Kron

Kron's Single Connect helps one of the world's leading banks to deploy PAM in 3 months

OVERVIEW

- One of the world's largest banks
- 16 million clients in 36 countries
- Market Cap. > 100B USD
- 89,000 employees

ABOUT THE COMPANY

Our client is one of North America's leading diversified financial services companies and provides personal and commercial banking, wealth management, insurance, investor services, and capital markets products and services at a global scale.

Our client has 89,000+ full-time and part-time employees who serve 17 million clients in Canada, the U.S., and 27 other countries.

The IT infrastructure is distributed due to their operations in different countries. They have 4 big data centers: Canada, New York, London, and Singapore, and operations teams are distributed all over the world.

CHALLENGE

Our client required a PAM solution that would comply with their distributed and populated architecture. Having 4 data centers in Canada, New York, London, and Singapore, and distributed operations teams, they required a system that would be scalable, highly available, and support a variety of connection types to different types of network elements, such as switches and routers, on top of Unix and Windows based systems. Additionally, they required a controller architecture where the changes/updates on the central node replicate in real-time to the distributed instances accommodated in other data centers. Due to legal regulations and the impact the slightest interruption in services has on financial liabilities, the assigned importance to access control and continuous and indisputable logging was inevitable.

Our client prioritized ease of deployment and scalability

Due to a bad experience with another PAM vendor with whom they could not make a deployment for two years, our client prioritized ease of deployment. They required a quick POC to test the PAM product on their complex infrastructure that results from a mix of interconnected legacy and new generation systems, such as network elements (switches, routers, firewalls), Unix and Windows based systems. Scalability was another concern as there were more than 19.000 devices to be integrated. They were looking for a system that would scale in a resource-efficient manner.

Controller-based architecture

For their complex and populated architecture, our client needed to manage the data centers' policies from a central location, which they called a controller node. Through the controller node, they needed to manage the policies of the 4 different datacenters. Pulling the access and session logs from the different data centers was also another significant use case for the client.

Easy Device and Account Onboarding

Our client required easy onboarding for devices and accounts for +15.000 devices. They thought installing agents would not only make the deployment period longer but also the maintenance of those agents would make their life harder.

SOLUTION

## Kron Technologies offered its agentless architecture for ease of deployment

Single Connect's modular, agentless, and pre-integrated architecture minimizes the project implementation time by unifying access management in a single pane of glass from day one and gives flexibility to the gradual implementation of multi-divisional integrations.

Controller architecture

The Single Connect Controller (SCC) is a controller layer within the layered architecture of Single Connect (SC) which sits above the SC Instances. The main purpose of the SCC is to manage SC in a controlled way within a centralized system.

Controller Benefits

- Single Centralized Management (Fault, Configuration, Performance, Security)
- The changes/updates on the Single Connect Controller replicate real-time to the Single Connect instances.
- Consolidated and local Log Access
- Simple Management for Distributed Architecture on Different Time zones (On-Premise, Cloud, Hybrid)
- Fastest Deployment (Single version of System Configurations & Parameters)
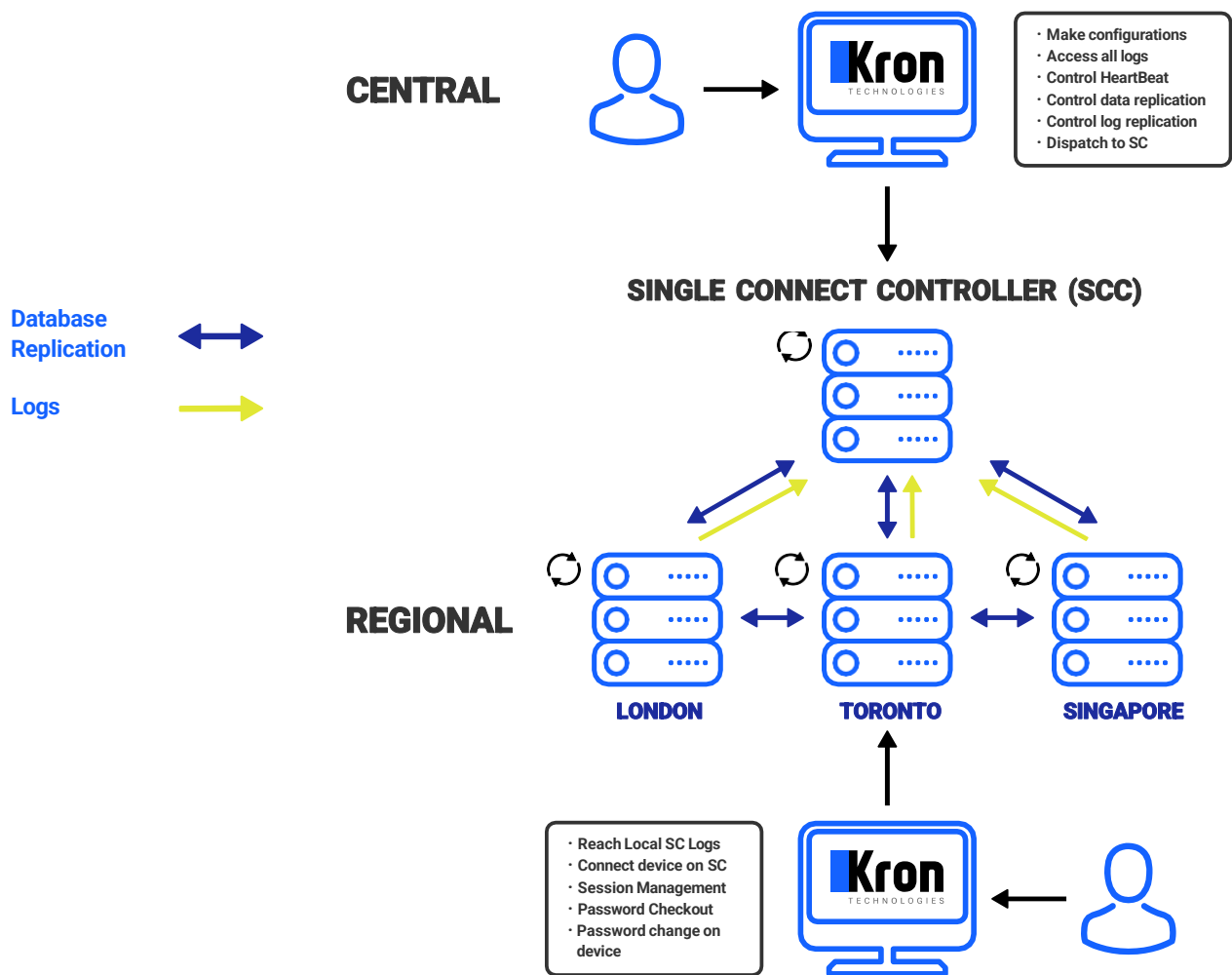
www.krontech.com

Privileged Session Manager and Password Management for Heterogenous Networks

To manage the client's heterogeneous and populated network composed of 19.000 devices, Kron Technologies has provided its Privileged Session Manager and Dynamic Password Controller to manage sessions and passwords for network devices, Windows and Unix based systems. Recognizing the importance of securing privileged accounts and devices, Kron Technologies implemented 360° onboarding of the client's infrastructure. Kron Technologies also consulted with the client on best practices to manage privileged access, password rotation strategies, approval workflows, dashboard views, and critical reports to provide comprehensive insight into the client's access security.

High availability for business continuity

To ensure the service continuity for critical IT infrastructure and uninterrupted access to company IT users, Kron Technologies provided a comprehensive redundancy plan. This plan included geo-redundancy by deploying multi-site clusters, and cluster-level redundancy by having multiple instances in each cluster with runtime replication across all instances and clusters.

RESULT

Fast deployment with Agentless architecture

Kron Technologies implemented this PAM solution in 3 months for 19.000 devices with geo-redundancy. By embracing a man-in-the-middle approach, our client does not need to make any operational changes through their IT infrastructure or deal with installing additional agents on target devices.

Our client manages all the PAM instances through a single-user interface

Thanks to the Single Connect Controller architecture, they can manage all data centers' instances, session policies, and logs through a single-user interface.

Unified Privileged Access Management

Single Connect's unified and centralized Privileged Access Management, bringing together company-wide IT and network environments.

www.krontech.com