DEPARTMENT OF VETERANS AFFAIRS

VA Enterprise Cloud (VAEC) Technical Reference Guide for Acquisition Support

July 2018

Version 1.3

Table of Contents

Table of Figures

Tables of Tables

1 VAEC Environment Overview

The Department of Veterans Affairs (VA) is embracing a "Cloud First" policy and Information Technology (IT) modernization initiatives as established by the Federal Chief Information Officer (CIO).

The VAEC will leverage the full spectrum of cloud services to efficiently provide high-quality, Government and service provider managed, rapidly delivered, innovative, secure, scalable, flexible, and modular environment to service applications for Veterans. The VAEC will provide VA the ability to use the latest technologies to deliver services to our Veterans in ways they are accustomed receiving them.

VAEC provides administrative support of the overall VAEC while the application owner administers and manages their own virtual environment in a self-service model. The VAEC provides the configuration management services to manage development and deployment activities.

2 VAEC Architecture

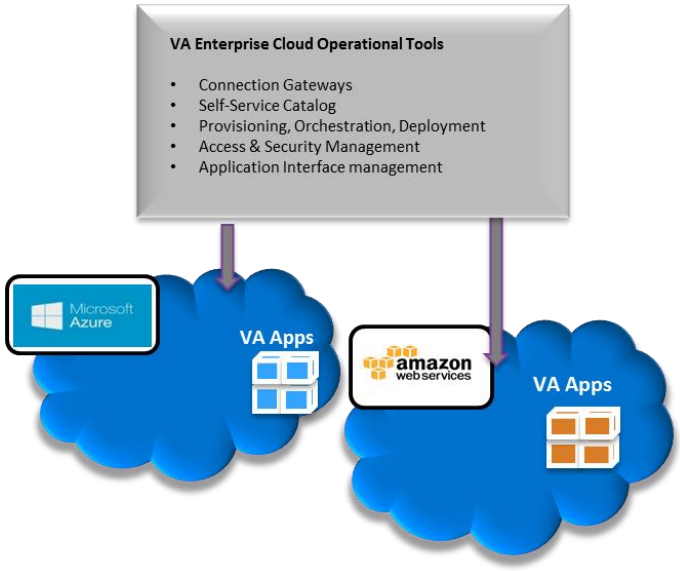
The architecture will consist of multiple CSP environments that offer Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and/or Software-as-a-Service (SaaS). The figure below depicts the high level VAEC. VAEC supports development, non-production (e.g. Pre- Prod, Staging, etc.) and production level environments. The graphics and sections below will provide greater detail into these areas including core services, tools and capabilities.

2.1 CSP Environment

As of the date of this document the available VAEC CSP environments are:

- Microsoft Azure Government Cloud
- Amazon Web Services (AWS) Government Cloud

FIGURE 1 - VAEC



2.2 VAEC Software Installation Policy

Any software installed on virtual machines (VM) operating in the VAEC at the IaaS or PaaS level s must be VA Technical Reference Model (TRM) compliant or have an approved waiver.

2.3 VAEC Management Tools

The VAEC will be managed by a set of VA Enterprise Cloud Operational Tools (VAECOT) (ETA Q3 FY2018), Cloud Service Provider (CSP)-native tools and other VA tools.

2.3.1 VA Enterprise Cloud Operational Tools (VAECOT)

The VAEC operational tools are part of the overall VAEC architecture, and consist of the following:

1. Self-Service Cloud Service Catalog
2. Provisioning Orchestration Deployment
3. Access and Security Management
4. Resource and Accounting Management
5. Cloud Access Security Broker (CASB)
6. Application Programming Interface (API) Gateway

2.3.2 VAEC Cloud Service Provider (CSP)-native Tools

When appropriate and approved by VA, contractor access to and utilization of the individual CSP management interfaces will be provided.

2.3.3 VAEC Other VA Tools

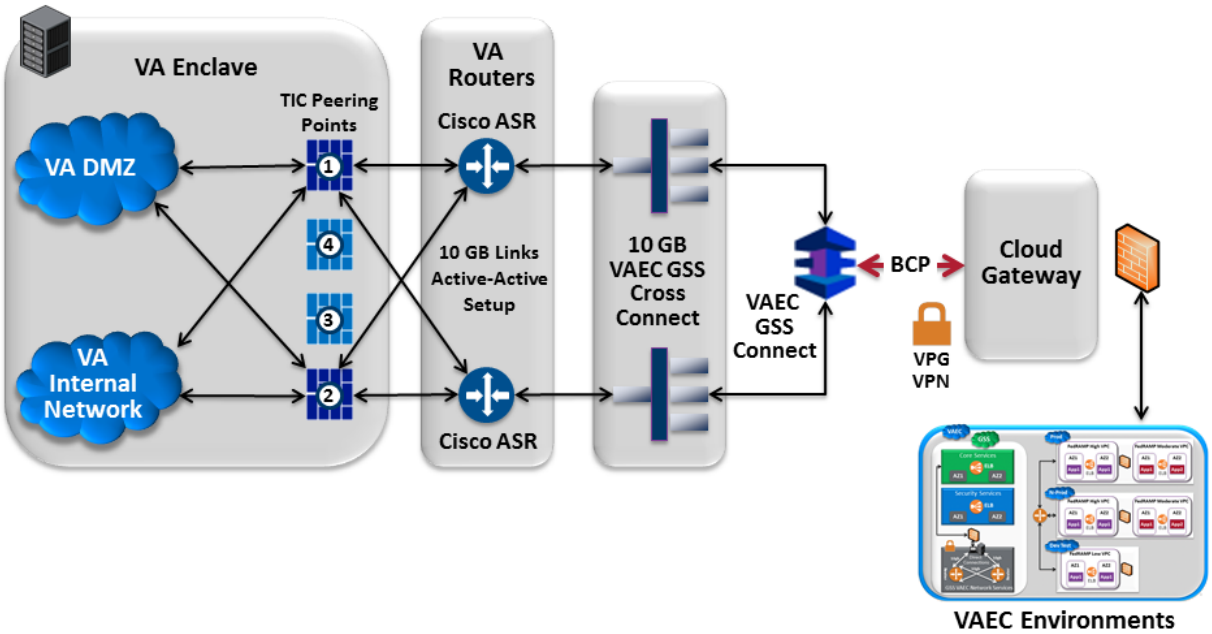
VA also uses numerous tools to manage its infrastructure. VA maintains a TRM listing tools approved for use on the VA network.

3 VAEC Connection to the VA Network

The VAEC environments use a common Trusted Internet Connections (TIC) compliant connection mechanism as shown in Figure 2. The connections are high bandwidth (e.g. 10 Gb), fully redundant, encrypted connections with load balancers and firewalls as necessary to the respective endpoints.

During onboarding, the VAEC team will work with the project team to determine IP addressing requirements for each project environment and issue the required VA public and private IP addresses. Public inbound connectivity is blocked by default. Inbound public interfaces require VA approval. All inbound traffic must traverse the VA TIC. The VAEC team will assist with the approval process.

FIGURE 2 - HIGH-LEVEL NETWORK (FLOW) DIAGRAM



4 VAEC General Support Services

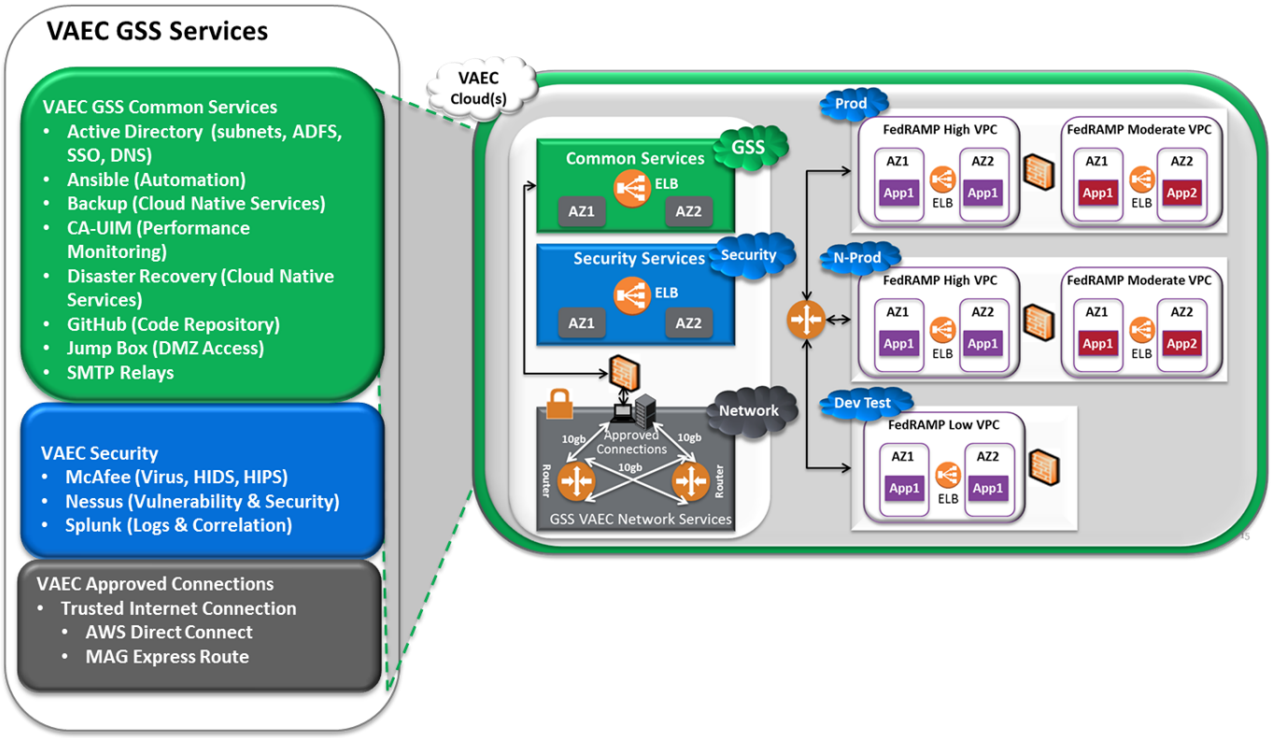
Each VAEC CSP environment provides general support services (GSS) to be leveraged by application/solutions hosted within the environment.

These services simplify migration and hosting of applications in the VAEC CSP environments. The table and graphic below shows the list of services available and how they relate to hosted applications.

TABLE 1 - VAEC GSS

Common Services	Common Security and Scanning Tools
• Active Directory (Subnets, ADFS, SSO, DNS) • Ansible • Backup • CA-UIM (Performance Monitoring) • Disaster recovery • GitHub • Jump Boxes • SMTP Relays	• BigFix • McAfee • Nessus • Splunk

FIGURE 3 - CURRENT VAEC SIMPLIFIED ARCHITECTURE SHOWING CORE SERVICES



4.1 Capabilities Provided by the VAEC

Service continuity/DR	VAEC provides access to native CSP features, for this purpose the application / Project team will provide VAEC guidance for use during onboarding. Project Team/Contractor (Project Team) is to architect solution using those features to meet project level SLA's.
Capacity Management (does VA Cloud monitor, auto add, add by request, etc)	The VAEC does monitor and within allocated project environments self-service is enabled for provisioning and auto scaling is available
Change and configuration management	The VAEC utilizes Ansible and GitHub to track and monitor all changes to cloud resources ITOP Monitoring extension into the VAEC cloud environment for configuration management as well as ability to use APIs to Service Now with Full Concept of Operations(FOC)
Network administration and ESCCB	VAEC team handles VAEC network baseline ESCCB requests and administration. Project team is responsible for project specific ESCCB requests and network administration within their environments (sub nets) Here are the various ESCCB links – 1) General information on OIS' Security Engineering page: https://vaww.portal2.va.gov/sites/infosecurity/ess/Enterprise%20Security%20Change%20Control%20Board.aspx 2) Here's the repository where all the ESCCB documents are located: https://vaww.portal2.va.gov/sites/infosecurity/ess/Enterprise%20Security%20Change%20Control%20Board/Forms/AllItems.aspx 3) The ChangeGear application, used to actually submit the ESCCB request, is here: https://esccb.va.gov
Performance management Monitoring	VAEC provides access to performance management tools as part of VAEC GSS and the use of Unified Infrastrucutre Moitoring UIM is proposed via VA Command Center as TBD. Application teams are required to resolve problems.
Release management	Application Team / Project Team.
Security management	Application / Project Team for project level controls/VAEC team for VAEC level controls
System administration	Application / Project Team within VAEC administered project environments
Security Monitoring	Security monitoring tools are provided via the VAEC GSS and required for use as part of the project ATO.
Software Licencing	Application / Project team licensing provided by CSP or project team provided. VAEC does not provide licenses

5 Service Level Agreements (SLAs)

Each VAEC environment provides access to standard services provided in accordance with the CSP's standard SLAs between VA and the CSP (VAEC Standard SLAs).

If the VA requirements for a given application/solution require more stringent SLAs between VA and project team (Project SLAs), it is the responsibility of the project team to meet all requirements using the VAEC Standard SLAs. This may require the project team to architect, deliver, and ensure that the required, more stringent Project SLAs are met using the VAEC Standard SLAs and maintaining this as it changes over time.

6 Authority to Operate (ATO)

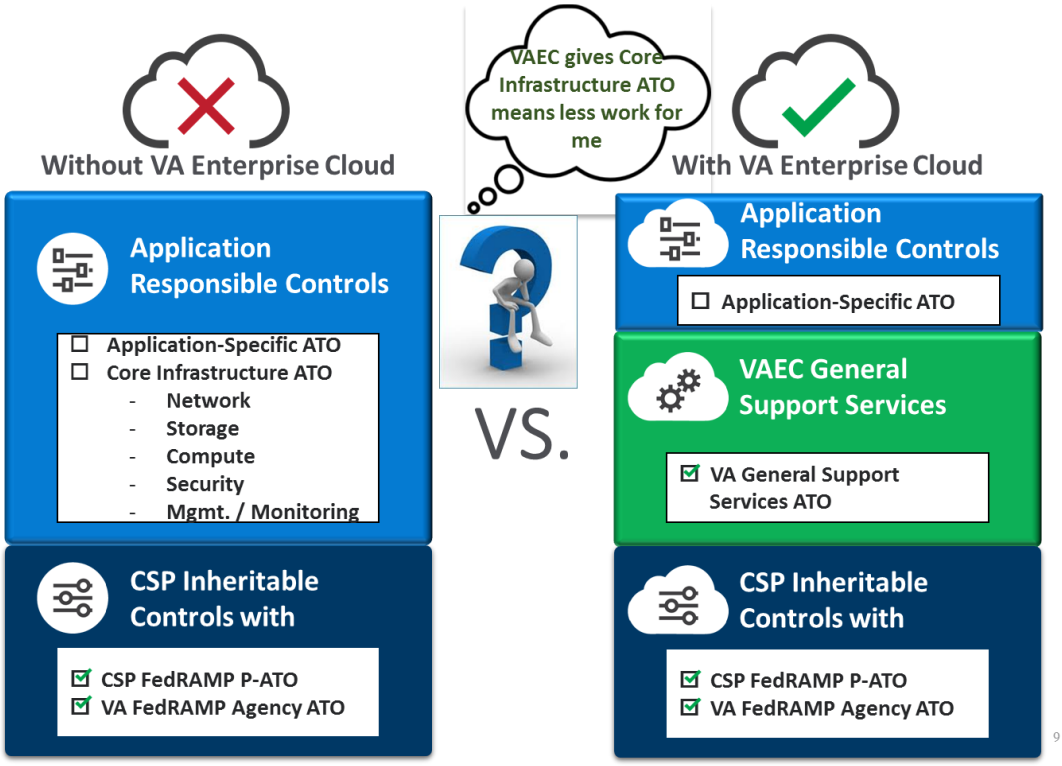
The VAEC CSP Environments all have a US Federal Risk and Authorization Management Program (FedRAMP) High Certified VA ATO. VAEC provides access to the FedRAMP certified services of each CSP. Upon request, non-certified services can be made available.

The ATO for an application residing in the VAEC is separate from the VAEC CSP Environment ATO. Each project team is responsible for its application level ATO.

The ability of a VAEC application level ATO to inherit security controls covered by the VAEC CSP Environment ATO simplifies the application level ATO process. The common services provided by the VAEC environment and included VAEC environment ATO will support the application level security control requirements.

Please refer to the VAEC CSP's website to determine which services are in scope, and have been fully assessed by third party auditors, resulting in a FedRAMP Certification, attestation, of compliance, or ATO.

FIGURE 4 - VAEC SECURITY CONTROL INHERITANCE



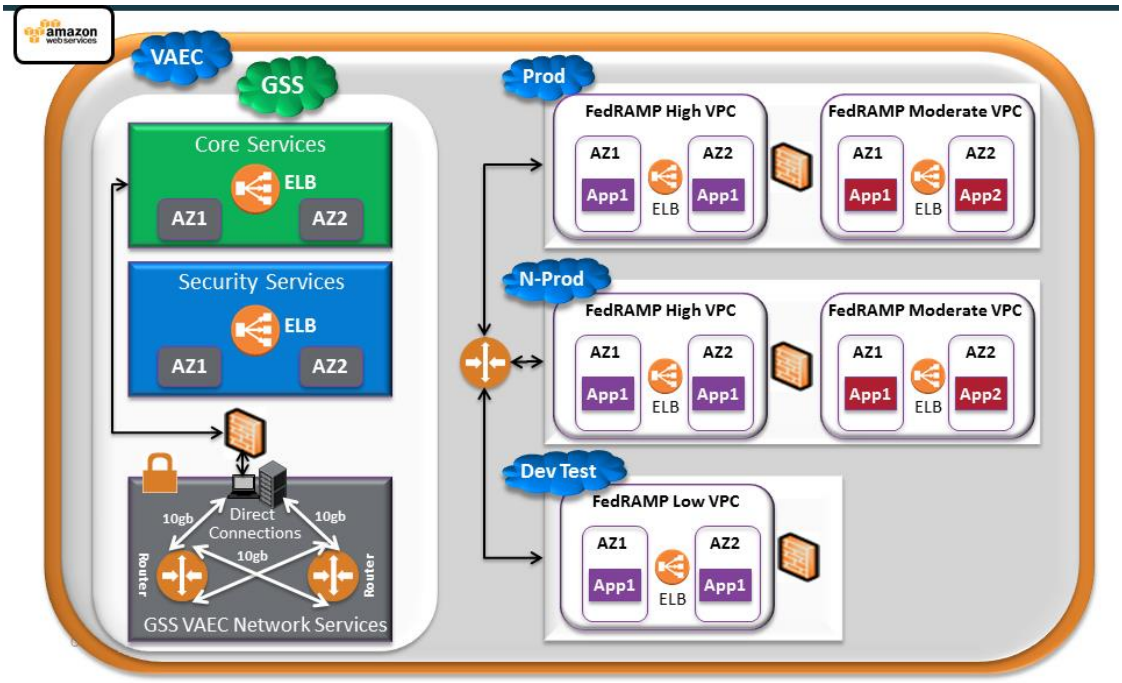
7 VAEC-AWS Amazon Web Services (AWS) Introduction

The VAEC-AWS environment is in the AWS GovCloud. The VAEC-AWS is connected to the VA network via AWS Direct Connect. Projects are provisioned one or more VPCs for their production, dev and any other required environments. The VAEC-AWS offers common services described above subject to any specific services described below. VAEC-AWS also provides access to the full suite of FedRAMP Certified AWS GovCloud Services by default. Access to Non FedRAMP Certified AWS GovCloud services may be provisioned upon request.

7.1 VAEC-AWS Architecture

The VAEC-AWS environment consists of environments within one (1) geographic region with multiple availability zones provided by AWS GovCloud. A simplified view of the VAEC-AWS architecture is provided below. Detailed architectural information will only be provided post contract award and/or during project provisioning.

FIGURE 5 - VAEC-AWS SIMPLIFIED ARCHITECTURE



7.2 VAEC-AWS General Support Services

The VAEC-AWS CSP environment provides general support services (GSS) to be leveraged by application/solutions hosted within the environment as described above in above VA Enterprise Cloud Operational Tools (VAECOT).

TABLE 2 - VAEC-AWS GSS

Common Services	Common Security and Scanning Tools
• None	• None

7.3 VAEC-AWS Deployed Production Application Lists

TABLE 3 - VAEC-AWS FEDRAMP COMMON SERVICES

FedRAMP High	FedRAMP Moderate
• None	• None

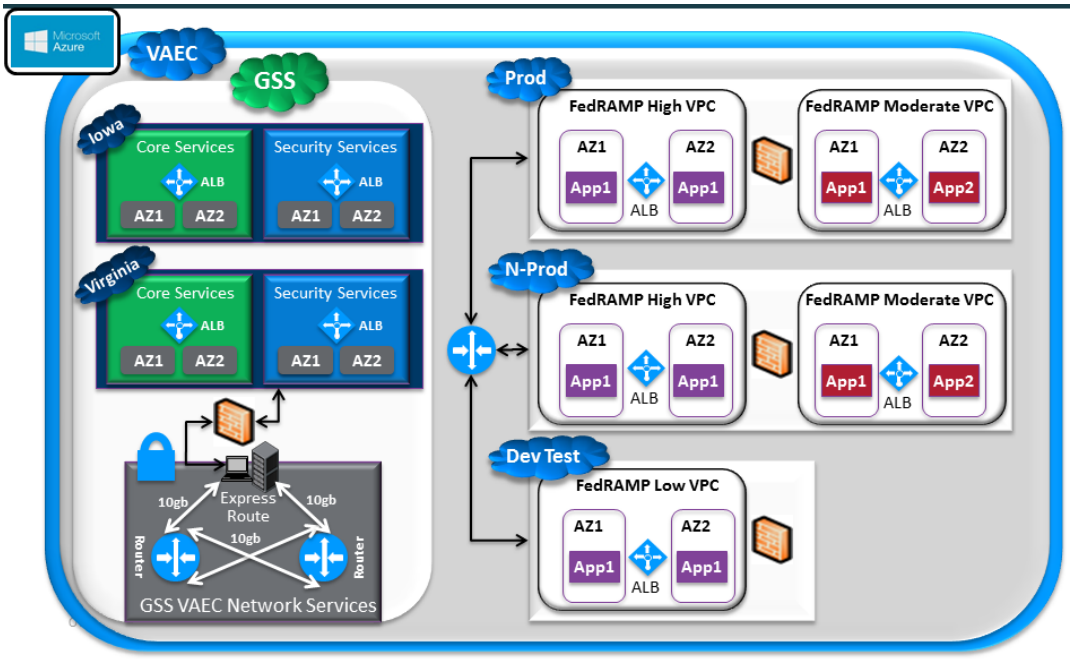
8 VAEC-Azure Introduction

The VAEC-Azure and AWS Environment use the same connectivity. The connection into VAEC-Azure end point is via VPN into the Azure Government GovCloud. Projects are provisioned one or more VPCs for their production, dev and any other required environments. The VAEC-Azure offers common services and specific services and access to the full suite of Azure GovCloud Services as well as the ability to leverage the VAEC-Azure ATO.

8.1 VAEC-Azure Architecture

The VAEC-Azure environment consists of two geographic regions environments, one in Iowa and one in Virginia. A simplified view of the VAEC-Azure architecture is provided below. Detailed architectural information will only be provided post contract award and/or during project provisioning.

FIGURE 6 - VAEC-AZURE SIMPLIFIED ARCHITECTURE



8.2 VAEC-Azure General Support Services

The VAEC-Azure CSP environment provides general support services (GSS) to be leveraged by application/solutions hosted within the environment as described above in above VA Enterprise Cloud Operational Tools (VAECOT).

TABLE 4 - VAEC-AZURE GSS

Common Services	Common Security and Scanning Tools
• None	• None

8.3 VAEC-Azure Deployed Production Application Lists

TABLE 5 - VAEC-AZURE FEDRAMP COMMON SERVICES

FedRAMP High	FedRAMP Moderate
• None	• None