Linux Server Access Via CyberArk – UCP User Guide

Document control

Prepared By

Version	Author	Date
V 1.0	Sai Krishna	29-04-2022
V 1.1	Sai Krishna / Keerthana	25-05-2022

Reviewed By

Version	Reviewer	Date
V 1.0	Priyadarshi Mishra	30-04-2022
V 1.1	Priyadarshi Mishra	27-05-2022

Approved By

Version	Approver	Date
V 1.0	Harmandeep Singh	30-04-2022
V 1.1	Harmandeep Singh	30-05-2022

Change Control

Version	Change Reason	Effective Date
V 1.0	Initial Release	30-04-2022
V 1.1	Introduction, Formatting, Corrections	30-05-2022

STATEMENT OF CONFIDENTIALITY

Contents

1. Introduction to UCP

Welcome to Universal Cloud Platform user guide. UCP is a multi-cloud Self-Service platform that allows users to provision Virtual Machines into Azure Environment. Along with provisioning Linux, SAP & Windows Virtual Machines, you will be able to manage them, perform 2nd Day operations, decommission, obtain or provide access to the virtual machine.

UCP not only does allow to provision the virtual machine but also configures monitoring via Splunk Monitoring, configures backup via Netbackup software, on-board Linux VMs to Cyberark Platform to obtain secure access, on-board Windows VMs to Active Directory.

You will be able to create Virtual machines for both Test & Production purposes.

UCP creates a CMDB CI entry in Global Service Now (GSN) for every virtual machine that get provisioned.

UCP also creates a Change Management ticket (RFC) for every VM that has been deployed for Production purposes only. Based on this RFC ticket, every virtual machine undergoes thorough automated and manual checks for its readiness on the day of the delivery.

This document emphasizes on accessing a server via Cyberark

1. Ordering for server access via UCP
2. Steps in Cyberark to access VM

2. How to get access to UCP?

In order to be able to get access to UCP, the user should be part of the "UDLDHL-UCP" Active Directory Group.

If you're a Team Manager for a Project, then you should request for a new project to be created in Azure via the GSD form https://gsd.dhl.com/forms/4887

General Information

This form will create a SPCS Managed IaaS Resource Group for you.

Prerequisite:

1. You would need a valid Service Contract

Tags: EMEA, GBS

Contact owner

Form Details

|	
Requestor Name	ITS Account Manager s.kammane_nadiminti@dhl.com
Resource Group Owner	Requestor will automatically be added to Owner Role in Resource Group
Resource Group Name	Resource Group Name
Please select your BU	○ Express ○ GBS&CC ○ DGFF ○ P&P ○ ITS ○ DSC ○ eCS
New Service Contract	Please provide Service Contract for charging purposes. Please contact account services for assistance
Who should have access to Power BI report?	[ ] Select

Clear

The form involves 4 steps where the SPCS Cloud Ops IaaS team will grant you the following

    a. The desired Project Name / Resource Group Name
    b. Assign you to the UDLDHL-UCP Active Directory Group
    c. Assign both Production & Test Subscriptions for the Project Name and
    d. Assign you the Team Manager role where you will be able to onboard and add other team members within your project.

Note: Only "@dhl.com" email ids can only be onboarded onto UCP.

Once you receive a confirmation email notification that your request has been fulfilled, you will be able to login to the platform with your Active Directory credentials i.e. email-id & password provided to you at the time of creating your DHL account. You will be able to use the same credentials for accessing other platforms too.

Step 1 – Navigate to https://ucp.dhl.com
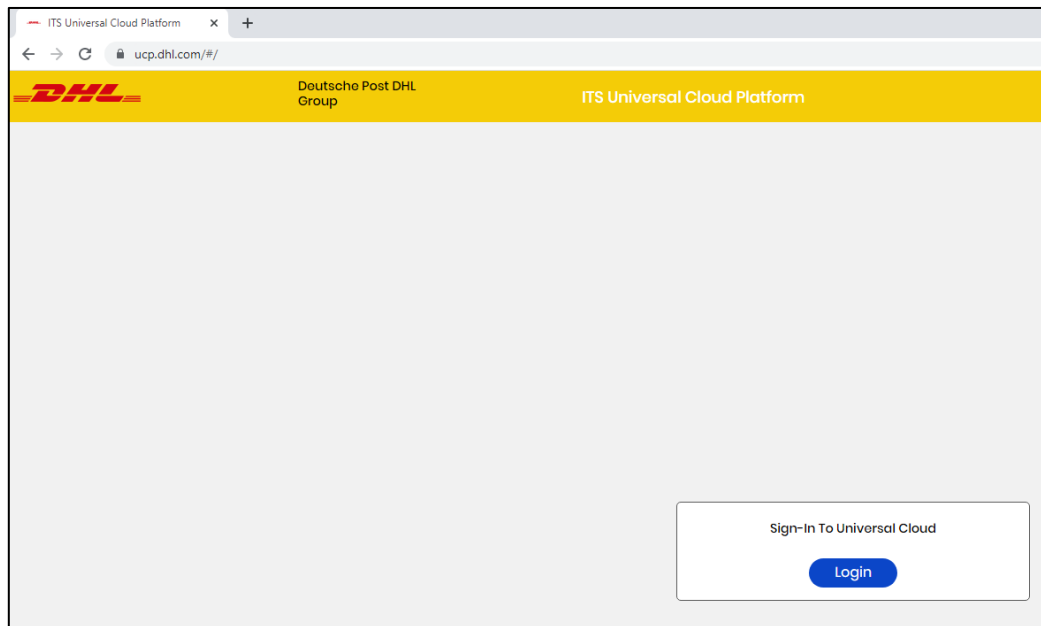
Step 1.a – Enter your DHL email id AD Credentials
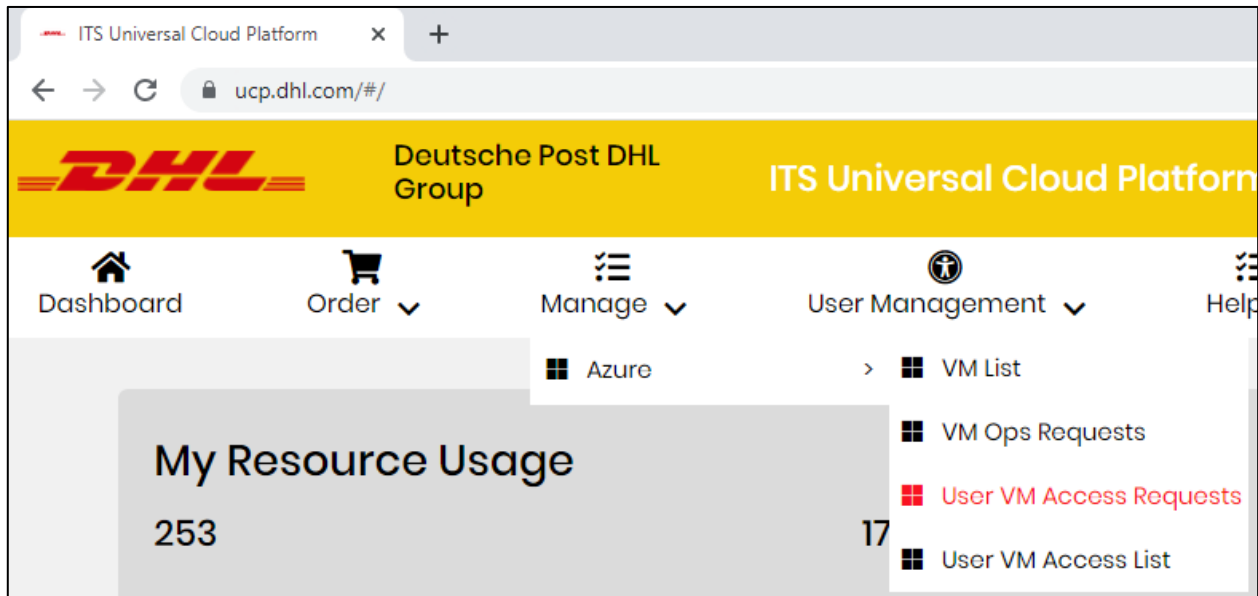

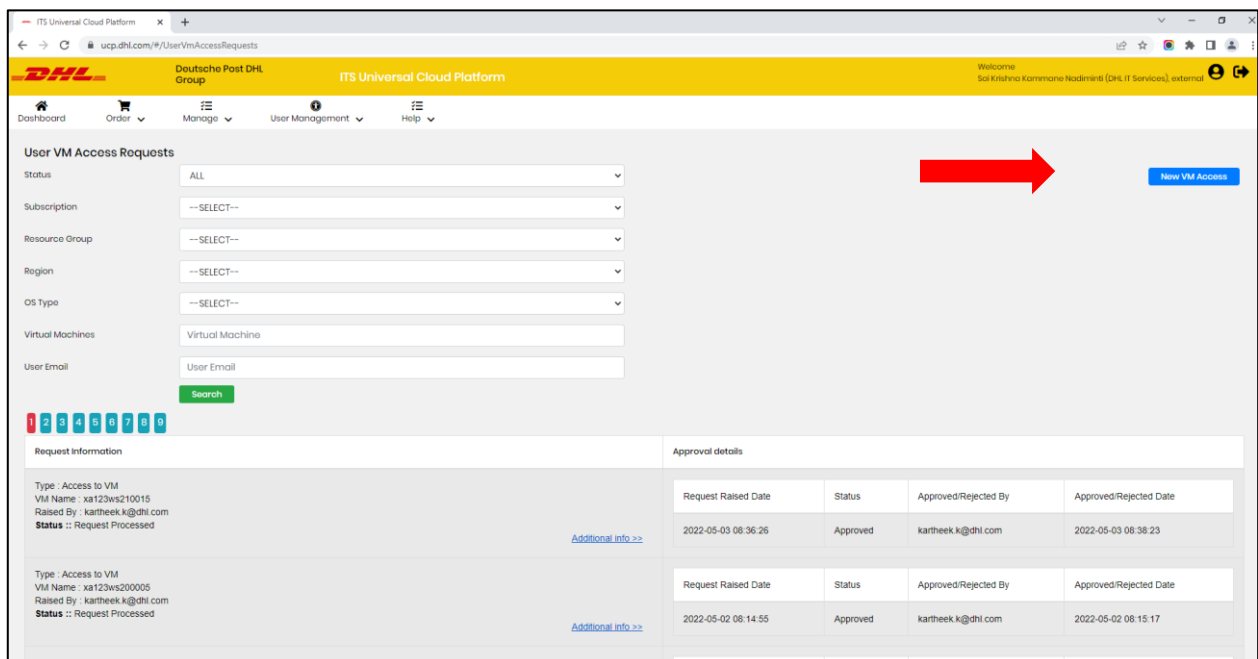The user will be landing on the dashboard as shown hereunder
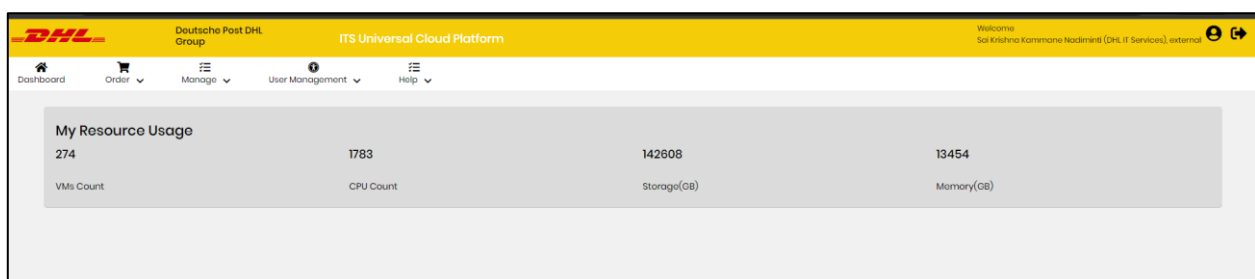
3. How to Access my Server ?

In order to access the server that you desire, you will have to raise a request via UCP or request the Resource group manager to grant you the access. Follow the steps shown below.

1. Navigate to Manage Menu -> Azure -> User VM Access Requests.

2. Click on New VM Access request

A Pop-up screen will appear.

3. Select the Subscription, Resource Group, OS Type: Linux, Account Type

BU Sysadmin – A Business user Admin who needs temporary access to all the virtual machines in the resource Group

BU Application Admin – A Business user Admin who needs temporary access to all the virtual machines of different application types such as Apache, Tomcat, JBOSS, Weblogic and Oracle Database, within the resource Group.

CLOUD4C

Select the email in the "Provide Access to" Dropdown list.

Note: If an email id is not visible in the dropdown list, then please refer to "AAD User Onboarding - UCP User guide v 1.0" to on-board the email id to UDLDHL-PVWA Group first. After 45-60 minutes the email id will appear in the dropdown list below.

4. Select the desired duration and click on "Submit"

User VM Access   ✕

Subscription *

7e8e1e96-c128-42b8-a445-d18281754604 / ITS-SPCS-Azure-Managed-VM-PROD-122 ⌄

Resource Group *

rg-dhl-testing ⌄

OS Type *

Linux ⌄

Account Types *

BU sysadmin ⌄

Provide Access To *

angelo.jumarang@dhl.com ⌄

Duration *

2   Days 10 ⌄ Hours

Submit   Reset

5. The request then goes for an approval to the Resource Group Owner / Team Manager

Request Information		Approval details			
Type : Access to VM Safe Name : SADMIN_EU_-dhl-testing, SADMIN_AP_-dhl-testing, SADMIN_US_-dhl-testing Raised By : s.kammane_nadiminti@dhl.com **Status ::** Pending		Request Raised Date	Status	Approved/Rejected By	Approved/Rejected Date
	Additional info >>	2022-05-03 05:22:20	Pending Approve Reject		

6. Click on Approve -> Proceed
7. The requestor will receive an acknowledgement

Request Information		Approval details			
Type : Access to VM Safe Name : SADMIN_EU_-dhl-testing, SADMIN_AP_-dhl-testing, SADMIN_US_-dhl-testing Raised By : s.kammane_nadiminti@dhl.com **Status ::** Request Processed		Request Raised Date	Status	Approved/Rejected By	Approved/Rejected Date
	Additional info >>	2022-05-03 05:28:15	Approved	s.kammane_nadiminti@dhl.com	2022-05-03 05:28:35

The user who needs the access to the Virtual Machine will receive an acknowledgement email with the steps to login to the requested machine.

4. Cyberark Login Procedure

All the servers that are provisioned via UCP will have to be accessed only via Cyberark PAM Console Procedure. Cyberark platform allows you to login to the server in a safe & secure fashion. Follow the below mentioned steps in order to access the desired server.

4.1 Cyberark Login Procedure

1. Login into DHL network (VDI/VPN) and access the below PAM URL based on Region.

Region	Server	URL
South East Asia	If the server is provisioned in South East Asia Region	https://pvwa-sea.dhl.com
West Europe	If the server is provisioned in South East Asia Region	https://pvwa-weu.dhl.com
East United States	If the server is provisioned in South East Asia Region	https://pvwa-eus.dhl.com
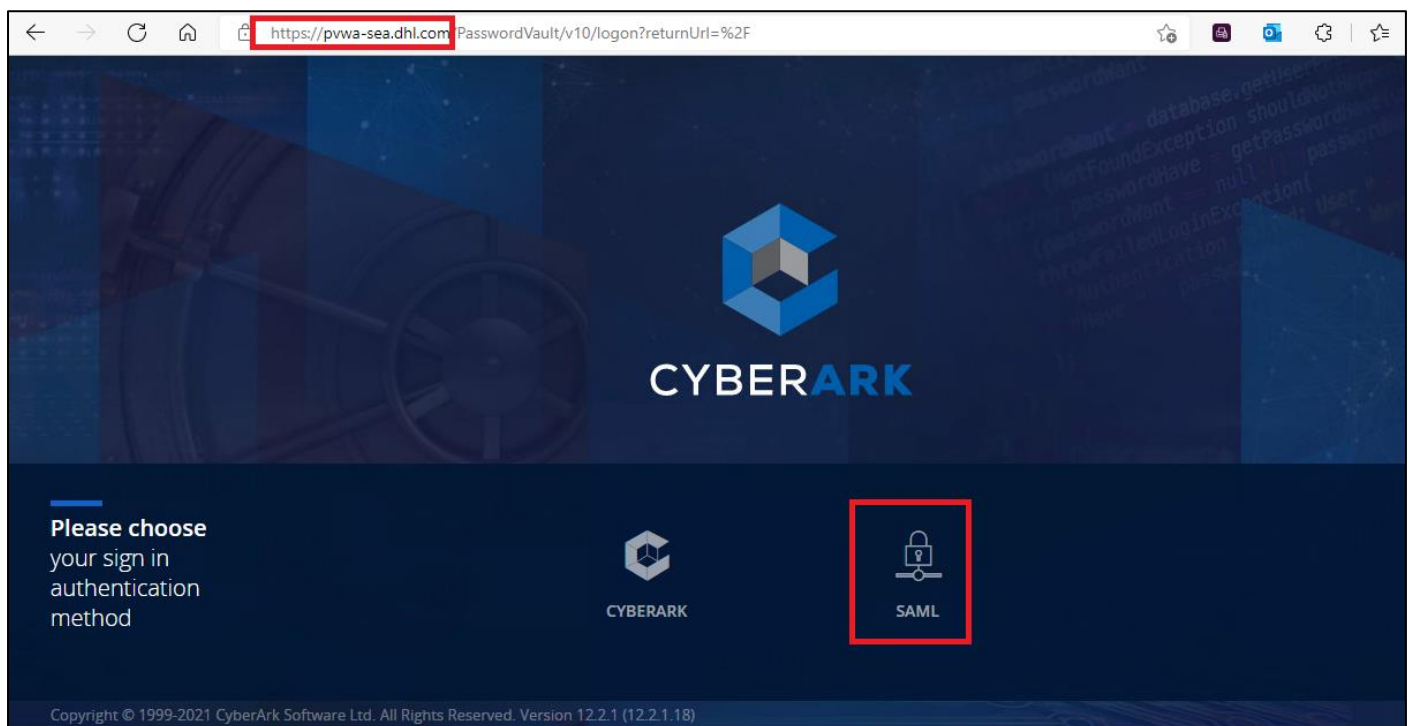
Figure-1: SEA PAM URL
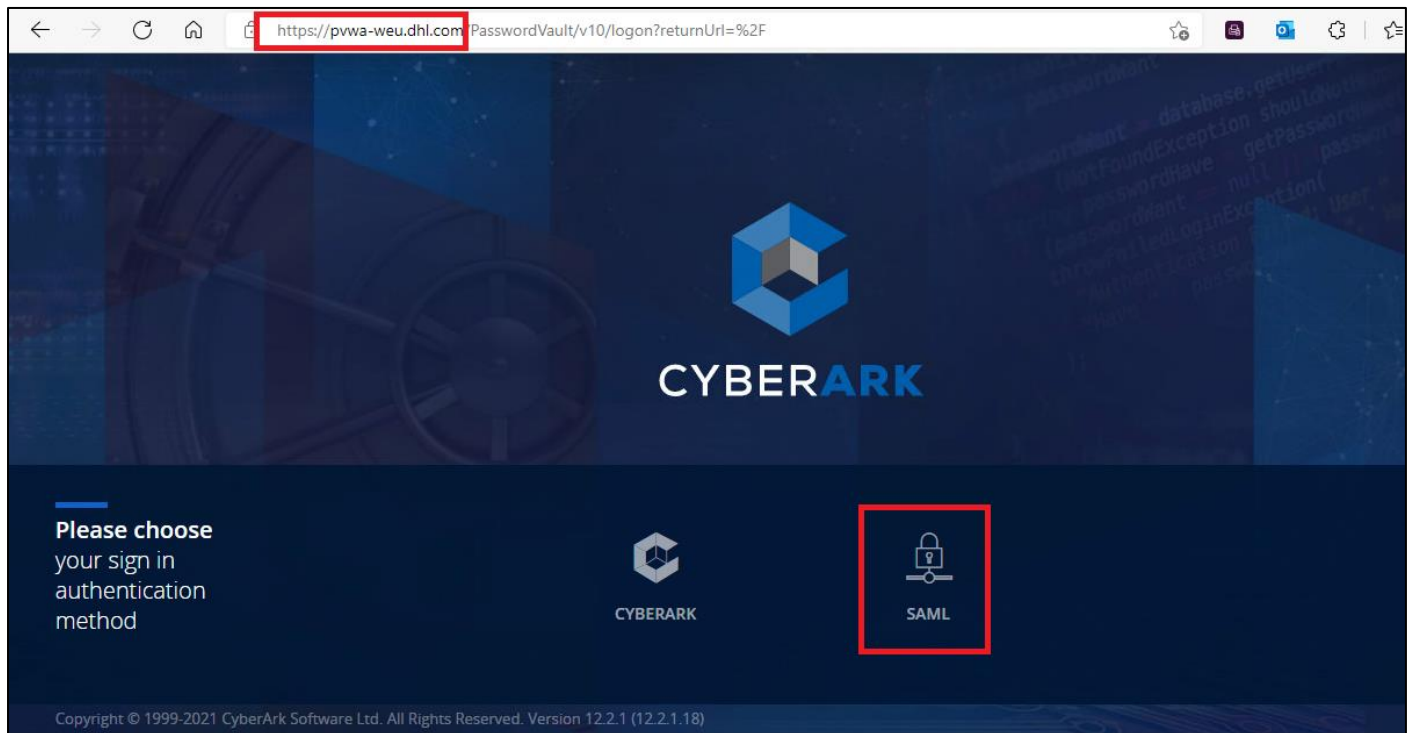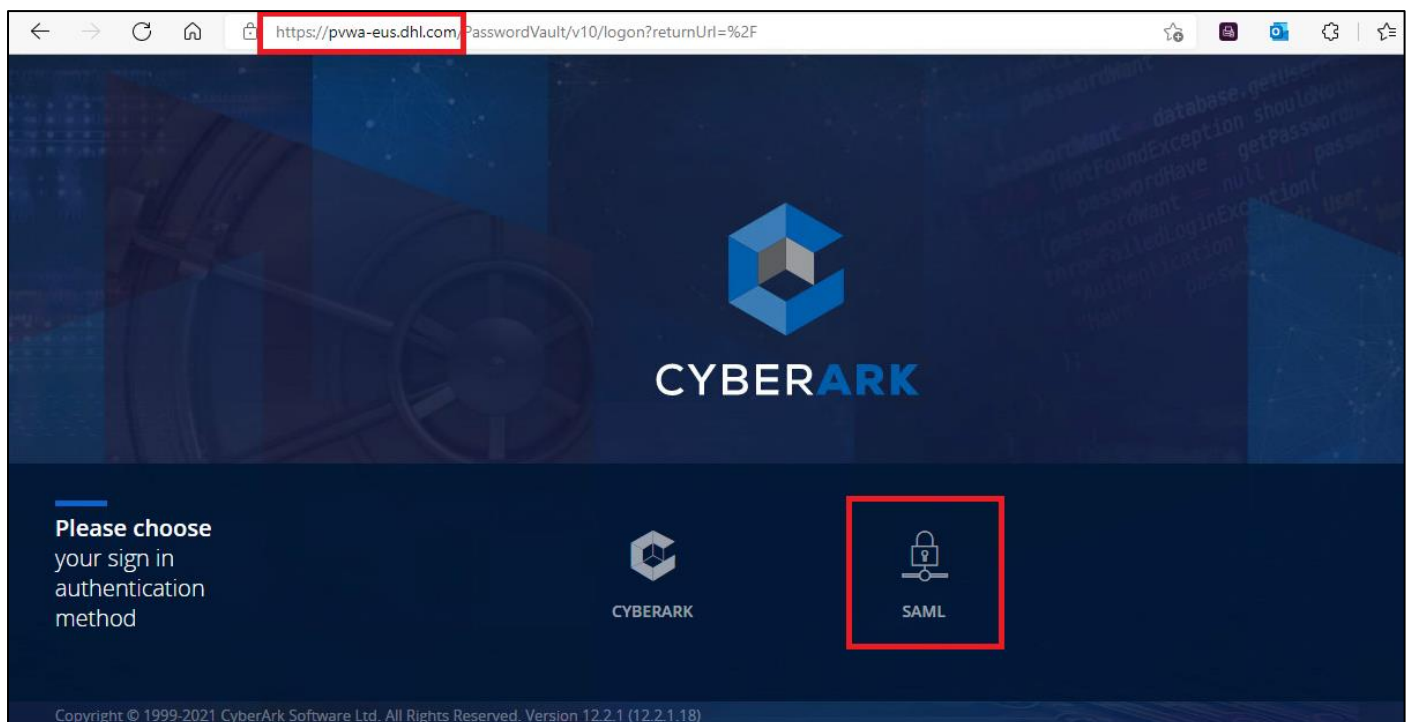
Figure-2: WEU PAM URL

Figure-3: EU.S PAM URL

2. Click on SAML authentication for login and you will be able to login directly to CyberArk Console using your Azure AD credentials.
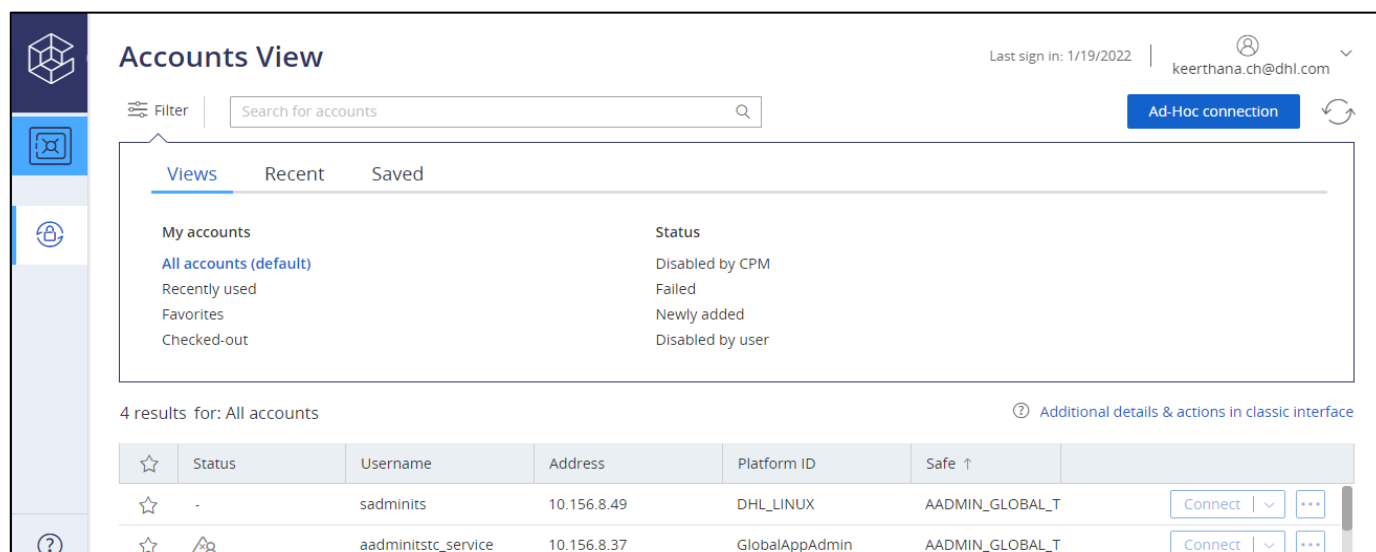

Figure-4: On Login End User Dashboard.

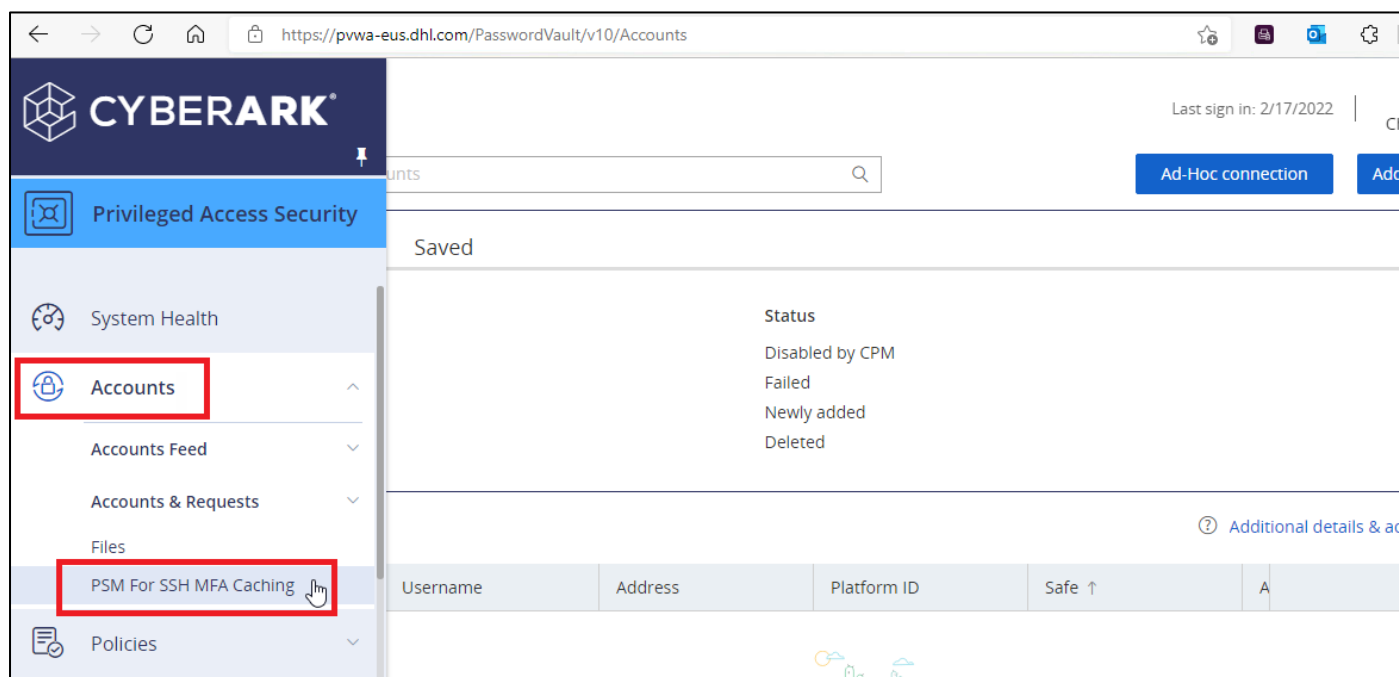3. Navigate (On Left Pane) to Accounts → PSM for SSH MFA Caching.

Figure-5: Navigating to PSM for SSH MFA Caching Tab.

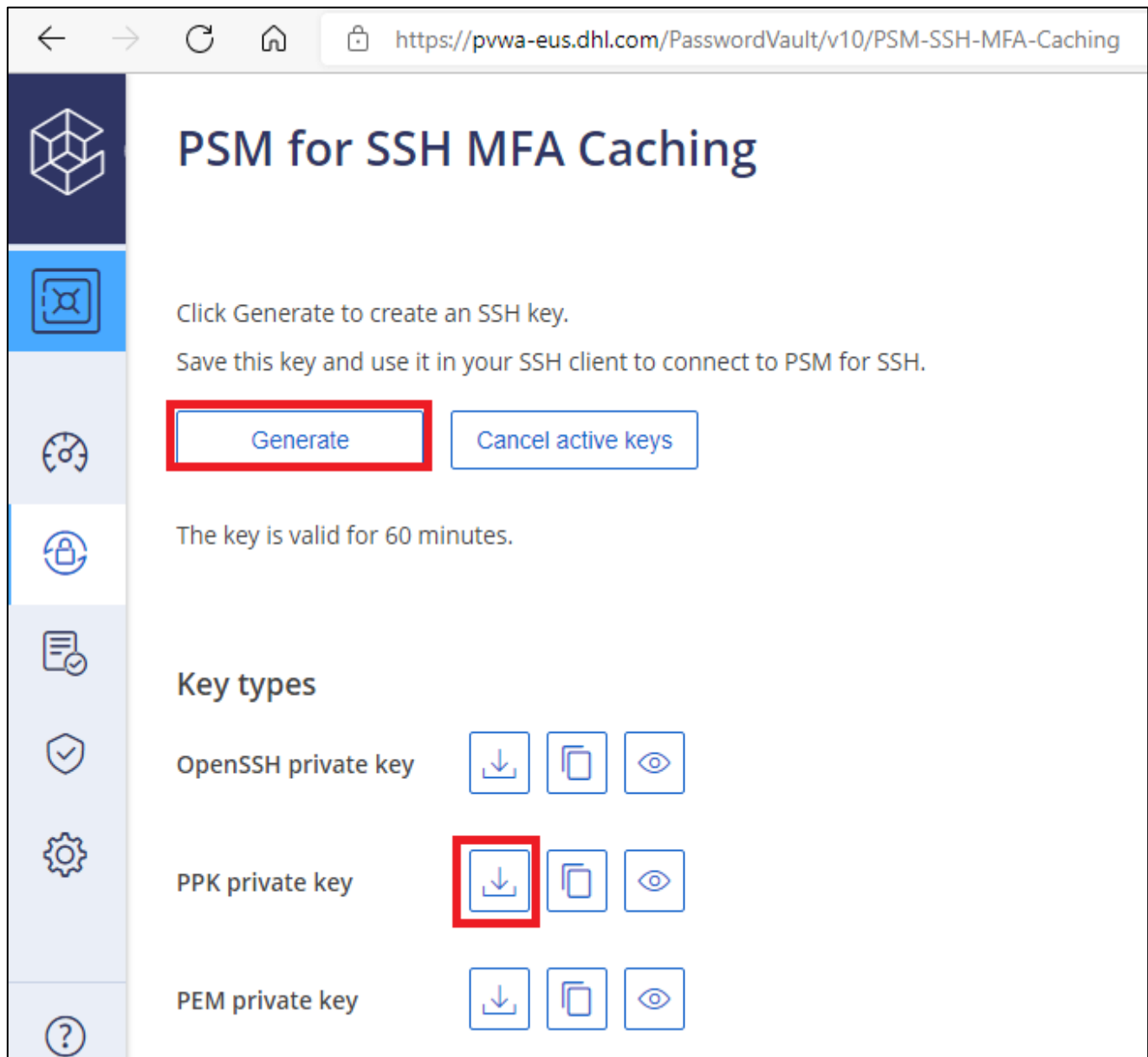4. Click on **Generate** and **Download PPK private key** from CyberArk portal (Which is valid for 60 minutes) from PSM for SSH MFA Caching window.

Figure-6: Generating Private Keys

5. Import the private key into putty (On Putty Application left pane select Connection → SSH → Auth → Private key file for authentication)
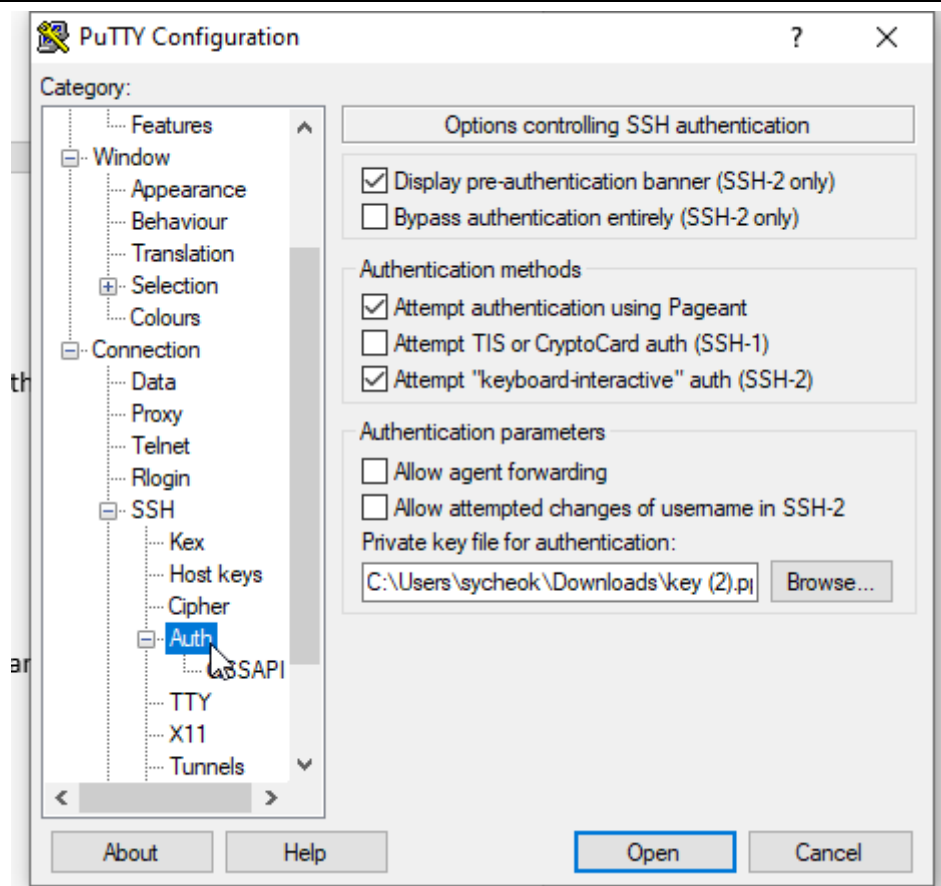
Figure-7: Connection through Putty Private Key

6. Prepare the connection string and put it into the hostname. (Session → Hostname)

Connection String: <**CyberArkUserID**>%<**TargetAccountName**>%<**TargetServerIP**>@<**RegionSpecificPSM-SSHServerLoadBalancerIP**>

Example: keerthana.ch@dhl.com%sadminits%10.224.174.4@10.224.18.42

CyberarkUserID : keerthana.ch@dhl.com

TargetAccountName: sadminits

TargetSeverIP: 10.224.174.4

East US PSM-SSH Load Balancer IP: 10.224.18.42 (As the above server is provisioned in East US region)

4.2   Cyberark Load Balancer IPs and Next Steps

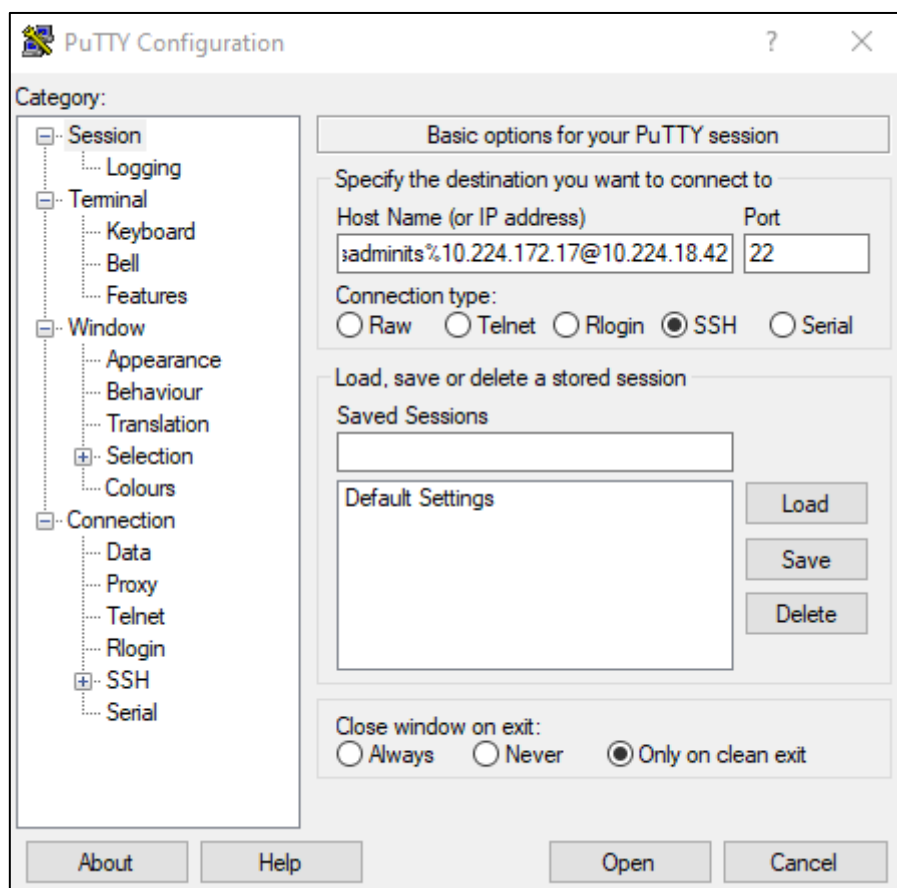| Load Balancer in Each Region	IP Address
East US PSM-SSH Load Balancer IP	10.224.18.42
West Europe PSM-SSH Load Balancer IP	10.156.9.145
SEA PSM-SSH Load Balancer IP	10.234.1.72

Figure-7: Connection to Target server using MFA Cache

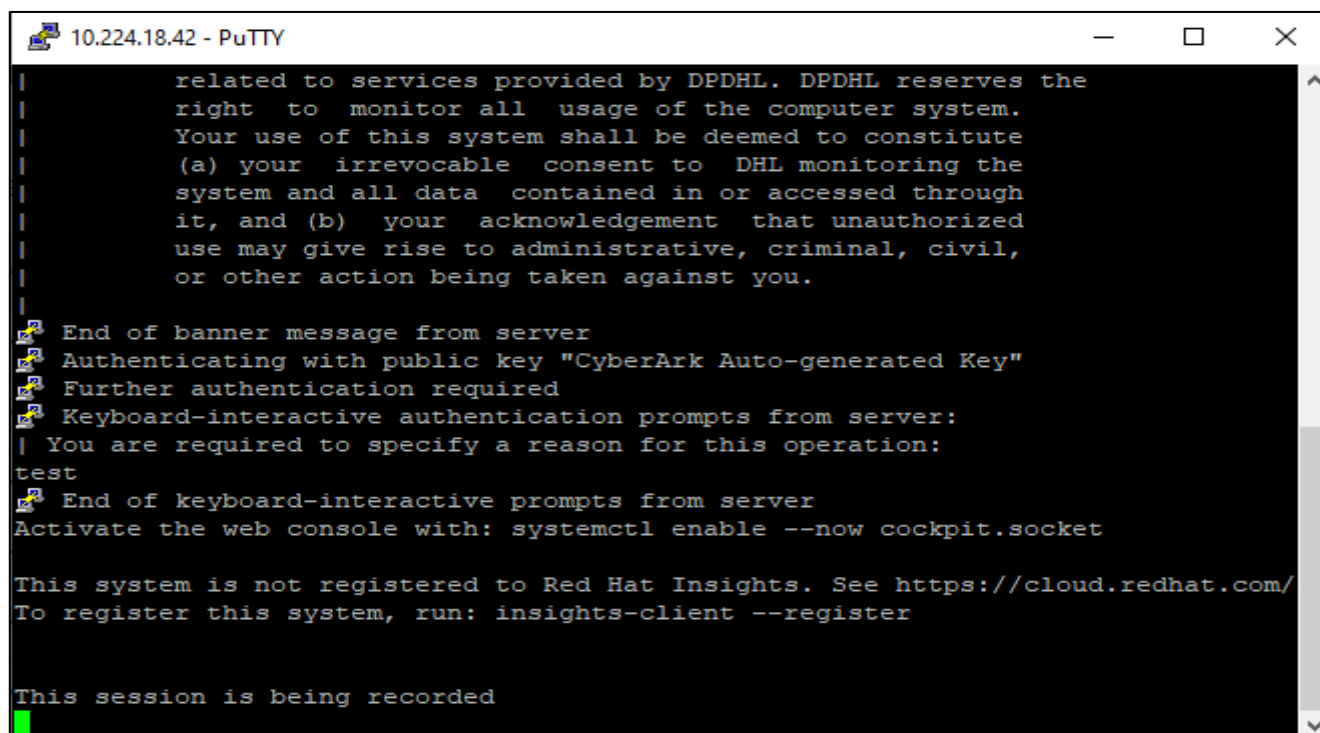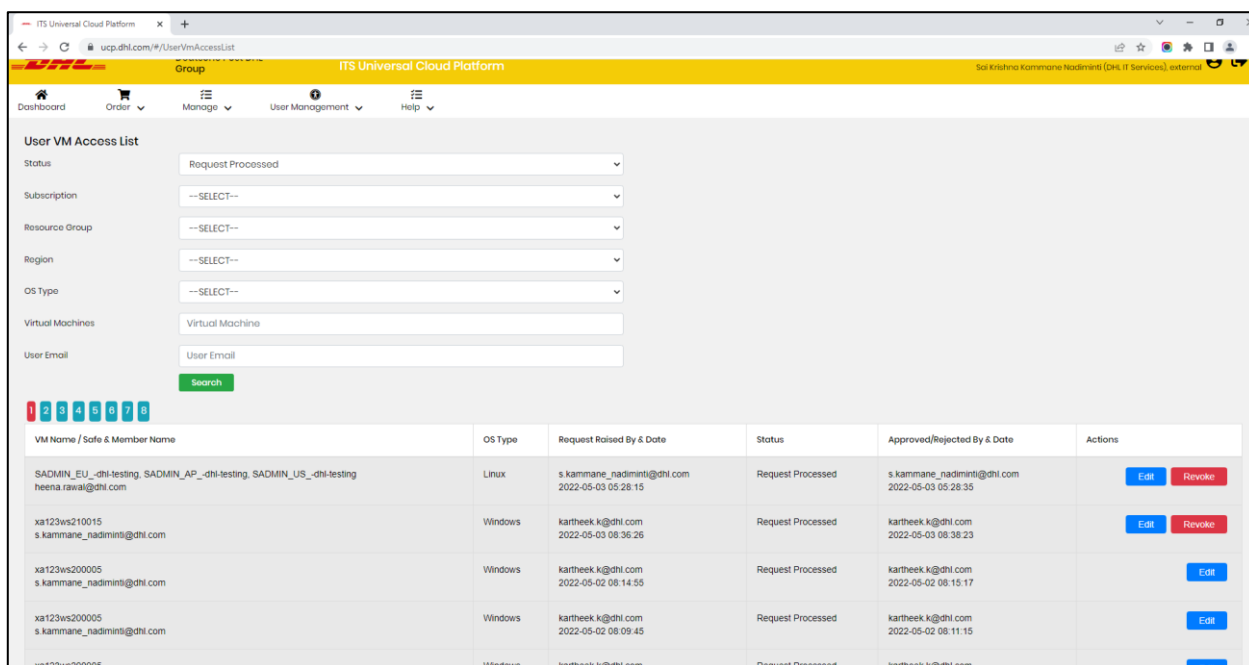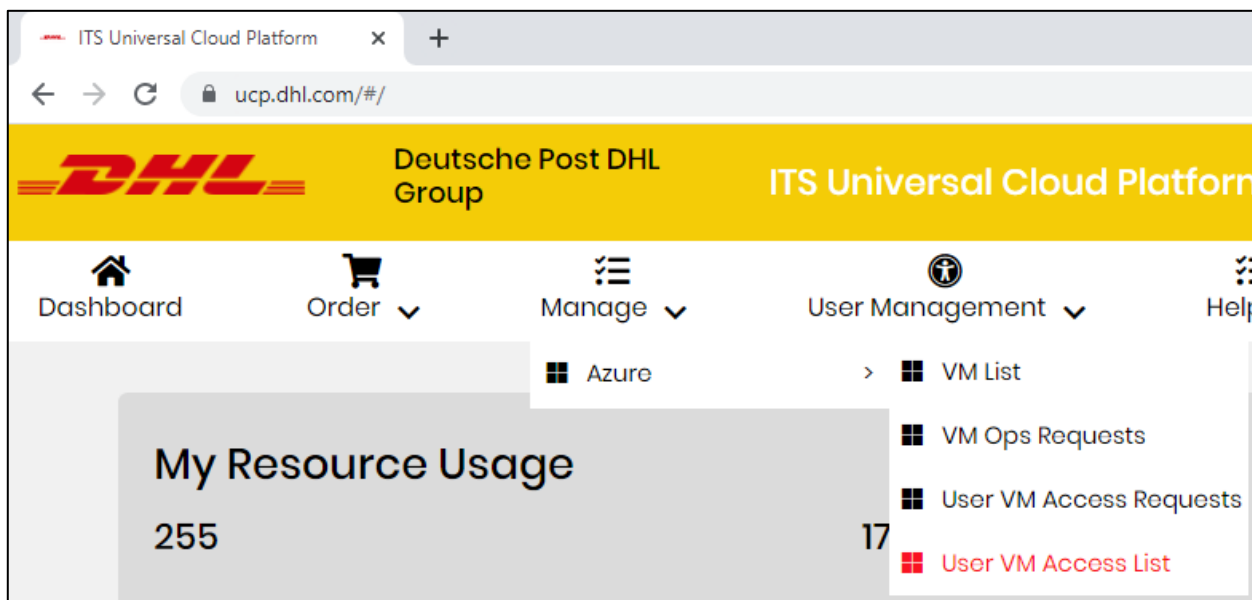Specify the reason for accessing the target server and continue accessing the server.

Figure-8: Access to target server

4.3   Modification of duration of access

If the duration of accessing the server needs to be increased or decreased beyond the approved duration, then you may request the Team Manager to extend or reduce the time limit for the server access. The following are the steps in extending the duration of the access.

1. Navigate to Manage -> Azure -> User VM Access List

2. The user can modify the duration of the by clicking on the edit button as shown below.

Click on "Update" for the duration to be updated.

The requestor will receive an acknowledgement email with the information about extended duration.

4.4   Revoke Access

The Resource group Owner can request to revoke the access of the virtual machines in the resource group at any time, so the business user is not allowed to access them at anytime.

Clicking on OK, will revoke the access of the servers to the business user.

5. Glossary

5.1 Definition

Terms	Abbreviation
VM	Virtual Machine
UCP	Universal Cloud Platform