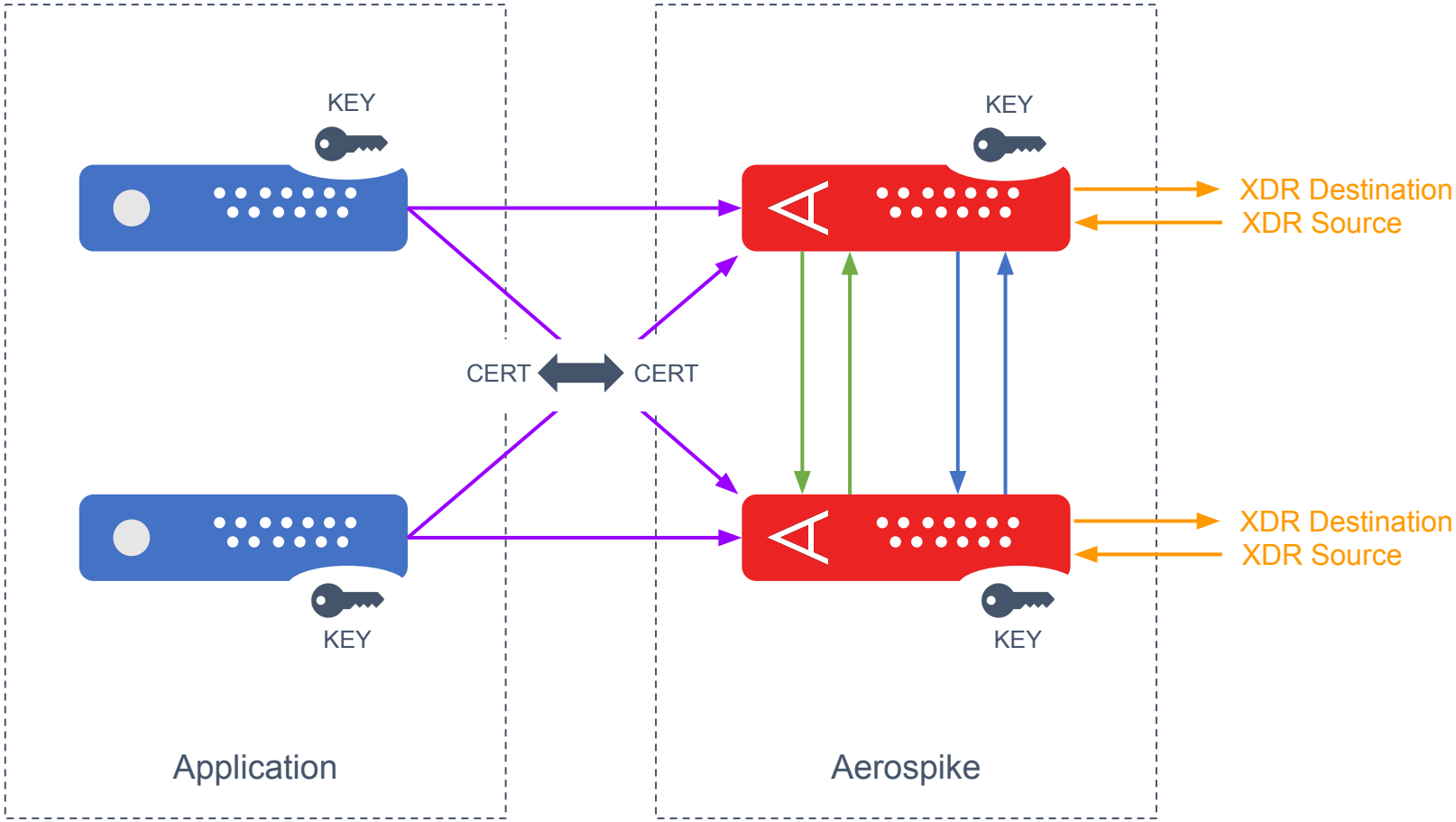
4 Allow TCP on **service** port



Client hello. Server hello.

Service

- Configure server cert
- Configure cipher suites
- Validate client cert (optional)



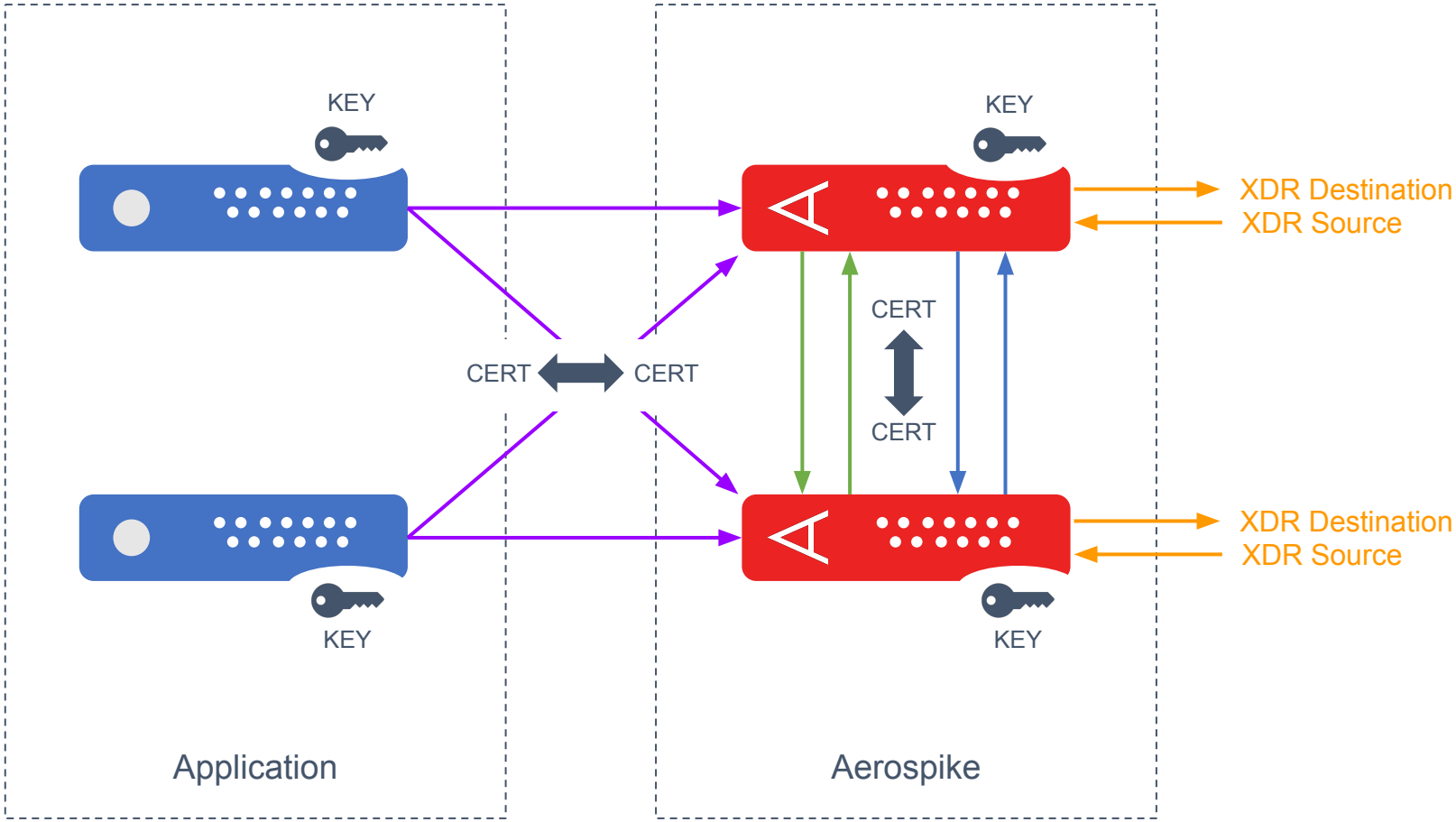
Client hello. Server hello.

Service

- Configure server cert
- Configure cipher suites
- Validate client cert (optional)

Heartbeat and fabric

- Configure server cert
- Configure cipher suites



Client hello. Server hello.

Service

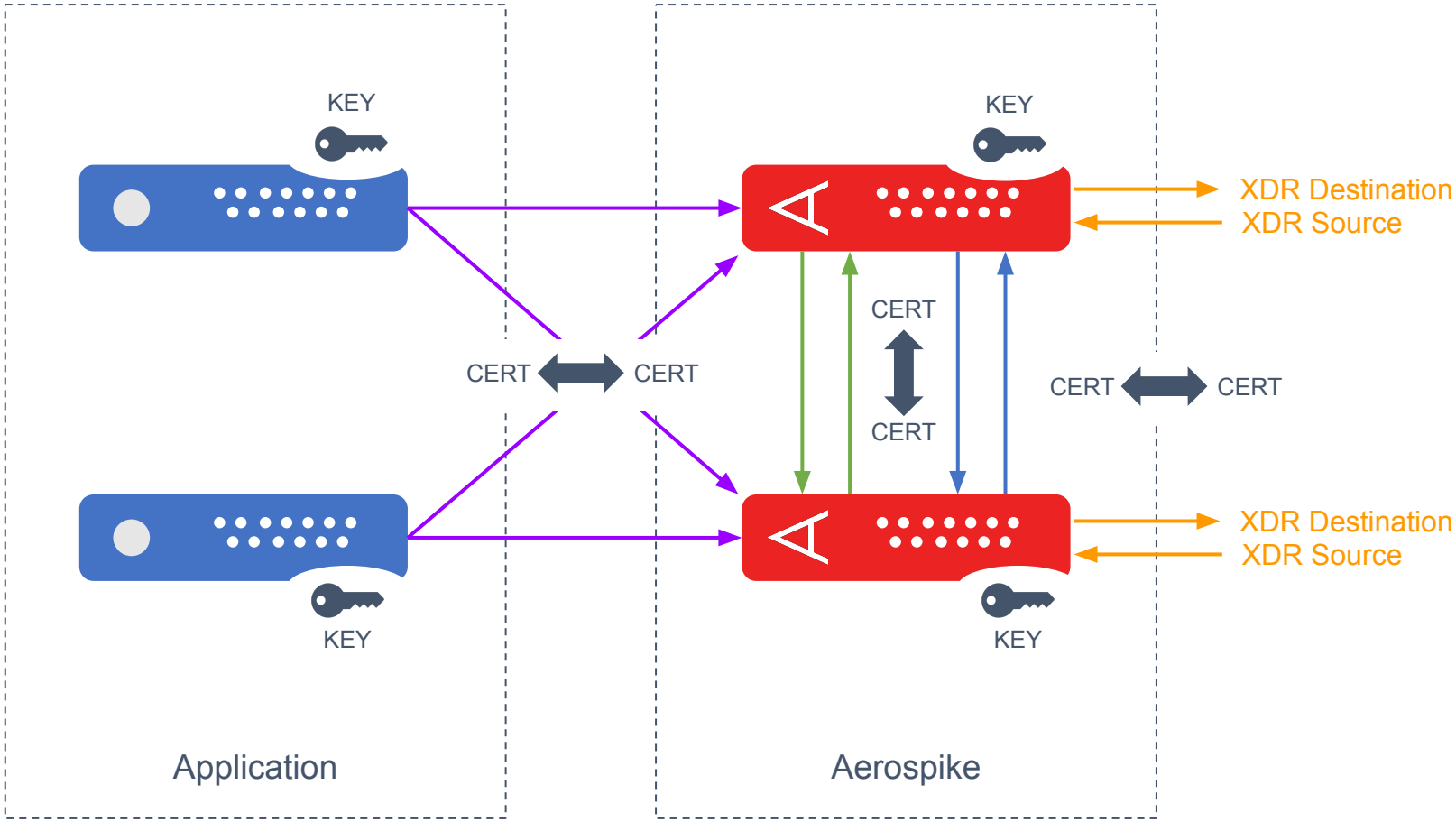
- Configure server cert
- Configure cipher suites
- Validate client cert (optional)

Heartbeat and fabric

- Configure server cert
- Configure cipher suites

XDR

- Configure server cert
- Configure cipher suites
- Validate client cert (optional)



Ciphering succotash

	ECDHE	-	ECDSA	-	AES128	-	GCM	-	SHA256	*(OpenSSL notation)*
TLS_	ECDHE	_	ECDSA	_WITH_	AES_128	_	GCM	_	SHA256	*(IANA notation)*

Message authentication

Encryption algorithm

Auth algorithm

Key exchange

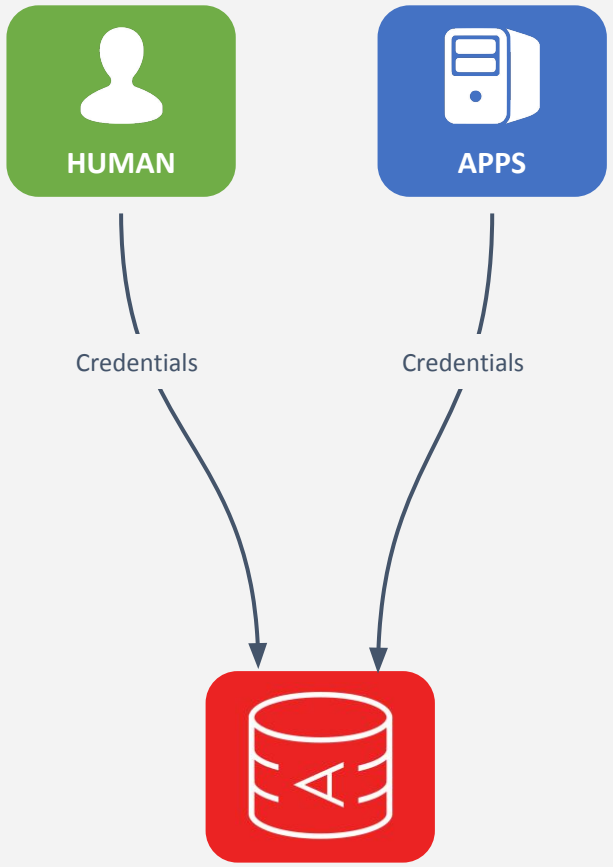
Different standards at different organizations (RSA vs ECDSA)

AES128/256 with GCM

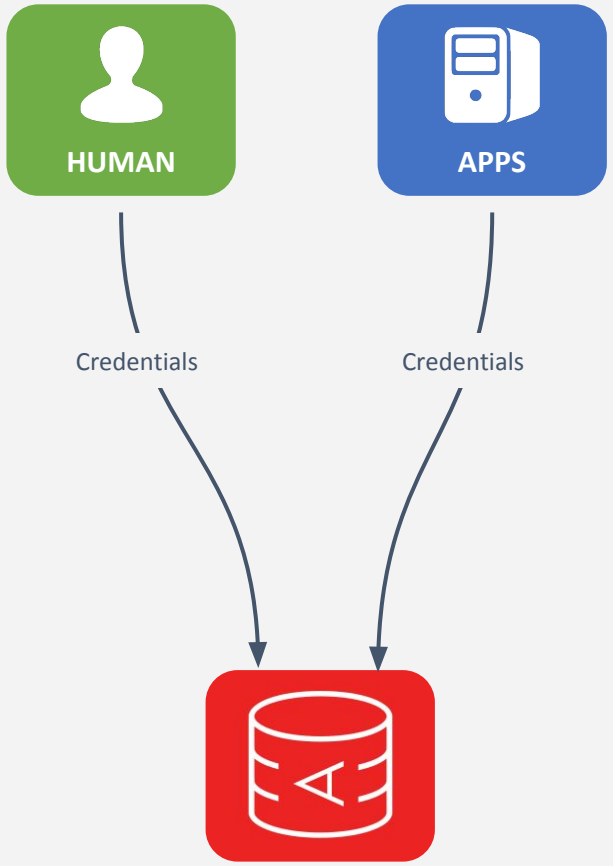
✅ performance
✅ security

Authentication & Access Control

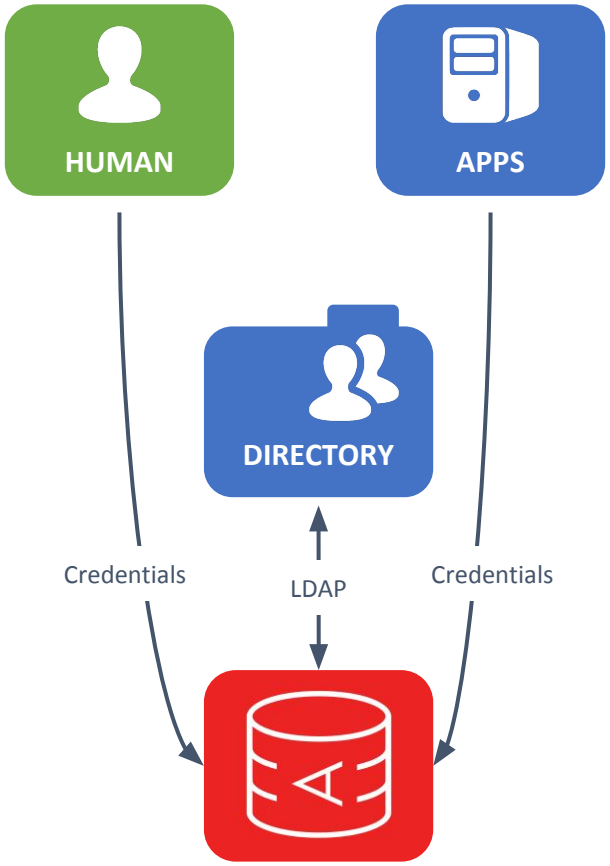
Internal Authentication

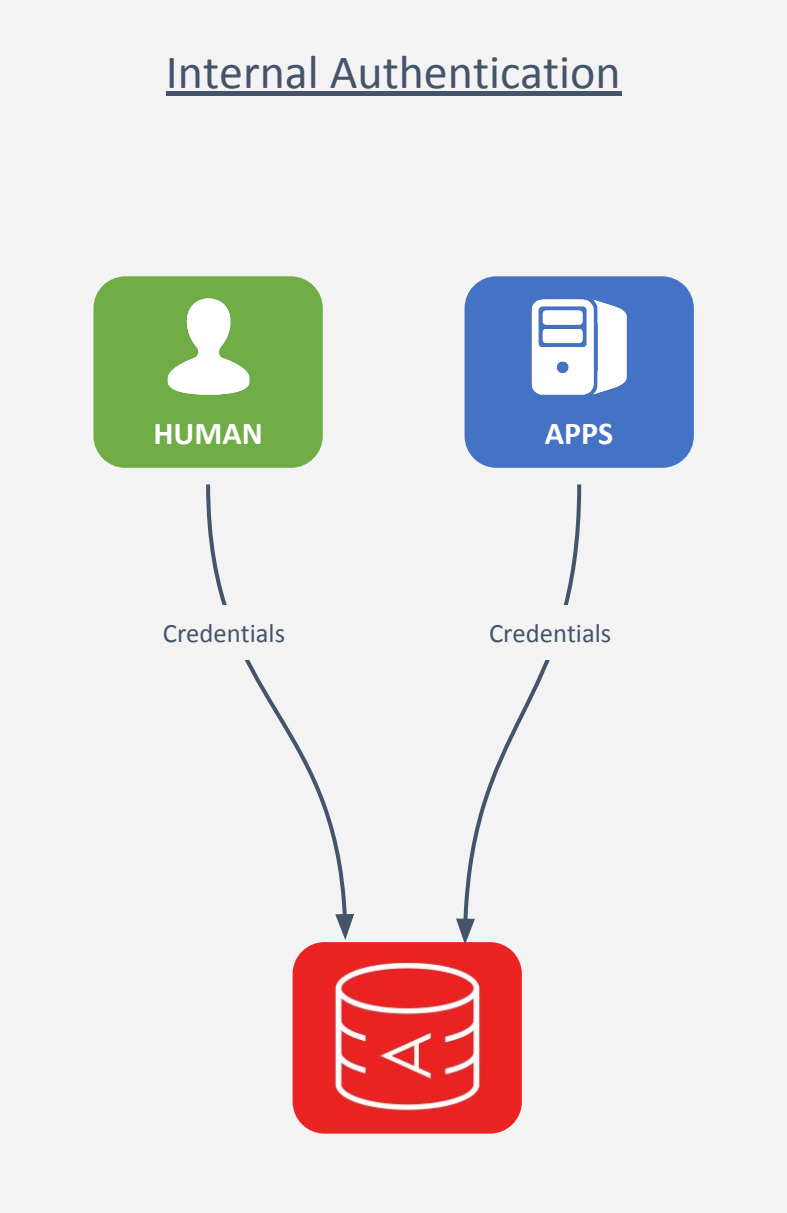


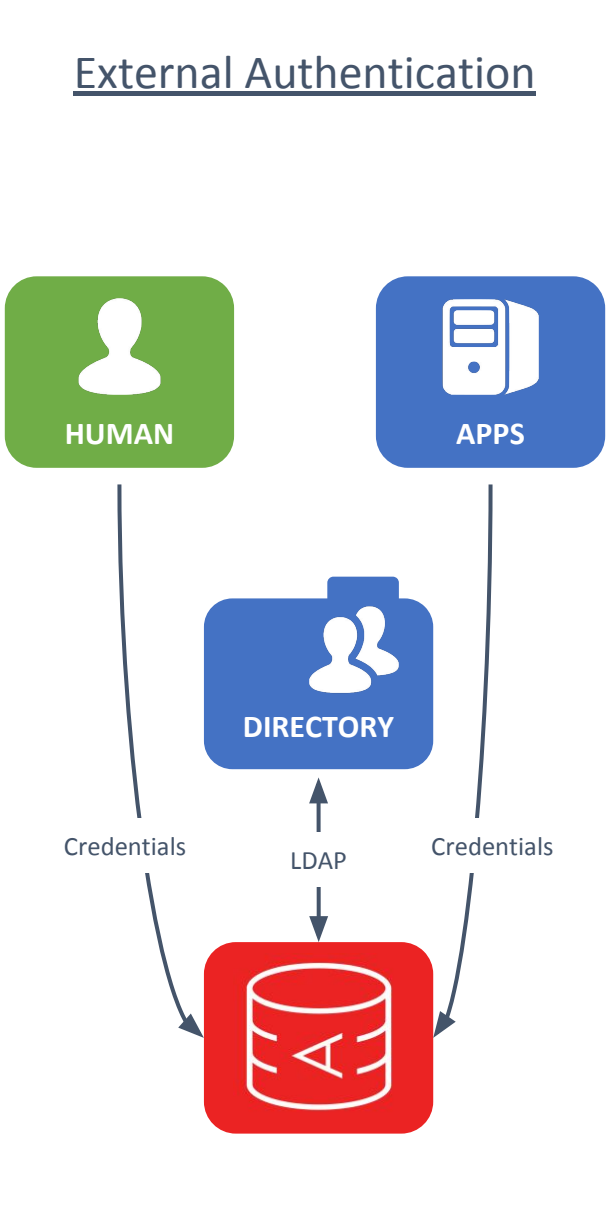
Internal Authentication

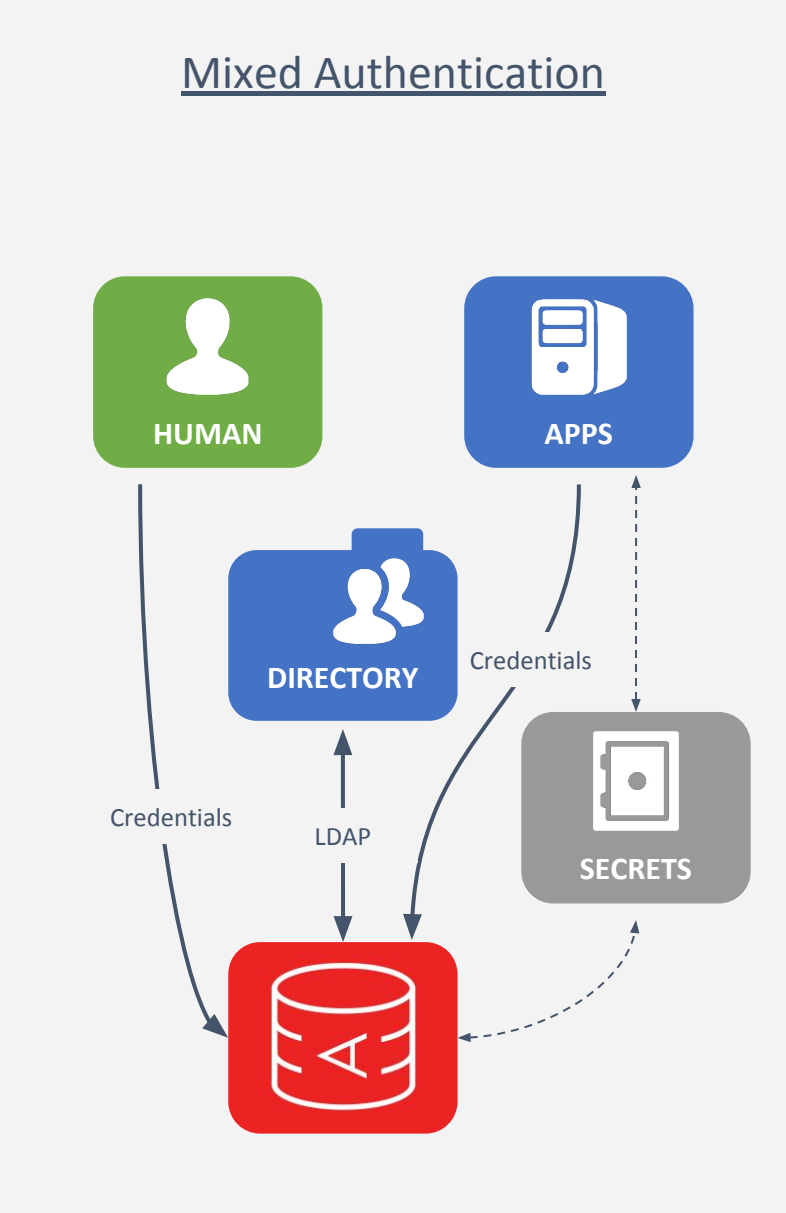


External Authentication




Internal Authentication
HUMAN
APPS
Credentials
Credentials


External Authentication
HUMAN
APPS
DIRECTORY
Credentials
LDAP
Credentials


Mixed Authentication
HUMAN
APPS
DIRECTORY
Credentials
Credentials
LDAP
SECRETS

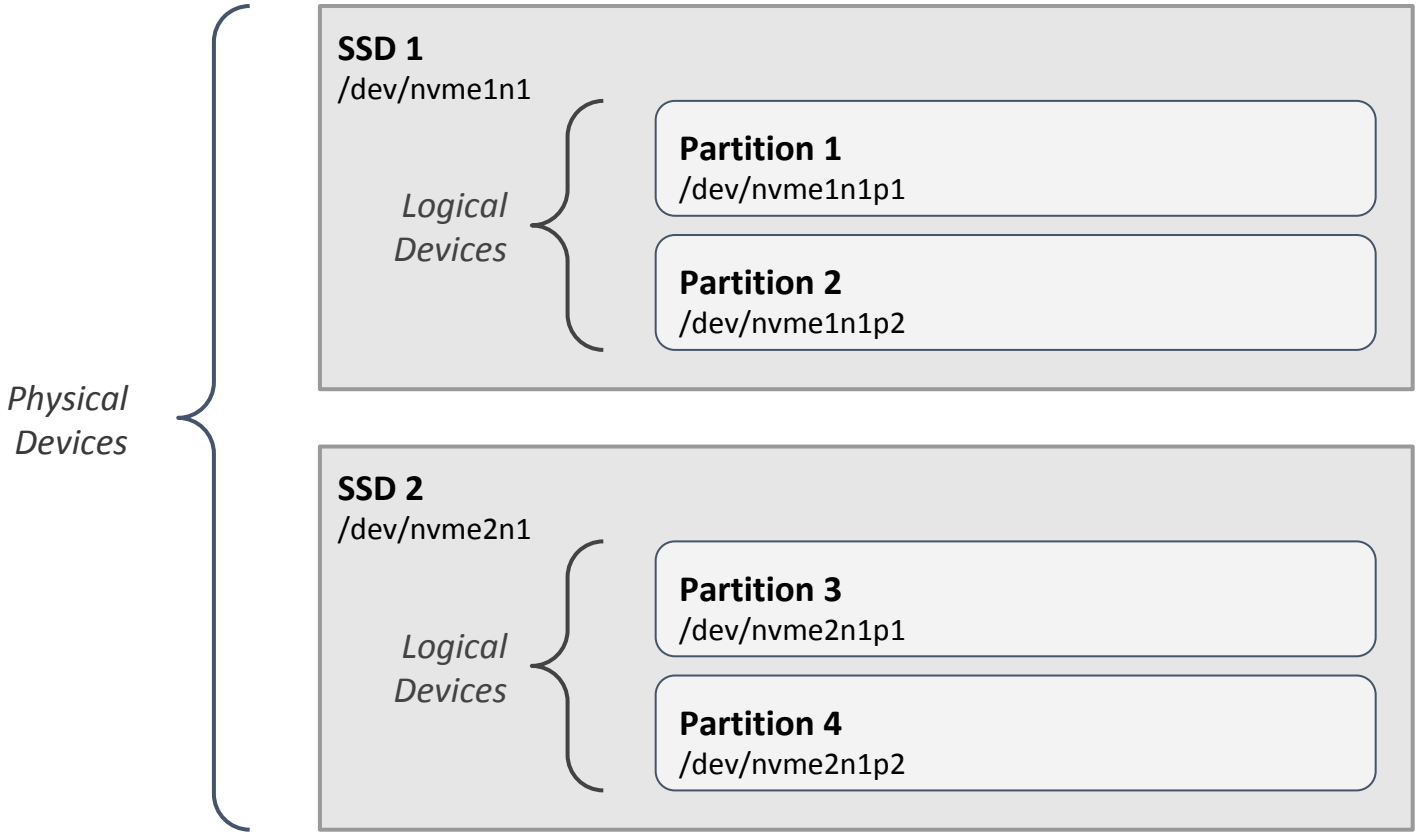
Slice ‘em and dice ‘em

Privilege

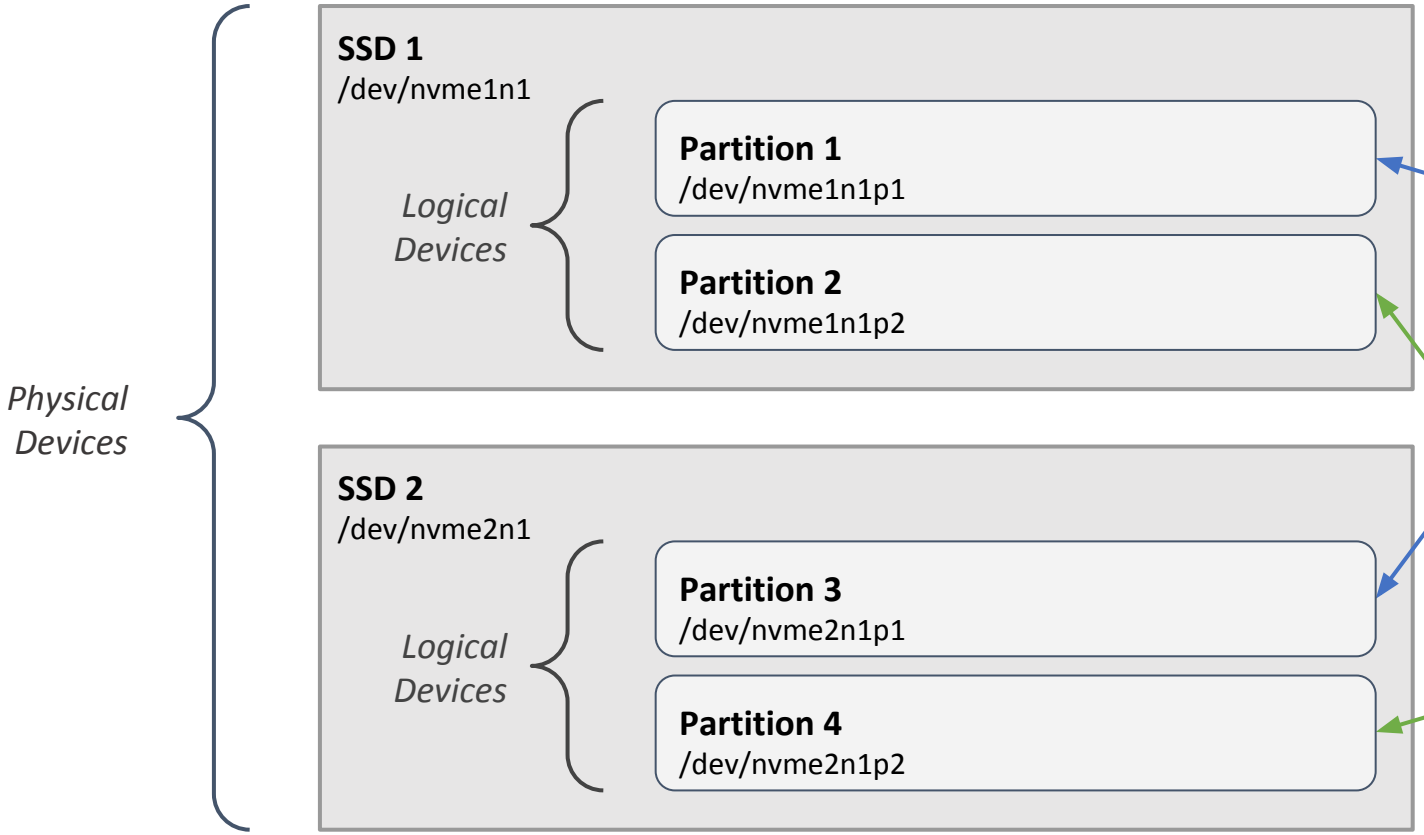
Role	Permission	Scope	Whitelist
Acme IAM	user-admin	Global	10.0.0.61/31
Acme SRE	sys-admin	Global	10.0.0.0/24
Acme DBA	data-admin	Global	10.0.0.0/24
Acme App1	read-write-udf	Namespace=ns1, Set=app1	-
Acme App2	read	Namespace=ns1, Set=app2	-
Acme Daily Loader	write	Namespace=ns1, Set=app2	-

Data Protection

Isolation and encryption



Isolation and encryption



Logical separation of data

Namespace #1

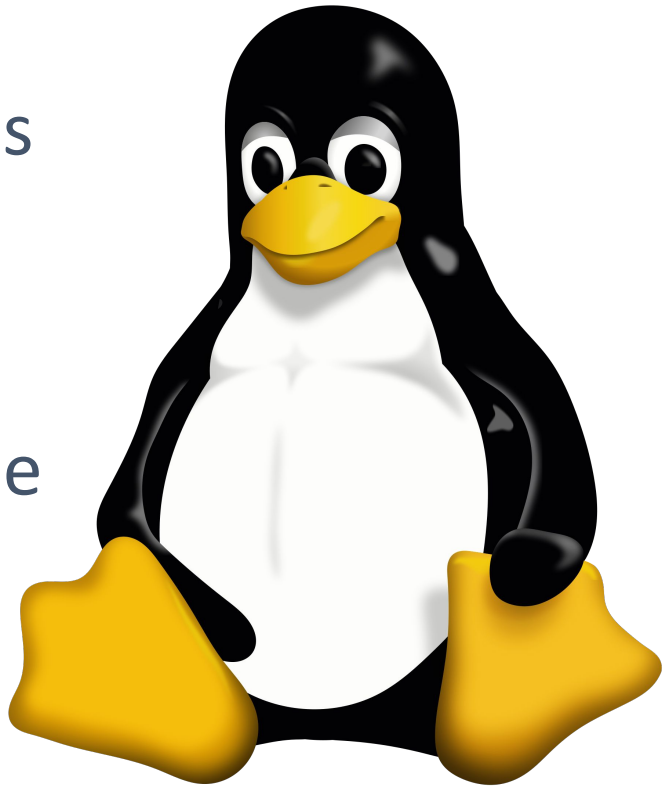
- Encryption: AES-256
- Key file: namespace-1.key
- Devices: nvme1n1p1, nvme2n1p1

Namespace #2

- Encryption: AES-256
- Key file: namespace-2.key
- Devices: nvme1n1p2, nvme2n1p2

sudo make me a sandwich

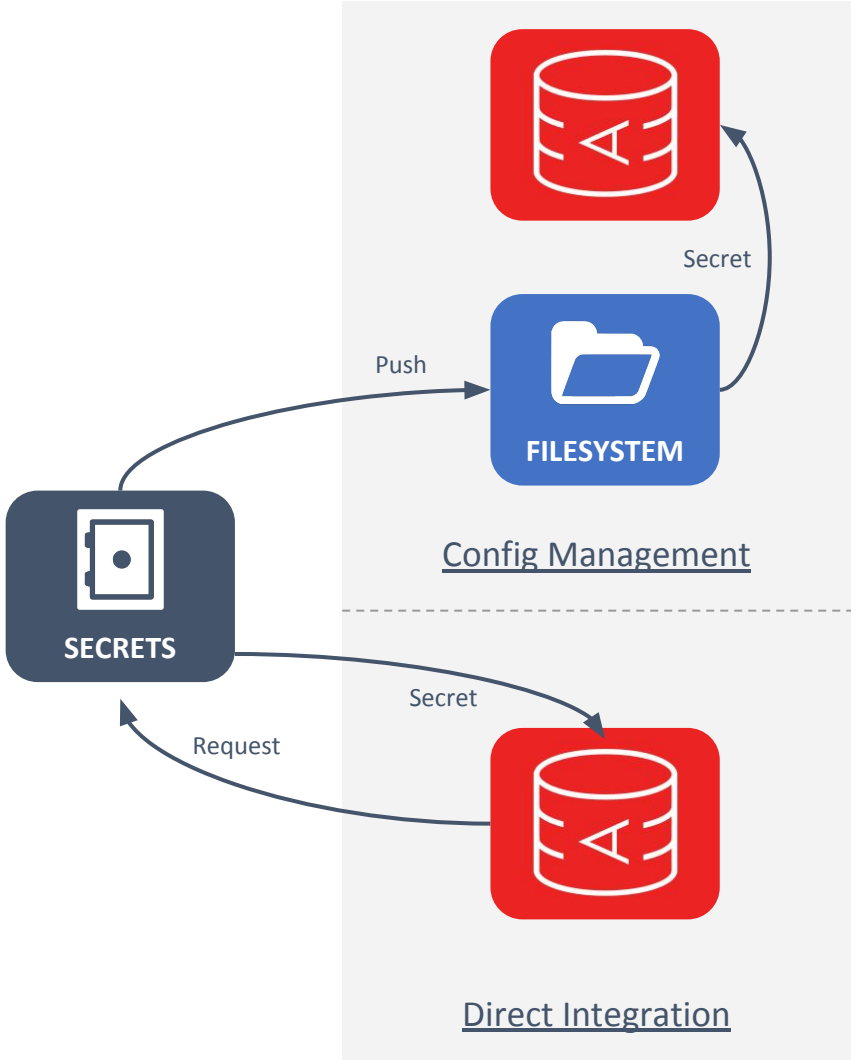
- The Aerospike daemon (`asd`) is a privileged process
- Apply your existing OS hardening best practices
- Do not use Aerospike nodes for auxiliary functionality
- Not all `asinfo` and `asadm` operations need to be run locally
- Protect secrets...



It’s a secret to everybody.

Protect Secrets

- TLS private keys
- Encryption-at-rest keys
- Credentials to external authentication (LDAP)
- Credentials to other Aerospike clusters (XDR)
- System MetaData (SMD)
  (Managed by Aerospike)



Security Events and Audit Logs

Micah showed this slide from 127.0.0.1