Architecture & Infrastructure design

HPC Upstream Compute platform – Post-PoC

**Document Signoff**

**Document Signoff**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Approved By | Approved Date | Approved By | Approved Date |
| 1.0 | **Name:** Jithendra Balakrishnan (Automation and DevOps Lead)  **Organisation:**  Dyson |  | **Name:** Suryanarayana Vaddadi (Senior Manager Solution Architect)  **Organisation:**  Dyson |  |
| Signature | Jithendra Balakrishnan | | Suryanarayana Vaddadi | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Approved By | Approved Date | Approved By | Approved Date |
| 1.3 | **Name:** Steve Messenger (HPC Specialist)  **Organisation:**  Amazon Web Service |  | **Name:** Simon Gray  (Senior Solutions Architect)  **Organisation:**  Amazon Web Service |  |
| Signature |  | |  | |

Document Revision List

|  |  |  |  |
| --- | --- | --- | --- |
| Revision No. | Revision Date | Author | Revision Description |
| V 0.1 | 18/05/2023 | Prithwiraj | Initial Design Document |
| V 0.2 | 26/05/2023 | Aruneet | Inter-Connectivity within the Parallel Cluster |
| V 0.3 | 08/06/2023 | Jeelan | Updated the Security Group Section for Workstation |
| V 0.4 | 09/06/2023 | Abdul | Updated the Security Group Section for FSx |
| V 0.5 | 15/06/2023 | Prithwiraj | Updated the Implementation Details |

Contents

1 Contents 4

2 Introduction 7

2.1 Purpose of the Document 7

2.2 AS-IS Model 7

2.3 Scope 9

2.4 Out of Scope 9

2.5 Approach 10

2.6 Design Consideration 10

2.7 Intended Audience 10

3 AWS Regions 11

4 AWS Accounts and Environments 12

4.1 AWS Account 12

4.2 Environment 12

5 Network Architecture and Connectivity 13

5.1 Overall Network Architecture 13

5.2 VPC/Subnet Structure for HPC workload using Parallel Cluster 14

5.3 Connectivity with Dyson on-prem 15

5.4 Connectivity for users using Dyson Laptop 15

5.5 IP Range and Integration with Dyson Network 16

5.6 IP CIDR Block for AWS Environment 16

5.7 Access to AWS Console 17

6 Inter-Connectivity within the Cluster 18

7 Security 19

7.1 AWS general approach for security 19

7.2 AWS Console and Service Access Management 19

7.3 Access Management using Dyson AD 20

7.4 Patching and Antivirus 21

7.5 Vulnerability Check 21

7.6 Network Security 21

7.7 Governing AWS Environment 22

7.8 Data Encryption 22

7.9 Logging and Monitoring 22

8 AWS Infrastructure provisioning and Management 24

8.1 EC2SelfService Portal 24

8.1.1 Architecture 24

8.1.1 Workflow 25

9 Storage Considerations 26

9.1 Storage Sizing and Recommendations 26

10 Availability, Resilience and Capacity Management 27

10.1 Availability and Resilience 27

10.2 Capacity Management 27

11 Regulatory Compliance 28

12 Implementation 29

12.1 Prerequisite 29

12.2 Implementation Approach 29

12.3 Implementation Details 30

12.4 App Installation 32

12.5 List Of Services 32

12.6 Subnet to Route Table Mapping 32

12.7 Route Table Details 33

12.8 Subnet to NACL Mapping 33

12.9 NACL Detail 33

12.10 Instance Details 34

12.11 Instance/Storage to Security Group Mapping 34

12.12 Security Group Detail 34

13 Assumptions 36

14 Appendix 37

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 Post-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
* Migrate the on-premises data to HPC environment
* Install Applications in Workstations to run HPC jobs
* Provide support for the HPC and workstation environment.

## 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.

## AS-IS Model

* **Existing Network Design:** Dyson’s corporate offices are connected to the AWS environment through SD-WAN. The AWS Account is sub-divided into OU level accounts. There are separations for Prod and Non-Prod accounts. The Transit Account is responsible for the SD-WAN connection at the AWS side and the Cisco CSRs are connected to the Transit Gateways as per Figure-1.

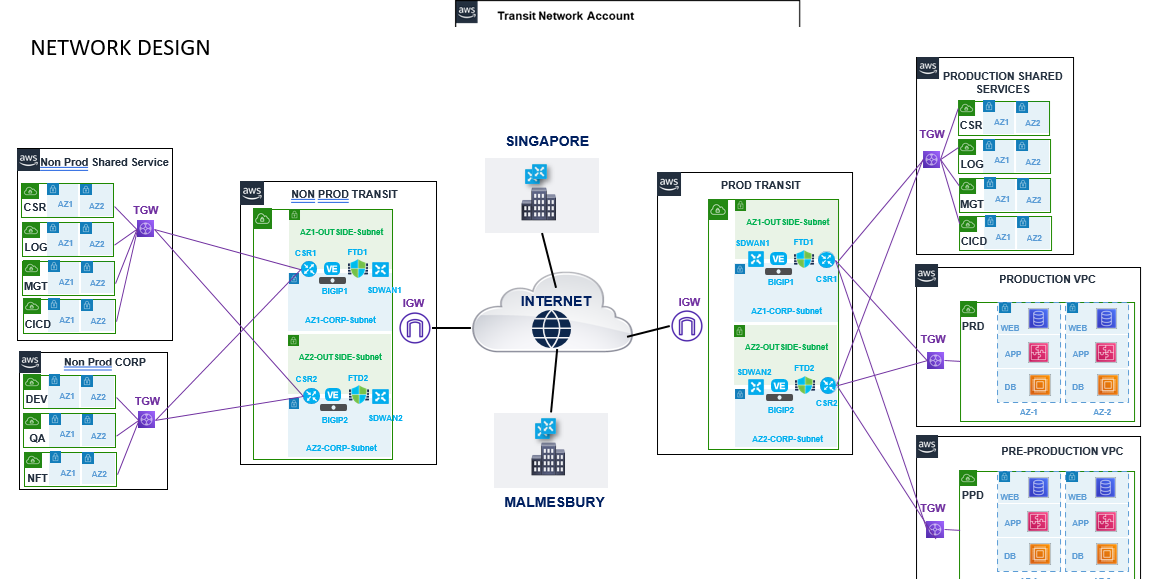


Figure 1 – DYSON Network Connectivity Overview

* **On-prem HPC Landscape:** There are two clusters in on-prem environment. The users are sitting with their local machine and connected to the clusters and underlying NFS storage. Domain-based authentication is required using Azure AD as per Figure-2.

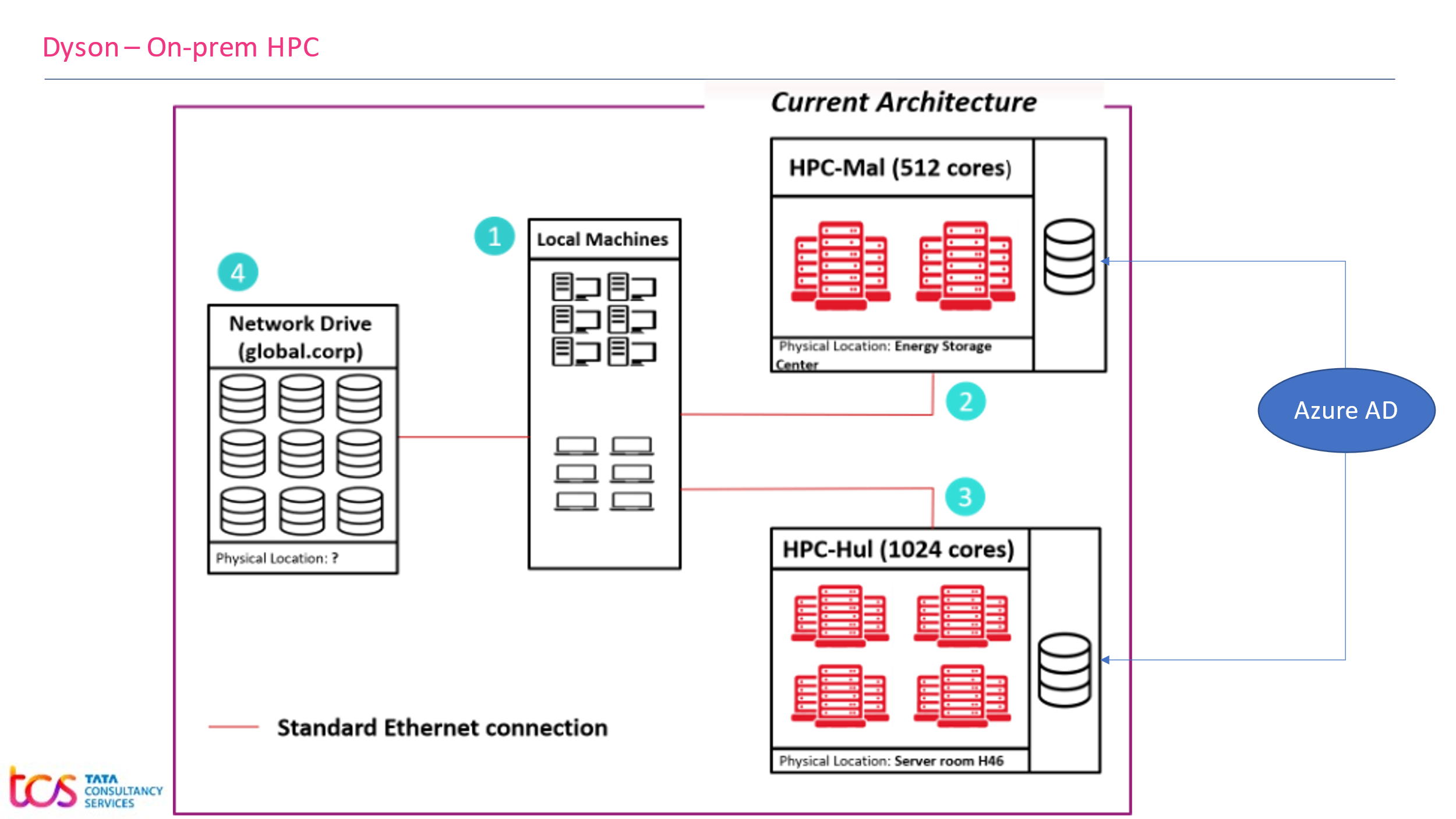


Figure 2 – DYSON On-Prem HPC Platform

* **On-Prem HPC Sizing Details:**

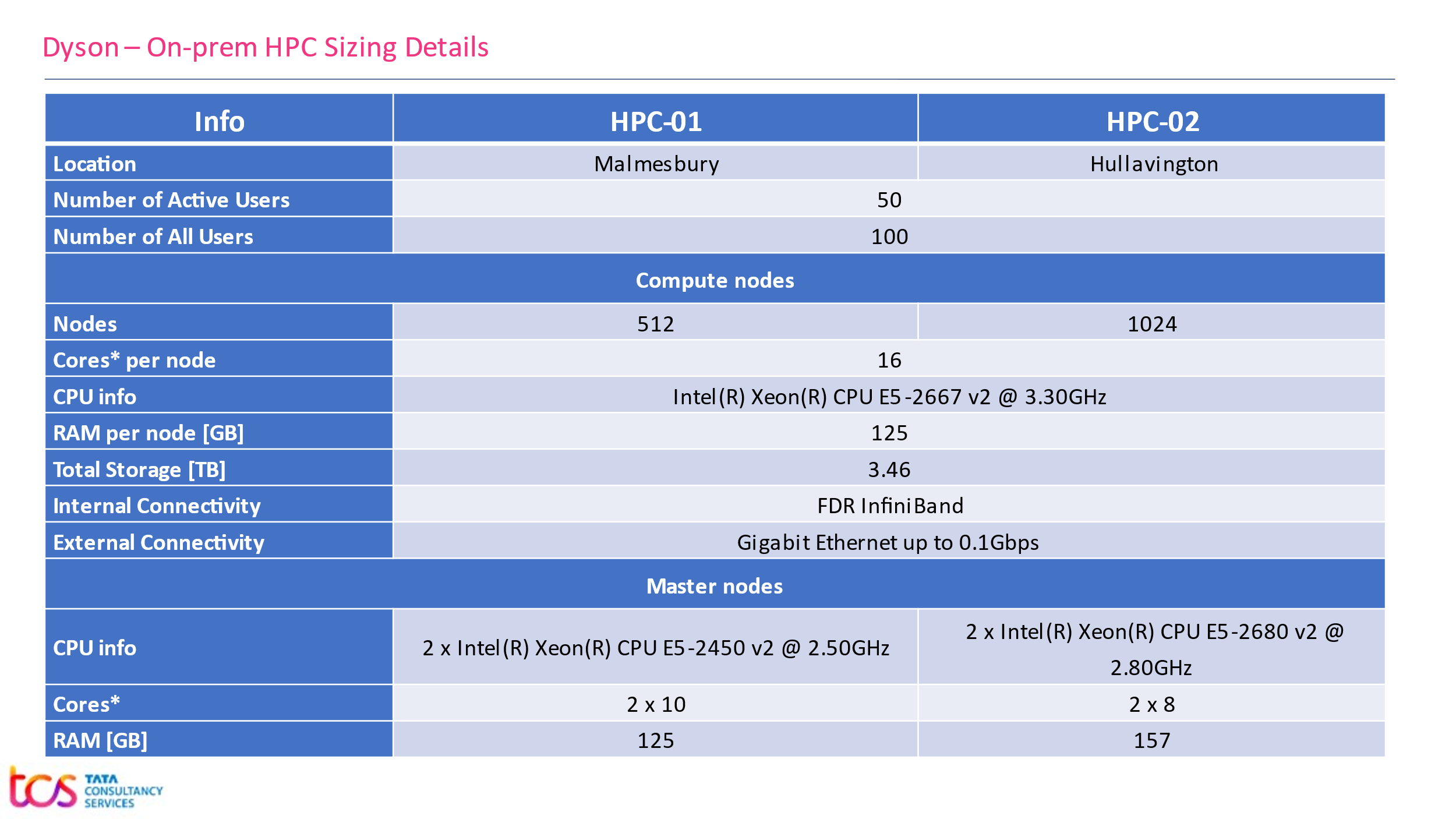


Figure 3 – DYSON On-Prem HPC Sizing

## Scope

Scope of this document is to describe the building blocks to setup AWS-HPC infrastructure for hosting DYSON-HPC-UPSTREAM platform. 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 PoC model, feedback and Dyson’s business requirement to provision infrastructure 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:

* 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.

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 “Prod RDD”. There are multiple shared VPCs available in the account however, for the sake of simplicity a dedicated VPC will be created.

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

## AWS Account

Shared account “Prod RDD” (Account Id:<Need to fill the AWS Account Number>) will be used to create the production platform.

## Environment

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

* **Prod Account**

# Network Architecture and Connectivity

## Overall Network Architecture

Diagram depicts the existing network architecture of Dyson’s AWS environment and connectivity with their respective branches. A new VPC has been proposed under “Prod RDD” account as highlighted below.

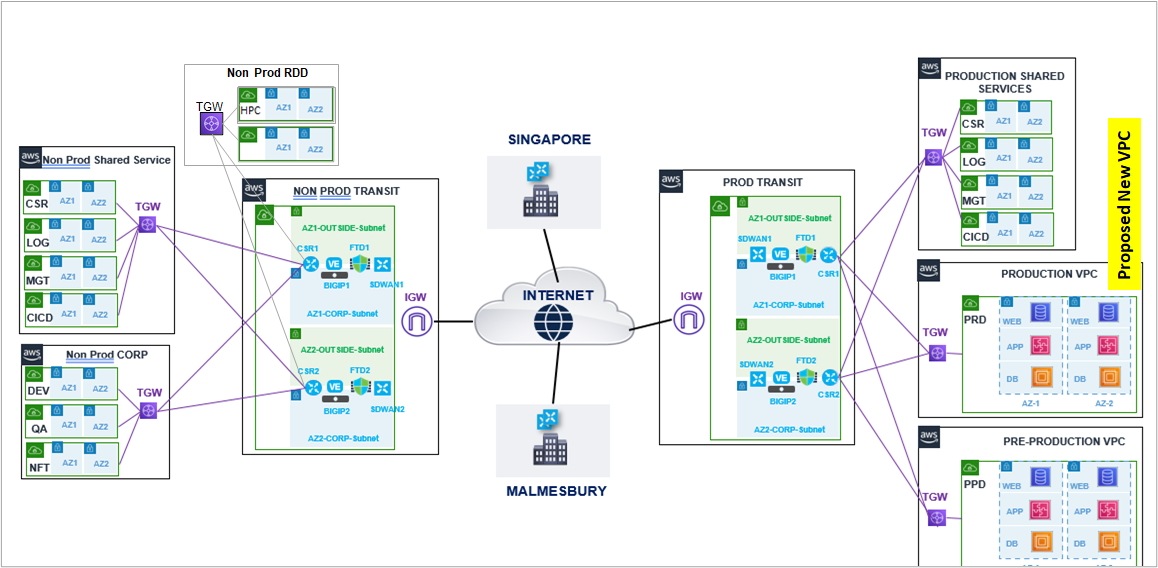


Figure 4 – DYSON-HPC-UPSTREAM Network Connectivity Overview

**Key points covered as part of the initial architecture design**

1. Centralized Transit Network account acts as a Network Hub. All VPCs within AWS environment are connected to Transit Gateway. The Transit Gateway is connected to SD-WAN to establish the connectivity between the on-prem and AWS environment
   * + The “Prod Transit Network” account is being used for all production workloads
2. The VPC under Transit Network account acts as an entry point from Dyson to AWS environment.
3. The new HPC VPC will be created under “Prod RDD” account
4. Users are connected to AWS environment as below

* Dyson users are connected to AWS environment through SD-WAN
* TCS Development team can be connected to AWS environment through Client VPN

1. To migrate data from Dyson to AWS, the SD-WAN can be being used.

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

The following diagram depicts VPC and Subnet structure of HPC workload

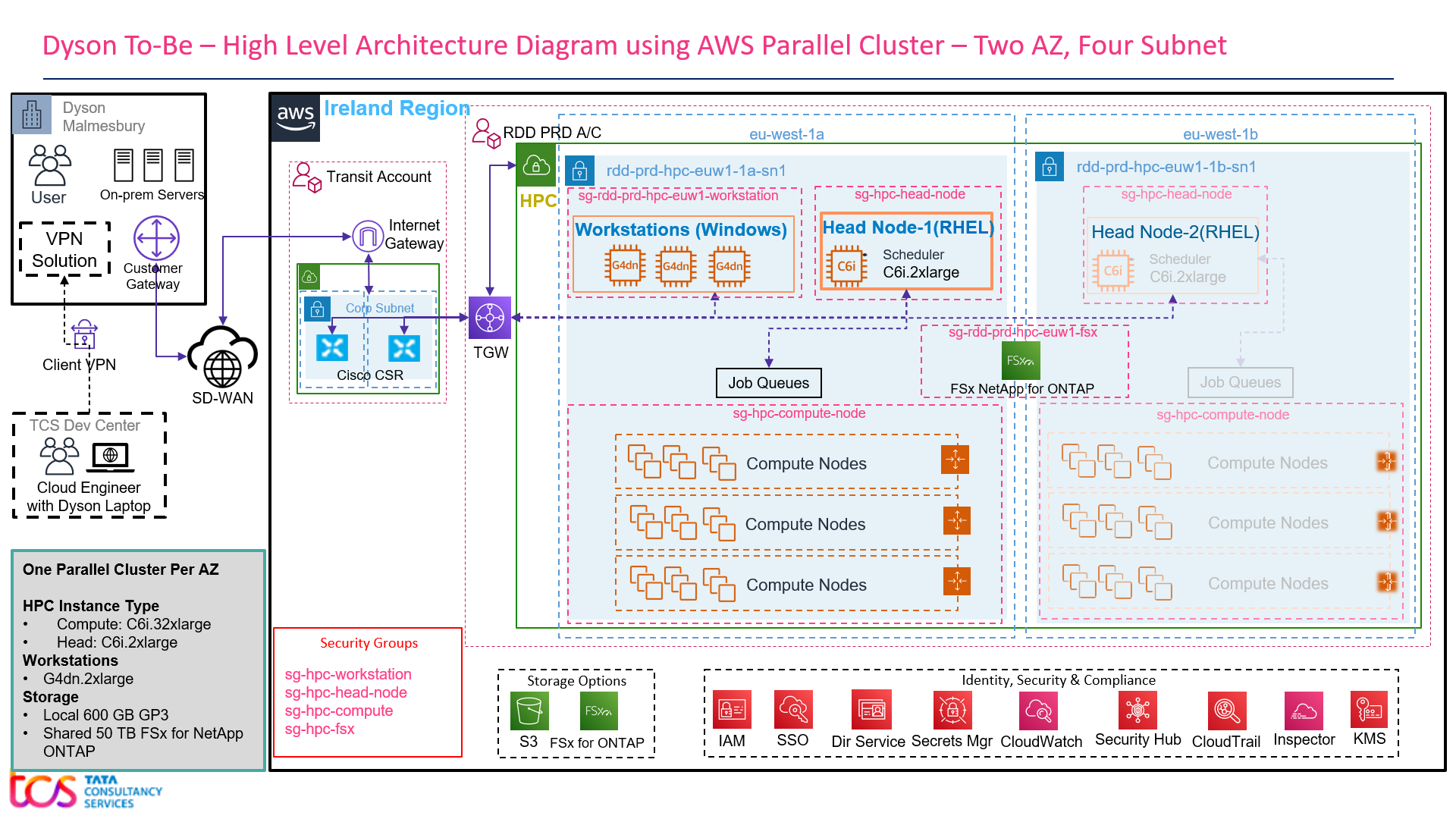


Figure 5 – DYSON-HPC-UPSTREAM VPC Overview

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

1. VPCs will be spanned in two Availability Zones in Ireland region
2. One Parallel Cluster Per AZ
3. No Public Subnet
4. VPC and Subnet structure

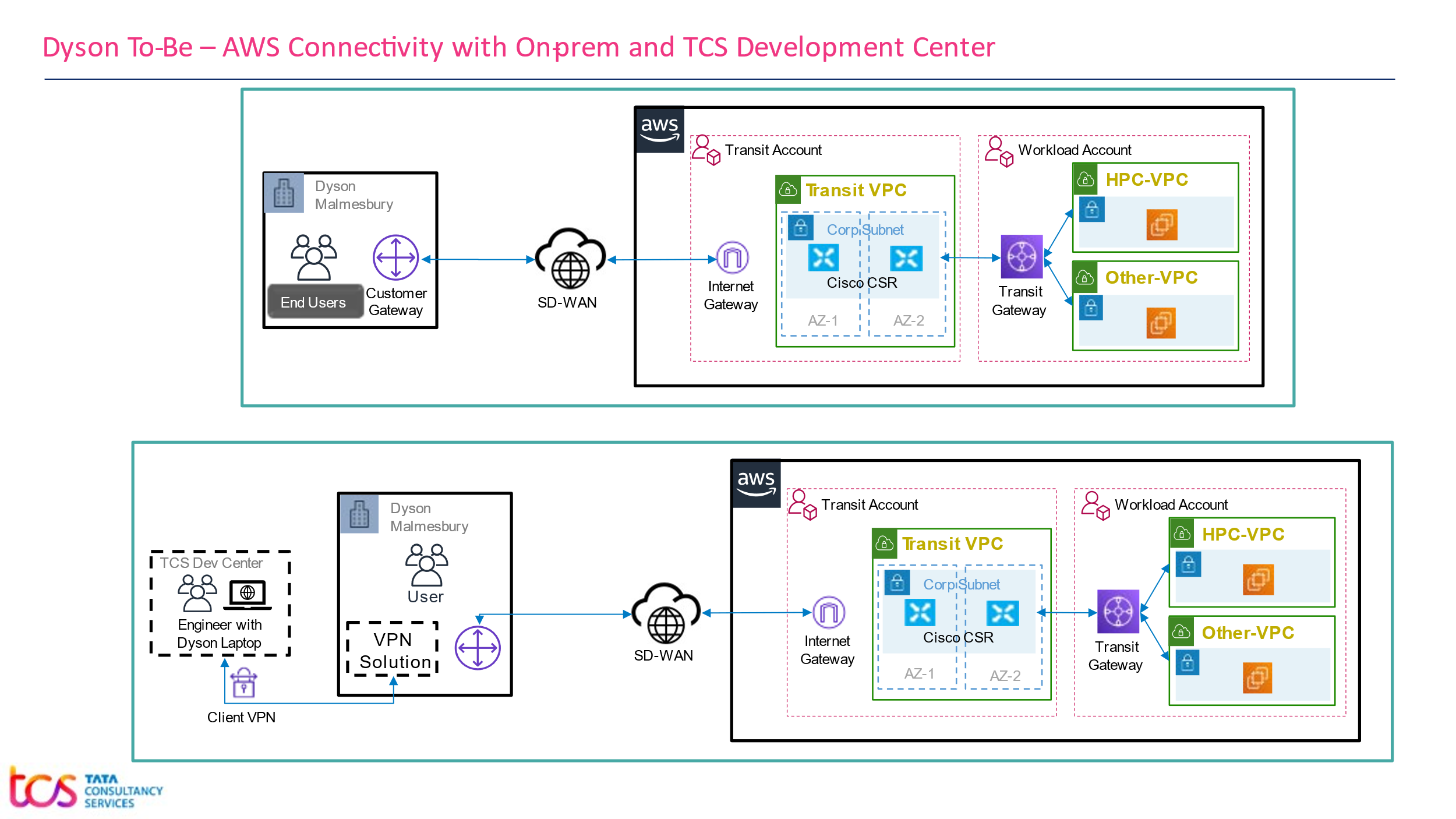
|  |  |  |
| --- | --- | --- |
| **HPC VPC** | | |
| **Subnets** | **Resource Details** | |
| rdd-prd-hpc-euw1-1a-sn1 | * FSx NetApp ONTAP * Compute Node (RHEL 8) under auto-scaling group | * Windows Workstations with NICE DCV installed. * One Head Node (RHEL 8) with Job Scheduler |
| rdd-prd-hpc-euw1-1b-sn1 | * One Head Node (RHEL 8) with Job Scheduler |

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.
3. Workstations and Parallel Cluster will be able to connect the on-premise servers (License Server, PLM servers and Production database as well)

## Connectivity with Dyson on-prem

Below are some of the key points to access AWS resources from Dyson office location (Malmesbury):

* Dyson’s Malmesbury location is connected to the Internet Gateway inside the Transit Account using SD-WAN over internet.
* Cisco CSRs from the Transit Account are connected to the Transit Gateway in the Workload Account where the HPC cluster will be created.
* RDP/DCV ports to be opened from Dyson to AWS VPC.
* Dyson user may use the DCV client from their local machine to remotely visualize the workstations.
* Alternatively, Dyson user may log on to their corresponding Workstations and access the cluster.



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

* Data transfer between Dyson and AWS will happen over intranet using SD-WAN.

## Connectivity for users using Dyson Laptop

Below are some of the key points to access AWS resources by the users having Dyson Laptop:

* User will have his/her Dyson laptop with Client VPN installed, which will be used to connect the Dyson’s N/W, and from there AWS cloud can be accessed.
* User will have their User ID created in Dyson’s existing Active Directory.
* DCV ports to be opened from Dyson to AWS VPC.

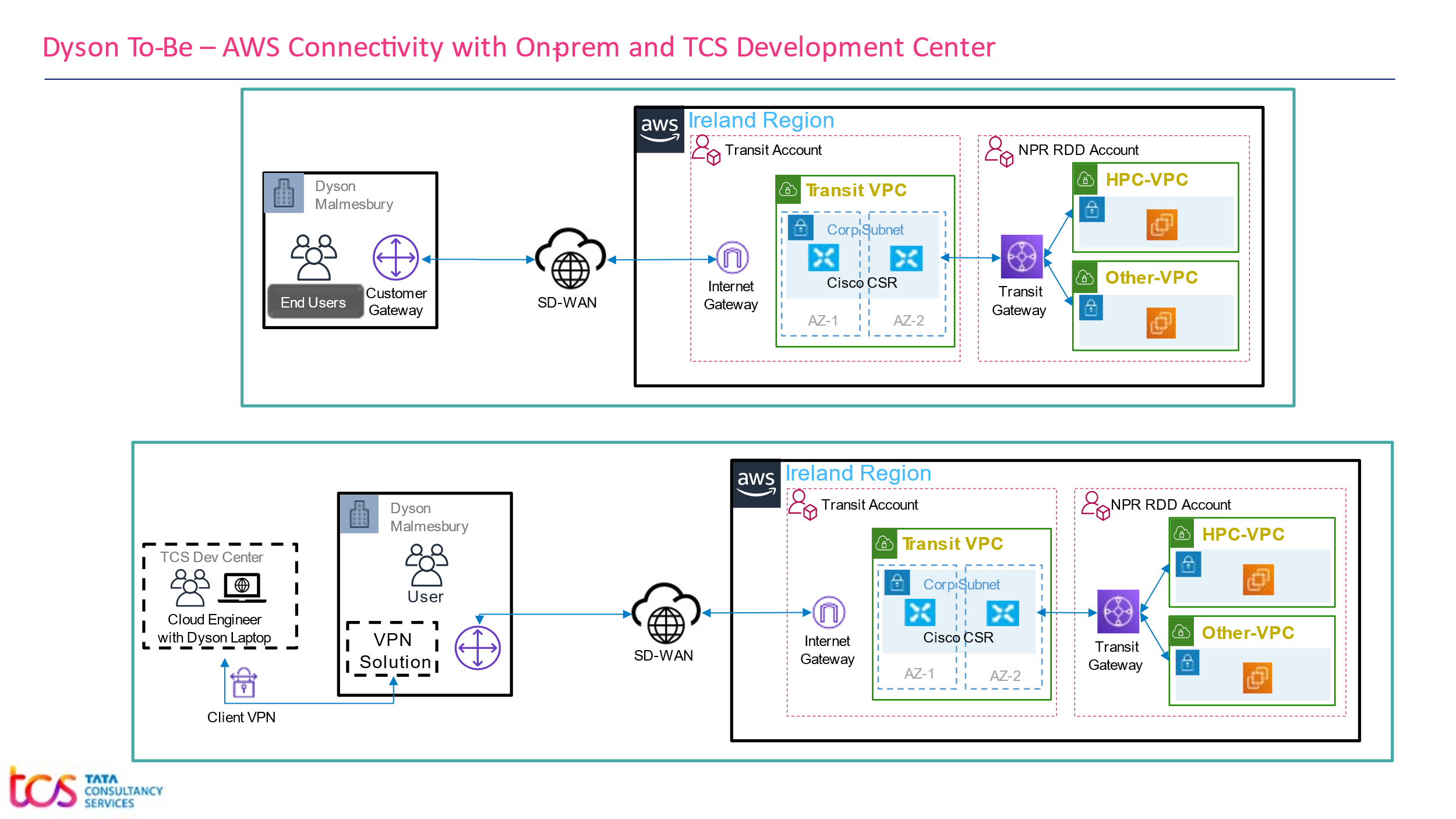


Figure 7 – Connectivity between AWS and Users using Client VPN

**Dependency to establish Connectivity**

To establish the connectivity between AWS and Dyson Corporate Network, need to take the following points into consideration

* Involvement of cloud team to attach the Transit Gateway to the newly created VPC for HPC Cluster to establish on-Prem to AWS connectivity for Dyson user.
* IP range of Dyson Corporate N/W should not overlap with CIDR Block **<Need to fill the CIDR Block>** which is planned to be used for the AWS HPC Cluster.

## IP Range and Integration with Dyson Network

As per proposed architecture all services like Head Node, Workstations will be available over Dyson’s corporate network using SD-WAN. Data Transfer will be done using SD-WAN.

AWS resources must meet Dyson specific security/compliance requirements, e.g., fully patched, Anti-Virus and Firewall Protection to establish the connection with Dyson Corporate Network. Domain join is required to establish the connection between Dyson on-premises resources and AWS Cloud.

## IP CIDR Block for AWS Environment

As per production workload prediction, the total number of IP requirement could grow up to 8000. So its recommended to take a CIDR block /18 which gives 16384 IP addresses.

|  |  |
| --- | --- |
| **AWS VPC** | **(EU-West-1)** |
| HPC VPC | **<Fill CIDR Block>** |

|  |  |  |  |
| --- | --- | --- | --- |
| **HPC VPC: xxx.xxx.xxx.xxx/19 to support 8192 IPs** | | | |
| **Subnets** | **Resource Details** | | **IP Allocation** |
| rdd-prd-hpc-euw1-1a-sn1 | * FSx * Compute Node | * Workstations * One Head Node | xxx.xxx.xxx.xxx/20 => 4096 IPs |
| rdd-prd-hpc-euw1-1b-sn1 | * One Head Node | xxx.xxx.xxx.xxx/21 => 2048 IPs |

## Access to AWS Console

AWS Console will be accessible from Dyson Corporate Network over SD-WAN.

* Console access will be centrally managed through AWS Single Sign On.
* MFA can be enabled for all Console Users.
* Least Privilege strategy will be enforced by using AWS Role and Policy.

# Inter-Connectivity within the Cluster

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

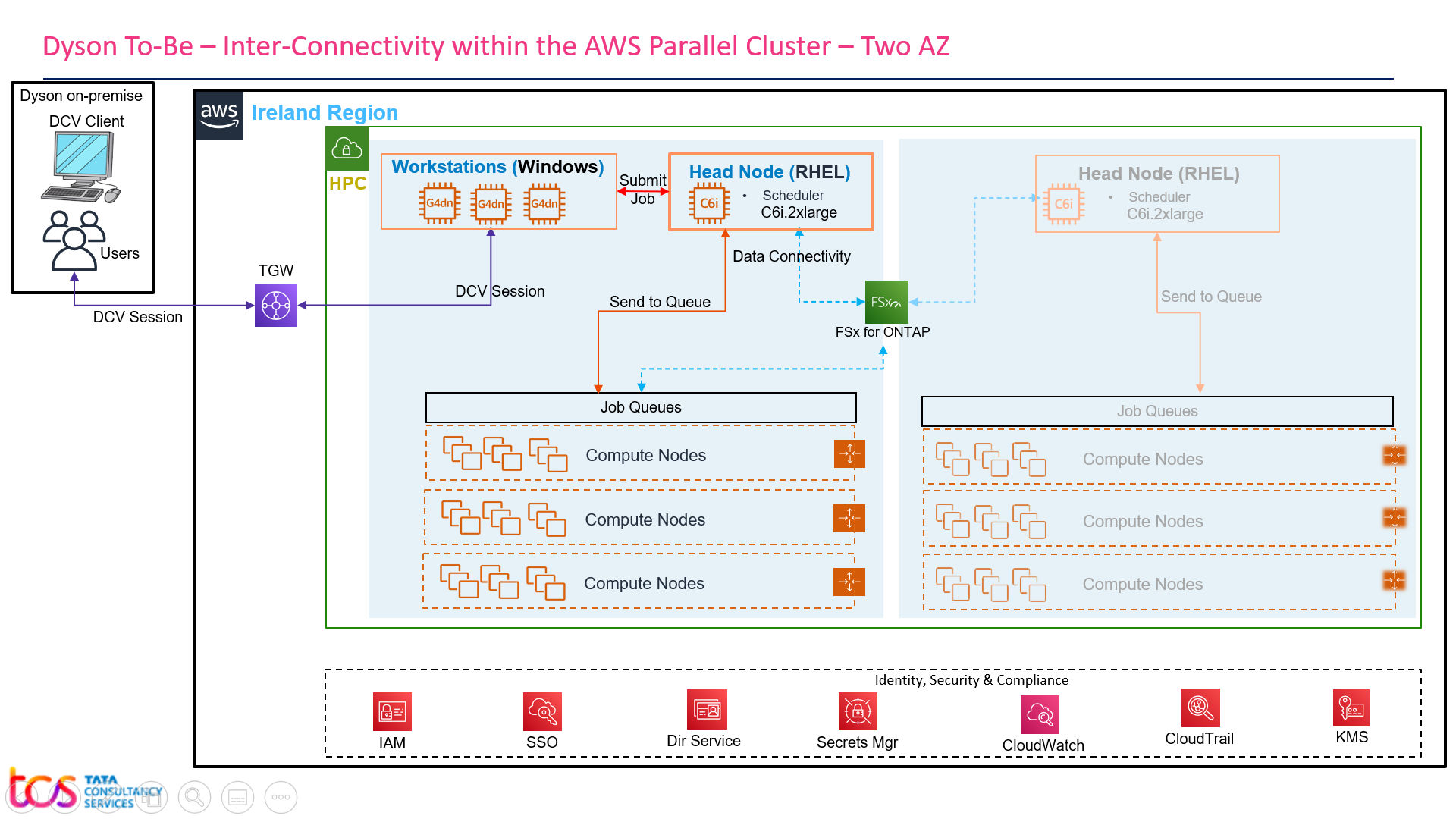


Figure 8 – Inter-Connectivity within the Cluster

* Workstations will have NICE DCV Server installed (note: free on AWS EC2).
* User may use the DCV Client and establish the remote session to their respective workstation.
* Windows based workstations will have required applications installed.
* Users will upload their data to the shared storage (FSx NetApp Ontap). The shared storage will be accessible throughout the cluster.
* Users will be able to access the cluster from the workstations, they should be able to submit jobs from their workstations to Parallel cluster Headnode.
* The Headnode scheduler will schedule the submitted job to the job queue based on scheduling policy.
* Compute Nodes will be provisioned on-demand and will be scaled up and down as per the scaling policy.

# Security

## AWS general approach for security

Proposed architecture will be based on AWS Security best practices. The entire AWS environment (Landing Zone) is already setup with Governance, Compliance and Security. SSO and MFA are also in place to ensure full centralized control over Access Management.

Actions taken by a user, on any AWS services are recorded as events in CloudTrail. Events include actions taken in the AWS Management Console, AWS Command Line Interface, and AWS SDKs and APIs.

Centralized log management for efficient monitoring and management functionality using CloudWatch, CloudTrail, VPC Flow Logs.

## AWS Console and Service Access Management

AWS SSO is only for Console Users (Developers, Administrator).

AWS SSO is being used to give permission/monitor access rights to various users. Some of the SSO related implementation details are given below

* Console access is centrally managed through AWS SSO and configured in the master/root account.
* Once the SSO user authenticated against the AD and MFA, the respective accounts will be listed to the user based on their privileges.
* Access to individual account is based on role policy defined and created in the respective AWS accounts.
* Third party soft token MFA (Google authenticator, Azure authenticator etc) can be used as an MFA device.
* Least privilege model is followed to grant necessary access to the accounts for individual console/CLI users.
* Service control policies can be configured to audit/restrict higher access privileges

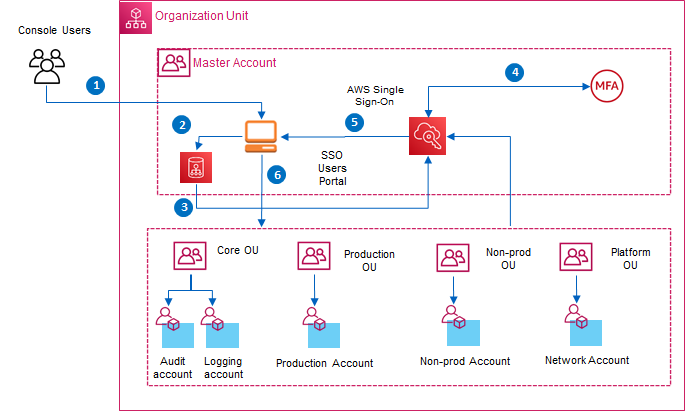


Figure 9 – AWS SSO Authentication Flow

**Authentication Flow steps:**

1. Console login user access the AWS SSO user’s portal
2. Users will be redirected to the Identity Provider if not already logged in.
3. Identity Provider response created and sent to AWS SSO
4. Second level authentication against MFA token
5. Based on the existing policies defined in the AWS accounts and attached to the SSO user, available AWS accounts will be listed to user
6. Select the account and will be redirected to the respective management console.

## Access Management using Dyson AD

Dyson’s existing Active Directory will be leveraged for authentication, AD is already integrated with AWS SSO as per the figure given below. Domain join is required to get the connectivity with the on premise servers such as license server, PLM server, and NFS.

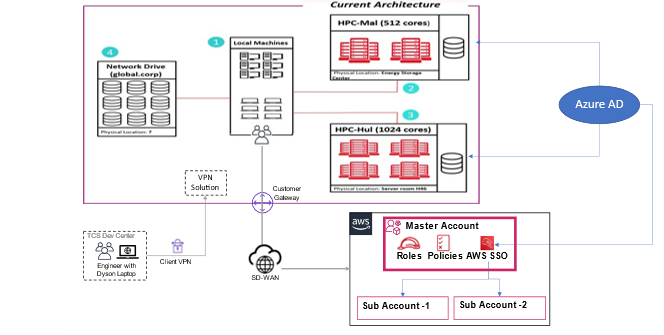


Figure 10 – AWS SSO and Microsoft AD Authentication

## 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.

## Governing AWS Environment

Governance for overall AWS environment will be taken care by **Guardrail**. Through guardrails, AWS Control Tower implements *preventive* or *detective* controls that help organization to govern resources and monitor compliance across groups of AWS accounts.

The existing **Guardrail** will be applied.

## Data Encryption

**Data in Rest:**

* 256-bit Advanced Encryption Standard (AES-256) are used to encrypt data in rest. EBS volumes are encrypted by default, server-side encryption for S3 is also a default behavior.
* All Amazon FSx file systems are encrypted at rest with keys managed using AWS Key Management Service (AWS KMS).

**Data in Transit:**

* Transfer of sensitive data or migration of data from Dyson to AWS will happen only through SD-WAN over internet. SD-WAN has its own security mechanism.
* Amazon FSx automatically encrypts data in transit using SMB encryption as and when we access the file system.

**Key Management:**

* Key management will be done through AWS Key Management Service (AWS KMS). Key can be managed either by AWS or Dyson. Dyson prefers – keys managed by AWS.

## Logging and Monitoring

Existing Logging and Monitoring strategies will be used as per the proposed architecture.

**CloudWatch:**

* Application and infrastructure monitoring from CloudWatch console.
* Required logs will be collected and metrics will be created for monitoring and alerting.
* Logs will be stored in CloudWatch and will be retain for number of days as per Dyson policy.
* Based on metrics threshold setting/system state changes, alarms will be triggered into Support team during managed support.
* CWAgent will be installed and configure to stream log from EC2 to CloudWatch

**CloudTrail:**

Logs user and API activities into S3 for Governance and are already integrated with Sentinel for compliance and operational auditing.

**VPC Flow Logs:**

VPC **Flow Logs is a feature** that enables you to capture information about the IP traffic going to and from network interfaces in a VPC. Flow logs can help to determining the direction of the traffic to and from the network interfaces

# 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 Production implementation.

However, TCS will configure FSx NetApp ONTAP and AWS Parallel Cluster post installation, and this is one time configuration.

# Storage Considerations

TCS will use the following options for storage in AWS

**Elastic Block Storage (EBS) for EC2 instances:**

Amazon Elastic Block Store (Amazon EBS) provides block level storage volumes for use with EC2 instances. EBS volumes behave like raw, unformatted block devices. You can mount these volumes as devices on your instances.

**FSx NetApp ONTAP:**

Amazon FSx for NetApp ONTAP is a fully managed service that provides highly reliable, scalable, high-performing, and feature-rich file storage built on NetApp’s popular ONTAP file system.  With FSx for ONTAP:

* Support for petabyte-scale datasets in a single namespace
* Multiple gigabytes per second of throughput per file system
* Security: AWS KMS, SMB Kerberos session keys, On-demand antivirus scanning
* ISO, PCI DSS, SOC, HIPAA compliant

**Amazon S3 Buckets:**

In proposed architecture Amazon S3 will be used to

* Store CustomActions shell script which shall be used by the Parallel Cluster
* Store some metadata files which shall be used by Parallel Cluster

## Storage Sizing and Recommendations

Actual sizes are given in the appendix-1 as part of the System requirements.

# Availability, Resilience and Capacity Management

## Availability and Resilience

The AWS global infrastructure is built around AWS Regions and Availability Zones. AWS Regions provide multiple physically separated and isolated Availability Zones, which relate to low-latency, high-throughput, and highly redundant networking.

According to proposed architecture:

* There are two AZs, two subnets, two separate parallel cluster, one in each subnet
* One active Parallel Cluster, another is passive. If one down, we can use the other one
* The S3 Standard storage class is designed for 99.99% availability.
* FSx are deployed in Multi-AZ

## Capacity Management

Capacity resizing will be done based on the performance test output and recommendation.

**AWS Trusted Advisor** inspects our AWS environment, and then makes recommendations when opportunities exist to save money, improve system availability and performance, or help close security gaps.

# Regulatory Compliance

All the existing regulatory compliances of Dyson will be adhered.

# Implementation

## Prerequisite

* AD group for FSx NetApp ONTAP, proposed AD group name is HPCFSxUser
* AD group for Workstations, the existing AD group for their on-prem HPC workstations can be used

## Implementation Approach

* Base infrastructure can be created using Terraform script. VPC, Subnets, Security Groups, Key-Pair, IAM Role, Policy, Route53 Resolver Outbound Endpoint, S3 Bucket can be created
* FSx NetApp ONTAP File System, SVM, Volumes can be created using Terraform script and can be configured

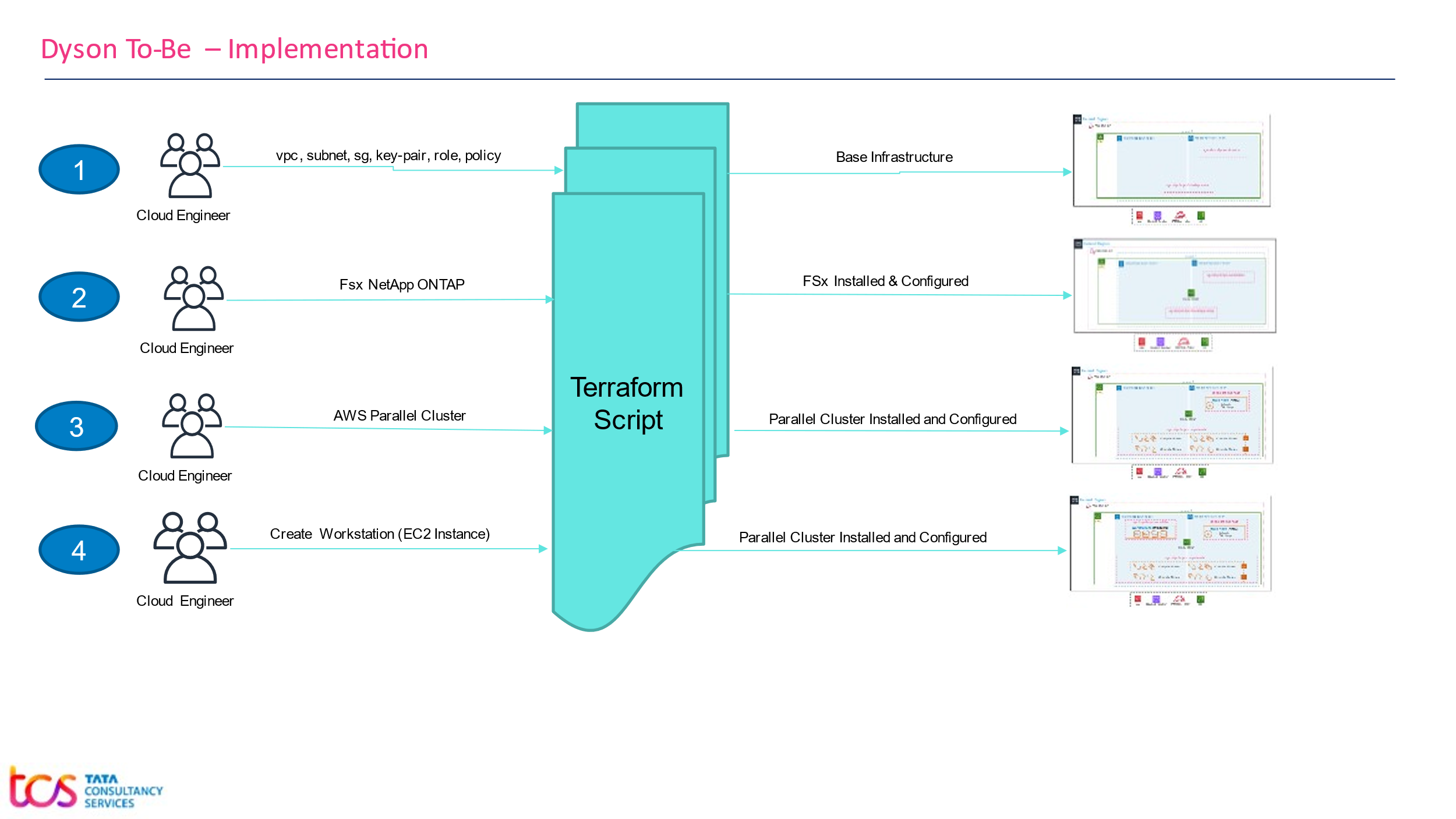


Figure 11 – Implementation plan

* Parallel Cluster can be created/provisioned using CloudFormation script
* Workstations can be created through Custom GUI “EC2 SelfService” from a predefined AMI, workstations can be domain joined and configured to be compliant with Dyson security standard
* Infrastructure can be created using Terraform script. However, linux/bash script can be used wherever Terraform does not support. However, Console/Manual steps can be performed wherever linux/bash script does support
* TCS Cloud Engineers will use their Dyson laptop to create the Terraform script. Script will be pushed/merged to Bitbucket, Dyson Cloud Team will validate and execute those scripts over Dyson AWS RDD Production account

## Implementation Details

|  |  |  |
| --- | --- | --- |
| **Sr#** | **Functionalities** | **Responsibilities** |
| 1 | **Base Infrastructure** | |
| 1.a | Get CIDR to be used for AWS Environment | TCS, Dyson |
| 1.b | Create VPC, Create Subnets | TCS, using TF Script |
| 1.c | TGW attachment with the newly created VPC | Dyson Cloud Team |
| 1.d | Whitelist the CIDR range in the Firewall | Dyson Cloud Team |
| 1.e | Create Additional Services:   * Create IAM Roles, Policy for Workstations * Security Groups with Inbound/Outbound rule for Workstations * Security Groups with Inbound/Outbound rule for FSx NetApp ONTAP * Create Key-Pair * Create Route53 Resolver Outbound Endpoint * Create S3 bucket * Upload Custom-Action-On-Node-Configured.sh in the above bucket * Modify VPC default SG to allow TCP, UDP for VPC CIDR range | TCS, Using TF Script |
| 1.f | Create workstation (Windows Server 2022) images in RDD NPR account. The images should have installed all the required applications, NiceDCV, NVDIA, security agents (MS Defender, Qualys), CloudWatch agent | TCS, NPR Account, Using Console |
| 1.g | Share the AMI with AWS RDD Prod account | TCS, NPR Account, Using Console |
| 1.h | Create AD group for Fsx NETAPP ONTAP – AWS FSXUsers, AWS FSXAdmins(this is already available) | Dyson Cloud Team |
| 1.i | Create Secret and store the AD read-only user credential in plain text | Dyson Cloud Team |
| 1.j | Install DCV client/browser to the User's machine | Dyson IT |
| 2 | **FSx NetApp ONTAP** | |
| 2.a | Create File System in FSx NetApp ONTAP, use the above SG for FSx   * Create SVM in the File System * Add two volumes app and data in SVM | TCS, Using TF Script |
| 2.b | Domain Join the FSx NetApp ONTAP SVM, AD password can be retrieved from vault | TCS, Using TF Script |
| 2.c | Share the volumes from FSx CLI | TCS, Using CLI |
| 2.d | Add AD group in volumes using fsmgmt.msc from any Windows instance | TCS, Using Windows |
| 3 | **AWS Parallel Cluster** | |
| 3.a | Create the Parallel Cluster Config file   * Include Directory Service * FSx CIFS mount through custom shell script * Set umount in compute node through custom shell script * Install additional libraries in HeadNode through custom shell script | TCS, Cloud Engineer |
| 3.b | Create the Parallel Cluster CFN Template (in yaml format) from the config file | TCS, Cloud Engineer |
| 3.c | Get the CFN Template JSON from the yaml file above | TCS, Cloud Engineer |
| 3.d | Create Terraform script with the JSON in **template\_body,** install Parallel Cluster | TCS, TF Script |
| 3.e | Point to be considered: ParallelCluster will use the PlainText password that has been created in step 1.g and the cluster will keep the password in sssd.conf file in PlainText in the Headnode with 600 permission (e.g. only root user can read/write) | Information |
| 3.e | Post Installation:   * Application installation on Headnode * Powerflow related manual configuration in Headnode * Install MS Defender on Headnode | TCS, Using Console |
| 4 | **Windows Workstation** | |
| 4.a | Create Unique Workstations (Windows Server 2022) with for distinct set of application to be installed for specific group of users in RDD PROD account | TCS, TF Script |
| 4.b | Domain join the Windows Workstations created above | TCS, TF Script |
| 4.c | Install/Configure security agents - MS Defender (using the script), Qualys | TCS, Using RDP |
| 4.d | Install/Configure NiceDCV, NVDIA, CWAgent to stream logs from Workstation to CloudWatch | TCS, Using RDP |
| 4.e | Install Applications on the above Workstations | TCS, Using RDP |
| 4.f | Validate the connectivity with License server, PLM server, NFS | TCS, Using RDP |
| 4.g | Remove the domain join from Workstations | TCS, Using RDP |
| 4.h | Create AMI having - Apps, MS Defender, Qualys, NiceDCV, NVDIA | TCS, Using RDP |
| 4.i | Create the Windows workstations (Windows server 2022) for users from AMIs using Terraform Script | TCS, Using TF Script |
| 4.j | Domain join the Windows Workstations | TCS, Using TF Script |
| 4.k | Add RDP user in the Windows Workstation | TCS, Using TF Script |
| 4.l | Users should be part of AD group AWS FSXUsers, user should be able to map map the FSx shared storage | User, Using RDP |

## App Installation

* User’s workstations can be created from AMIs having installed all the required apps and s/w installed in it.
* Windows Defender, Qualys agent will be there in workstations for vulnerability check
* For app installation over the HPC – TCS App Support Team will be given the local credential of the Head Node to configure and install required applications.

## List Of Services

|  |  |  |  |
| --- | --- | --- | --- |
| **Resource List of RDD-NPR in** **EU-West-1** | | | |
| **Service Type** | **CIDR** | **Name Tag** | **Name** |
| VPC | <CIDR Range> | 2001493-HPC Upstream Compute | rdd-prd-hpc-euw1-vpc |
| Subnet-1 | <CIDR Range> | 2001493-HPC Upstream Compute | rdd-prd-hpc-euw1-1a-sn1 |
| Subnet-2 | <CIDR Range> | 2001493-HPC Upstream Compute | rdd-prd-hpc-euw1-1b-sn1 |
| Route Table |  | 2001493-HPC Upstream Compute | rdd-prd-hpc-euw1-rt |
| NACL |  | 2001493-HPC Upstream Compute | <TBD> |
| S3 bucket |  | 2001493-HPC Upstream Compute | rdd-prd-hpc-euw1-s3-bucket |
| Security Groups |  | 2001493-HPC Upstream Compute | Naming convention shall be followed |
| FSx For OnTAP |  | 2001493-HPC Upstream Compute | rdd-prd-hpc-euw1-fsx |
| Key-Pair |  | 2001493-HPC Upstream Compute | rdd-prd-hpc-euw1-key-pair |
| Secret Manager |  | 2001493-HPC Upstream Compute | rdd-prd-hpc-euw1-domain-credential |
| EC2 |  | 2001493-HPC Upstream Compute | Naming convention shall be followed |

## Subnet to Route Table Mapping

|  |  |
| --- | --- |
| **VPC: rdd-prd-hpc-euw1-vpc in RDD-PRD account in EU-West-1a** | |
| **Availability Zone – eu-west-1a** | |
| **Subnet Name** | **Route Table** |
| rdd-prd-hpc-euw1-1a-sn1 | rdd-prd-hpc-euw1-rt |
| rdd-prd-hpc-euw1-1a-sn2 | rdd-prd-hpc-euw1-rt |

|  |  |
| --- | --- |
| **VPC: rdd-prd-hpc-euw1-vpc in RDD-PRD account in EU-West-1b** | |
| **Availability Zone – eu-west-1b** | |
| **Subnet Name** | **Route Table** |
| rdd-prd-hpc-euw1-1b-sn1 | rdd-prd-hpc-euw1-rt |
| rdd-prd-hpc-euw1-1b-sn2 | rdd-prd-hpc-euw1-rt |

## 

## Route Table Details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Subnet Type** | **Subnet Name** | **Route Table** | **Destination** | **Target** |
| Private Subnet | rdd-prd-hpc-euw1-1a-sn1 | rdd-prd-hpc-euw1-rt | 0.0.0.0/0 | <TBD>  local |
| rdd-prd-hpc-euw1-1a-sn2 |
| rdd-prd-hpc-euw1-1b-sn1 | <VPC CIDR Range> | local  local |
| rdd-prd-hpc-euw1-1b-sn2 |

## Subnet to NACL Mapping

|  |  |
| --- | --- |
| **Subnet Name** | **NACL** |
| rdd-prd-hpc-euw1-1a-sn1 | <TBD> |
| rdd-prd-hpc-euw1-1b-sn1 | <TBD> |

## NACL Detail

|  |  |  |  |
| --- | --- | --- | --- |
| **NACL** | **Allowed Inbound CIDR** | **Allowed Outbound CIDR** | **Description** |
| <TBD> | All traffic 0.0.0.0/0 | All traffic 0.0.0.0/0 |  |

## Instance Details

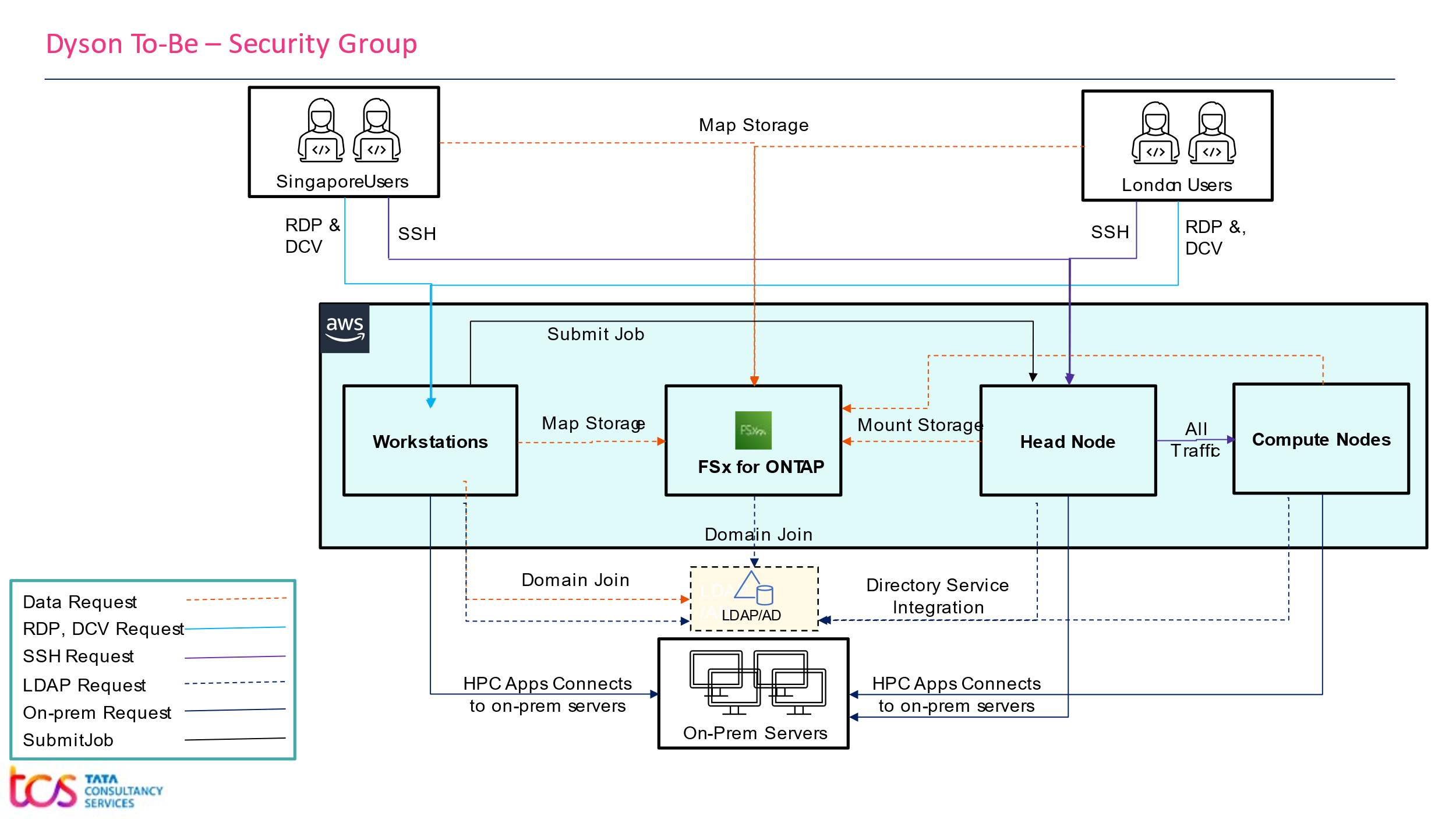
|  |  |  |  |
| --- | --- | --- | --- |
| **VPC: rdd-npr-hpc-vpc-euw1 in PRD-RDD account in EU-West-1a** | | | |
| **Subnet** | **EC2 Instance** | **Node Name** | **Operating System** |
| rdd-prd-hpc-euw1-1a-sn1 | Workstation-1 | As per naming convention | Windows Server 2022 |
| Workstation-2 | As per naming convention | Windows Server 2022 |
| Workstation-3 | As per naming convention | Windows Server 2022 |
| Workstation-4 | As per naming convention | Windows Server 2022 |
| Workstation-5 | As per naming convention | Windows Server 2022 |
| Could be many more WS |  | Windows Server 2022 |
| Head Node | As per naming convention | RHEL 8.n |
| Dynamic Compute Nodes |  | RHEL 8.n |

|  |  |  |  |
| --- | --- | --- | --- |
| **VPC: rdd-npr-hpc-vpc-euw1 in PRD-RDD account in EU-West-1b** | | | |
| **Subnet** | **EC2 Instance** | **Node Name** | **Operating System** |
| rdd-prd-hpc-euw1-1b-sn1 | Head Node | As per naming convention | RHEL 8.n |
| Dynamic Compute Node |  | RHEL 8.n |

## Instance/Storage to Security Group Mapping

|  |  |  |
| --- | --- | --- |
| **Instance to Security Group Mapping** | | |
| **Instance Type** | **Security Group Name** | **Description** |
| FSx NetApp ONTAP | sg-rdd-prd-hpc-euw1-fsx |  |
| Workstation | sg-rdd-prd-hpc-euw1-workstation |  |
| Cluster Head Node | Shall be created by Parallel Cluster |  |
| Cluster Compute Node | shall be created by Parallel Cluster |  |

## Security Group Detail



|  |  |  |
| --- | --- | --- |
| **Security Group for on-prem server connectivity: sg-rdd-prd-hpc-euw1-on-prem-servers** | | |
| **Type** | **Allowed** | **Description** |
| Outbound | Specific port to on-prem license server |  |
| Outbound | Specific port to on-prem PLM server |  |
| Outbound | Specific port to on-prem database server |  |
| Outbound | Other on-prem servers |  |

|  |  |  |
| --- | --- | --- |
| **Security Group for FSx NetApp ONTAP Consumers: sg-rdd-prd-hpc-euw1-fsx-consumer** | | |
| **Type** | **Allowed** | **Description** |
| Outbound | TCP (139, 445), UDP (137, 138) to FSx NetApp OnTap <IP> | SMB/CIFS, Get IP Address of FSx |
| Outbound | TCP (111, 2049, 635, 4046), UDP (111, 2049, 635, 4046) to FSx NetApp OnTap <IP> | NFS, Get IP Address of FSx |

|  |  |  |  |
| --- | --- | --- | --- |
| **Security Group for FSx NetApp ONTAP: sg-rdd-prd-hpc-euw1-fsx** | | | |
| **Type** | **Allowed** | | **Description** |
| Inbound | All Traffic, All port from sg-rdd-prd-hpc-euw1-fsx-consumer | |  |
| Inbound | NFS, SMB/CIFS, ICMP, HTTPS, SSH from London users <IP Range> | | Get IP Range from Dyson |
| Inbound | NFS, SMB/CIFS, ICMP, HTTPS, SSH from Singapore users <IP Range> | | Get IP Range from Dyson |
| Outbound | Dyson Active Directory traffic | | Get IP Range from Dyson |
| Outbound | Dyson DNS traffic | | Get IP Range from Dyson |
| ~~Outbound~~ | ~~All Traffic, All port from sg-rdd-prd-hpc-euw1-fsx-consumer~~ | | ~~Get IP Range from Dyson~~ |
| ~~Outbound~~ | ~~DHCP, DHCPS server (if required) traffic~~ | | ~~Get IP Range from Dyson~~ |
| **Security Group for Workstation: sg-rdd-prd-hpc-euw1-workstation** | | | |
| **Type** | **Allowed** | **Description** | |
| Inbound | RDP traffic, TCP Protocol, 3389 from London users <IP Range> | Get IP range from Dyson | |
| ~~Inbound~~ | ~~DCV traffic, port 8443 from London users <IP Range>~~ | ~~Get IP range from Dyson~~ | |
| Inbound | RDP traffic, TCP Protocol, 3389 from Singapore users <IP Range> | Get IP range from Dyson | |
| ~~Inbound~~ | ~~DCV traffic, port 8443 from Singapore users <IP Range>~~ | ~~Get IP range from Dyson~~ | |
| Inbound | DCV Proxy, Port should be allowed | IP TBD | |
| Outbound | All Traffic, All port to sg-rdd-prd-hpc-euw1-on-prem-servers |  | |
| Outbound | All Traffic, All port to sg-rdd-prd-hpc-euw1-headnode |  | |
| Outbound | All Traffic, All port from sg-rdd-prd-hpc-euw1-fsx-consumer |  | |
| Outbound | Dyson Active Directory traffic | Get IP Range from Dyson | |
| Outbound | Dyson DNS traffic | Get IP Range from Dyson | |
| Outbound | TCP Port 80 and 443 to 0.0.0.0/0 |  | |

|  |  |  |
| --- | --- | --- |
| **Security Group for Head Node: Created by Parallel Cluster itself** | | |
| **Type** | **Allowed** | **Description** |
| ~~Inbound~~ | ~~SSH Traffic, TCP Protocol, Port 22 from 0.0.0.0/0~~ | ~~Comes by default~~ |
| Inbound | SSH Traffic, TCP Protocol, Port 22 from London users <IP Range> | Get IP range from Dyson |
| Inbound | SSH Traffic, TCP Protocol, Port 22 from Singapore users <IP Range> | Get IP range from Dyson |
| Inbound | SSH Traffic, Port 22 from Workstation subnet <IP Range> | Get IP range from Dyson |
| Inbound | Application data, jobs from Workstation subnet <IP Range> | Get IP range from Dyson |
| Inbound | All Traffic, All Protocol, All Port from Compute node security group | Comes by default |
| ~~Outbound~~ | ~~All Traffic, All Protocol, All Port from 0.0.0.0/0~~ | ~~Comes by default~~ |
| Outbound | All Traffic, All Protocol, All Port to Compute node security group |  |
| Outbound | All Traffic, All port to sg-rdd-prd-hpc-euw1-on-prem-servers |  |
| Outbound | All Traffic, All port from sg-rdd-prd-hpc-euw1-fsx-consumer |  |
| Outbound | Dyson Active Directory traffic | Get IP Range from Dyson |
| Outbound | Dyson DNS traffic | Get IP Range from Dyson |
| Outbound | TCP Port 80 and 443 to 0.0.0.0/0 |  |

|  |  |  |
| --- | --- | --- |
| **Security Group for Compute Node: Created by Parallel Cluster itself and not recommended to change** | | |
| **Type** | **Allowed** | **Description** |
| Inbound | All Traffic, All Protocol, All Port from Compute node security group | Comes by default |
| Inbound | All Traffic, All Protocol, All Port from Head node security group | Comes by default |
| Outbound | All Traffic, All Protocol, All Port from 0.0.0.0/0 | Comes by default |
| Outbound | All Traffic, All Protocol, All Port from Compute node security group | Comes by default |

# Platform Management

## Prerequisite

What are the thing we need here? All the services we need to define here

# Assumptions

* Dyson should have connectivity set-up from AWS to on-premise from Prod VPC
* Dyson should have proper n/w bandwidth available for data transfer from on-prem to cloud
* Dyson should have patching process implemented for RHEL 8, Windows Server 2022
* Dyson should create the required AD group within SLA period
* Dyson should whitelist the VPC CIDR to their firewall
* Dyson should whitelist the breakout IPs from London and Singapore users in their firewall to connect to AWS resources

# Appendix

**Appendix 1:** System requirements for Prod

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sl. No** | **Description** | **Instance Type** | **vCPU** | **RAM (GB)** | **Storage** |
| 1 | Head Node | C6i.2xlarge | 8 | 16 | 1000 GiB GP3, 3000 IOPS, 250 GiBs, No backup |
| 2 | Compute Node | C6i.32xlarge | 128 | 256 | 35 GiB GP3, 3000 IOPS, 250 GiBs, No backup |
| 2 | Workstation-1 | G4dn.2xlarge | 8 | 32 | 600 GiB GP3, 3000 IOPS, 250 GiBs, No backup |
| 3 | Workstation-2 | TBC |  |  | 600 GiB GP3, 3000 IOPS, 250 GiBs, No backup |
| 4 | Workstation-3 | TBC |  |  | 600 GiB GP3, 3000 IOPS, 250 GiBs, No backup |
| 5 | Workstation-4 | TBC |  |  | 600 GiB GP3, 3000 IOPS, 250 GiBs, No backup |
| 6 | Workstation-4 | TBC |  |  | 600 GiB GP3, 3000 IOPS, 250 GiBs, No backup |
| 7 | FSx for NetApp ONTAP | Shared Storage | | | 50 TB, 60000 IOPS, 512 MBps, Daily backup-7days retention |

**Appendix 2:** Functionalities during PoC and Post-PoC

|  |  |  |  |
| --- | --- | --- | --- |
| **Sl. No** | **Functionalities** | **PoC** | **Post PoC** |
| 1 | Deployment | Using Console, Cloud9, AWS-CLI | Fully automated IaC script |
| 2 | Workstation Creation | Manually created instances | Workstations may be created using Terraform script |
| 3 | Patching/AV | In-Scope for Windows, evaluate the feasibility for CentOS | In-Scope |
| 4 | Domain Join | In-Scope | In-Scope |
| 5 | Multi-region, Data Replication | Not In-Scope | Not In-Scope |
| 6 | Backup | Not In-Scope | FSx shared storage daily backup with 7 days retention  <Abdul to provide EBS volume default backup> |
| 7 | High Availability | Single AZ, single subnet in Ireland region | The Parallel Cluster can be deployed in 2 AZ, 2 subnets in Ireland region |
| 8 | Disaster Recovery | Not In-Scope | Dyson is internally working on to provision a new region in Frankfurt. |
| 9 | Managed Support | Not In-Scope | In-Scope |
| 10 | Log monitoring | Not In-Scope | CloudWatch log messages and metric can be monitored |
| 11 | Custom GUI for create and manage workstation | In-Scope with limited functionalities and security | Not yet finalized for Prod. In case the users need it – the custom GUI may be given with full functionalities and security at every layer |

**Appendix 3:** Data Transfer from on premise to AWS Cloud (FSx NetApp ONTAP). This will be validated by Dyson security.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Use Case** | **Tyoe of data** | **Extension** | **Size/ Volume** | **Purpose** |
| 1 | Various file types of ANSYS Workbench Project | .cas, .dat, .msh, .wbpj, .jpg, and other | 2-4GB | To test ANSYS WB automated design of experiment. Fluent, Meshing, CFD-Post, Workbench. |
| 2 | Binary file format input to ANSYS FLUENT | \*.cas  \*.dat | 4.5 GB  5.4 GB | To run the ANSYS FLUENT simulation |
| 3 | Binary file format input to ANSYS FLUENT like 2. | \*.cas  \*.dat | 4.5 GB  5.4 GB | To run the ANSYS FLUENT simulation |
| 4 | Binary file format input to PowerFLOW sim | \*.case  \*.cdi | 1 GB  0.5 GB | To run PowerFLOW CFD simulation |