securosys

Partition Remote Administration

Take control of your CloudsHSM partition

Customers who opt for Primus HSM as a service do not need to trust Securosys to handle their security. Instead, they can control their partition access and security settings without any interference – even from Securosys administrator.

Details

Digital identities and keys are commonly used to secure infrastructures and services. Additionally, they are becoming increasingly important for holding crypto assets. A Hardware Security Module (HSM) is built to safeguard the generation, storage, and usage of such keys. Companies that would like to take advantage of an HSM's capabilities, but are not ready to procure their own device, can opt for Securosys' CloudsHSM service.

Previously, the benefits were linked with the disadvantage of having to trust Securosys' integrity. This was because the HSM operator (Security Officer) has to issue the customer's access credentials and could potentially change the security settings of the HSM.

We would never betray the trust placed in us of course and we are also contractually prohibited from abusing our control in such a way. Nonetheless, that guarantee is not sufficient for many organizations, no matter how small, especially when their customers' cryptographic assets or identities are at stake.

The Partition Administration feature allows our customers' operators to perform the same administrative tasks usually done at a device level with Security Officers privileges.

These include:

- Resetting credentials
- Changing the partition's security configuration
- Management of invalidated keys
- Exporting logs
- Partition backup/ restore

By using the Partition Administration, you do not need to trust anyone with the control over the access to your CloudsHSM's keystore if you do not want to.

Important note: please be aware, that by enabling this feature and disabling the HSM admin access, the partition administrator is not only taking control, but also responsibility for the partition access and security settings. This means that Securosys can no longer access the partition to help the partition user reset credentials or change the settings. However, as the CloudsHSM service provider Securosys will still maintain the operation of the clustered setup with additional redundancy. Accordingly, Securosys will still carry the responsibility of providing high availability and recoverability as a part of the service offered.

Benefits

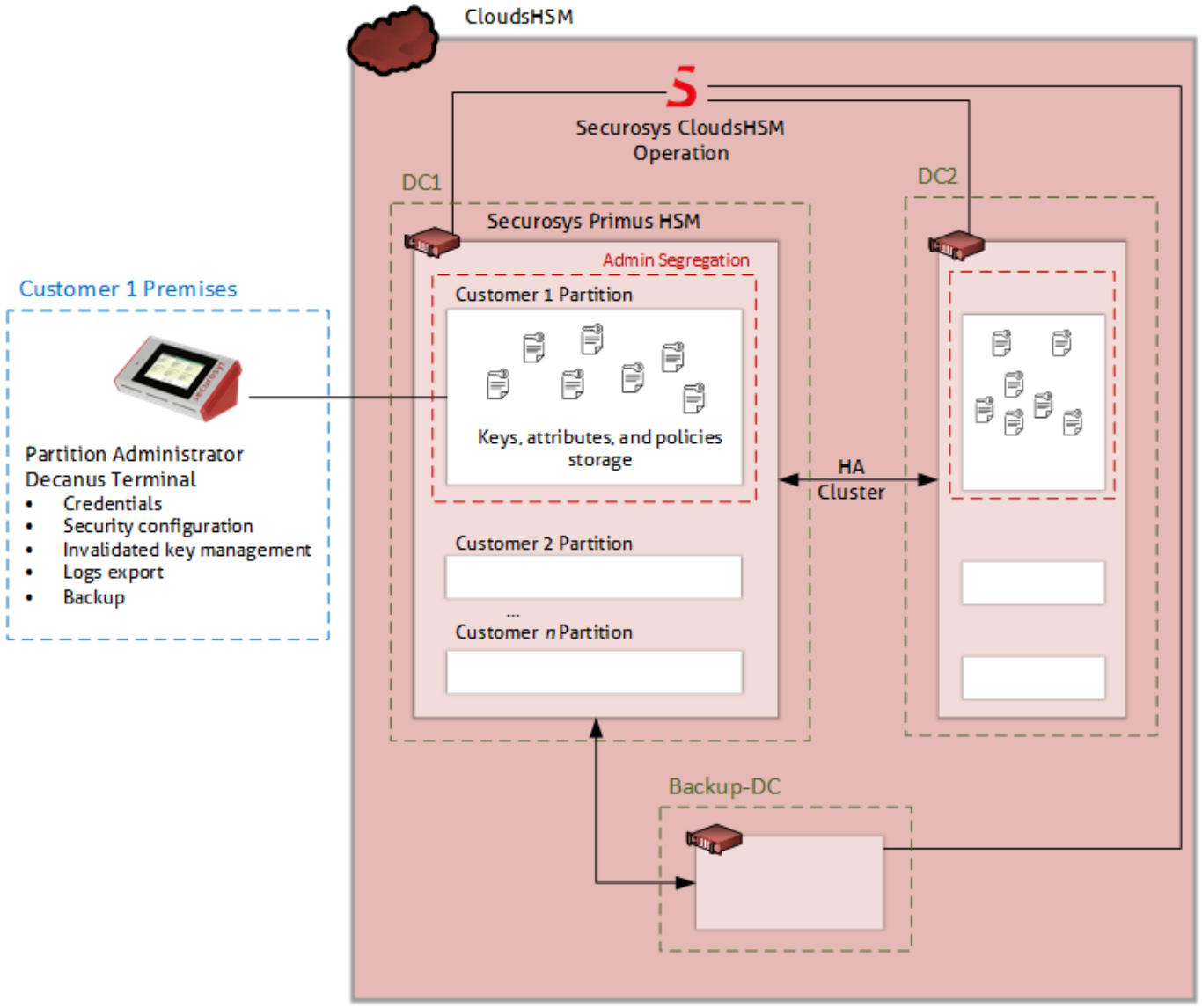
Advantages of a Securosys HSM...

- Tamper protection of the key material storage
- Keys generated with true hardware entropy
- Advanced key operation approval capabilities
- Simple integration via CNG, PKCS#11, and Java
- Designed, developed, and manufactured in Switzerland

... without the costs and operational overhead

- High-availability cluster
- Backed up in a military-grade bunker in the heart of Switzerland
- We manage the hardware, you control the access
- Scalable performance, capacity, and pricing

Architecture



High-level overview of the architecture as well as the segregation of access and responsibilities