CASE STUDY

ROBUST TIME-BASED SSH KEY PROVISIONING

– Managed Secure Access to Big Data in the Cloud

The customer provides an enterprise big data analysis solution – the end-customers range in size from SMEs to corporate giants. The offered service by necessity requires operators to have fully audited system-level access to the end customers' data in the cloud-hosted services. This data access over the SSH protocol requires an automatic and controlled time-based provisioning of SSH keys with appropriate approval processes. The Universal SSH Key Manager® provided the access controls that enabled secure, controlled, and audit-compliant SSH key management.

BRIEF BACKGROUND

The customer's data analysis solution is provided as a managed cloud service. Their customers range from SMEs to corporate giants, and the service infrastructure consists of a very large cloud-based Linux environment that is managed and accessed remotely using the SSH protocol. The connections are established with strong public-key authentication (with SSH keys) for security and convenience.

The customer's staff requires constant secure and controlled access to the cloud hosts, and the customer required automated time-based provisioning of SSH key-based access for defined users. The automated provisioning was required to integrate with a proper change management approval process for auditability and visibility.

SOLUTION SELECTION CRITERIA

The customer's solution selection process was driven by their need for operational and cost efficiency. They had a strong preference for an off-the-shelf product-based solution (as opposed to a development project). In addition to product maturity, they also valued the vendors based on their subject matter expertise as this was seen as key to lower risk and higher return on investment. The customer also required integration with their user orchestration solution for user provisioning and de-provisioning.

From a technical perspective, the requirements hinged on fast and automated provisioning of time-based access that addressed their concerns for risk and governance – both the operators' access and server accounts were required to only be valid for a defined and approved time period, after which they must be automatically de-provisioned.

QUICK FACTS ABOUT THE CUSTOMER

- Initial deployment 4 000 servers with a growth path to 40 000
- Automatic SSH access and key provisioning and de-provisioning
- Annual subscription business model
- Entire system deployed in AWS
- Integration to existing tools for automatic account provisioning and de-provisioning

SOLUTION

The customer selected a solution based on Universal SSH Key Manager® from SSH Communications Security. The entire solution was deployed in the Amazon Web Services platform in which the customer's service also resides.

The User Portal component of Universal SSH Key Manager provides the customer a single, unified interface for complete request and approval workflows. The access and key provisioning and de-provisioning are performed by the key management functions of the Universal SSH Key Manager. The required SSH keys are created and access provisioned as requested, and in accordance with the approval process. The solution also tracks the life-time of the access and removes it automatically when it is set to expire (this logic is all built-in to the solution as SSH keys do not expire by default). Solution also logs all the requests, approvals and performed actions.

This access control mechanism is integrated with the existing security solutions of the customer. Operators are authenticated against the corporate AD according to their roles, while the access data is visible to the corporate SIEM solution. The solution is also integrated to the enterprise cloud change management and provisioning solutions for a fully integrated and automated access management workflow with enterprise-wide visibility and governance.

WHY SSH COMMUNICATIONS SECURITY?

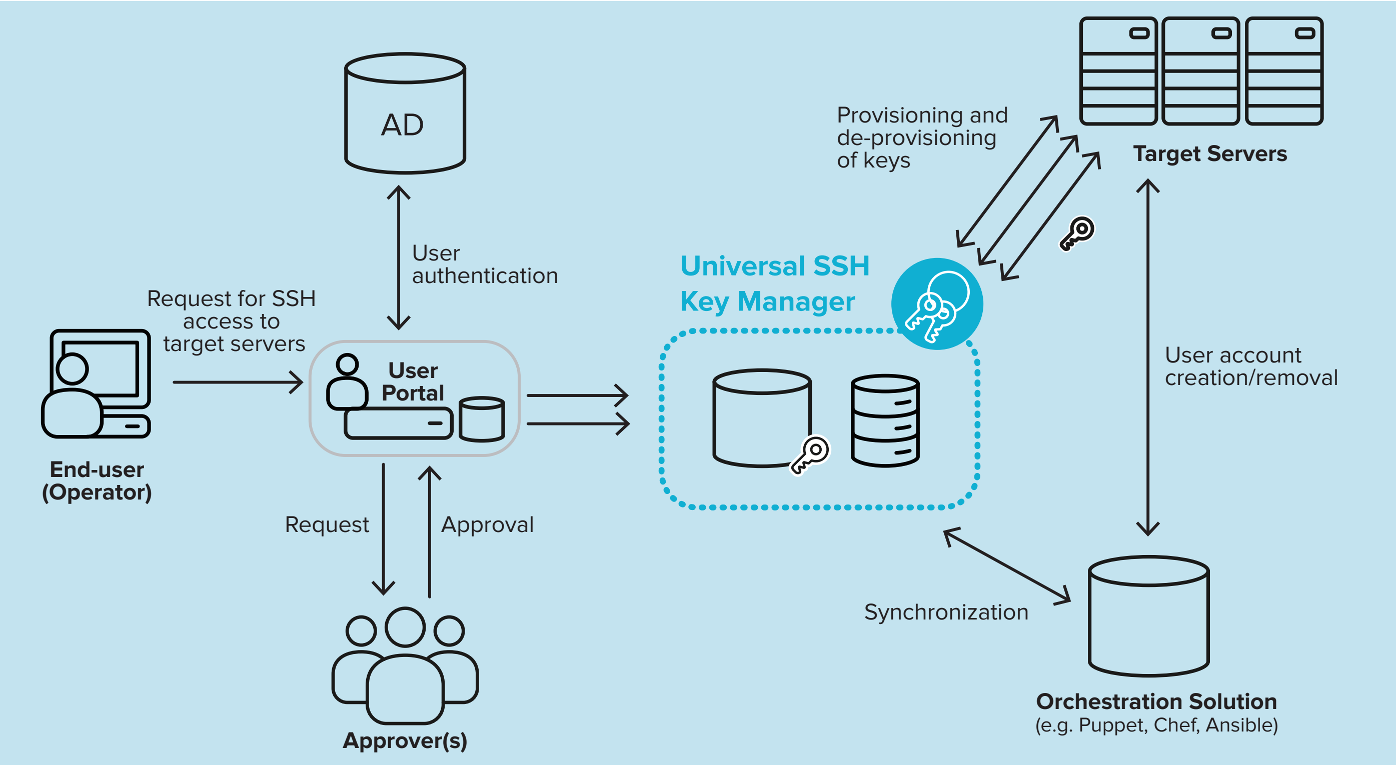
The customer's selections were quickly narrowed down to two – in-house development or the product-based approach from SSH Communications Security. SSH Communications Security's offering was selected based on the product and service maturity, as well as because of the readily available provisioning workflows. As the inventor of the SSH protocol, the subject matter expertise of SSH Communications Security was undeniable, and the availability of consultation and high-quality support tipped the scale to the company's favor.

A quote from one of customer's security architects summarize their evaluation of SSH Communications Security's customer service and consultation:

> ***"You guys are the SSH Communications Security – the inventors of the protocol. Why would I look for anyone else [for SSH key management]?"***

The SSH solution was also a clear favorite in the customer's "Value vs. Cost"-analysis. As in-house development of an SSH key management system is far removed from the core business of the customer, the TCO of an in-house system was seen as prohibitive.

Time-based SSH Access


AD
User authentication
Request for SSH access to target servers
User Portal
End-user (Operator)
Request
Approval
Approver(s)
Universal SSH Key Manager
Provisioning and de-provisioning of keys
Target Servers
User account creation/removal
Synchronization
Orchestration Solution
(e.g. Puppet, Chef, Ansible)