8K Miles
Cloud | Identity | Big Data | Mobile
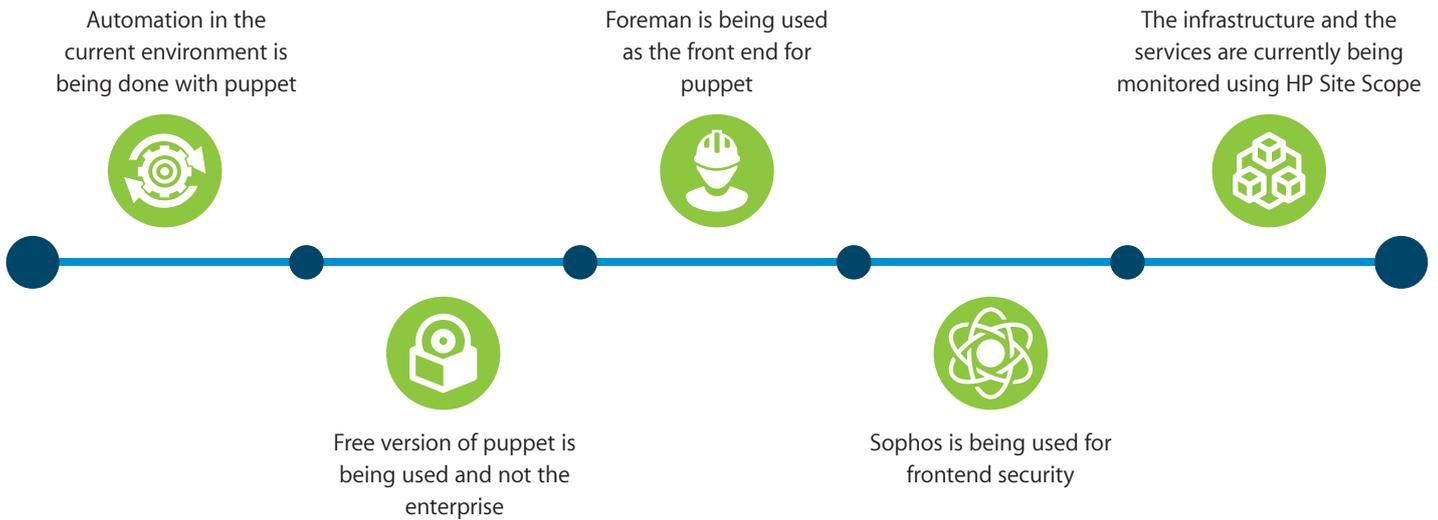
PUPPET DEVOPS FOR NAVIGATION ENTERPRISE

About the Client

Trimble Hosting Services provides global managed IT services for industry leading ASP and Software as a Service product. These application services include applications for mobile resource management, construction machine, construction site management and precision surveying. Companies use these services to maximize the productivity and efficiency of their mobile workforces and to optimize productivity of machines and other assets.

The Challenge

Being AWS customer this Enterprise Company already had basic setup to suffice their limited DevOps requirements. But the limitation of existing setup started creating hindrance on their ever growing infrastructure. To overcome that they decided to redesign their DevOps/Automation architecture which can adhere to their future growth. Along with this they were looking to achieve fault tolerance by virtue of high availability for all the critical components participating in this design.

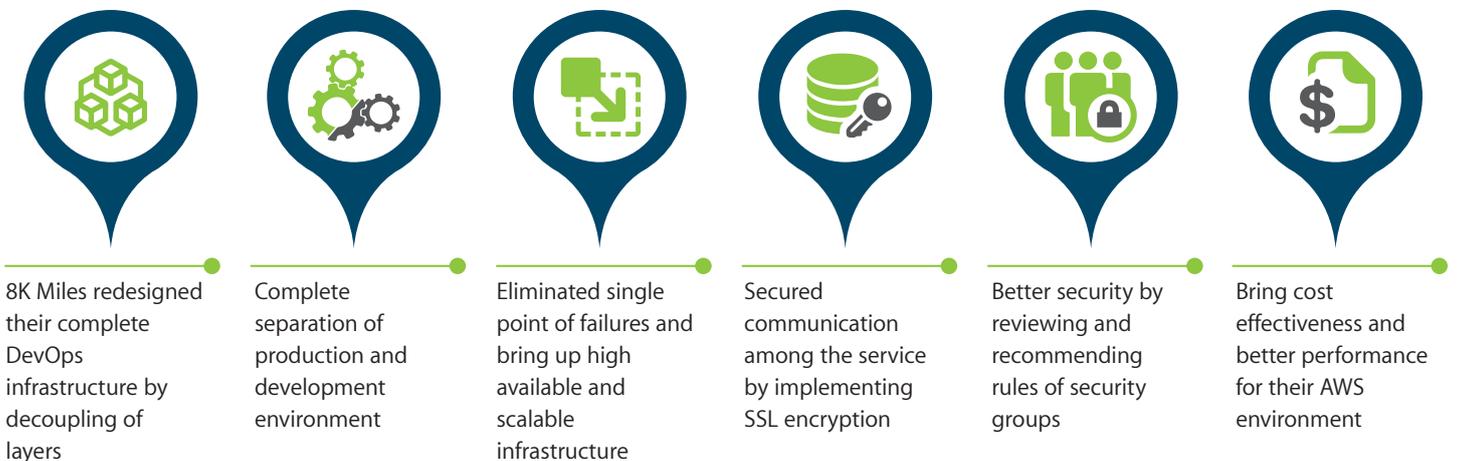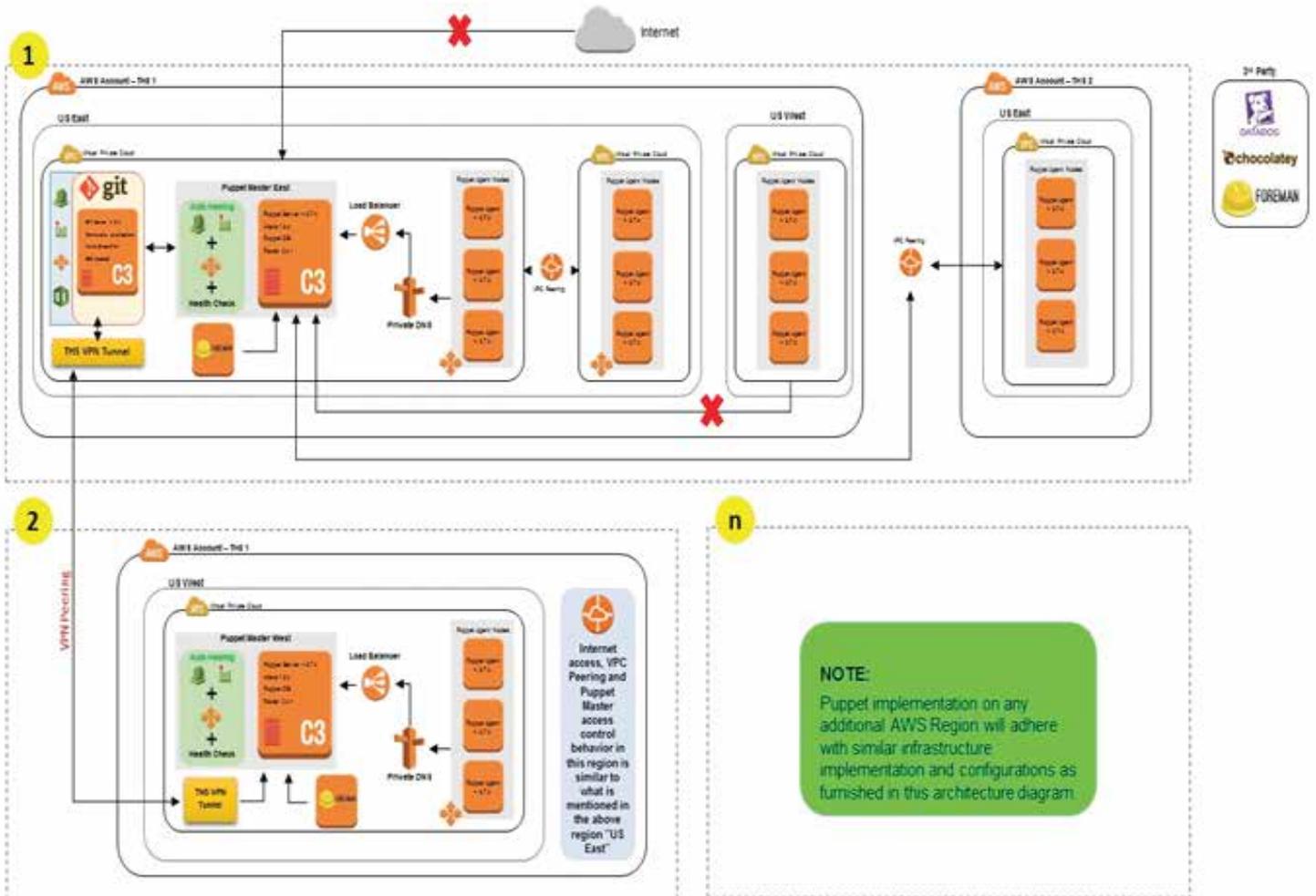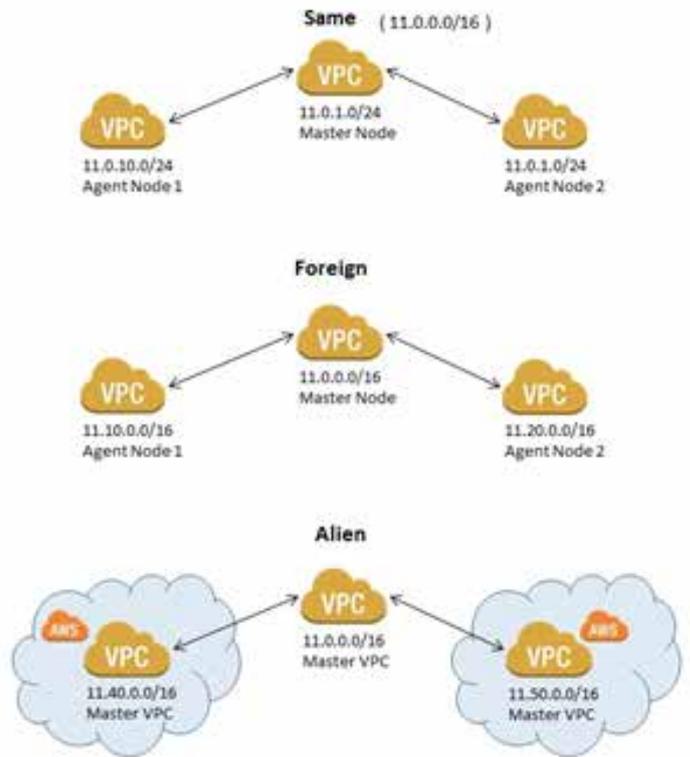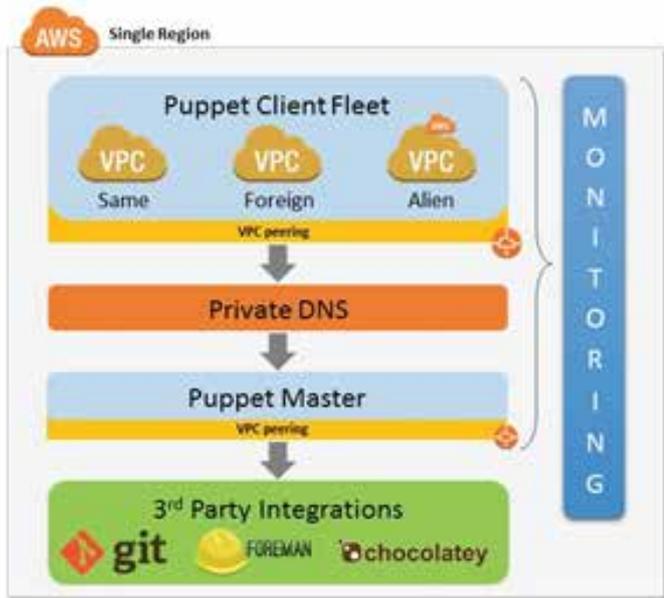## Existing setup of their DevOps is explained below-

Automation in the current environment is being done with puppet

Foreman is being used as the front end for puppet

The infrastructure and the services are currently being monitored using HP Site Scope

Free version of puppet is being used and not the enterprise

Sophos is being used for frontend security

Why AWS

AWS provides a set of flexible services designed to enable companies to more rapidly and reliably build and deliver products using AWS and DevOps practices. These services simplify provisioning and managing infrastructure, deploying application code, automating software release processes, and monitoring your application and infrastructure performance. DevOps is the combination of cultural philosophies, practices, and tools that increases an organization's ability to deliver applications and services at high velocity: evolving and improving products at a faster pace than organizations using traditional software development and infrastructure management processes. This speed enables organizations to better serve their customers and compete more effectively in the market.

Our Solution

After understanding their requirement, use-cases, pain points, we proposed an architecture where the whole setup has to be redesign inside Amazon VPC with all the AWS security best practices in place. We took to the tasks of DevOps implementation of their setup on AWS Cloud, along with 24/7 Managed Services, rendering the client Scalability, High Availability, Security, DevOps and Support.

8K Miles redesigned their complete DevOps infrastructure by decoupling of layers

Complete separation of production and development environment

Eliminated single point of failures and bring up high available and scalable infrastructure

Secured communication among the service by implementing SSL encryption

Better security by reviewing and recommending rules of security groups

Bring cost effectiveness and better performance for their AWS environment

Same (11.0.0.0/16)

VPC
11.0.1.0/24
Master Node

VPC
11.0.10.0/24
Agent Node 1

VPC
11.0.1.0/24
Agent Node 2

Foreign

VPC
11.0.0.0/16
Master Node

VPC
11.10.0.0/16
Agent Node 1

VPC
11.20.0.0/16
Agent Node 2

Alien

VPC
11.0.0.0/16
Master VPC

VPC
11.40.0.0/16
Master VPC

VPC
11.50.0.0/16
Master VPC

AWS Single Region

Puppet Client Fleet

VPC Same | VPC Foreign | VPC Alien

VPC peering

Private DNS

Puppet Master

VPC peering

3rd Party Integrations
git   FOREMAN   chocolatey

MONITORING

Internet

NOTE:
Puppet implementation on any additional AWS Region will adhere with similar infrastructure implementation and configurations as furnished in this architecture diagram

DevOps on AWS

- Entire stack was provisioned automatically in AWS using Amazon CloudFormation template. AWS CloudFormation offered the developers and systems administrators an easy way to create and manage a collection of related AWS resources, provisioning and updating them in an orderly and predictable fashion
- DevOps automation with Puppet, CFT, PowerShell DSC
- Monitoring tool (ForeMan and its integration with Cloud Watch)
- Deployment to various environments was handle using GIT Hub
- Load Balanced using Amazon Elastic Load balancers
- Region based puppet master provisioning i.e. each region will have their own puppet master
- All virtual machines will be within a VPC
- All VPC's will be VPC peered
- Traffic route to Puppet master to happen via Private DNS
- Puppet server will reside on a C3 Linux box (Redhat 6.6) with
  - Hiera 1.3.4
  - Puppet DB
  - Facter 2.4.1
- Puppet master will be made highly available via Auto Healing
- Separate Git server will be provisioned and configured for version control management
- Foreman will be installed, paired with the Puppet master and will be used for view purposes
- Role based node identification while catalogue run and corresponding configuration management via Puppet master
- Secured Assets stored and delivered from Amazon S3
- Amazon CloudWatch and Amazon SNS set up to monitor resources, send notifications, track logs and metrics
- AWS CloudTrail and AWS Config set up for Security and Governance
- If any major change is being made to the Puppet Master Server, an automated script will take a new AMI of this machine and make it the Golden AMI for further Autohealing operation of the Puppet Master

Design for HA/DR

- HA ensured by using Multiple AWS Availability Zones within a region
- Usage of Fault tolerant building blocks like ELB, S3, SNS for HA
- ELB + Auto healing of puppet master was ensuring HA for newly created setup

Design for Security

- Isolated network using Virtual Private Cloud (VPC)
- Each layer of the architecture will be encapsulated with multiple layers of security which comprises of ACL's, Security Groups and user accounts accesses
- All puppet related communication will be private. Each and every layer will have individual security groups created in AWS which will have layer specific inbound access. No other port communication will be allowed across layers
- VPC peering will be configured for inter VPC communication within the account and across accounts for the same region
- Inter region VPC communication will be made possible via VPN peering, which is already established and managed by the customer
- AWS IAM and MFA for access control deciding what role and how one will interact with provisioned services
- VPC Flow logs and CloudWatch logs for security

Business Impact

- By leveraging AWS services, customer's environment became Robust and stable
- A production grade Puppet Master server is functional and the same is backed up on a regular basis
- Sensitive and Stateful information related to Puppet Masters functionality is maintained and paired with the in house GIT server thus, making it enterprise grade DevOps process
- The whole process of provisioning and configuring existing/new infrastructure has been reduced to one click to ensure minimal downtime

San Ramon, CA (HQ)

12647 Alcosta Boulevard,
Suite 450,San Ramon, CA 94583, USA
www.8kmiles.com
sales@8kmiles.com
Direct   : 925-270-4800
Toll-Free   : 855-856-4537

Chicago, IL

1827 Walden Office Square
Suite #460
Schaumburg, IL 60173
Phone : 708-289-5111

Dallas, TX

17740 Preston Road
Suite #200
Dallas, TX -75252
Phone : 214-272-2404

Chennai, India

Srinivasa Towers
New No.5, Old No. 11,
Cenotaph Road,
Alwarpet,Chennai – 600 018
Phone : +91-44-6602-8000
Fax   : +91-44-4300-9049

Ontario, Canada

4 Robert Speck Parkway,
Suite 1500,
Mississauga, Ontario L4Z 1S1
Phone : 416-366-7762

Sharjah, UAE

Q1-05-109/C
SAIF Zone
PO Box 121213
Sharjah-UAE