Intro…

Myself Abhishek and i have been holding my graduation.i have around 2 years of experience in IT industry and

i started my professional career with tcs ..

Currently i am working under the Secure Home Gateway project and im the part of L1 team, having the size of 9 members including one team lead. Coming to my role in this project as a apps engineer and we work in 24/7 shifts.

1-My day start with health checks of the production environments(ODIN & ALOE) by running health check scripts against production environments and see all the services are up and running ..

2 - And then check for the INCIDENTS in Service now ticketing Tool and resolve accordingly (DISK SPACE, MEMORY, CPU, SERVICE not running, URL's unreachable with http error code (500, 404, 403)

3 - we configured **CLOUDWATCH and SiteScope** in our environment .

4 - As per requirement, every day check for **cloudwatch** alerts according to that, when the threshold limit reached(for example >80% ), I used to respond accordingly. We configure SNS topics for getting notification for particular user for getting alerts. Internally we keep our own mail to get alerts and use to clear accordingly . By the end of the day we used to get reports of monitoring for production environment from sitescope, and send them to manager.

5 - As per requirement I modify ec2-instance and change their type by asking manager if get alerts.

I used to create **AMIs** for test environment.

6 –In our test environment everyday work on different modules and once in a while integration test. For that I manage to create VPC’s, S3 –buckets, and to maintain ACL’s in S3 and I write policies to S3 bucket. And I create **IAM users** for **production environment** and **test environment** for giving console access or programmatic access .

7 – I use to work on Build Automation Tool MAVEN by using Maven Plugin into Jenkins and also Git plugin is added to Jenkins.

8 - I use to work in Configuration Management  Tool Ansible

1. To push user keys to developers for multiple environments. Many developers come up with asking access to Beta environments so we push their public keys using Ansible.
2. Patching servers for security for every 3 months
3. Upgradation of packages and services .
4. Whiletlisting IPs (for few customers to access support portal to monitor the health check of production environmets)
5. Repeated tasks like stopping and starting for services in mutliple servers
6. Basic deploymensts(So we deploy package code developers send this package through shared path or copy to S3, We use development scripts and push to respective environment folder since our servers are in autoscaling group we increase autoscaling count and see the new package come into server and service up and running)

**TELL ME ABOUT YOUR PROJECT**

**Our project details with the router Level security for IOT(internet of things) devices in home . By clicking the website DNS name**

**In our GIT DB and sees if that site is flagged as maliciuas site or not , it allows the users to access the site if not mark's as a maliciuas ,it will not allow it is maliciuas website ..**

**Memory alert** : if memory is impacting application (app not funtioniong) then we disable it from Load balancer and restart the application )

**CPU** : becasue of this some time server gets hung , this can impact application , so we disable it and if needed we reboot the server

**Disk Space** : most of the time we clear the old log files , /var/log/ (df -h , du -hsc \* | grep G )

**Service down alerts** : we login to the respective server and check the service status ( systemctl status service , service status servicename)

**Network issues** : port not listening ( netstat -nlp | grep portnum) , tracert , ping

**Erros: 500**( internal server error =server unable to process the request there could multiple reasons like , server is loaded (memory , CPU )

**Error :404** : page not found (clinet trying to access a page which is not avaiblable )

**error: 403**: Forbidden ( trying to access a page which user don't have access)

**Error : 401** : page requires credentiasl (userame and password)

GOOD response codes : 200 ok success , 302 - redirection

**SSL**

1. create private key for ssl <https://www.digitalocean.com/community/tutorials/how-to-create-a-ssl-certificate-on-apache-on-arch-linux>

We generate key using openssl tool (steps are in above link)We use the same key to generate .csr file and send this this file by logging a request to our internal Domain teamby attacing only .csr file , they process the request and send the mail , we dowload the file and convert to .pem and upload to aws using IAM , then we use this ssl for the loadbalacers ..

1. CN = \*.w3schools.com
2. OU = IT
3. O = Verizon Digital Media Services, Inc.
4. L = Los Angeles
5. S = California
6. C = US