SAP SuccessFactors

SuccessFactors

HCM Datacenter Infrastructure & Encryption

Customer

THE BEST RUN SAP

Overall approach to Data Encryption

SuccessFactors is a 100% web browser based application, with all access over HTTPS \ Port 443 exclusively. Every page of the SuccessFactors application is currently delivered via Transport Layer Security (TLS). SuccessFactors currently supports up to TLS version 1.2. All data is encrypted in transit over HTTPS with 256-bit AES encryption.

Any files sent for batched\scheduled imports are over a customer-specific SFTP account, with recommended use of PGP file encryption prior to transfer. We do not support un-encrypted transfer protocols, such as standard FTP.

All database backups are stored on-disk only and encrypted using the AES 256-bit protocol. Database backups are never stored on removable media or with external, third-party storage providers.

We provide data encryption-at-rest via a hardware-based approach. Encryption is provided for all data stored on our SAN, by the SAN hardware itself. SuccessFactors uses both Hitachi VSP and EMC VMAX solutions for our SAN hardware. Whenever data is written to disk, it is written and saved in encrypted format. AES 256-bit encryption is the method used. Hardware-level encryption provides superior performance to Software-level encryption, such as at the database software \ database memory layer.

Encryption key management is automated\scheduled through the SAN Administrative Tools. SAP SuccessFactors does not currently support customer-controlled encryption keys.

Storage Architecture – Encryption

Storage

- EMC XtremeIO and VMAX
- Netapp NSE disks
- HDS VSP

Backup

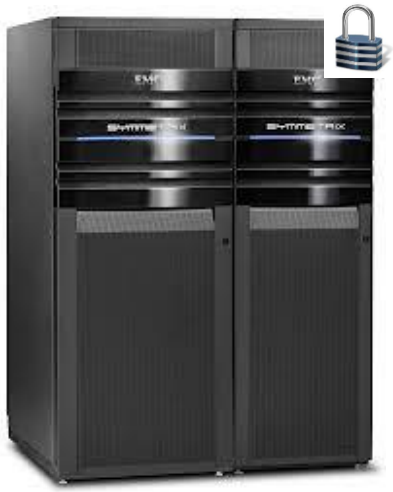
- EMC Datadomain
- NetApp NSE disks

All the storage infrastructure at SAP datacenter has full disk encryption. This technology leverages the encryption at rest mechanism using 256-bits AES algorithms.

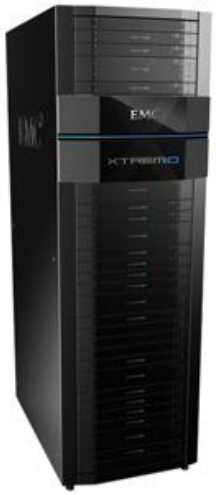
Storage Architecture – Encryption

HDS VSP

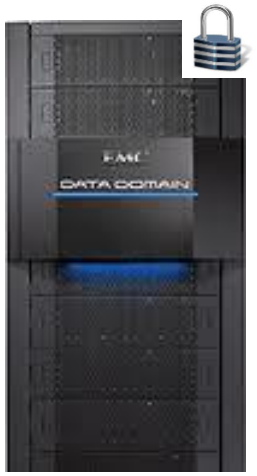
EMC VMAX



EMC XtremeIO



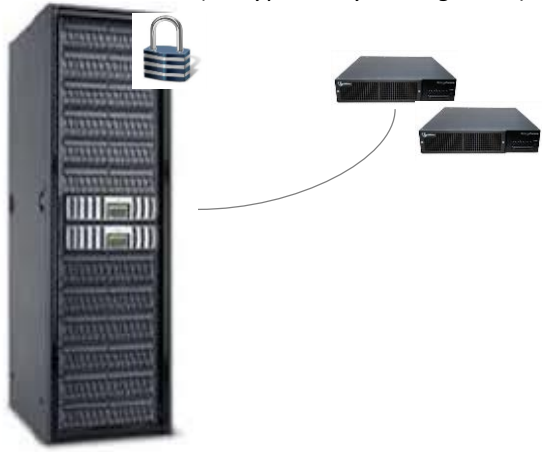
EMC Datadomain



Netapp

Safenet KeySecure Cluster

(Encryption Key Management)



- Full disk encryption
- Encryption at rest
- AES 256-bit encryption keys

Full Disk Encryption & Encryption at rest

- The full disk encryption technology helps to preserve the product core values (compression, de-duplication, replication, etc) and offers Data at Rest Encryption without affecting the system performance.
- In the case of HDS & EMC, the encryption keys are generated prior the creation of the data volumes and they are stored inside the storage arrays. External key management is NOT required but optional.
- The NetApp NSE disks require a 3rd party tools used to centralize key management and enable lifecycle rotation but this is just optional, as the keys are fully protected within the devices.
- The full disk encryption approach ensures that data will be safe in the event of a disk being lost or stolen.
- The devices also offer an extra layer of protection in case of the entire array would leave the datacenter. Authorized access is required to bring the data volumes online, offering an extra layer of protection.

SAP SuccessFactors

Thank you.

THE BEST RUN SAP®