

AWS Current-State Configuration

Account ID:

Account Alias:

American Express Global Business Travel

SOW# 00007620

Architecture Assessment

**Deliver To:**

Neil Kirk

VP – Global Technology Services Platform Engineering and Technology

**Prepared By:**

Computacenter US

AJ Cruz, CCIE 50268

Principal Consultant

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| One University Ave,  Suite 102  Westwood, MA 02090 |  | p. 714-861-2200 |  | www.computacenter.com |

Table of Contents

1. [Document Control 3](#_Toc131827692)
2. [Introduction 4](#_Toc131827693)

[Document Overview](#_Toc131827694)

1. [AWS Account Dashboard 4](#_Toc131827695)
2. [Best Practices & Health Static Auto-Analysis 4](#_Toc131827696)

[Transit Gateway Analysis](#_Toc131827697)

[VPN Analysis](#_Toc131827698)

[VPC Analysis](#_Toc131827699)

[Load Balancer Analysis](#_Toc131827700)

[EC2 instance Analysis](#_Toc131827701)

1. [VPCs 5](#_Toc131827702)
2. [Route Tables 5](#_Toc131827703)
3. [Route Tables - Routes 5](#_Toc131827704)
4. [Prefix Lists 5](#_Toc131827705)
5. [Subnets 5](#_Toc131827706)
6. [Network ACLs 5](#_Toc131827707)
7. [Network ACL – Inbound Entries 5](#_Toc131827708)
8. [Network ACL – Outbound Entries 5](#_Toc131827709)
9. [Security Groups 5](#_Toc131827710)
10. [Security Group – Inbound Entries 6](#_Toc131827711)
11. [Security Group – Outbound Entries 6](#_Toc131827712)
12. [Internet Gateways 6](#_Toc131827713)
13. [Egress-Only Internet Gateways 6](#_Toc131827714)
14. [NAT Gateways 6](#_Toc131827715)
15. [Endpoint Services 6](#_Toc131827716)
16. [Endpoints 6](#_Toc131827717)
17. [Peering Connections 6](#_Toc131827718)
18. [Transit Gateways 6](#_Toc131827719)
19. [Transit Gateway Routes 7](#_Toc131827720)
20. [VPN – Customer Gateways 7](#_Toc131827721)
21. [VPN – Site-to-Site Connections (Connected to Transit Gateways) 7](#_Toc131827722)
22. [VPN – Virtual Private Gateways 7](#_Toc131827723)
23. [Direct Connect Gateways 7](#_Toc131827724)
24. [Load Balancers 7](#_Toc131827725)
25. [Load Balancer Target Groups 7](#_Toc131827726)
26. [EC2 Instances 7](#_Toc131827727)

# Document Control

**Preparation**

|  |  |  |
| --- | --- | --- |
| ****Action**** | ****Name**** | ****Date**** |
| Technical Content & Formatting | [Engineer’s Name] | 7/2/2015 |

**Release**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | ****Date Released**** | Change Notice | Pages Affected | ****Remarks**** |
| 1.00 | 7/2/2015 | All | All | Initial release |

**Distribution List**

|  |  |  |  |
| --- | --- | --- | --- |
| ****Name**** | ****Organization**** | ****Role**** | ****E-mail**** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Introduction

GBT has engaged Computacenter US to provide consulting services to assess GBT’s network architecture and configuration to provide recommendations and a roadmap to optimize and stabilize the environment.

## Document Overview

This document captures the current network configuration of an AWS account (identified on the title page and the account dashboard below). All data is gathered via the AWS API using the Python Boto3 client.

Additionally, data returned by the API is used to auto-generate some basic best-practices analysis as well as health status of various objects (VPN connections, etc.)

Amazon-published best practices are used for reference:

* <https://docs.aws.amazon.com/vpc/latest/tgw/tgw-best-design-practices.html>
* <https://docs.aws.amazon.com/vpc/latest/userguide/vpc-security-best-practices.html>
* <https://aws.amazon.com/blogs/networking-and-content-delivery/best-practices-for-deploying-gateway-load-balancer/>
* <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking.html>

# AWS Account Dashboard

{{py\_account\_dashboard}}

# Best Practices & Health Static Auto-Analysis

## Transit Gateway Analysis

{{py\_tgw\_best\_practices}}

## VPN Analysis

{{py\_vpn\_health}}

## VPC Analysis

{{py\_vpc\_health}}

## Load Balancer Analysis

{{py\_lb\_health}}

## EC2 instance Analysis

{{py\_inst\_health}}

# VPCs

{{py\_vpcs}}

# Route Tables

{{py\_rts}}

# Route Tables - Routes

{{py\_rt\_routes}}

# Prefix Lists

{{py\_prefix\_lists}}

# Subnets

{{py\_subnets}}

# Network ACLs

{{py\_netacls}}

# Network ACL – Inbound Entries

{{py\_netacl\_in\_entries}}

# Network ACL – Outbound Entries

{{py\_netacl\_out\_entries}}

# Security Groups

{{py\_sgs}}

# Security Group – Inbound Entries

{{py\_sg\_in\_entries}}

# Security Group – Outbound Entries

{{py\_sg\_out\_entries}}

# Internet Gateways

{{py\_igws}}

# Egress-Only Internet Gateways

{{py\_eigws}}

# NAT Gateways

{{py\_ngws}}

# Endpoint Services

{{py\_endpoint\_services}}

# Endpoints

{{py\_endpoints}}

# Peering Connections

{{py\_pcx}}

# Transit Gateways

**NOTE:** If the Owner ID is in red, the TGW has been shared from a different account (the owner ID does not match the current account ID).

{{py\_tgws}}

# Transit Gateway Routes

{{py\_tgw\_routes}}

# VPN – Customer Gateways

{{py\_vpn\_cgws}}

# VPN – Site-to-Site Connections (Connected to Transit Gateways)

{{py\_vpn\_s2s}}

# VPN – Virtual Private Gateways

{{py\_vpn\_vpgs}}

# Direct Connect Gateways

{{py\_dcgws}}

# Load Balancers

{{py\_load\_balancers}}

# Load Balancer Target Groups

{{py\_lb\_target\_groups}}

# EC2 Instances

{{py\_ec2\_inst}}