Subex Case Study

Migration from Azure EA to CSP

Subex at a glance

Subex is a leading provider of digital trust solutions to telecom operators, with a focus on enabling digital transformation and enhancing customer experience. Their solutions cover areas such as revenue assurance, fraud management, and cybersecurity.

Key Results

1. Successfully Migrated 173 machines in 24 hours.

2. Maximum down time was 8 hours and minimum was 1 hour.

3. Over 90 machines were migrated without boot partition including 25 different OS versions.

4. Some machines involved OS from the Top 5 Linux Distributions.37 of them were from different Linux Kernel versions.

5. Including various storage and partition types and all known file system types.

G7 CR Technologies

www.g7cr.in

Bangalore, India

CHALLENGES

Subex had a combination of Linux and Windows operating systems, but many of them were old or outdated versions. There were only a few machines that were compatible with ASR. Additionally, they had several different Linux distributions, including RHEL, CentOS, and Ubuntu. Moving the para-virtualized environment on the Zen platform technology on AWS was a challenging task.

SOLUTIONS

ASR Approach

A configuration server was established for machines that are compatible with automatic speech recognition (ASR) technology. This server was used to install mobility services and linked to Amazon Web Services (AWS). The synchronization process commenced to capture data from the source and transfer it to the destination. The collected data was stored in various storage accounts.

Failover

To ensure that everything is operating correctly, a test failover was performed. During the final failover, Azure created virtual machines using data that was previously collected from various storage accounts.

R-Sync Approach

To ensure that everything is operating correctly, a test failover was performed. During the final failover, the creation of a machine on Azure was carried out with a configuration that was similar to the one on AWS. Data synchronization from AWS to Azure was accomplished using R-sync. After this, the customer went live and the VPN tunnel was established successfully.

ROADMAP

After the migration, the virtual machines (VMs) do not have direct access to the internet to ensure security. Disk encryption was implemented to provide an additional layer of protection. To prevent accidental deletion of machines, a resource group lock was implemented. Automation was set up within the Azure environment, including auto-shutdown and email triggers. Communication between the machines was restricted to private IP addresses. Finally, OMS was utilized for data collection and optimization.