Architecture & Infrastructure LLD

HPC Upstream Compute platform - PoC

**Document Signoff**

**Document Signoff**

Document Revision List

|  |  |  |  |
| --- | --- | --- | --- |
| Revision No. | Revision Date | Author | Revision Description |
| V 0.1 | 20/03/2023 | Prithwiraj | Initial Design Document |
| V 0.2 | 01/06/2023 | Abdul | Added the sections for base infra infrastructure |
| V 0.3 | 15/06/2023 | Prithwiraj | Added the section for Custom GUI |

Contents

1 Contents 4

2 Introduction 7

2.1 Purpose of the Document 7

2.2 Scope 7

2.3 Out of Scope 7

2.4 Approach 8

2.5 Design Consideration 8

2.6 Intended Audience 8

3 AWS Regions 9

4 AWS Accounts and Environments 10

4.1 AWS Account 10

4.2 Environment 10

4.3 VPC/Subnet Structure for HPC workload using Parallel Cluster 10

4.4 Connectivity with Dyson on-prem 11

4.5 Connectivity for users using Dyson Laptop 11

4.6 IP CIDR Block for AWS Environment 11

5 Inter-Connectivity within the Cluster 13

5.1 Patching and Antivirus 13

5.2 Vulnerability Check 13

5.3 Network Security 13

6 AWS Infrastructure provisioning and Management 14

7 Baseline Infrastructure (VPC, Subnet, Cloud9) 15

7.1 Create VPC in Ireland region 15

7.2 Create private subnets in eu-west-1a & eu-west-1b respectively with correct CIDR range 15

7.3 Create cloud9 instance in eu-west1a and attach IAM instance profile. 15

7.4 Create Security Group for Windows Workstations 16

7.5 Modify Default Security Group of VPC 16

7.6 Create Route53 Resolver Outbound Endpoints 16

7.7 Create Security Group for FSx 17

7.8 TGW attachment with the newly created VPC by Dyson Cloud Team 17

7.9 Whitelist the CIDR range in the Firewall 17

7.10 Create Secret and store the AD read-only user credential in plain text 17

7.11 Create S3 Bucket 17

7.12 Provide the required access to the users to the s3 bucket: 18

7.13 Generating the key file: 18

8 Create Fsx Netapp Ontap 19

8.1 Create the FSx filesystem 19

8.2 Create the Storage Virtual Machine in the Filesystem 19

8.3 Create Volume in SVM 19

8.4 Share the Volumes 20

8.5 Create AD group by creating ticket with Dyson 21

8.6 Add the AD group to the shared volumes 21

8.7 Map Volumes in Windows Machine 21

8.8 Mount Volume in Parallel cluster 21

9 Create Windows Workstation 22

9.1 Create IAM Role 22

9.2 Create the Windows workstations (Windows server 2022) as Workstation-1 for UseCase-1 22

9.3 Install/Configure security agents - MS Defender, using the script 22

9.4 Domain joins the Windows Workstation 22

9.5 Map the Fsx volumes in Windows Workstations 23

9.6 Install NICE DCV 23

9.7 Install DCV client/browser to the User's machine 23

9.8 App installations 23

9.9 Validate the connectivity with the on-prem License server, PLM server, NFS 23

9.10 Create AMI from the Workstation-1 23

9.11 Install RDS service to enable multi-user RDP session concurrently 24

9.12 Raise request to increase the EC2 limit in AWS for more G4dn instances 24

9.13 Restore the AMI to create other workstations for UC-2, UC-3, UC-4 24

10 Create AWS Parallel Cluster 25

10.1 Create Config for the parallel cluster and save it in the cloud9 25

10.2 Config file of AWS Parallel Cluster with Directory Service and Fsx 25

10.3 Validate the Headnode, AD integration, Fsx integration 25

10.4 Install security agents - MS Defender on the HeadNode 26

10.5 App installations on HeadNode 26

10.6 Scheduler test and validation 26

10.7 Compute node validation 26

10.8 Upscaling Test and Validation 26

10.9 Validate the connectivity with the on-prem server 27

10.10 Validate the cluster 27

10.11 Raise request to increase the EC2 limit in AWS for the compute nodes which falls in "All Standard (A, C, D, H, I, M, R, T, Z) instances" group to 2560 28

11 Custom GUI 29

12 Application Configuration & Data Transfer 31

12.1 App Configuration on workstations to connect to the PA Cluster 31

12.2 Data Transfer from OnPrem to AWS 31

Abbreviations

|  |  |
| --- | --- |
| Abbreviation | Description |
| ACL | Access Control List(s) |
| AWS | Amazon Web services |
| ISO | International standards organisation |
| ITSM | Information Technology Service Management |
| SOC | Security Operation Centre |
| TCS | Tata Consultancy Services |
| Dyson | Dyson Technology Limited |
| HPC | High Performance Computing |
| PoC | Proof Of Concept |
| AD | Active Directory |
| SSO | Single Sign On |
| SOCA | Scale Out Computing on AWS |

# Introduction

This document describes the AWS infra design specifications for DYSON-HPC-UPSTREAM Environment for PoC phase

* Provision the target environment in Ireland region under Dyson’s existing AWS landing zone
* Provision the target environment for Workstations, HPC, NICE DCV /Engine Frame
* Migrate the on-premises data to HPC environment for the Use Cases/Scenarios
* Deploy Applications in HPC environment for running the PoC Use Cases/Scenarios
* Test the Use Cases/Scenarios
* Provide support for the HPC and workstation environment during the use case execution.

## Purpose of the Document

The primary purpose of this document is to provide a holistic view of AWS Hosting platform and its functional delivery models.

## Scope

Scope of this document is to describe the building blocks to setup AWS-HPC infrastructure for hosting DYSON-HPC-UPSTREAM platform for the PoC. This document describes key infrastructure components as

* AWS Regions and Locations
* Accounts and Subscriptions
* AWS Environments
* Network Connectivity
* VPC/Subnet Structure
* Authentication/Authorization
* Infrastructure as a Code
* HPC Cluster (AWS Parallel Cluster)
* Storage (EBS, FSx for NetApp ONTAP)
* Security and monitoring

## Out of Scope

* Design and implementation of any third-party tools
* Procurement of AWS Cloud services by making an Enterprise Agreement with AWS
* Procurement of network links/bandwidths, addressing/resolving issues with existing Dyson network
* Definition of security and compliance policies as per Dyson existing Cloud Standards
* Responsibility on any third-party vendor deliverables will remain with Dyson (Dyson will facilitate communications with any third-party vendor)
* Definition and implementation of ITSM process for cloud
* Configuration changes to ITSM tool
* Decommissioning of existing Infrastructure
* AI/ML related services

## Approach

Approach is based on the Dyson’s business requirement to provision a quick PoC model considering the Future Operating Model using AWS and AWS-HPC as the platform.

## Design Consideration

Consideration is made by analyzing two approaches – SOCA and AWS Parallel Cluster. Based on our analysis, AWS Parallel Cluster has been found as the best suited approach considering the business requirements, success criteria, future support and advisory from AWS.

## Intended Audience

This document will enable Dyson Stakeholders to understand TCS recommended technical design specifications.

Stakeholders: <Placeholder: Need to check with Dyson who else can be added in the list>

* Solution Architect
* Cloud Architect
* Network Architect
* Domain Architects
* Security Architect
* IT Infrastructure Architect
* Service Delivery Owners

# AWS Regions

Regions in AWS are geographically distributed and isolated locations, consisting of one or more AWS Data centers connected to each other through low latency and high throughput network. Each AWS region is paired with another region within the same geography, together making a regional pair.

AWS region is determined based on the user’s geographical presence and considering the requirement criteria.

Dyson has their AWS footprints in **Ireland** region.

Below region is identified based on the hosting requirements of DYSON-HPC-UPSTREAM platform to AWS, such that AWS-HPC services availability, commercial implications, and feasibility to execute the given use cases as per the Business Requirement Document.

|  |  |  |
| --- | --- | --- |
| **Geography** | **Region** | **Primary/Secondary** |
| EU | Ireland | Primary (DC) |

TCS plans to host and manage the entire services to meet Dyson requirement in AWS EU – Ireland region across multiple zones as a primary data center. Our solution does not include any DR strategy for the PoC.

AWS Cloud EU region Data Centers are Tier 4, and every Availability Zone is equipped with High Availability compute clusters to provide the defined services and highly resilient network connected to data centers. The Multiple Availability Zones in a region are close enough for low latency connectivity.

# AWS Accounts and Environments

AWS organization structure is in place for Dyson. Dyson will be sharing an existing AWS account in “Non-Prod RDD” for this PoC. There are multiple shared VPCs available in the account however, for the sake of simplicity a dedicated VPC will be created for the PoC.

Managing the OU level control policy and guardrails are not considered here. Existing policies will be considered for the PoC.

## AWS Account

Shared account “Non-Prod RDD” (Account Id: **178920580136**) will be used for this PoC.

## Environment

DYSON-HPC-UPSTREAM PoC program we will leveraging the Non-Prod RDD account.

* **Non-Prod Account**

## VPC/Subnet Structure for HPC workload using Parallel Cluster

The following diagram depicts VPC and Subnet structure of HPC workload for the PoC

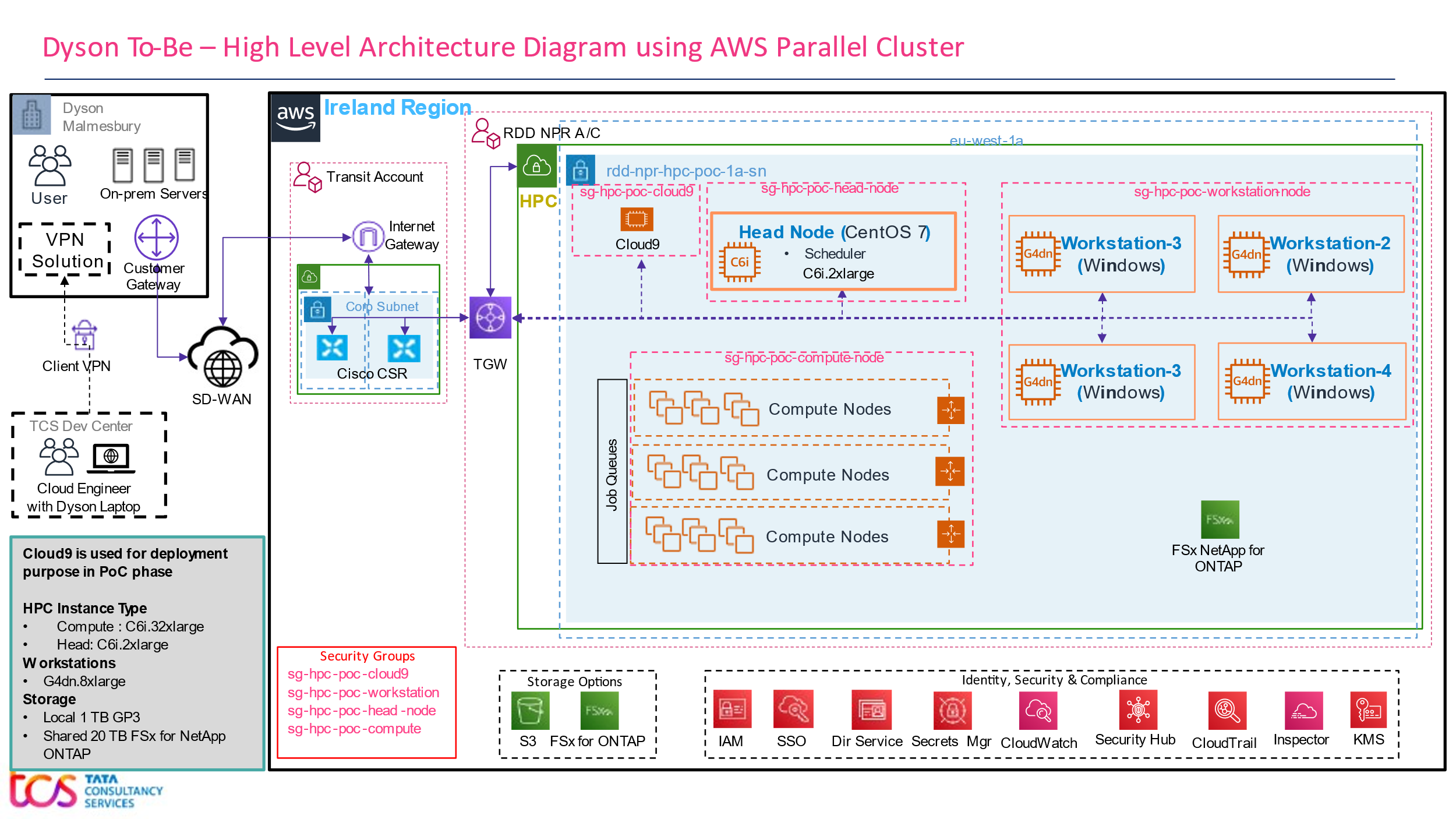


Figure 5 – DYSON-HPC-UPSTREAM VPC Overview

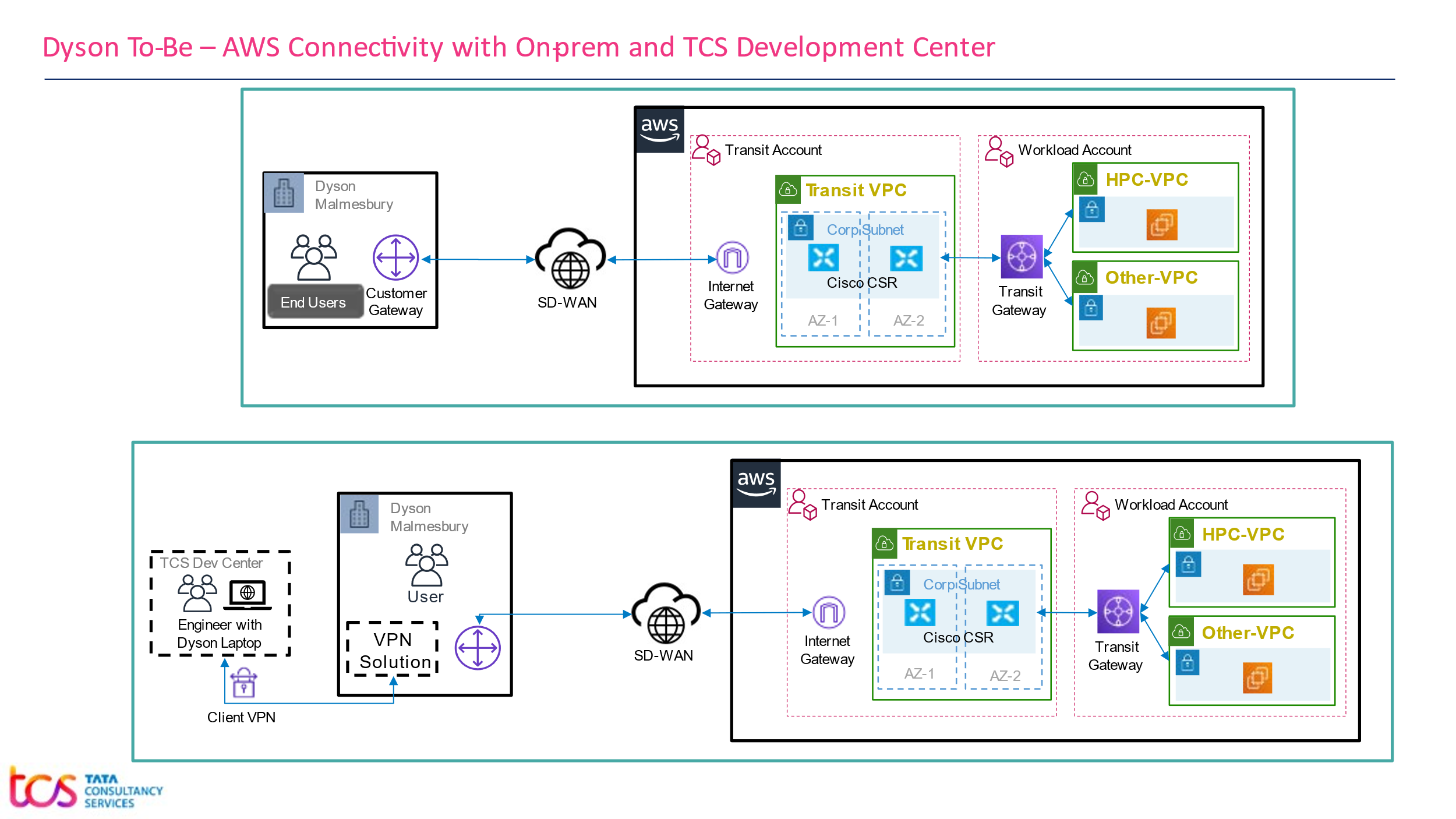
Below are some of the key points covered as part of the initial architecture design

1. VPCs will be spanned in one Availability Zone in Ireland region in PoC phase.
2. VPC and Subnet structure

* No Public Subnet:
* 1 Private Subnet:
  1. One Head Node (CentOS 7) will have Job Scheduler, NICE DCV server will be installed on it.
  2. Four Workstations (Windows); NICE DCV server will be installed.
  3. CentOS based on-demand Compute Nodes under auto-scaling group

1. All internet traffic will pass through firewall deployed in the Transit Account
2. Access to Workstation instances will be enabled through AWS SSO authentication through console. Alternatively – the user should be able to RDP/DCV to the Windows based Workstations.

## Connectivity with Dyson on-prem



*Figure 6 – High Level Diagram of Connectivity from Dyson to AWS over SD-WAN*

## Connectivity for users using Dyson Laptop

Figure 7 – Connectivity between AWS and Users using Client VPN

## IP CIDR Block for AWS Environment

IP CIDR Block for AWS HPC VPC: **10.221.90.0/24**

|  |  |
| --- | --- |
| **AWS VPC** | **(EU-West-1)** |
| HPC VPC | **10.221.90.0/24** |

# Inter-Connectivity within the Cluster

Key points to describe the workflow and cluster inter-connectivity.

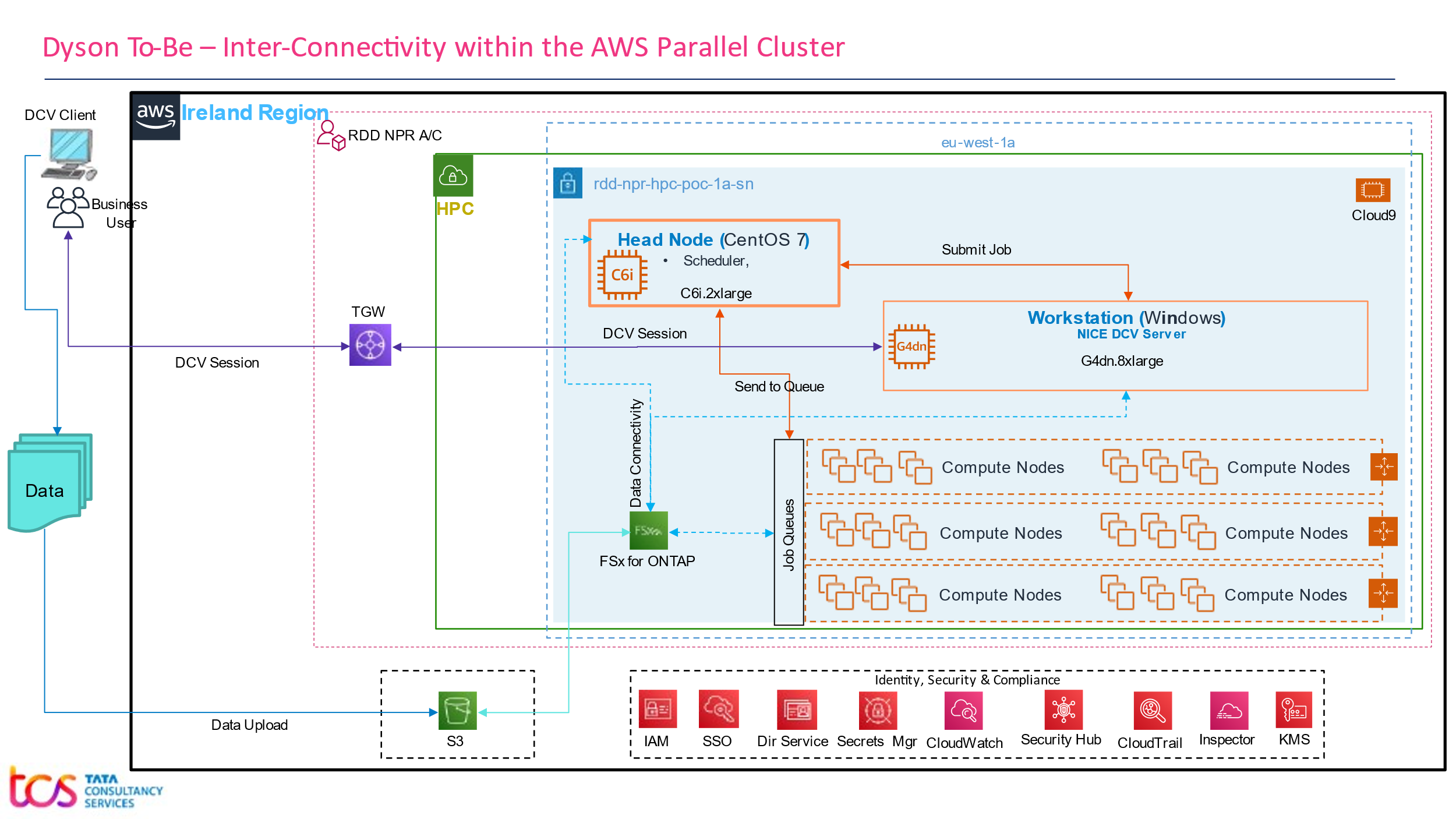


Figure 8 – Inter-Connectivity within the Cluster

## Patching and Antivirus

As per vulnerability assessment report patching will be done.

## Vulnerability Check

Qualys is a cloud-based solution that detects vulnerabilities on all networked assets, including servers and instances. MS Defender or Qualys will be installed to check the vulnerability.

## Network Security

Below are the key components to manage Network Security.

1. All internet traffic will pass through existing firewall solution.
2. Access will be restricted in Firewall to blacklist all other sources except the traffic coming from the Dyson Corporate Network.
3. All EC2 Instances will be protected by **Security Group** (Stateful Access Control list). Only required port will be opened.
4. **Network Access Control List** are being used to filter traffic at Subnet level in the Transit A/C.
5. Head Node, Workstations and Compute Nodes will be kept in private Subnets.

# AWS Infrastructure provisioning and Management

TCS will leverage Infrastructure as a code in the way of using Terraform, Cloud formation templates to drive the entire PoC phase using a Cloud9 instance. However, TCS will leverage the fully automated way in the form of Terraform and CloudFormation Stack to provision the infrastructure.

TCS will adopt few additional components which h will provide more feature rich cluster in later phase of PoC which will include Engine Frame etc

# Baseline Infrastructure (VPC, Subnet, Cloud9)

## Create VPC in Ireland region

Provide the below details and create VPC.

|  |  |  |
| --- | --- | --- |
| **Sl. No** | **Field Name** | **Value** |
| 1 | Region | Ireland |
| 2 | Name | aws-rdd-euw1-hpc-poc-npr-vpc-01 |
| 3 | CIDR Block | 10.221.90.0/24 |
| 4 | Name Tag | 2001493-HPC Upstream Compute |

## Create private subnets in eu-west-1a & eu-west-1b respectively with correct CIDR range

Create the private subnets with the below details

**Subnet 1**

|  |  |  |
| --- | --- | --- |
| **Sl. No** | **Field Name** | **Value** |
| 1 | VPC ID | aws-rdd-euw1-hpc-poc-npr-vpc-01 |
| 2 | Name | rdd-npr-hpc-poc-1a-sn |
| 3 | Availability Zone | eu-west-1a |
| 4 | CIDR Block | 10.221.90.0/26 |
| 5 | Name Tag | 2001493-HPC Upstream Compute |

**Subnet 2**

|  |  |  |
| --- | --- | --- |
| **Sl. No** | **Field Name** | **Value** |
| 1 | VPC ID | aws-rdd-euw1-hpc-poc-npr-vpc-01 |
| 2 | Name | rdd-npr-hpc-poc-1b-sn |
| 3 | Availability Zone | eu-west-1b |
| 4 | CIDR Block | 10.221.90.128/25 |
| 5 | Name Tag | 2001493-HPC Upstream Compute |

## Create cloud9 instance in eu-west1a and attach IAM instance profile.

Create the cloud9 with the below details

|  |  |  |
| --- | --- | --- |
| **Sl. No** | **Field Name** | **Value** |
| 1 | Cloud9 instance name | AWSPCVMCloud90003 |
| 2 | Instance id | i-0b5e18e1b6b890707 |
| 3 | VPC id | vpc-076dfb25e10919e49 |
| 4 | Subnet id | subnet-06208e6dab35e187d |
| 5 | Instance profile name | Cloud9SSMInstanceProfile |

## Create Security Group for Windows Workstations

We have added below mentioned rules as part of security group **(**[**sg-0a7f8e0f78e655240 (rdd-npr-hpc-poc-workstation-node-sg-allow-all)**](https://eu-west-1.console.aws.amazon.com/ec2/home?region=eu-west-1#SecurityGroup:securityGroupId=sg-0a7f8e0f78e655240)**)** for the windows workstation  
   
**Inbound Rules**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sl. No** | **Security group rule ID** | **Type** | **Protocol** | **Source** |
| 1 | sgr-0263c25f6364d5d3a | All traffic | All | 10.0.0.0/8 |

**Outbound Rules**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sl. No** | **Security group rule ID** | **Type** | **Protocol** | **Source** |
| 1 | sgr-0e6a4dace74ed1979 | All traffic | All | 10.0.0.0/8 |
| 2 | sgr-08fe19d4c7eab85ca | All traffic | All | 0.0.0.0/0 |

## Modify Default Security Group of VPC

Modify the security group with the below Rules   
**Inbound Rules**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sl. No** | **Security group rule ID** | **Type** | **Protocol** | **Source** |
| 1 | sgr-03f91c2a8c6bcfecb | DNS (TCP) | TCP | 10.221.90.0/24 |
| 2 | sgr-0c8f3ff7222858357 | DNS (UDP) | UDP | 10.221.90.0/24 |

## Create Route53 Resolver Outbound Endpoints

Create the Route53 Endpoint outbound with the below details.

|  |  |  |
| --- | --- | --- |
| **Sl. No** | **IPv4 Address** | **Port** |
| 1 | 10.208.160.199 | 53 |
| 2 | 10.208.160.19 | 53 |
| 3 | 10.208.160.215 | 53 |
| 4 | 10.208.160.14 | 53 |

## Create Security Group for FSx

We have added below mentioned rules as part of security group **(sg-080a1de42e6c35730 - rdd-npr-hpc-poc-fsx-all-allowd-sg)** for the FSx  
  
**Inbound Rules**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sl. No** | **Security group rule ID** | **Type** | **Protocol** | **Source** |
| 1 | sgr-047407e189fadc4dd | All traffic | All | 0.0.0.0/0 |

**Outbound Rules**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sl. No** | **Security group rule ID** | **Type** | **Protocol** | **Source** |
| 1 | sgr-06fad53e3fcc7856b | All traffic | All | 0.0.0.0/0 |

## TGW attachment with the newly created VPC by Dyson Cloud Team

The TGW has been attached by Dyson Cloud team.

## Whitelist the CIDR range in the Firewall

The CIDR has been whitelisted by Dyson Cloud Team

## Create Secret and store the AD read-only user credential in plain text

Domain read-only credentials has been created and stored by Dyson Domain Architect

## Create S3 Bucket

Create S3 bucket with the below details

S3 Bucket Details

|  |  |  |
| --- | --- | --- |
| **Sl. No** | **Field Name** | **Value** |
| 1 | Name | euw1-rdd-npr-hpc-poc |
| 2 | Region | eu-west-1 |
| 3 | Object Ownership | ACLs enabled |
| 4 | Bucket Versioning | Enable |
| 5 | Encryption key type | AWS Key Management Service key (SSE-KMS) |
| 6 | AWS KMS Key | Enter AWS KMS key ARN |
| 7 | Bucket Key | Enable |
| 8 | Object Lock | Disable |
| 9 | Name Tag | 2001493-HPC Upstream Compute |

## Provide the required access to the users to the s3 bucket:

Raise Service now ticket to provide the users the required access in S3 bucket

## Generating the key file:

Create the key file with the name **rdd-npr-hpc-poc.eu-west-1.pem** with the key-pair type as **RSA**

# Create Fsx Netapp Ontap

## Create the FSx filesystem

* Create a file system with Amazon FSx for NetApp ONTAP
* Select Single-AZ (post PoC: please select multi-AZ)
* Current SSD storage for root is 1 GB
* Select the desired VPC and Create the Filesystem.

## Create the Storage Virtual Machine in the Filesystem

* Select the file system
* Provide a name of the SVM
* Password is optional
* Select security style as ntfs (in PoC env – we have Unix, that needs to be changed)
* Join an Active Directory with the below details

## Create Volume in SVM

* Select the file system
* Select SVM
* Provide volume name, size, path etc
  + File System Details

|  |  |  |
| --- | --- | --- |
| **Sl. No** | **Field Name** | **Value** |
| 1 | File System Name | rdd-npr-hpc-poc-fsx-netapp-ontap |
| 2 | File System Id | fs-0dea6343b3497239f |
| 3 | File System Management Endpoint | 10.221.90.80 |
| 4 | File System Administrator Credential | fsxadmin/<Please contact the TCS AWS team> |

* + SVM Details

|  |  |  |
| --- | --- | --- |
| **Sl. No** | **Field Name** | **Value** |
| 1 | Storage Volume Machine (SVM) Name | svm-hpc-poc4 |
| 2 | SVM ID | svm-0929d44ac01218804 |
| 3 | Security Style | Unix (need to be changed to ntfs) |
| 4 | SVM ID | app, /app, share: hpc-poc-app |
| 5 | data, /data, share: hpc-poc-data |
| 6 | SVM Management Endpoint | 10.221.90.68 |
| 7 | SVM NFS IP Address | 10.221.90.68 |
| 8 | File System Administrator Credential | vsdmin/password |
| 9 | SVM AD Details | Service A/C: \_svc\_aws\_autoscaling/ <pwd from Domain Administrator> |
| 10 | NetBios Name: SVM-HPC-POC4 |
| 11 | FQDN: DYSON.GLOBAL.CORP |
| 12 | OU DN: OU=WIN, OU=RDD, OU=Non-production, DC=dyson,DC=global,DC=corp |
| 13 | DNS Ips: 10.221.64.2, 10.221.76.2 |
| 14 | Service A/C to mount in Linux | \_svc\_aws\_fsx/password |
| 15 | AD Group Name | AWS FSXAdmins (It’s not attached yet) |
| 16 | Tool Name for adding group | fsmgmt.msc from Windows Machine |

## Share the Volumes

* Use FSx CLI by using ssh fsxadmin@10.221.90.80 from command prompt
  + Set Security Style = ntfs for /app:
* qtree security -vserver svm-hpc-poc4 -volume app -qtree "" -security-style ntfs
  + Set security style = ntfs for /data:
* qtree security -vserver svm-hpc-poc4 -volume data -qtree "" -security-style ntfs
  + Create share for /app with full permission to everyone:
* vserver cifs share access-control create-share hpc-poc-app -user-or-group Everyone -permission Full\_Control
  + Create share for /data with full permission to everyone:
* vserver cifs share access-control create-share hpc-poc-data -user-or-group Everyone -permission Full\_Control

## Create AD group by creating ticket with Dyson

AD group (AWS FSXAdmins) has been created by Dyson AD Admin

## Add the AD group to the shared volumes

* Open Fsmgmt from any Windows machine (which has PING connectivity to the FSX) and change the Sharing and security
* Select the share
* Add the group "AWS FSXAdmins" in Shared Permission and provide full access
* Add the group "AWS FSXAdmins" in Security and provide full access

## Map Volumes in Windows Machine

* Members from the "AWS FSXAdmins" can map the volumes
* \\10.221.90.68\hpc-poc-app
* \\10.221.90.68\hpc-poc-data

## Mount Volume in Parallel cluster

* Mount volumes in Parallel Cluster using the configuration file
* Members from the "AWS FSXAdmins" can access the volumes in Parallel Cluster

# Create Windows Workstation

## Create IAM Role

Create IAM Role rdd-npr-hpc-poc-ec2-server-role **and Security group**

([sg-0a7f8e0f78e655240(rdd-npr-hpc-poc-workstation-node-sg-allow-all)](https://eu-west-1.console.aws.amazon.com/ec2/home?region=eu-west-1#SecurityGroup:securityGroupId=sg-0a7f8e0f78e655240)) **which needs to be attached to the workstation**

## Create the Windows workstations (Windows server 2022) as Workstation-1 for UseCase-1

Create the workstations with the below configuration

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Instance Type** | **NVDIA T4 Tensor Core GPU** | **vCPU** | **Cores** | **Memory**  **(GiB)** | **Storage** | **Network Bandwidth Gbps** | **EBS Bandwidth Gbps** |
| g4dn.2xlarge  (User-1) | 1 | 8 | 4 | 32 | 600 GiB GP3, 3000 IOPS, 250 GiBs, No backup | Up to 25 | Up to 3.5 |
| g4dn.4xlarge  (User-2) | 1 | 16 | 8 | 64 | 600 GiB GP3, 3000 IOPS, 250 GiBs, No backup | Up to 25 | 4.75 |
| g4dn.8xlarge (TBD) | 1 | 32 | 16 | 128 | 600 GiB GP3, 3000 IOPS, 250 GiBs, No backup | 50 | 9.5 |
| g4dn.16xlarge (TBD) | 1 | 64 | 32 | 256 | 600 GiB GP3, 3000 IOPS, 250 GiBs, No backup | 50 | 9.5 |

## Install/Configure security agents - MS Defender, using the script

Open the below mentioned folder in workstation, run the script click Y then hit enter.   
MS defender agent will be installed.



## Domain joins the Windows Workstation

Windows workstations has been domain joined by Dyson Domain Administrator

## Map the Fsx volumes in Windows Workstations

* Go to File Explorer and navigate to left side pane.
* Right click the Network option.
* Using Map Network Drive option, we can map the network drive.

## Install NICE DCV

* Download NICE DCV from <https://download.nice-dcv.com/>
* Run the .msi by accepting the default values
* Update the configuration file of DCV
* Under permission add - %any% allow built-in
* Validate the installation of DCV by running the DCV commands in Command Prompt

## Install DCV client/browser to the User's machine

DCV client/browser has been installed by Dyson Domain Architect

## App installations

Applications has been installed by TCS-App-Support team

## Validate the connectivity with the on-prem License server, PLM server, NFS

We can validate the connectivity of License server, PLM Server, NFS using **ping & telnet**

## Create AMI from the Workstation-1

We have followed the below steps to create the AMI from the Workstation-1

* Stop the Workstation 1
* Removed Workstation-1 from AD
* Created AMI from the Workstation-1
* Added Workstation-1 back to the AD and started it

Note: It has been taken 1 hour to get the AMI ready. It varies as per the storage of the ec2 instances.

## Install RDS service to enable multi-user RDP session concurrently

* We need to install RDS service to enable Multi-user RDP session.
* Login to Windows workstation open Power shell.
* Run the below comments one by one
  + PS:\> Import-Module ServerManager
  + PS:\> Add-WindowsFeature RDS-RD-Server
  + PS:\> Add-WindowsFeature RDS-Licensing
* Once run these three commands successfully restart the server.

## Raise request to increase the EC2 limit in AWS for more G4dn instances

This is being done from the AWS console

## Restore the AMI to create other workstations for UC-2, UC-3, UC-4

We have created workstations for UC-2, UC-3& UC-4 from the AMI of workstation-1 by following the below steps

* Create workstation from the AMI of workstation 1
* Add the workstation into the AD
* Change the computer name
* Start the workstation

# Create AWS Parallel Cluster

## Create Config for the parallel cluster and save it in the cloud9

* Create config file inside cloud9 and from there spin the parallel cluster.
* The cluster created would have FSX mounted along with AD integrated.
* Adding the frequently used commands for the AWS Parallel Cluster.

|  |  |  |
| --- | --- | --- |
| **Sl. No** | **Commands** | **Use for** |
| 1 | pcluster create-cluster –cluster-name AWSPCVMHPC0010 –cluster-configuration config-main.yaml | To Create the AWS Parallel Cluster |
| 2 | pcluster update-cluster –cluster-name AWSPCVMHPC0010 –cluster-configuration config-main.yaml | To update the AWS Parallel Cluster |
| 3 | pcluster update-compute-fleet -n AWSPCVMHPC0010 –status STOP\_REQUESTED | To stop the compute fleet instance |
| 4 | pcluster update-compute-fleet -n AWSPCVMHPC0010 –status START\_REQUESTED | To start the compute fleet instance |
| 5 | pcluster describe-compute-fleet -n AWSPCVMHPC0010 | To check the status of compute instance |

## Config file of AWS Parallel Cluster with Directory Service and Fsx

Attaching config file of AWS Parallel Cluster below



## Validate the Headnode, AD integration, Fsx integration

* **To validate the Headnode** à We logged into the Headnode as root user from the EC2 instance console successfully.
* **To validate the AD Integration** à We logged in to the Headnode using our corporate credentials and it worked fine as expected.
* **To validate FSx Integration à** We have checked whether the FSx is mounted into parallel cluster (or) not by using df -h and we were able to see the FSx has been mounted. Also, we have created, modified and deleted the files inside FSx directory. Hence FSx integration is working as expected.

## Install security agents - MS Defender on the HeadNode

* Install MS Defender package, Microsoft GPG public key and mdatp using command line.
* Run the MicrosoftDefenderATPOnboardingLinuxServer.py script provided by Dyson.
* Install latest OMS/MMA agent.
* Validate the OMS/MMA agent reporting status.
* Install the ARC agents.
* Validate ARC agent reporting status.

## App installations on HeadNode

This category will be taken care by TCS-App-Support team

## Scheduler test and validation

* Confirm the installation of SLURM in Head Node.
* Create a test batch file.
* Execute the batch file.
* Using SLURM commands verify the jobs are executing successfully

## Compute node validation

* SSH to the Compute Node to validate the integration of AD to compute node.
* Validate whether is FSX mounted to the compute node by checking the file system disk space.

## Upscaling Test and Validation

* Execute a test job within the Headnode
* Validate the creation of compute node in the console
* Execute the SLURM command to validate the upscaling of compute node.

## Validate the connectivity with the on-prem server

* Ping the License server, PLM server, NFS from the Headnode
* Successful ping response indicate the connectivity to the server.

## Validate the cluster

* Resources in the CloudFormation stacks are created successfully including the HeadNode
  + Headnode Details

|  |  |  |
| --- | --- | --- |
| **Sl. No** | **Field Name** | **Value** |
| 1 | Instance Name | HeadNode-10 |
| 2 | Instance ID | i-03d2cd4c6c5d4e252 |
| 3 | Instance Type | c6i.2xlarge |
| 4 | Private IPv4 Address | 10.221.90.29 |
| 5 | VPC ID | vpc-076dfb25e10919e49 |
| 6 | Subnet ID | subnet-06208e6dab35e187d |

* + Security Group Details

|  |  |  |
| --- | --- | --- |
| **Sl. No** | **Field Name** | **Value** |
| 1 | Security Group Name | AWSPCVMHPC0010-HeadNodeSecurityGroup-121Y7JEUCSW7E |
| 2 | Security Group ID | sg-03f2afbac3bd23e86 |
| 3 | Inbound Rule | Source 0.0.0.0/0 , Port -22, Protocol -TCP |
| Source – SG of Compute Nodes, Port -All, Protocol – All |
| Source – 10.0.0.0/8, Port -All, Protocol – All |
| 4 | Outbound Rule | Source – 0.0.0.0/0, Port – All, Protocol – All |

## Raise request to increase the EC2 limit in AWS for the compute nodes which falls in "All Standard (A, C, D, H, I, M, R, T, Z) instances" group to 2560

It has been fulfilled from the AWS console

# Custom GUI

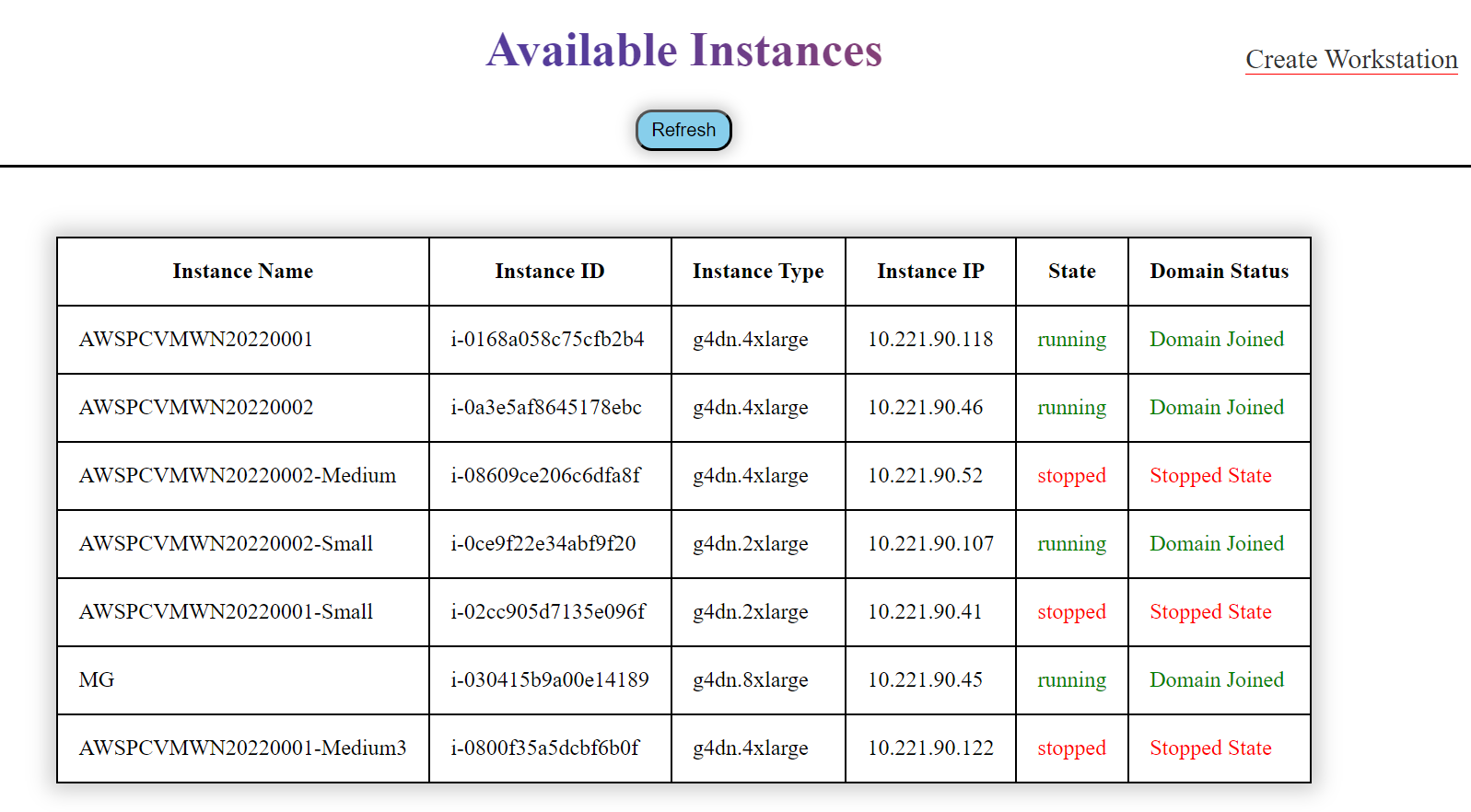
* Custom GUI for users to manage and create instances as per requirement.
* GUI is created using HTML, JavaScript and CSS.
  + index.html
  + administration.html
  + script.js
  + style1.css
  + style2.css
* The GUI is currently deployed on one of the EC2 server.

|  |  |
| --- | --- |
| Instance Name | AWSPCVMWN20220002-Small |
| Instance ID | i-0ce9f22e34abf9f20 |
| Instance IP | 10.221.90.107 |

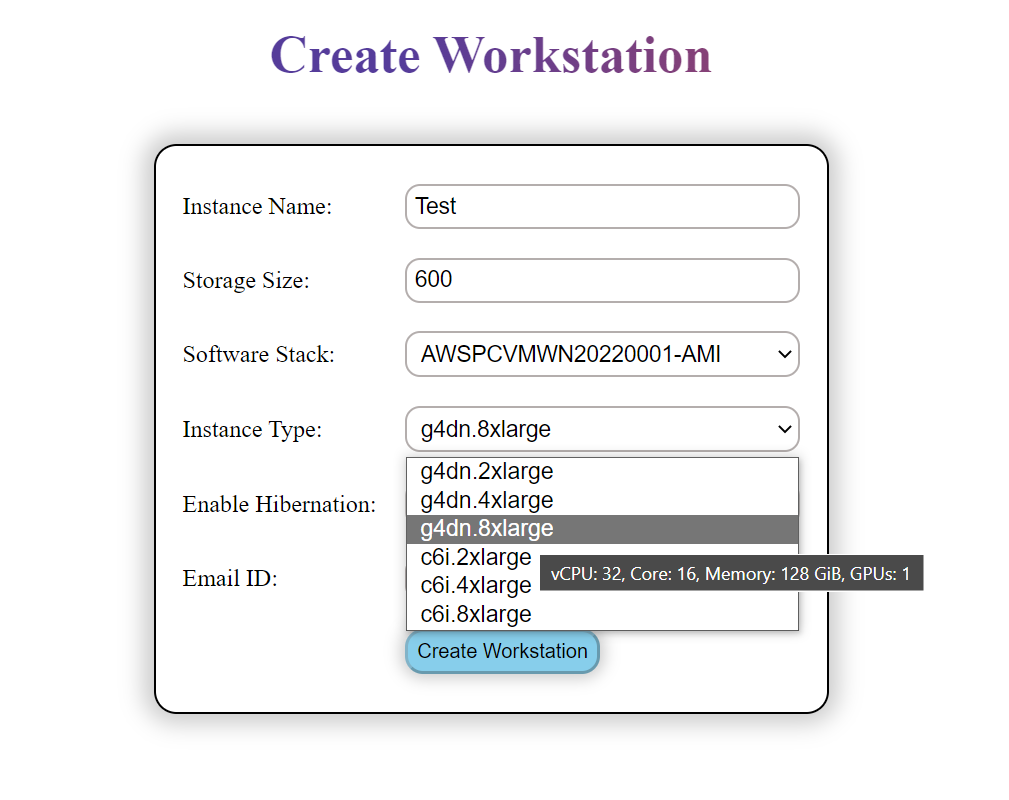
* GUI url: <http://10.221.90.107/ec2selfservice/>
* GUI Backend.

|  |  |  |
| --- | --- | --- |
| **GUI** | **API Gateways** | **Lambda Functions** |
| https://ew4mxrwhjc.execute-api.eu-west-1.amazonaws.com/default/hpc-poc-create-ec2-instance | hpc-poc-create-ec2-instance |
| https://q71yur66e8.execute-api.eu-west-1.amazonaws.com/default/hpc-poc-list-ec2-instance | hpc-poc-list-ec2-instance |
| https://5zu1p7wkh1.execute-api.eu-west-1.amazonaws.com/default/hpc-poc-domainjoin-status | hpc-poc-domainjoin-status |

* Snapshots of GUI
  + Home Page



* + Administration page.



# Application Configuration & Data Transfer

## App Configuration on workstations to connect to the PA Cluster

Application has been configured by TCS-App-Support team

## Data Transfer from OnPrem to AWS

Data transfer has been done by Dyson Business Users