Infrastructure Specification Document

DevOps WS 2023

Team 1

Alexander Nachtmann,
Markus Rösner,
Max Sinnl and
Stephanie Rauscher

Network Topology

VPC (Virtual Private Cloud) overview

VPC CIDR: 10.0.0.0/16

Subnets

one private subnet and one public subnet
Public subnet: 10.0.1.0/24 (Ranges 10.0.1.0 to 10.0.1.255)
Private subnet: 10.0.2.0/24 (Ranges 10.0.2.0 to 10.0.2.255)

EC2 instances placed in the **public subnet** (for direct internet access):

- **GitLab Server**

  Hosts a GitLab instance for source code management, CI/CD pipelines, and collaborative features, accessible from the internet for user interactions.

- **Bastion Host**

  Acts as a secure entry point for administrators to remotely access other EC2 instances, particularly those in private subnets.

EC2 instances placed in the **private subnet** (access only via Bastion Host, no internet access):

- **Main DNS Server**

  Provides domain name resolution within the VPC, translating domain names into IP addresses for network communication.

- **Backup DNS Server**

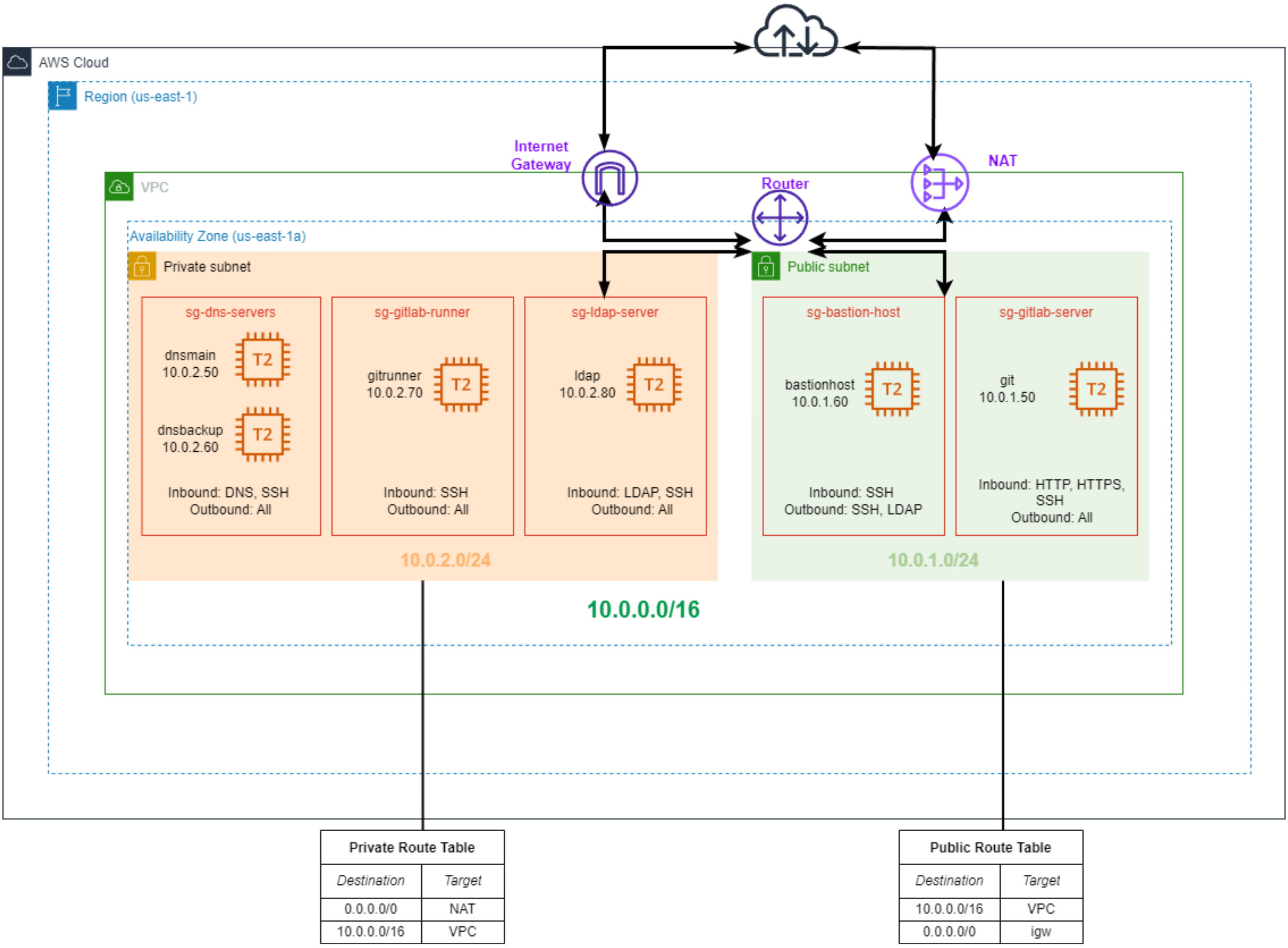
  Serves as a redundant DNS service, ensuring continuous domain name resolution in case the main DNS server fails.

- **GitLab Runner**

Executes automated scripts for the GitLab CI/CD pipeline, running jobs assigned by the GitLab server.

- **LDAP Server**

Manages Lightweight Directory Access Protocol services, handling user authentication and directory services within the network.



Private Route Table	
Destination	*Target*
0.0.0.0/0	NAT
10.0.0.0/16	VPC

Public Route Table	
Destination	*Target*
10.0.0.0/16	VPC
0.0.0.0/0	igw

Routing Tables

Public Subnet Route Table

Destination IP	Target name
10.0.0.0/16	VPC
0.0.0.0/0	Internet Gateway

Destination IP 10.0.0.0/16 - Target: VPC
This entry indicates that any traffic destined for an IP address within the 10.0.0.0/16 range) should be routed internally within the VPC. It essentially means that all IPs in this range are part of the VPC network. This is a standard entry for internal network routing within the VPC.

Destination IP 0.0.0.0/0 - Target: Internet Gateway
This entry is for routing all other traffic (not destined for the internal VPC network) to the Internet Gateway. The destination IP 0.0.0.0/0 represents all IP addresses not covered by more specific routes.

Private Subnet Route Table

Destination IP	Target name
0.0.0.0/0	NAT Gateway
10.0.0.0/16	VPC

Destination IP 0.0.0.0/0 - Target: NAT Gateway
This route directs all traffic that is not for local destinations (i.e., any destination not within the VPC) to a Network Address Translation (NAT) Gateway. It's used for allowing instances in the Private Subnet to access the internet for updates or downloads, but not allowing incoming internet traffic to initiate connections with those instances.

Destination IP 10.0.0.0/16 - Target: VPC
Similar to the Public Subnet, this entry ensures that traffic destined for the VPC's internal IP range is kept within the VPC network.

Security Groups Configuration

Inbound Rules

SG Name	Type	Port Range	Source	Description
sg-gitlab-server	HTTP, HTTPS, SSH	TCP 80, TCP443 TCP 22	0.0.0.0/0 0.0.0.0/0 10.0.1.60	Allows web traffic (HTTP/HTTPS) from all IPs and SSH access from Bastion Host for secure GitLab server administration.
sg-bastion-host	SSH	TCP 22	10.0.2.0/24	Permits SSH access to the Bastion host exclusively from the private subnet for internal network resource management.
sg-gitlab-runner	SSH	TCP 22	10.0.1.60	Enables SSH connectivity from the GitLab Server at 10.0.1.60 for configuring and managing GitLab Runners.
sg-ldap-server	LDAP, SSH	TCP 389, TCP 22	10.0.1.50 10.0.1.60	Facilitates LDAP services from GitLab Server at 10.0.1.50 and SSH management access from Bastion Host for LDAP server operations.
sg-dns-servers	DNS, SSH	TCP/UDP 53, TCP 22	10.0.0.0/16 10.0.1.60	Allows DNS queries from within the VPC for domain name resolution and permits SSH access from Bastion Host for DNS server management

Outbound Rules

SG Name	Type	Port Range	Source	Description
sg-gitlab-server	All Destinations	-	0.0.0.0/0	Allows unrestricted outbound traffic from the GitLab server, facilitating external data exchange and updates.
sg-bastion-host	SSH LDAP	TCP 22 TCP 389	10.0.2.0/24 10.0.2.0/24	Permits outbound SSH and LDAP traffic to the 10.0.2.0/24 subnet, enabling secure access and directory service interactions with internal network resources.
sg-gitlab-runner	All Destinations	-	0.0.0.0/0	Allows all outbound traffic from GitLab Runners, ensuring unrestricted access for external services and resources required for CI/CD jobs.
sg-ldap-server	All Destinations	-	0.0.0.0/0	Enables unrestricted outbound traffic for LDAP server, supporting external communications and synchronization services.
sg-dns-servers	All Destinations	-	0.0.0.0/0	Allows all outbound traffic for DNS servers, facilitating DNS resolution services and updates from external sources.

Domain Configuration

Top-Level Domain (TLD): .team01

Country Code TLD: .at

Subdomains under team01.at:

Bastion Host: bastionhost.team01.at

GitLab Server: git.team01.at

GitLab Runner: gitrunner.team01.at

Main DNS Server: dnsmain.team01.at

Backup DNS Server: dnsbackup.team01.at

LDAP Server: ldap.team01.at

EC2 Instances Overview

Name	IP	Domain	OS/Packages	Security Group
Main DNS Server	10.0.2.50	dnsmain.team01.at	Ubuntu Server 22.04 LTS Packages: BIND 9.18	sg-dns-servers
Backup DNS Server	10.0.2.60	dnsbackup.team01.at	Ubuntu Server 22.04 LTS Packages: BIND 9.18	sg-dns-servers
Bastion Host	10.0.1.60	bastionhost.team01.at	Ubuntu Server 22.04 LTS	sg-bastion-host
GitLab Server	10.0.1.50	git.team01.at	Ubuntu Server 22.04 LTS Packages: GitLab 16.5	sg-gitlab-server
GitLab Runner	10.0.2.70	gitrunner.team01.at	Ubuntu Server 22.04 LTS	sg-gitlab-runner
LDAP Server	10.0.2.80	ldap.team01.at	Ubuntu Server 22.04 LTS Packages: OpenLDAP 2.5.16	sg-ldap-server

Test Cases

Service	Test Description	Tools/Methods	Additional Info
DNS Service	Test DNS resolution internally and externally	nslookup, dig, automated scripts	Include tests for primary and secondary DNS fallback
GitLab Server	Access the GitLab web interface	Web browser, automated test scripts	Test for both HTTP and HTTPS access
LDAP Server	Query the LDAP directory	ldapsearch, LDAP client applications	Include user authentication tests
GitLab Runner	Execute CI/CD pipelines	GitLab UI, direct runner commands	Include pipeline build, test, and deploy jobs

Team Roles and Responsibilities

Alexander Nachtmann - Project Manager:
Oversees AWS setup and coordination, responsible for meeting requirements, documentation, and presentations.

Stephanie Rauscher - Server Administrator:
Manages AWS server instances, configuration and maintenance.

Markus Rösner - DevOps Engineer:
In charge of GitLab and GitLab Runner, focusing on integration and deployment processes.

Max Sinnl - Test Engineer:
Conducts tests to ensure functionality and performance.