Streamlined OPENVPN Management

Overview

Our client is a leading Indian multinational technology company headquartered in Vadodara, renowned for its expertise in engineering research and development (ER&D) services. Their diverse portfolio encompasses a wide spectrum of specialized fields, including automotive engineering, embedded systems, semiconductor engineering, industrial internet of things, manufacturing plant engineering, and medical engineering. Within this dynamic environment, the client's infrastructure is a hub of multifaceted activities. To ensure seamless operations and resolve challenges promptly, our dedicated team engages in daily support and assistance, addressing the client's evolving needs with agility and expertise.

Opportunity

Our client is a global leader in Engineering and R&D (ER&D) services. With 1145 patents filed for 57 of the Global Top 100 ER&D spenders, the company lives and breathes engineering and technology.

Our client encountered a series of challenges with their AWS-hosted OPENVPN software. Firstly, users were struggling with persistent connectivity issues, leading to disruptions in remote access. The troubleshooting process for these problems was often complex and time-consuming. Additionally, users required clearer guidance on connecting to the software, and some faced difficulties during the installation process. The management of user accounts within OPENVPN, involving tasks such as user ID creation, password setting, permission updates, and account management, was complex and unwieldy. Ensuring secure access to specific servers through OPENVPN was a priority, as was the need to upgrade the license to accommodate growing demands. Furthermore, the client required Linux and Windows administration support to maintain system stability and performance.

These challenges collectively impacted the reliability and user experience of the OPENVPN service, necessitating ACC's intervention to address and resolve these issues effectively.

Why ACC?

Our client chose Applied cloud computing for this project due to ACC’s demonstrated expertise in AWS services, a track record of successful problem-solving, comprehensive and security-focused solutions, tailored support, prompt response, and cost optimization strategies.

Solution | Architecture & Services

We recommended SAP service connectivity with AWS infrastructure in LTTS-SAP like SAP HANA service allows to consume the SAP HANA database from applications running on SAP Business Technology Platform, as well as from applications running elsewhere using the standard SAP HANA clients.

Using Amazon Web Services (AWS) we have helped users to integrate and create value from data and extend their SAP and third-party solution landscapes to meet evolving business needs.

ACC recommended a comprehensive solution to address the various issues surrounding their AWS-hosted OPENVPN software:

- **Rightsizing Instances**: To optimize resource costs and performance, ACC recommended a rightsizing strategy for instances. This involved ensuring that resources were appropriately scaled to match their workload, while also leveraging cost-saving options like purchasing savings plans.
- **Daily Server Monitoring**: The solution included daily server monitoring using AWS CloudWatch. This proactive approach ensured the smooth operation of systems and enabled the timely identification and resolution of any issues, thus minimizing service disruptions.
- **Server Backup with AWS Backup**: To safeguard data and system configurations, ACC implemented a robust backup strategy using AWS Backup for EC2 instances. Scheduled backups and storage management were configured to ensure data integrity and recoverability.
- **VPN Tunnel Setup**: To enhance connectivity with critical applications and improve overall network security, ACC established VPN tunnels. This measure ensured secure and reliable connections between various components of the infrastructure, reducing the risk of unauthorized access or data breaches.
- **Security Best Practices**: As part of the solution, ACC also addressed security concerns by implementing best practices for major AWS services, including Identity and Access Management (IAM), S3, EC2, and Virtual Private Cloud (VPC). This comprehensive approach aimed to bolster the overall security posture of the OPENVPN infrastructure, safeguarding sensitive data and ensuring compliance with security standards.
- **AWS Transfer Family**: ACC proposed the implementation of the AWS Transfer Family to enable seamless and efficient access to S3 buckets for both internal and external users, including third-party organizations. This solution aimed to enhance data accessibility while maintaining security.

- **Integrations with applications:**

1.The SAP SLM to S4 connectivity was established with Cloud connector VM

2.Ariba Integration was achieved. We provided VMs with required configurations and provided connection between Source and Destination IPs. For integration in Ariba with Data center configuration we whitelisted IPs of Ariba US data center (QAS S4H to Ariba - IP whitelisting) We had provisioned VM Provision - SLT Server for CDC

3. Anaplan Connect – We provided VM for Anaplan Application. Also provided SFTP server and Bucket which for their training documents and another bucket for public URLs

4.SLT Application: SLT server was setup according to requirement

5.Ariba Application : VM provisioning for Ariba Application was implemented along with SFTP server provision. OpenVPN users were created for Ariba users

6.Azure to Immidart connectivity: S4 Prod to Immidart Connectivity was established tunnel was successfully setup and connections were tested on port 50000

- **AWS SES**: SES Email notification for SES Workflow for sending mails for SAP systems has been setup. Email bounce notifications has been setup and Account level suppression is enabled

By implementing these solutions, ACC's goal was to not only resolve the immediate challenges faced by the client but also to establish a robust and secure foundation for their AWS-hosted OPENVPN software, ensuring long-term reliability, performance, and data protection.

AWS services used are:

- **EC2 (Elastic Compute Cloud):** Provides resizable compute capacity for running virtual servers.
- **VPC (Virtual Private Cloud):** Allows the creation of isolated network environments with control over IP addressing, subnets, and routing.
- **IAM (Identity and Access Management):** Manages user identities and permissions for secure AWS resource access.
- **S3 (Simple Storage Service):** Provides scalable object storage for data and file storage.
- **EFS (Elastic File System):** Offers scalable and highly available file storage for EC2 instances.
- **AWS Transfer Family:** Facilitates secure data transfers to and from Amazon S3, including internal and third-party transfers.
- **CloudWatch:** Monitors AWS resources and applications, enabling performance optimization and issue detection.
- **CloudTrail:** Records AWS account activity for auditing, governance, and compliance.
- **AWS Backup:** Automates data backup and recovery for EC2 instances and other AWS resources.
- **Direct Connect:** Establishes dedicated network connections between on-premises and AWS resources.

- **Site-to-Site VPN:** Enables secure communication between on-premises and AWS networks.
- **Security Hub:** Provides a comprehensive view of security alerts and compliance status across AWS accounts.
- **KMS (Key Management Service):** Manages encryption keys to safeguard data at rest and in transit.
- **Lambda:** Allows serverless computing for automating tasks and handling event-driven actions.
- **Route53:** Provides scalable and reliable DNS (Domain Name System) management.
- **SNS (Simple Notification Service):** Sends real-time notifications to a variety of endpoints.
- **SES (Simple Email Service):** Sends and receives email using a scalable and reliable email platform.
- **Config:** Helps assess, audit, and evaluate AWS resource configurations for compliance.
- **Systems Manager:** Simplifies the management and operation of AWS infrastructure and applications.

Outcome

ACC's solutions successfully resolved the client's OPENVPN challenges. Connectivity issues were eliminated, troubleshooting became efficient, and user guidance improved. User management processes were simplified, server access was secured, and the OPENVPN license was upgraded for scalability. Security was enhanced through AWS best practices, while resource optimization and proactive monitoring ensured cost-efficiency and reliability. Data protection was prioritized with robust backup strategies. Efficient network management, compliance assessments, and streamlined operations further improved the client's infrastructure. Overall, ACC's intervention led to a secure, efficient, and scalable AWS-hosted OPENVPN environment, addressing the client's immediate needs and ensuring long-term reliability.