# vSAN Encryption

- Requirements
  - Hybrid or All Flash supported
  - Supported external key management server
    - KMIP 1.1 supported
    - Review validated list [link]
  - vSAN Enterprise licence (standard + ROBO)
  - vSAN 6.6 or higher
    - FIPS 140-2 validated
    - Encryption module certified
    - Improved with 6.7u1
    - vSphere 6.5
  - Works with any vSAN hardware
    - Software based
    - No special drives
- Process
  - Validate KMS
    - Support
    - Profile
    - Availibiity of KMS
      - External to vSAN datastore it is used to protect
  - Connection trust associated between vCenter & KMS server
  - KMS associated with Hosts via vCenter Role
    - Key Exchange
      - Host key provided
      - Key ID given
  - Hosts then request to KMS directly
    - Requests direct to KMS
    - KEK provided by KMS & stored in each host KeyCache in Memory
      - Not persistant
  - Encryption of devices
    - Host creates a DEK from KEK
    - Encrypts disk
    - Requires change of vSAN Disk Format
    - Evacuation & reformat host disks
- Operational & Design Thoughts
  - Plan enablement of the feature
    - Can be enabled with VMs online
      - Consider the amount of data if enabling with workloads already placed
      - Allow reduced redundancy and impact to the availibility
  - Security
    - KEK stored in memory
      - Non persistant
    - RBAC
      - vCenter Role based
      - No cryptography administrator
        - Same as admin role
          - No host to vCenter permission
          - No vSAN encryption
    - Key Rotation
      - Needs the vCenter
        - KEK ID change
      - Depends on business policy
        - Types
          - Shallow
            - Regenerates the KEK from the KMS
            - Quick and low impact
            - No change of DEK
          - Deep
            - Changes the KEK ID via vCenter request
            - Hosts request new KEK
            - Changes the DEK
            - Data re-encrypted
            - consider impact of data movement
              - Network
              - Slack space
  - KMS availbility
    - KMS Profile Use
      - 1 KMS Profile per cluster
    - Without the KMS being up and healthy hosts will lose access to devices if rebooted
      - No KEK
    - Do not host the KMS server on the same datastore as the one its used to protect
    - Loss of KMS
      - Data loss of KMS - potential loss of data
      - Do not reboot hosts
      - Change KMS
        - Rekey operation
    - Consider stretched cluster & DR
      - Witness node does not have data
  - vCenter availbility
    - Needed to enable feature
    - Cannot add hosts to solution
    - Re-keying of data
    - Can be protected by the solution with external KMS
    - Loss of vCenter
      - Rebuild from back up
        - Possible to recreate from new vCenter deployment
          - Needs manual recreation of system
      - Reconnect & establish trust process to KMS
  - VM placement
    - DRS Rules
      - Monitoring
    - If the VM leaves the datastore it is not encrypted
  - Performance
    - 5-10% CPU rule of thumb
    - ENable and check AES-NI
    - Consider workload behavior
      - Read
      - Write
    - Speed of disk tiers
  - Reporting
    - Part of proactive tests
    - vSAN Encryption Report - [Link]
    - Core dumps
      - control contents
    - Consider VM-support passwords
- Overview
  - Data encryption at rest for vSAN
  - Part of vSAN data services
  - Encrypts the whole vSAN Datastore
    - Cluster based setting
    - Different to vSphere VM based
      - No agents needed
      - All vSphere guest OS supported
      - VM must remain on the cluster datastore for security feature to remain
    - Works with vSAN Data services
      - Data is encrypted and unencrypted then deduped & re-encrypted
      - Deduplication / compression values still achieved
- Architecture
  - KMS Infrastucture
    - vCenter associates & trusts the cluster with enterprise KMS
      - 1 per cluster
      - KMS is needed when hosts restarted
    - Keys Used
      - KMS
        - KEK
          - Key encryption key
            - One per vSAN cluster
        - HEK
          - Host encryption key
            - Encrypts the host core dumps
        - AES-128 or AES-256
        - Key length controlled by the KMS
      - Host DEK
        - Data encryption key
          - For vSAN use
          - Per host
            - per device
          - Encrypts the data
            - AES-256
  - vCenter
    - Cluster based setting
      - Ensure disks before used
        - Impact to deployment
      - Allow reduced redundancy
        - Insufficient data space
        - Consider impact
      - All disks reformatted
    - vCenter is not required to be up at subsequent boot times
    - Can be reattached
  - Hosts
    - Trust the KMS via link created by the vCenter
    - Stores information on infrastructure
    - Uses Host ID
    - /etc/vmware/esx.conf
  - Disks
    - Both disk tiers are encrypted
      - Cache layer
      - Capacity layer

Paul McSharry | vSAN Encryption
www.elasticsky.co.uk | Nov 2018