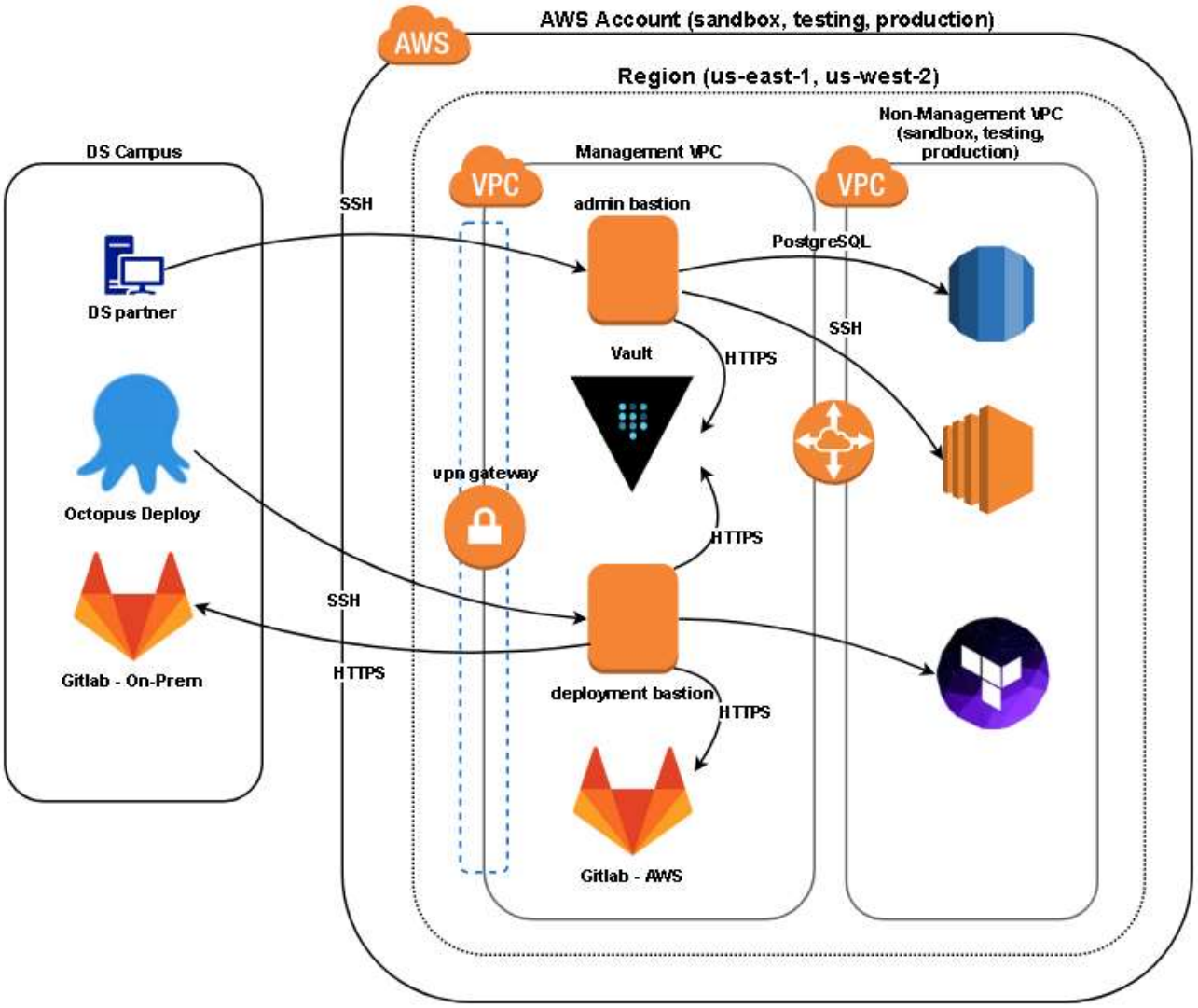
Bastion Servers (Jump Hosts)

Each region in Direct Supply's AWS accounts is configured with two bastion servers. The bastions exist in the region's management VPC which is peered with the rest of the VPCs in that region. The role of the bastions is to allow users and applications to interact with EC2 instances and other applications that are running in that region's non-management VPCs. The bastions exist because on-premise connectivity is limited to each account's management VPCs only. Currently, that connectivity is accomplished via a proof of concept VPN connection.

The two bastions play different roles. The admin bastions exist for Direct Supply partners to interact directly with instances and applications running in AWS. The deployment bastions are used for the automated build and deployment of the AWS resources and applications themselves.



Admin Bastion

The admin bastions are linux servers built from the Ubuntu admin bastion AMI and exist for user interaction with EC2 instances and applications running in AWS. MFA is required upon connecting to these servers, push notification or phone calls will be used for this - this can be set here.

DNS records

- **Sandbox**: admin-bastion.devops.management.directsupply-sandbox.cloud
- **Testing**: admin-bastion.devops.management.directsupply-testing.cloud
- **Production**: admin-bastion.devops.management.directsupply.cloud

Key Features

- attached to the MTOLYMPUS domain
- configured to use on-premise DNS servers
- security group only allows port 22 (SSH) in from DS on-premise networks

Usage

- SSH tunnels to postgres DB instances for management with local pgAdmin installs
- Authenticating to Vault for user access to secrets, SSH one time passwords, and temporary database credentials
- SSH connections to other EC2 instances running in AWS

Deployment Bastion

The deployment bastions are linux servers built from the Amazon Linux base AMI and exist for the automated build and deployment of resources and applications in AWS.

Key Features

- not attached to MTOLYMPUS domain
- configured to use on-premise DNS servers
- security group only allows port 22 (SSH) in from DS on-premise networks
- configured as Octopus Deploy tentacles for SSH deployments
- configured as Gitlab CI/CD runners for use with Gitlab in AWS
- equipped with Packer, Terraform, and Vault for builds and deployments
- granted AWS AdministratorAccess in their respective accounts
- granted root access to Vault
- Runs Docker builds and pushes into ECR repositories

Usage

- build and deployment of AWS AMIs with Packer via Octopus Deploy
- this includes cloud-core AMIs and product AMIs with application code baked in
- deployment of AWS cloud-core resources with Terraform via Octopus Deploy
- deployment of application infrastructure resources with Terraform via Octopus Deploy
- deployment of Vault resources with Terraform via Octopus Deploy
- build and packaging of Vault infrastructure and configuration code with Gitlab CI/CD via gitlab.directsupply.cloud

Windows AD Bastion

These are Windows based bastions that are primarily used to manage the AWS AD domain. They can also be used to remote into pet Windows 2008 Standard servers that live in AWS.

Usage

- you will need to use this server as a jump server to remote into a pet Windows 2008 Standard server
- the traditional RD gateway does not support the older Windows 2008 standard servers
- the flow will be to RDP into the following respective server based on the account, and once on the AD bastion to remote into the Windows 2008 Standard server

Account	Domain	AD Bastion
Sandbox	sand-us-east-1.ad	ad-bastion.sandbox.devops.management.directsupply-sandbox.cloud
Testing	test-us-east-1.ad	ad-bastion.testing.devops.management.directsupply-testing.cloud
Production	prod-us-east-1.ad	ad-bastion.devops.management.directsupply.cloud