Rapid Environment Spin Up

anm

Using RPA to check Home Assistance Applications

ANM deployed an AWS based environment of Automation Anywhere to ingest, validate and check applicant eligibility to greatly reduce the time required for applications to be approved.

Client Challenge

The Department of Labor has been inundated with housing assistance applications since the start of COVID. They needed a mechanism to help check that housing applications were properly filled out and not fraudulent.

ANM has been working with customers using Automation Anywhere, an RPA software to validate forms and check them for fraudulence and validity. While the customer has an on-premises datacenter, they needed more resources spun up quickly to deploy and configure this software.
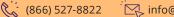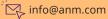
ANM SOLUTION

Following a thorough requirements gathering process, ANM developed and deployed a multi account AWS solution to accommodate the Automation Anywhere software. ANM deployed a fully managed EC2 solution managed by AWS Directory Service and AWS SSM. The solution also employed AWS FSx to share machine data between all the worker nodes

For the compute stage, ANM developed custom EC2 instances to support the needs of the software. The instances were connected to a central domain using AWS's Directory services for simple management. AWS FSx for Windows File server was using to mount CIFS drives that all worker nodes used to share files. Each instance was centrally managed using SSM for automated deployment of configurations, directory joins and script executions.

aws

We'd love to hear from you.

(866) 527-8822   info@anm.com   anm.com

The Result

Using our four-step solution methodology, ANM completed the project on time and on budget, in tandem with other high- priority projects. The automated nature of this solution also ensures that newly created accounts do not require additional deployment efforts.

Benefits

Reduced time to Housing Assistance for Families

Increased Security

Centralized IT configuration and administration

Customized policy exemptions access roles

Robust security protocols, including role-based access and customer-managed granularity

Customized approach

AWS SSM

The worker nodes needed to be able to join a domain, run scripts and have software deployed once they were brought online. AWS SSM made it easy to centrally control all the worker nodes from a single pane of glass to handle any changes the environment required.

AWS FSx

The worker nodes needed to be able to join a domain, run scripts and have software deployed once they were brought online. AWS SSM made it easy to centrally control all the worker nodes from a single pane of glass to handle any changes the environment required.

MONITORING

To ensure that any changes to the environment were logged and sent to a central repository ANM enabled CloudTrail for organizations. This enabled the logs from all accounts to be centrally stored in a single account for simple monitoring going forward. This also improved the security of the worker accounts as any tasks done in the worker account was moved to a separate account to prevent tampering within the worker account.

SECURITY

ANM needed to ensure the environment was secure from every possible angle. To ensure the edge of the network stayed secure the use of Palo Alto edge firewalls were deployed. Inside the environment all S3 buckets and SSD drives were encrypted to ensure data integrity. In the network the use of Security Groups was used to limit communication between instances to the ports and protocols required to limit bad actors from moving east/west.

INFRASTRUCTURE AS CODE

To keep the environment in a pristine condition the use of IaC was used to ensure the environment was deployed to a predetermined spec. ANM made use of Terraform and Terraform Cloud to rapidly deploy the environment and ensure that all pieces were deploy correctly. Including EC2, Palo Alto, VPC, AWS Directory Services, AWS SSM, IAM Roles, AWS FSx, S3, CloudTrail, and Security Groups. This allows for the environment to be easily modified without having to have multiple touchpoints within the environment. It also limits who has access to what resources ensuring only a single role attached to Terraform has the permissions to make changes.