**Infrastructure as code and Automation of a Security Agent Installation**

Using infrastructure as a code to automate security agent installation on multiple VMs in AWS

Tools/Services:

* Terraform
* AWS System Manager
* Amazon Simple notification Services (SNS)

A screenshot of a computer

Description automatically generated

**Hands On Project - Part 1 - Terraform**  
  
- Download VSCode and install the Terraform extension:  
https://code.visualstudio.com/download  
  
- Download and unzip Terraform files  
https://tcb-bootcamps.s3.amazonaws.com/bootcamp-aws/en/terraform-mod5.zip  
  
  
- Edit Terraform main.tf file using the VSCode:  
-- Change the VPC\_ID and SUBNET\_ID according to your default VPC  
  
- Create SSH Key Pair  
-- name: sshkey1  
-- format: .pem  
  
- Install Terraform on AWS Cloud Shell  
  
sudo yum install -y yum-utils  
sudo yum-config-manager --add-repo https://rpm.releases.hashicorp.com/AmazonLinux/hashicorp.repo  
sudo yum -y install terraform  
  
- Upload your edited terraform code to AWS Cloud Shell and unzip it  
  
- Run terraform  
  
$ terraform init  
$ terraform plan  
$ terraform apply  
  
- Explore more about Terraform on https://learn.hashicorp.com/terraform  
  
**Hands On Project - Part 2 - AWS Systems Manager**  
  
- Create an IAM role SystemsManagerToSNS  
  
Policy: AmazonSNSFullAccess  
  
- Create a Notification Topic DevOpsNotification | Copy the ARN  
  
- Create a subscription - email:  
  
- Run the System Manager Quick Setup  
-- Targets: choose instances manually  
  
- Validate the 'configuration':  "Success" status  
  
- Explore the Session Manager connecting by SSH browser (please note: if the EC2 instances don't show up, reboot both instances using the EC2 console to re-run the SSM-agent startup script)  
  
- Execute "Run Command" to deploy the "security agent instalation"  
  
-- Command document: AWS-RunShellScript  
  
-- Command parameters:  
  
sudo wget -q https://tcb-bootcamps.s3.amazonaws.com/bootcamp-aws/en/install\_security\_agent.sh -P /tmp  
sudo chmod +x /tmp/install\_security\_agent.sh  
sudo /tmp/install\_security\_agent.sh  
ls -ltr /usr/bin/security\_agent  
  
-- Targets: choose instances manually  
  
-- Uncheck enable writing to S3 Bucket.  
  
-- Enable SNS Notification  
  
IAM Role: SystemsManagertoSNS  
SNS Topic: <ARN>  
  
Events notifications:  all Events  
  
Change notifications  
  
Notify me for: Per instance basis  
  
- Open the AWS Cloud Shell and remove the resources created by Terraform  
  
(If needed, re-install the Terraform following the same steps used previously)  
  
cd terraform  
./terraform destroy  
  
That's All! Congrats, Bootcamper!  
  
**Supporting Links:**  
  
https://aws.amazon.com/premiumsupport/knowledge-center/systems-manager-ec2-instance-not-appear/