Microsoft Windows Server Upgrades on AWS for George Mason University

George Mason University

Founded

1980

Headquarters

Arlington, VA

Industry

Education

About George Mason University

The George Mason University (GMU) is the world's premier university source for market-oriented ideas, bridging the gap between academic ideas and real-world problems. A university-based research center advances knowledge about how markets work to improve people's lives by training graduate students, conducting research, and applying economics to offer solutions to society's most pressing problems.

Challenge

The GMU was using Amazon Web Services (AWS) for cloud hosting services. They were using a Cisco Anywhere Virtual Private Network (VPN) to connect from the GMU network using four end user Virtual Local Area Networks (VLAN). The environment had a single AWS Account with four Virtual Private Clouds (VPC), 2 for load balancing, 1 for Active Directory Federation Service (ADFS), and 1 for other workloads. The entry point for all traffic to the VPCs was through the GMU network with a single backdoor entry point for situations when access through the GMU network might be down. The GMU was seeking an AWS Consulting Partner to assist them with upgrading their 3 Windows 2012 R2 servers to Windows 2019. They were primarily looking to improve the security posture of their AWS environment.

Solution

stackArmor performed the task by deploying an experienced team of AWS certified Solution Architects with specific experience with Windows workloads on AWS. The team conducted a thorough assessment of the environment – including data, services, roles, applications (including third-party). Given that the requirement was to keep the same hardware and all the server roles

set-up without flattening the server, stackArmor performed an “in-place upgrade”, which basically means you go from an older operating system to a newer one, keeping your settings, server roles, and data intact.

As part of the migration, stackArmor was able to analyze the current configuration, perform backup, conduct upgrade for production server, re-route traffic, and re-configure tools (Amazon Elastic Compute Cloud) for monitoring. In addition to these tasks, testing and validation were also included as part of the service. stackArmor was successfully able to complete the live server migration and support project for GMU.

About stackArmor

stackArmor is an Advanced AWS partner specializing in FedRAMP, FISMA, MARS-E 2.0 and DFARS compliance for DOD, Federal Agencies, Government Contractors, ISVs and SaaS providers as well as Educational Institutions. stackArmor provides cloud architecture strategy & assessments, cloud migration, managed services, and managed security services for compliance focused customers. stackArmor provides NIST and cybersecurity services using the stackArmor ThreatAlert™ security system to accelerate compliance with NIST, FedRAMP, FISMA, and DFARS requirements for AWS based applications. Our solutions are delivered by certified and battle tested solution architects and information assurance professionals. Please visit our website and learn more about our education focused cloud security and compliance services at https://www.stackArmor.com/Education