GOVERNMENT OF INDIA
INDIRA GANDHI CENTRE FOR ATOMIC RESEARCH
COMPUTER DIVISION
KALPAKKAM – 603102

THIS DOCUMENT IS THE PROPERTY OF INDIRA GANDHI CENTRE FOR ATOMIC RESEARCH. THIS SHALL NOT BE REPRODUCED OR COMMUNICATED WITHOUT OWNER'S PERMISSION.

SYSTEM	**VIRTUAL DESKTOP INFRASTRUCTURE**
TITLE	**Virtual Desktop Infrastructure setup: Overall configuration and procedure for deploying Virtual Machines**

A	Original Issue	03/07/2019	R. Jehadeesan
No	Revisions	Date	Approved

IGCAR	**EIG**	**RCCG**	**CD**	**CSS**	**VDI**	**4**	**REV**	**A**			

Electronics Instrumentation Group

Virtual Desktop Infrastructure

	NAME	SIGN	DATE
PREPARED	**Thirupurasundari D**		28/6/2019
	Deepika Vinod		28/6/19
	Molly Mehra		28-6-2019
	Subrahmanyam D N V R	D.N.V.R. Subrahmanyam	28/06/2019
REVIEWED	**M L Jayalal**		01/07/2019
APPROVED	**R Jehadeesan**	R. Jehadeesan	03/07/2019

Distribution:
Head, CSS;
Head, CD;
AD, RCCG;
Director, EIG;

SUMMARY

This document describes the overall configuration of the VDI setup and the procedure followed for creating the Virtual Machine (VM) in HyWorks controller, adding the users in the active directory domain controller and Thin client configuration.

Virtual Desktop Infrastructure setup: Overall configuration and procedure for deploying Virtual Machines

1. Introduction

VDI (Virtual Desktop Infrastructure) is a term used to describe a specific field of virtualization in computing, which deals with creating and maintaining virtual desktops within an organization's IT environment. The VDI allows the migration of desktop operating systems from physical computing resources to Virtual Machines, or VMs, hosted on centralized servers. VDI setup at IGCAR consists of twenty VDI servers, two management servers, and Unified storage with usable space of 185TB. All the servers are configured in high availability and the setup is designed for connecting 1000 thin clients with user VMs. The setup is configured with 700 VMs of windows 10 and 200 VMs of Linux. VDI is implemented across IGCAR and the centralized datacenter where the virtual desktops are created, managed and delivered is housed in Computer Centre. This internal report covers about the overall configuration of the VDI infrastructure implemented at IGCAR and steps involved in the deployment of Virtual Machine (VM).

2. Architecture of VDI

2.1 Hardware Configuration of VDI setup

VDI setup consists of twenty numbers of Boston x86 virtualization (VDI1 to VDI20) servers (VDI servers) and two numbers of management (MGMT1 & MGMT2) servers. Each VDI server and management server are equipped with 44 CPU cores, 192 GB RAM and four 10g Ethernet ports. The VDI and MGMT servers are connected to a 185 TB usable unified storage through redundant 10-Gigabit fiber optic connections. The storage is configured with dual storage controller (active-active) for fault tolerance which contains user desktop images as well as user data files. User VMs are hosted in the twenty numbers of VDI servers and infrastructure VMs are hosted in two numbers of management servers at computer centre. Figure 1 depicts the details about the overall setup of VDI at IGCAR. The configurations of each category of the server are given below:

Hardware configuration of a VDI server / Management server

Make & Model	: Boston
Processor	: E5-Intel Xeon 2699A v4 (VT-x enabled)
Clock Speed	: 2.4 GHz
No. of CPUs	: 2
No. of Cores per CPU	: 22
RAM	: 192 GB 1600MHZ DDR4 with ECC
HDD	: 2x 300GB SAS
Network	: 4x10Gbps, 4x1Gbps
Power Supply	: Redundant with efficiency

Hardware configuration of storage server

Make and model	: HP 3PAR
SAS drives	: 146 SAS drives of 1.8TB each
SSD drives	: 14 SSD drives of 1.92TB each
Capacity	: 185 TB unified storage
RAID	: RAID 6
Power Supply	: Redundant with efficiency

Hardware configuration of network switches

Model	: 2 X Brocade – ICX7750 10g Switches
Port	: 48 ports 10g ports
Power Supply	: Redundant

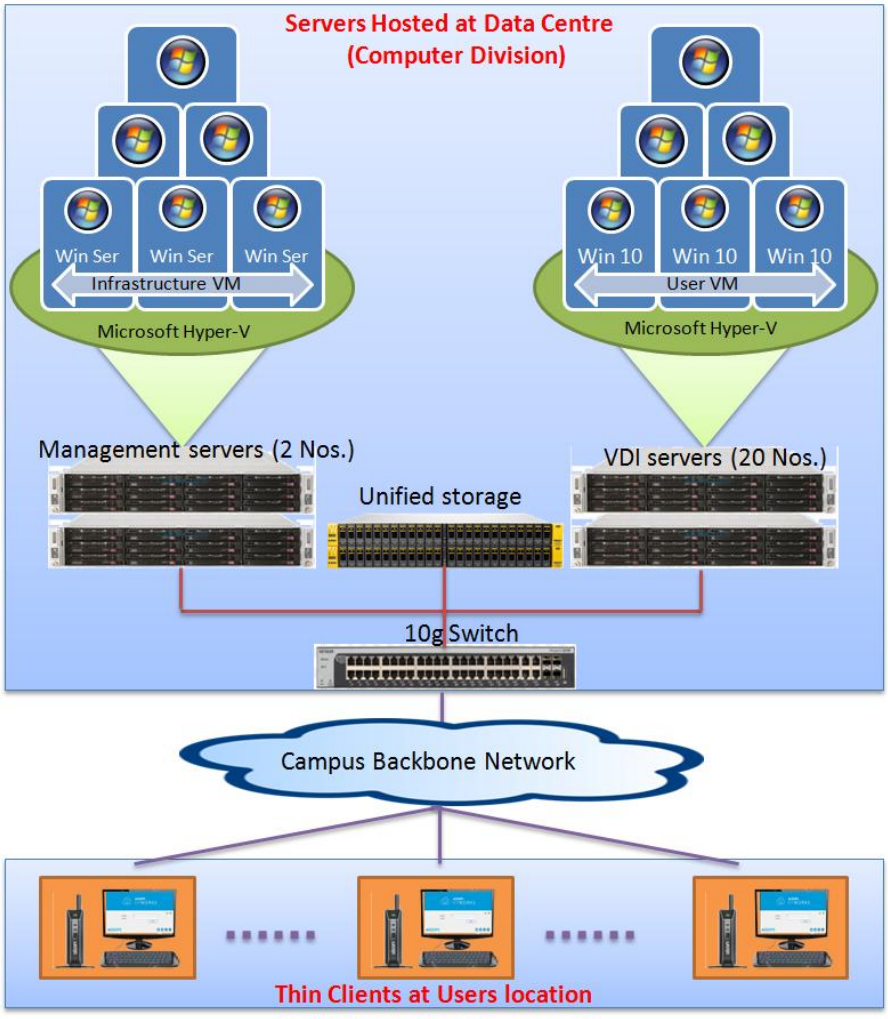

Figure 1: Components of VDI setup at IGCAR

All the twenty VDI servers together have the capability of hosting 1000 desktop VMs. Each desktop VM is provisioned with two numbers of virtual CPU cores, 4 GB RAM, C drive of 50 GB and H drive of 200 GB. The desktop VMs are loaded with Windows-10 or Ubuntu OS based on the user choice. The management servers host the virtual machines required for authentication, management and connection brokering (infrastructure VMs).

VDI Network Setup

The VDI setup comprises of four different networks for administration, management, storage access and external connectivity. The administration and management networks use 1GE. The storage and external networks use 10GE. The network connections are shown in Figure 2.

The purpose and connectivity of each of the four different networks is described below:

1. External network (10G SFP+): This network connects the individual thin-client systems located across the campus to the VDI Setup through the campus backbone network. It is used for accessing the user VMs running on VDI servers through the thin-clients systems. For this purpose the VDI servers and management servers are connected via 10G SFP+ fiber links to the core switch (that provides connectivity to the campus backbone network).From the core switch 10G connections are made to the workgroup switches at various locations. The core switch and workgroup switch connections form the campus backbone network.

2. VDI Storage network (10G SFP+): It connects the VDI & management servers with the storage using two numbers of 48 port 10G switches. The block I/O operations are done over this network. Each of the VDI & management servers are connected with both the switches for achieving the redundancy.

3. VDI Administration Network for Clustering (1G teamed): This network connects the 2 Management servers and 20 VDI servers through two numbers of 24 port 1G switches and 1x 48 port 1G switch. On each server two 1G interfaces are teamed together to form a virtual 2G interface. IP address is assigned to this virtual interface. In case of one link failure the connectivity is still maintained but with reduced throughput. This network is used for all communication between the Management Servers and VDI servers, necessary for clustering, authentication etc.

4. VDI Management Network (1G): This network connects the VDI & management servers to the management PC through one 24 port 1G switch. It is used for management of the servers using IPMI.

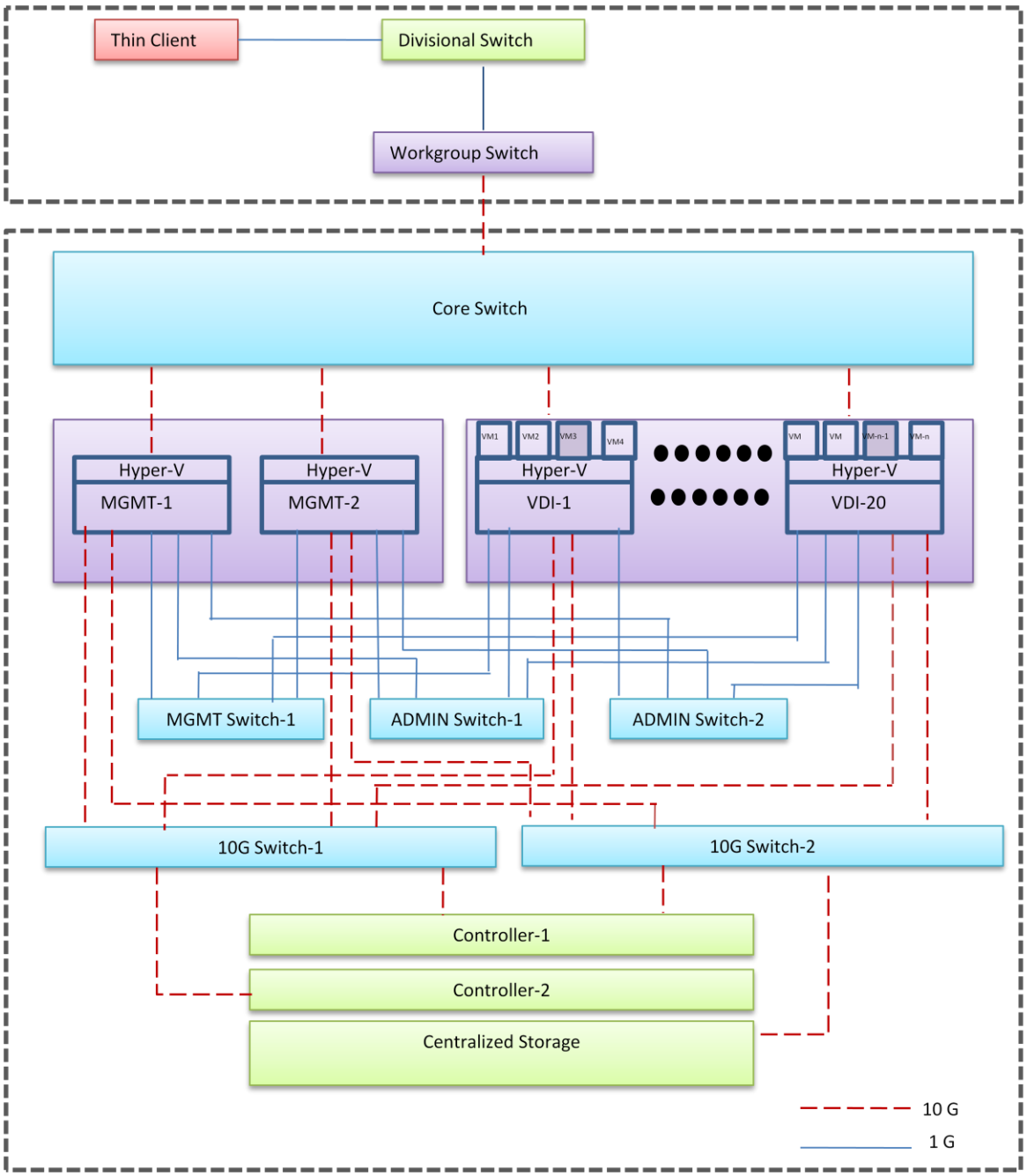

Figure 2: Network Connectivity diagram of VDI servers with user's thin clients

VDI servers and management servers are assigned with the IP address as shown in the Table 1.

Sl. No	Server Name	Storage Network1 IP	Storage Network2 IP	Cluster(teamed) Network IP	Campus Network IP
1.	vdi1.VDIDOM.GOV.IN	192.168.105.23	192.168.104.23	192.108.101.23	10.29.1.23
2.	vdi2.VDIDOM.GOV.IN	192.168.105.24	192.168.104.24	192.108.101.24	10.29.1.24
3.	vdi3.VDIDOM.GOV.IN	192.168.105.25	192.168.104.25	192.108.101.25	10.29.1.25
4.	vdi4.VDIDOM.GOV.IN	192.168.105.26	192.168.104.26	192.108.101.26	10.29.1.26
5.	vdi5.VDIDOM.GOV.IN	192.168.105.27	192.168.104.27	192.108.101.27	10.29.1.27
6.	vdi6.VDIDOM.GOV.IN	192.168.105.28	192.168.104.28	192.108.101.28	10.29.1.28
7.	vdi7.VDIDOM.GOV.IN	192.168.105.29	192.168.104.29	192.108.101.29	10.29.1.29
8.	vdi8.VDIDOM.GOV.IN	192.168.105.30	192.168.104.30	192.108.101.30	10.29.1.30
9.	vdi9.VDIDOM.GOV.IN	192.168.105.31	192.168.104.31	192.108.101.31	10.29.1.31
10.	vdi10.VDIDOM.GOV.IN	192.168.105.32	192.168.104.32	192.108.101.32	10.29.1.32
11.	vdi11.VDIDOM.GOV.IN	192.168.105.33	192.168.104.33	192.108.101.33	10.29.1.33
12.	vdi12.VDIDOM.GOV.IN	192.168.105.34	192.168.104.34	192.108.101.34	10.29.1.34
13.	vdi13.VDIDOM.GOV.IN	192.168.105.35	192.168.104.35	192.108.101.35	10.29.1.35
14.	vdi14.VDIDOM.GOV.IN	192.168.105.36	192.168.104.36	192.108.101.36	10.29.1.36
15.	vdi15.VDIDOM.GOV.IN	192.168.105.37	192.168.104.37	192.108.101.37	10.29.1.37
16.	vdi16.VDIDOM.GOV.IN	192.168.105.38	192.168.104.38	192.108.101.38	10.29.1.38
17.	vdi17.VDIDOM.GOV.IN	192.168.105.39	192.168.104.39	192.108.101.39	10.29.1.39
18.	vdi18.VDIDOM.GOV.IN	192.168.105.40	192.168.104.40	192.108.101.40	10.29.1.40
19.	vdi19.VDIDOM.GOV.IN	192.168.105.41	192.168.104.41	192.108.101.41	10.29.1.41
20.	vdi20.VDIDOM.GOV.IN	192.168.105.42	192.168.104.42	192.108.101.42	10.29.1.42
21.	MGMT1.VDIDOM.GOV.IN	192.168.102.21	192.168.103.21	192.108.101.21	10.29.1.21
22.	MGMT2.VDIDOM.GOV.IN	192.168.102.22	192.168.103.22	192.108.101.22	10.29.1.22

Table 1: VDI and MGMT server names with IP address details

2.2 Software Configuration

For installing all VDI related software and services, multiple infrastructure servers are hosted in the Management Cluster as VMs. Management server1 hosts the following infrastructure services in the form of VMs and are listed in Table 2. Infrastructure VMs which are running in the management server 2 are listed in Table 3.

S.No	Server Type	Host Name	Management Switch IP	Core Switch IP
1	Active Directory server (redundant server)	ADC.VDIDOM.GOV.IN	192.168.101.11	10.29.1.11
2	File server (This is a role not a VM)	FILESERVER	192.168.101.253 192.168.102.253 192.168.103.253	10.29.1.253
3	Hyworks Controller 1	HYWORKS1.VDIDOM.GOV.IN	192.168.101.19	10.29.1.19
4	SCVMMHA1	SCVMMHA1.VDIDOM.GOV.IN	192.168.101.51 192.168.104.54	-
5	SQLHA1	SQLHA1.VDIDOM.GOV.IN	192.168.101.56	-

Table 2: Infrastructure VMs at management server 1 (MGMT1)

S.No	Server Type	Host Name	Management Switch IP	Core Switch IP
1	Active Directory server	AD.VDIDOM.GOV.IN	192.168.101.10	10.29.1.10
2	Hyworks Controller 2	HYWORKS2.VDIDOM.GOV.IN	192.168.101.20	10.29.1.20
3	Key Management Server (KMS)	KMS.VDIDOM.GOV.IN	192.168.101.17	10.29.1.17
4	SCVMMHA2	SCVMMHA2.VDIDOM.GOV.IN	192.168.101.50 192.168.101.52 192.168.101.54	-
5	Windows Server Update service (WSUS)	WSUS.VDIDOM.GOV.IN	192.168.101.18	10.19.3.189

Table 3: Infrastructure VMs at management server 2 (MGMT2)

The main software component used for virtualization is the hypervisor. Hypervisor is the software that is used to virtualize hardware resources and manages the resources for every virtual machine. Microsoft Hyper-V virtualization software stack and Accops Hyworks controller are used for provisioning and managing the desktop VMs.

Microsoft Hyper-V: It is a hypervisor which requires hardware resources like processor, memory and storage devices to virtualize and creates virtual machines. Hyper-V manages the interactions between the hardware and the virtual machine and it runs each virtual machine in its own isolated space, which enables to create more than one virtual machine on the same hardware at the same time.

System Center Virtual Machine Manager (SCVMM): Hyper-V Manager provides management capabilities only to the Hyper-V hosts and respective VMs. If hundreds of VMs spread across multiple Hyper-V hosts, it is difficult and time-consuming to locate one specific VM using Hyper-V Manager. To overcome these difficulties, System Center Virtual Machine Manager (SCVMM)is used on top of Hyper-V. SCVMM provides a consolidated view of Hyper-V resources, for easily locating a particular VM without having to search each individual host. SCVMM also enables increased physical server utilization by making possible simple and fast consolidation on virtual infrastructure. This is configured in SCVMMHA1 and SCVMMHA2 which runs in high availability mode.

Accops HyWorks Controller (hyworks1 and hyworks2): It is the core of the VDI setup offering centralized management of the virtual desktop infrastructure. HyWorks Controller also provides device management, connection broker features like fetching, provisioning and maintaining desktops from dedicated session providers (Microsoft Hyper-V or SCVMM). Apart from this, authentication services from Microsoft Active Directory, assignment of desktops to users, connection management and performance management are also provided. Once HyWorks Controller is configured, devices and users will connect with HyWorks Controller, login and get access to their virtual desktops through thin clients.

HyWorks Controller Service runs as a windows service on supported windows platforms and is the primary controller layer for HyWorks environment. The core operations of HyWorks Controller Service are:

- Managing End-Point HyDesk devices i.e. thin-clients
- In built connection broker for managing and assigning desktops to clients
- Enabling authentication of users with Authentication Servers
- Managing sessions
- Managing DVMs (Desktop Virtual Machines)
- Provisioning of new DVMs using gold images
- Detailed device and controller logging for troubleshooting and reporting

The web interface used for facilitating all the above tasks is HyWorks Controller Management Console. HyWorks Controller Management Console is a web interface accessible on browsers and provides the interface for administrators to manage the devices, sessions, creation and management of desktop providers, connection profiles and other settings.

The VDI setup at Computer Division is configured with two virtual machines (VMs) namely, hyworks1 and hyworks2 for running HyWorks Controller Service and web server for the above interface. The VMs are loaded with Windows Server 2016 and run in high availability mode. Apart from these services, Accops Hyworks license service, Hyworks monitoring service and Hyworks upgrade service are also being run in the VMs. All the services are configured with the SQL server as supporting database.

Active Directory (AD & ADC): Hyworks controller uses active directory for domain user authentication and further joining the users to domain 'vdidom.gov.in'. Group policies like profile redirection, windows update policies etc. are configured through active directory. AD and ADC acts in high availability mode and are configured as DNS servers too.

Fileserver: Fileserver is configured as a role in management servers which runs in a cluster named 'MGMT.VDIDOM.GOV.in'. Fileserver

WSUS: Windows Server Update Services (WSUS) periodically contacts Microsoft's update server, downloads the updates and applies the updates periodically to the user VM's.

KMS: Key management server manages the keys for Windows activation of user VM's.

3. Procedure for deploying Virtual Machines

3.1 Creation of virtual Machines

Creation of virtual Machines carried out through HyWorks Controller Management Console. This management console is a web interface accessible on browsers and provides the interface for administrators to manage the devices, sessions, creation and management of Session Providers, connection profiles and other settings.

Hyworks controller URL for login: ***https://hyworks1/Admin/en-US/Account/SignIn.*** Once the link is invoked user name (hyworks.admin) and password has to be entered which is shown in figure 3. After successful login, the page will be redirected to the dashboard which is shown in figure 4.

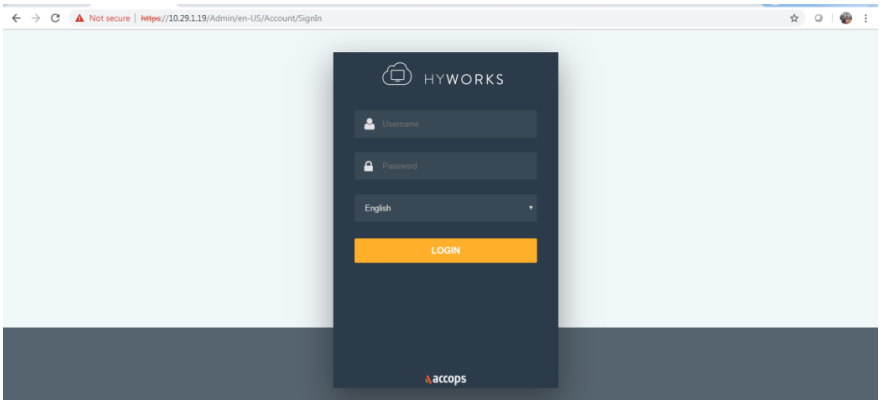

Figure 3: Login screen

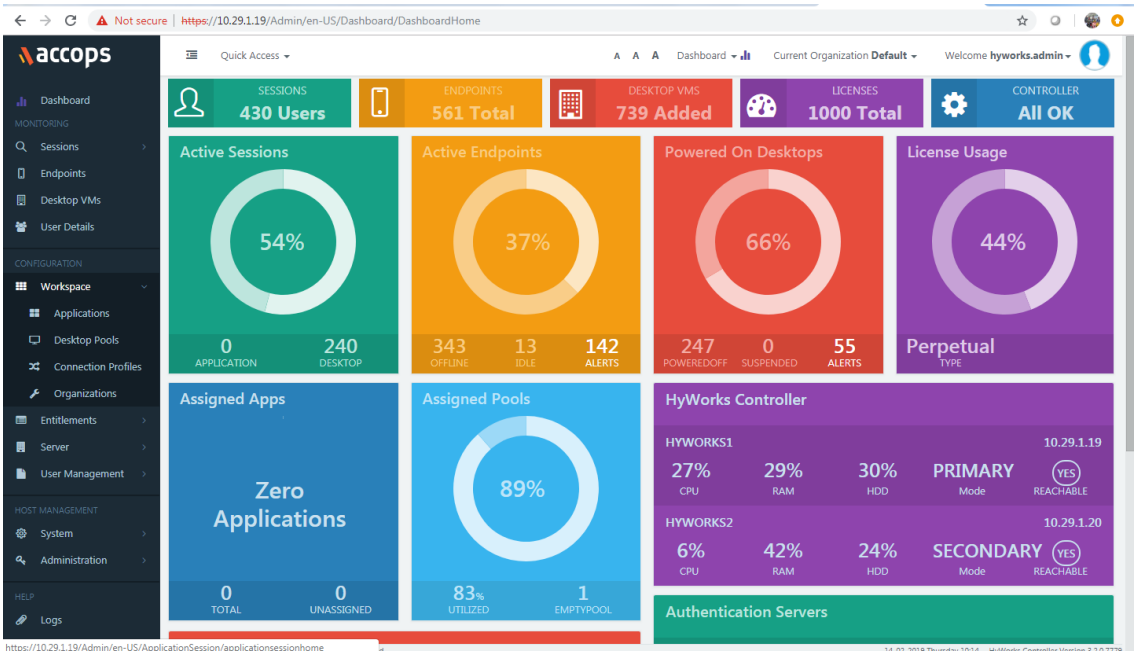

Figure 4: Hyworks controller web console Dashboard

3.1.1 Adding or editing Desktop Pools

Desktop Pools tab available under the workspace menu provides interface for creating and managing pools of desktops and associating the desktops to intended clients. The existing desktop details are viewed by going into “Workspace” and select “Desktop Pools” tab from the left side menu. The overall description of the existing desktop pool is given in table 4. Overview of desktop pool details is depicted in figure 5.

Sl. No	Field Name	Description
1.	Pool Name and Type:	Desktop Pool Name and Type of the pool (Provisioning / non provisioning)
2.	Provider/Team Name and Type	Name of session provider (SCVMM) Type of session provider (Hyper-V)
3.	Desktop Provisioning and Connection Profile	Desktop Provisioning configuration as Deployed for dynamic and None Connection Profile if configured else None
4.	Assignment Life Span: Permanent or Temporary	Type of the desktop pool
5.	Desktops Ready	Total number of ready Desktops Not applicable (NA)
6.	Desktops in Use	Desktops already assigned or being used in session Not applicable (NA) for Microsoft RDS Server Desktop Pools
7.	Free Desktops	Unassigned Desktops in Pool, available for assignments and connection
8.	Status	Ready or Cloning Desktops (If provisioning is in progress)
9.	Active	If Desktop Pool is active or not

Table 4: Description about the desktop pools

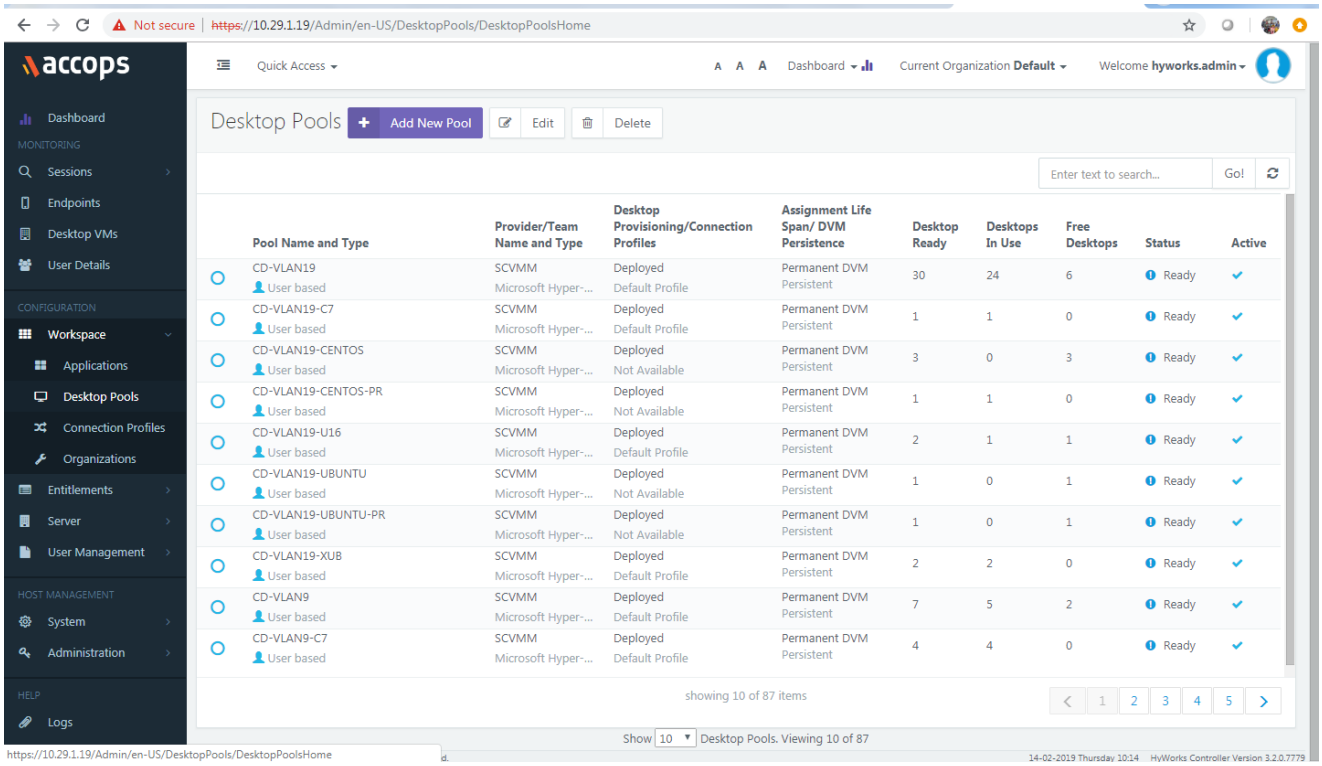

Figure 5: Overview of existing Desktop pools

A) Creating new VMs in new Desktop pool

Invoke “Add Desktop Pool” wizard, for creating new VMs by creating new desktop pool.

- Go to Workspace -> Desktop Pools tab
- In Desktop Pools screen, click on Add New Pool button
- Add Desktop Pool wizard will be launched and General screen will be displayed by default
- Now Add Desktop Pool wizard is invoked, next step is to configure General Configurations of Desktop Pool.

Table 5 summarizes the flow and configurations of Desktop Pool wizard.

S.No	**Desktop Pool wizard**	**Configuration attributes**
1	General	**Name of the pool** : Division name with VLAN information **Entitlement Type** : User based **Desktop Pool Type** : Persistent Virtual Desktop **Select Session provider** : SCVMM **Provisioning** : Dynamic Assignment Life Span : Personal Desktop Connection Profiles : Default profile Figure 6 depicts the screenshot of General Tab
2	Deployment	**Select a source VM** : GOLD-VM-WIN-10 **Desktop Name Prefix** : Division name with DESK and VLAN information **Clone Type**: Full Clone **Max Desktop Capacity** : number of VMs required **Desktop Creation Schedule**: Provision all Desktops now Check ->**Power On Desktop post provisioning** Figure 7 depicts the screenshot of Deployment Tab
3	Customization	**Computer Name** : Division name with DESK and VLAN information **Local Username** : admin **Local Password**: provide local admin password Confirm Local Password : local admin password **Join Domain**: Choose Domain **Domain Name**: VDIDOM.GOV.IN **Username** : administrator **Password**: Provide domain administrator password **Confirm Domain Password** : Confirm password **Preferred DNS** - Specify preferred DNS entry to be configured post provisioning : 192.168.101.10 **Alternate DNS** - 192.168.101.11 **Select Locale** : English (India) Figure 8 depicts the screenshot of Customization Tab
4	Desktops	No need to configure
5	Users	No need to configure
6	Client Groups	Choose unrestricted access
7	Advance	Check -> Use last known IP Address
8	Summary	Displaying the summary of all the configurations. Figure 9 depicts the screenshot of configuration summary

Table 5: Steps for creating the desktop pool

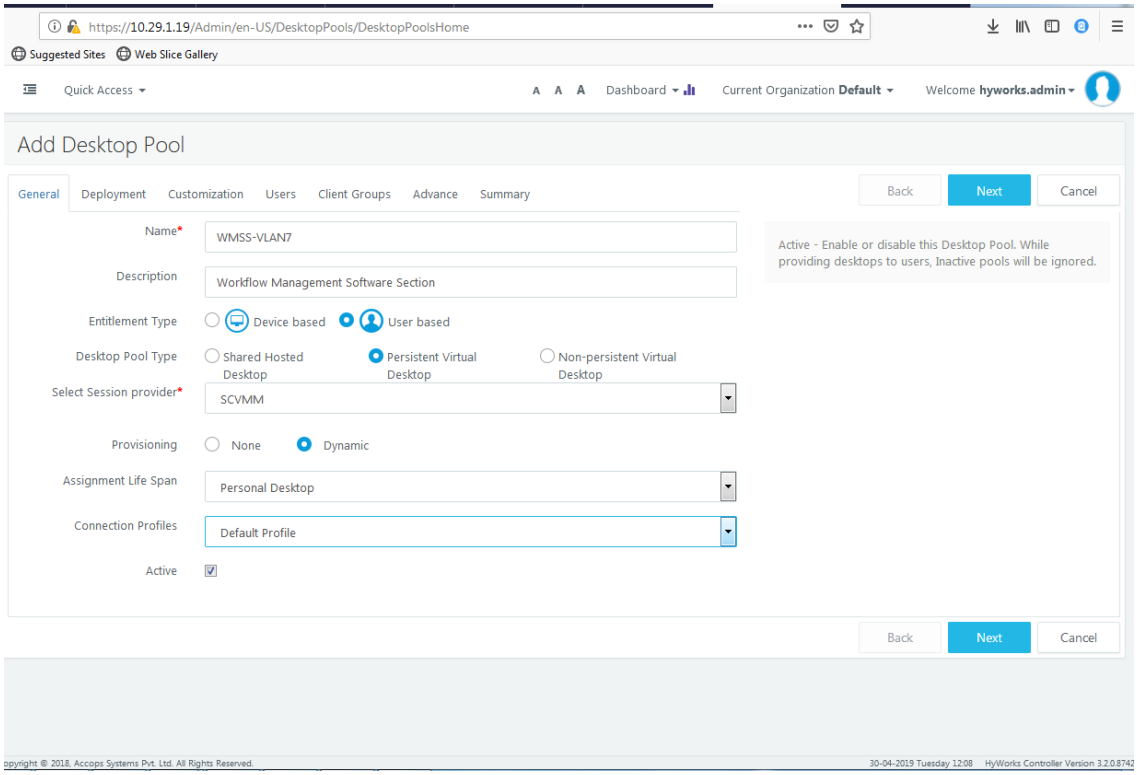

Figure 6: Add desktop pool - General information tab

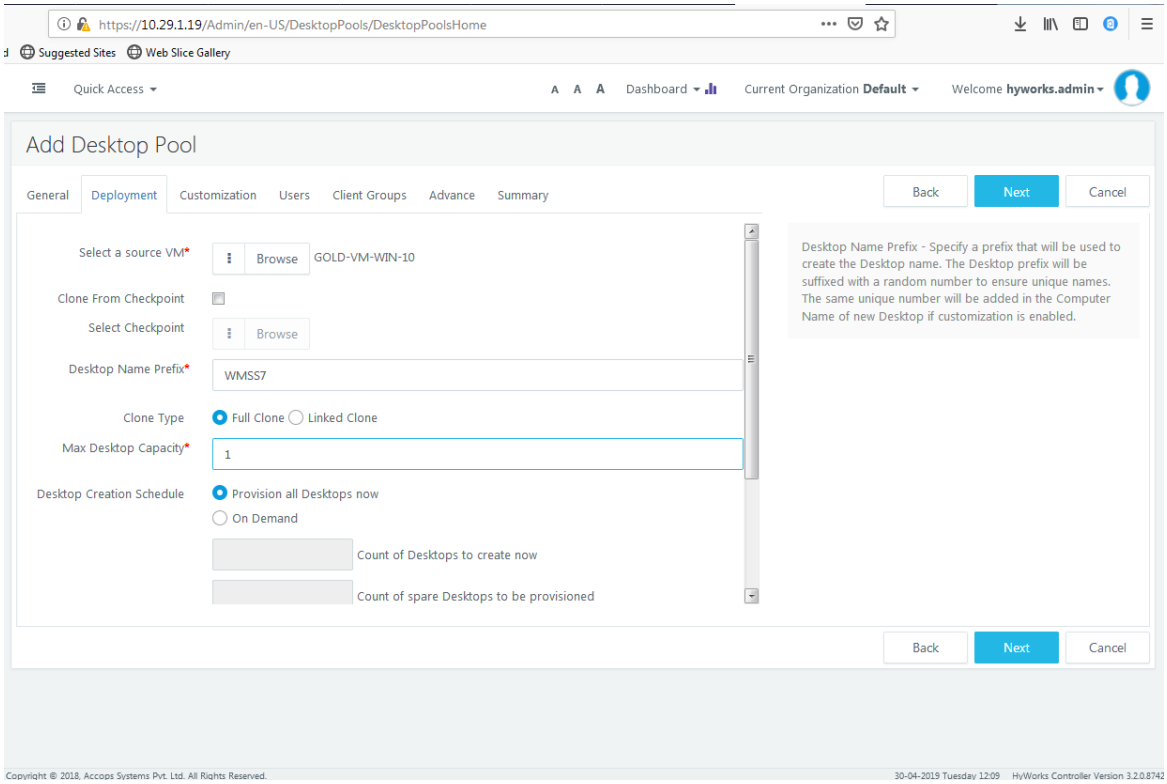

Figure 7: Add desktop pool - Deployment information tab

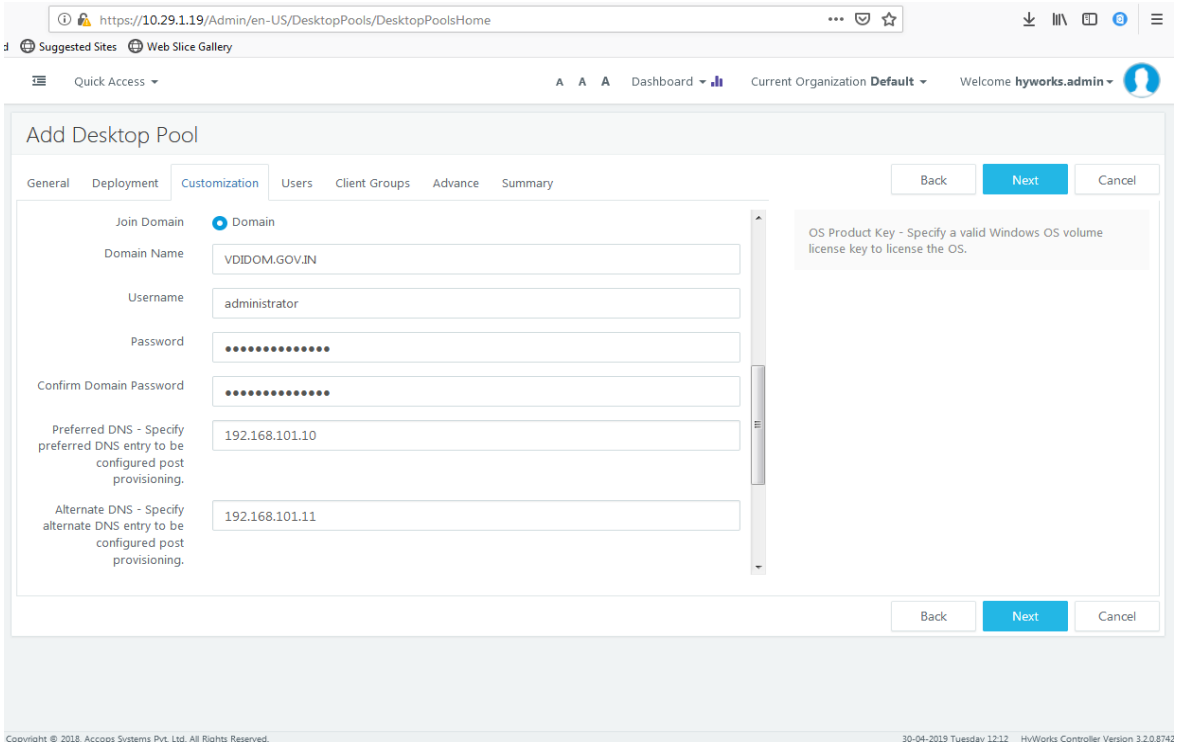

Figure 8: Add desktop pool - Customization information tab

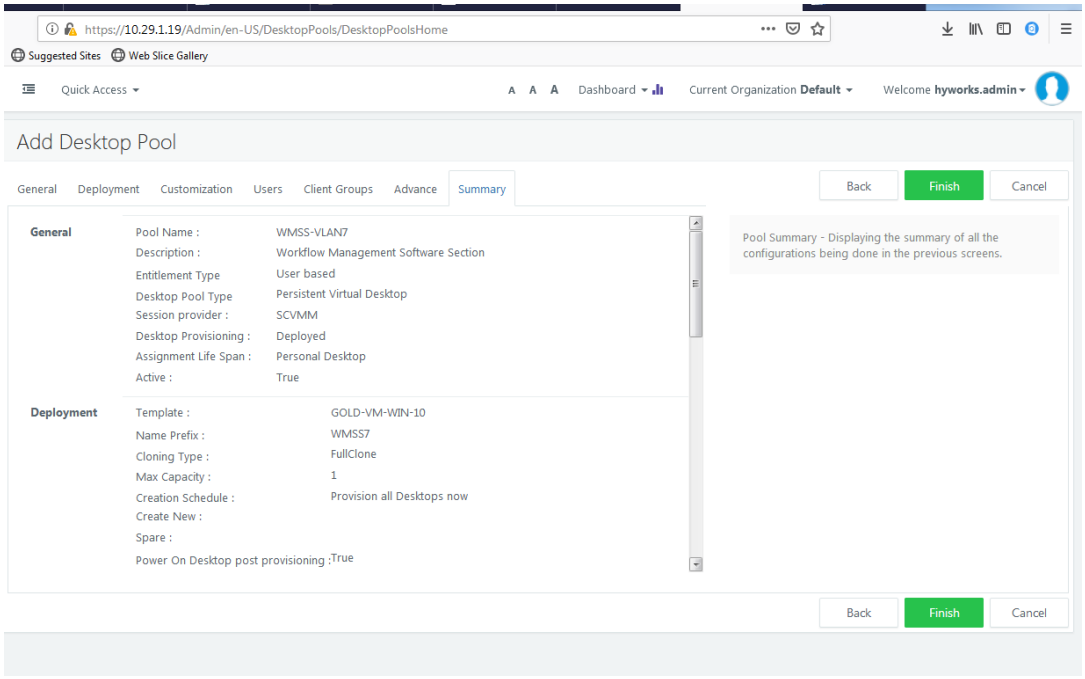

Figure 9: Add desktop pool - summary of pool information tab

Once the desktop pool wizard is finished, Desktop pools tab shows the status as Cloning Desktop which is indicated in Figure 10.

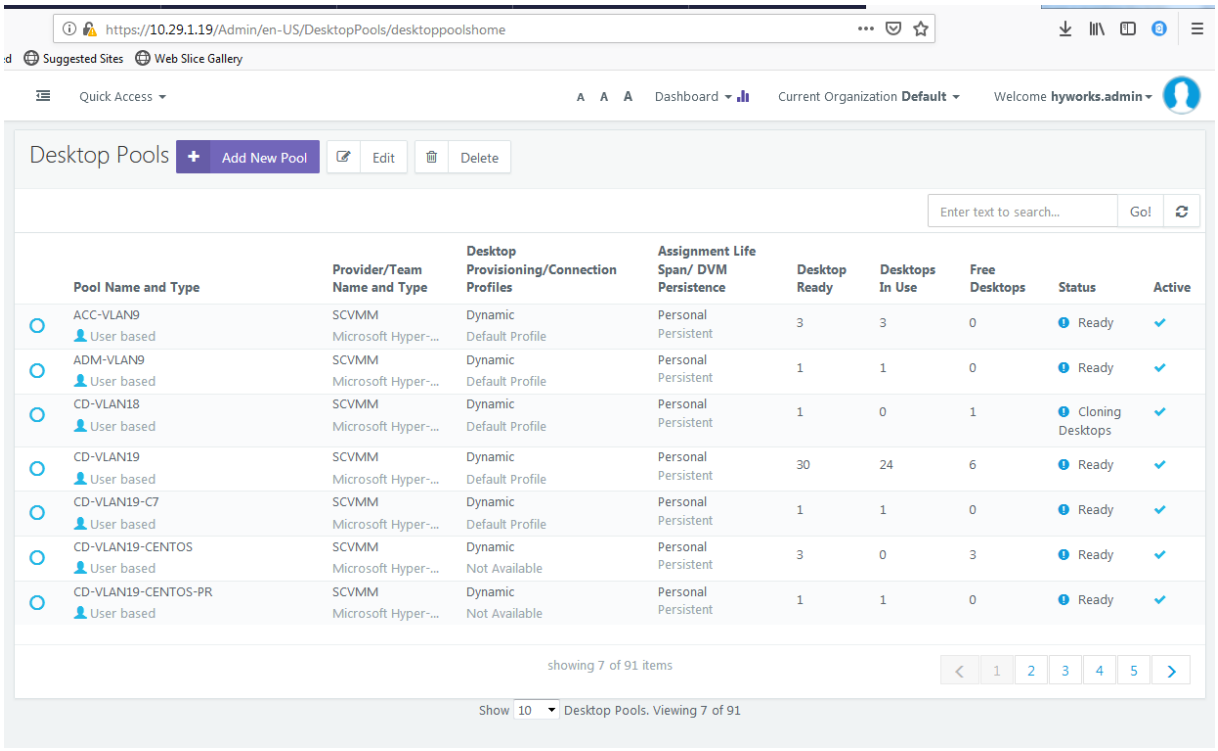

Figure 10: Desktop Pool status

Desktop VMs tab can be used to see the provisioning progress as well to check the Desktop Creation schedule. New desktops are cloned one by one and once the provisioning starts the status will be displayed as rotating symbol tagged as 'Creating Desktop' which is shown in the figure 11. Once the creation of desktop is done, configuring desktop will take place which is shown in figure 12.

After all configurations are done, Desktop Agent status should be indicated as “responding” and Desktop Name should be assigned. The IP address and DNS field should be displayed with IP address of the desktop and desktop name affixed with configured domain name. These indications states that the desktop is configured correctly according to the configuration of the desktop pool. For example, Figure 13 indicates a properly configured desktop named as MDTD16-0015 and appended with domain name VDIDOM.GOV.IN.

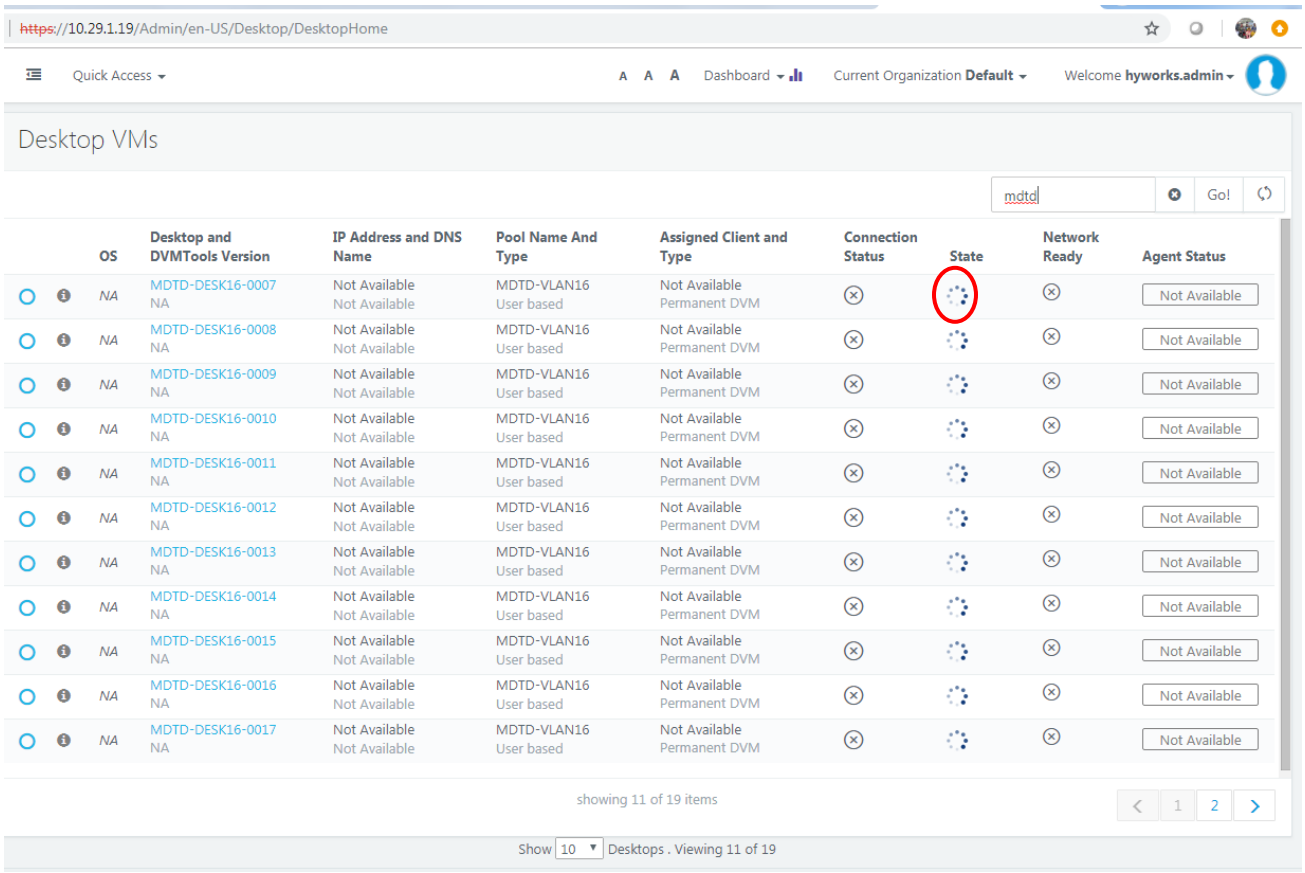

Figure 11: Screen shot of desktop provisioning status

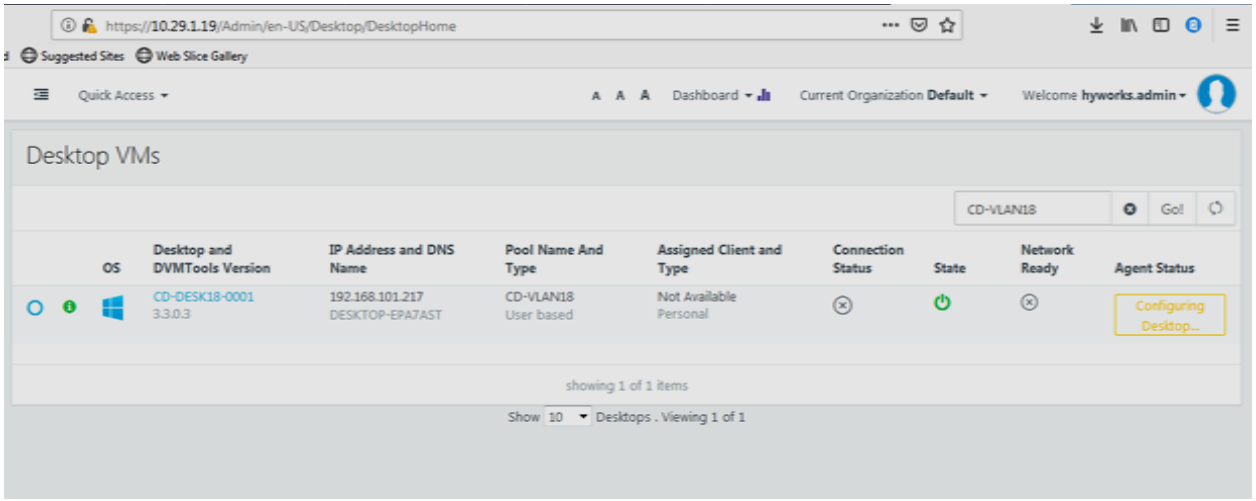

Figure 12: Screen shot of configuring desktop status

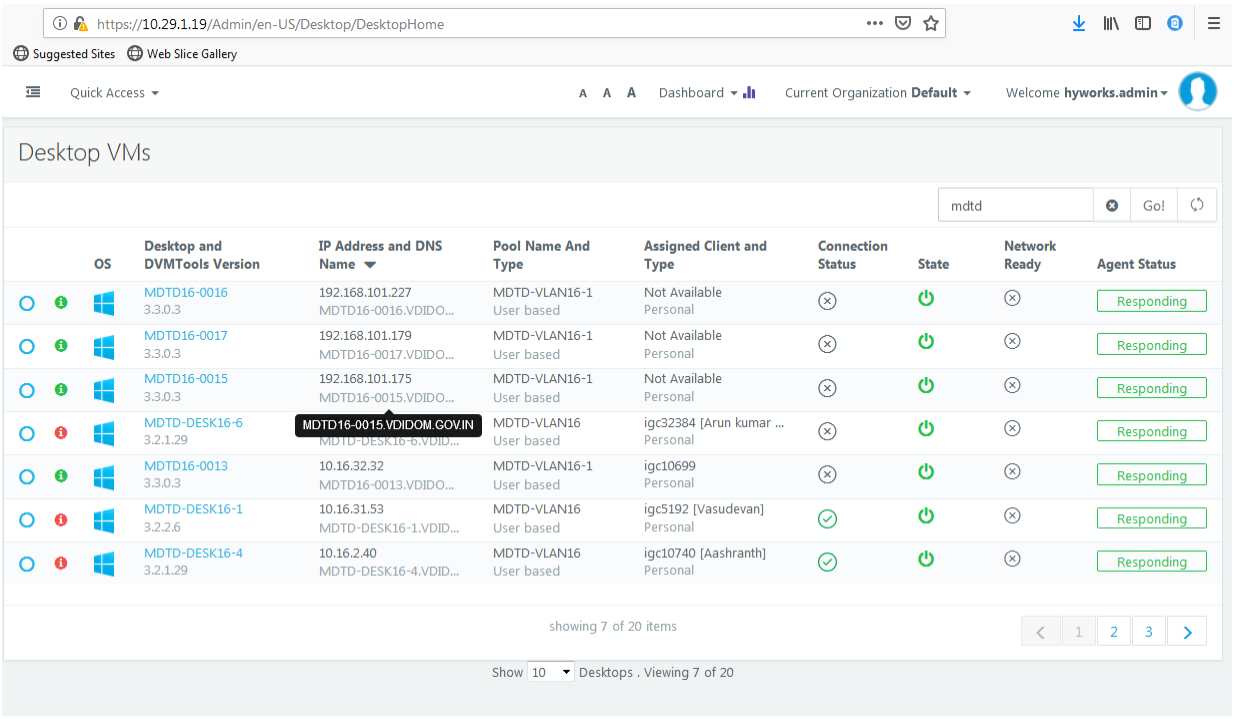

Figure 13: Screen shot of agent and VM status

B) Editing Desktop pool

Edit Desktop Pool wizard provides different editable options to administrator according to the requirement of changes in the desktop pool. Most of the time maximum capacity of the desktop pool can be varied using this option. Figure 14 depicts the editing of desktop pool.

To edit a pool, following steps are followed:

1. Go to ***Desktop Pools*** page
2. Select the desktop pool needs modifications
3. Click on ***Edit*** button – It will open Edit Desktop Pool wizard
4. Update the configurations as per requirement in General, Desktops (for pools using existing desktops), Deployment/Customization (for pool using dynamic provisioning), Users/ Devices, Desktop Assignments (for pools using existing desktops) or Advance screens
5. On ***Summary*** screen, verify the information and press finish

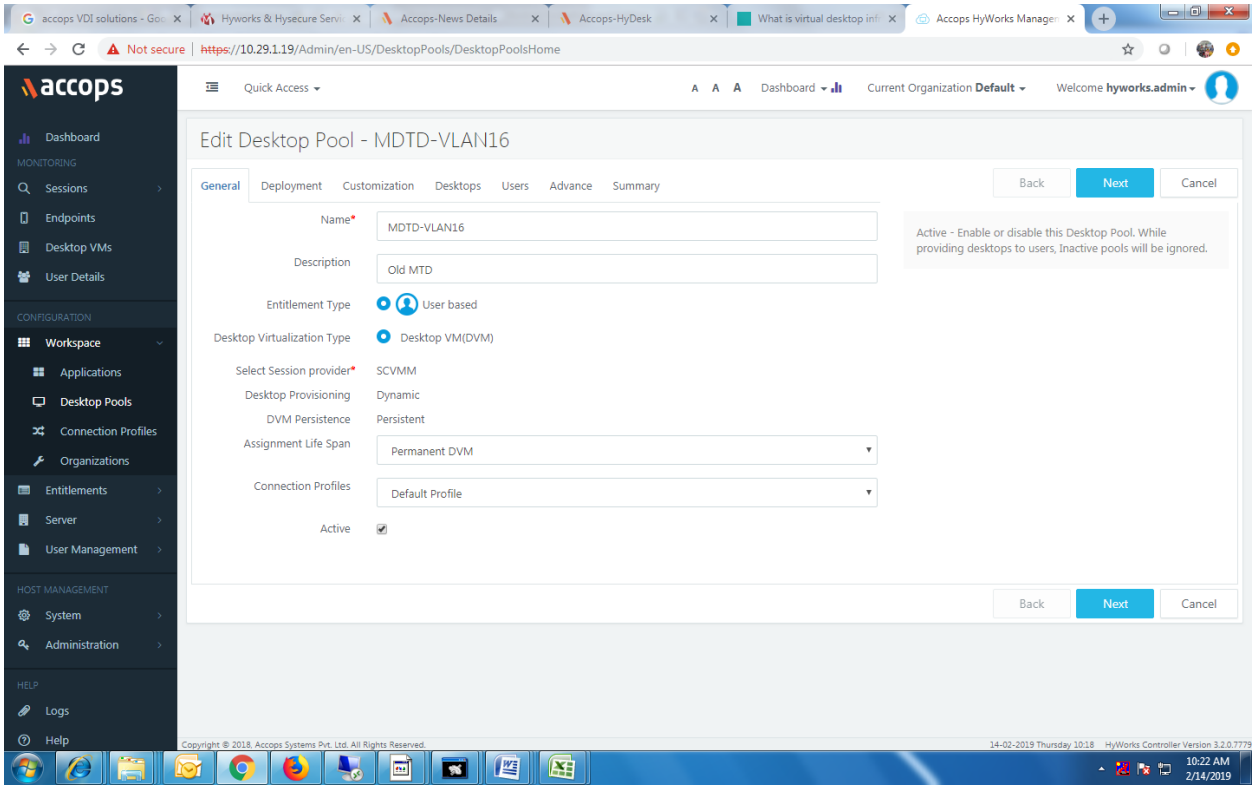

Figure 14: Edit Desktop Pool

3.2 Adding Users and Computers to the Active Directory Domain

Active Directory (AD) domain is established with the name VDIDOM.GOV.IN in the AD server hosted in the management servers. To create a user account in that domain following steps are followed.

1. Remote Login to any of the management node (IP address: 10.29.1.21 / 10.29.1.22) with administrator privilege.
2. Open Fail over Cluster Manager. Click MGMT.VDIDOM.GOV.IN -> Roles. Right side pane will list the list of roles. From the list choose AD.VDIDOM.GOV.IN and click "connect" option as shown in figure 15.
3. Click Start, point to Administrative Tools, and then click **Active Directory Users and Computers** to start the Active Directory Users and Computers console in AD server

    - Click the domain name VDIDOM.GOV.IN, and then expand the contents and point to IGCAR Organization Unit (OU).

- Right-click IGCAR OU, point to New, and then click Organization Unit. Name the OU with the Division Name (Ex. MDTD, WMSS). Division OU is shown in figure 16.
- Inside the division OU create two groups with the naming terminology as Division name affixed with VDIs and other one Division Name affixed with Group (Eg. WMSS VDIs, WMSS Group).
- Create the list of users who belong to the respective division OU. Right-click ->Users, point to New, and then click 'User'. Provide the name and user logon name (based on the category of the request) and press 'Next'. Refer Figure 17 a.
- Type a new password, confirm the password, and then click to select one of the following check boxes:

    - Users must change password at next logon (Uncheck)
    - User cannot change password (Uncheck)
    - Password never expires (check)
    - Account is disabled (Uncheck)
- Click Next.

- Summary of user information will be displayed as shown in figure 17 b, and then click Finish.

4. After creation of new user, add created desktops as members to the "Division VDIs" (Eg. Name of the Desktop: WMSS7-0001) and add the users as members to the "Division Group" (Eg. User Logon Name: igc6775@VDIDOM.GOV.IN). Figure 18 displays the groups and user details of particular division OU. The following steps are used to add the members to the respective groups.
    1. Right-click the groups created, and then click Properties.
    2. Click the Member Of tab, and then click Add.
    3. Search for Users / Computers name.
    4. Click OK to finish.

This process ensures the redirection of the profiles to the VMs allows the users to login from the thin client and also applies the organizations group policies.

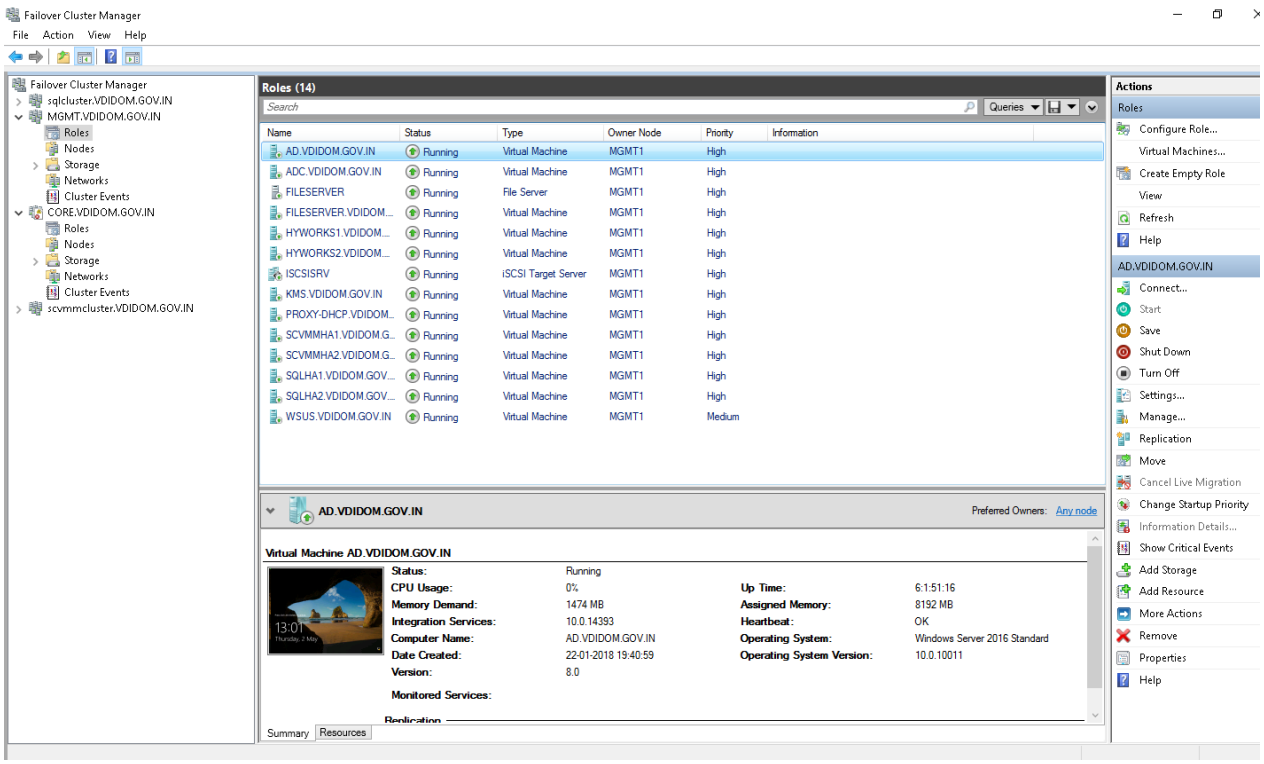

Figure 15: Connect to AD server through fail over cluster

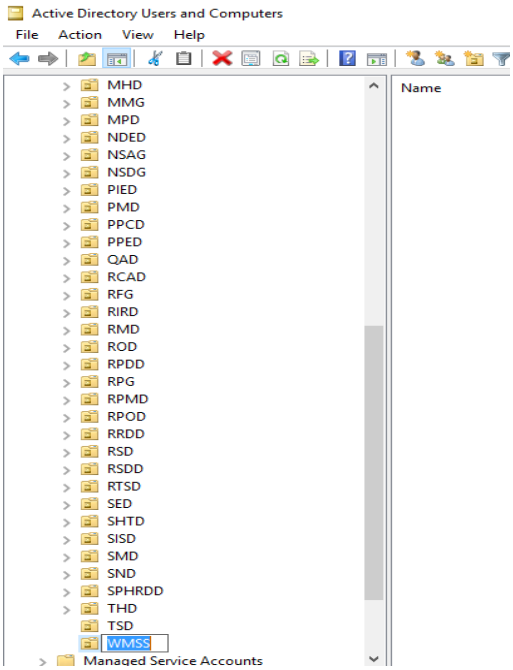

Figure 16: Creation of Division OU inside IGCAR OU

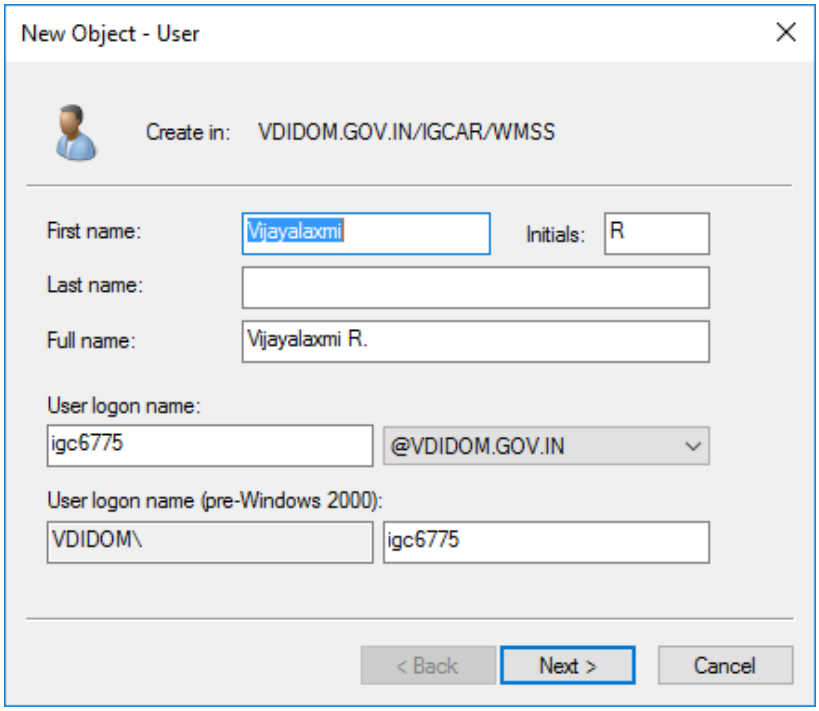

Figure 17 a: User creation inside division OU

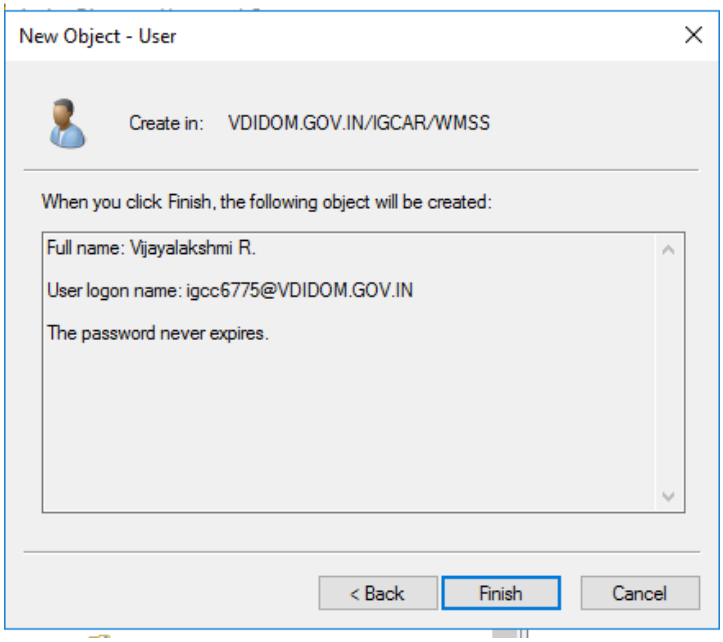

Figure 17 b: Summary of new user details

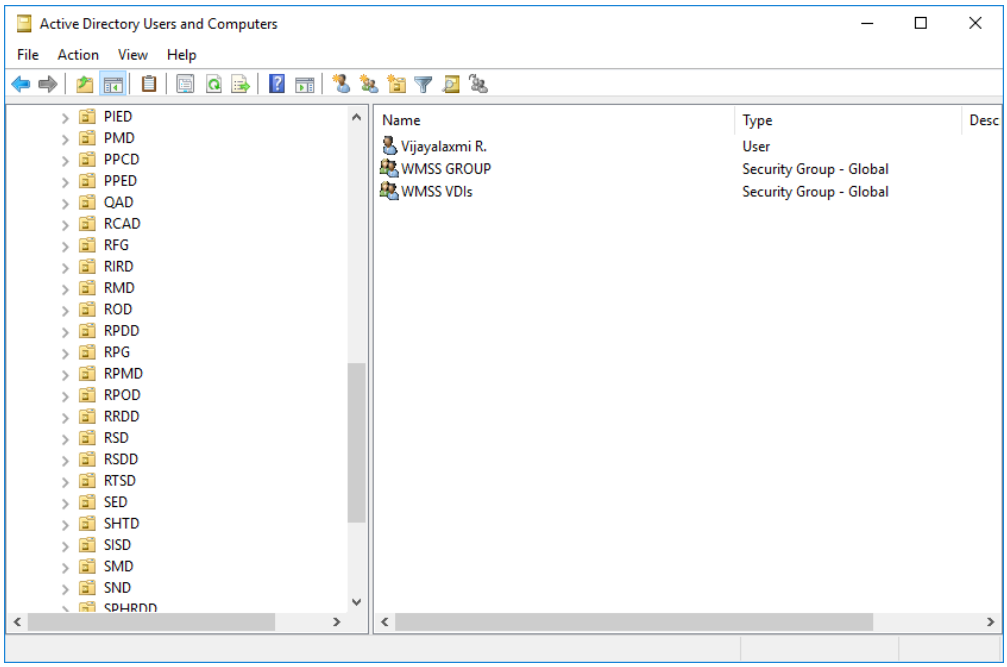

Figure 18: List of groups and users under the Division OU

3.3 Assignment of users to the Desktop

After creating the users in the AD server, assignment of user to their respective desktops should be done. Hyworks web interface provides desktop assignment for associating users with Desktops using the following steps.

- Go to Desktop VMs menu
- Choose the required desktop from the list of desktops, where user has to be assigned
- Select the “assign” option from top menu
- Search the user, using logon name which is created in the AD server
- Select the particular user from the available user list
- Press ‘Assign’

Assignment of user to the selected desktop is shown Figure 19.

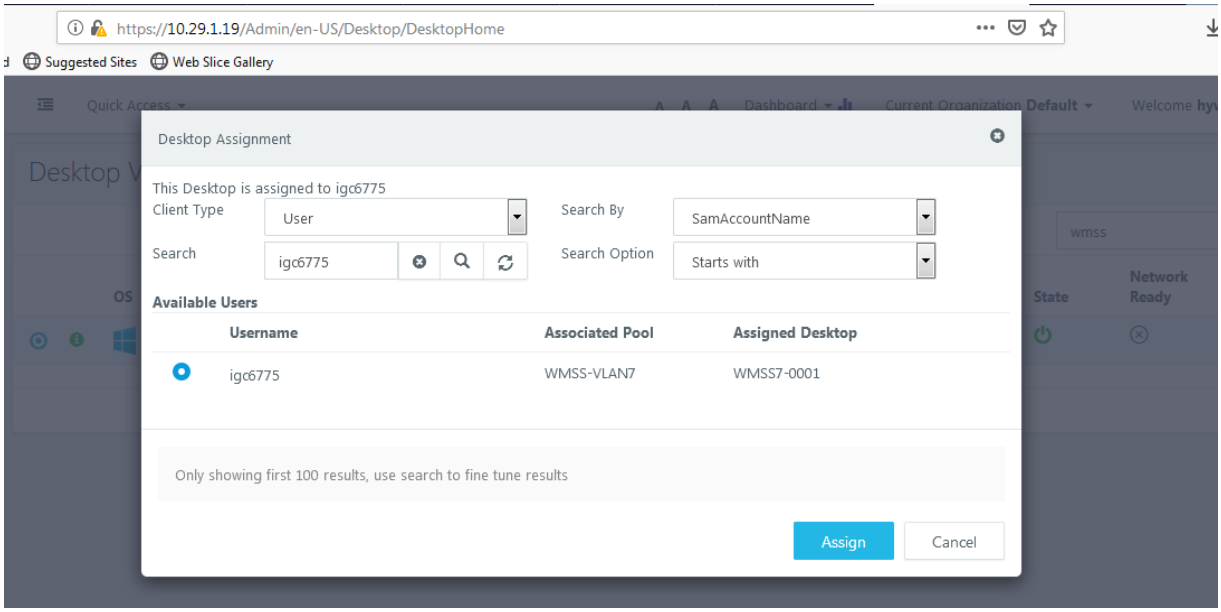

Figure 19: Assignment of user to the desktop

3.4 Configuration of VM

Configuration of VM is done through the console of the VM. The VM console is invoked through failover cluster manager from the management server.

A) Configuring the VLAN identifier

VLAN identifier is an important parameter through which the VM will be communicated to the IGCAR backbone network. Figure 20 depicts the configuration of the VLAN identifier to the desktop. The following steps are involved to configure the VLAN identifier of the VM.

- Choose CORE.VDIDOM.GOV.IN from fail over cluster manager
- Select Roles
- Search the VM using desktop name (Desktop name: as per Hyworks web console) from the right side pan
- Choose the required desktop and right click on that desktop
- Choose settings: Settings for the respective VM will be popped up
- Choose the network from the hardware list
- Choose the core switch from the drop down menu
- Check Enable Virtual LAN configuration
- Enter the VLAN identifier based on the IP address of the VM. (Eg. If IP address of the VM is 10.18.1.200 then 18 should be given as VLAN identifier)
- Press OK

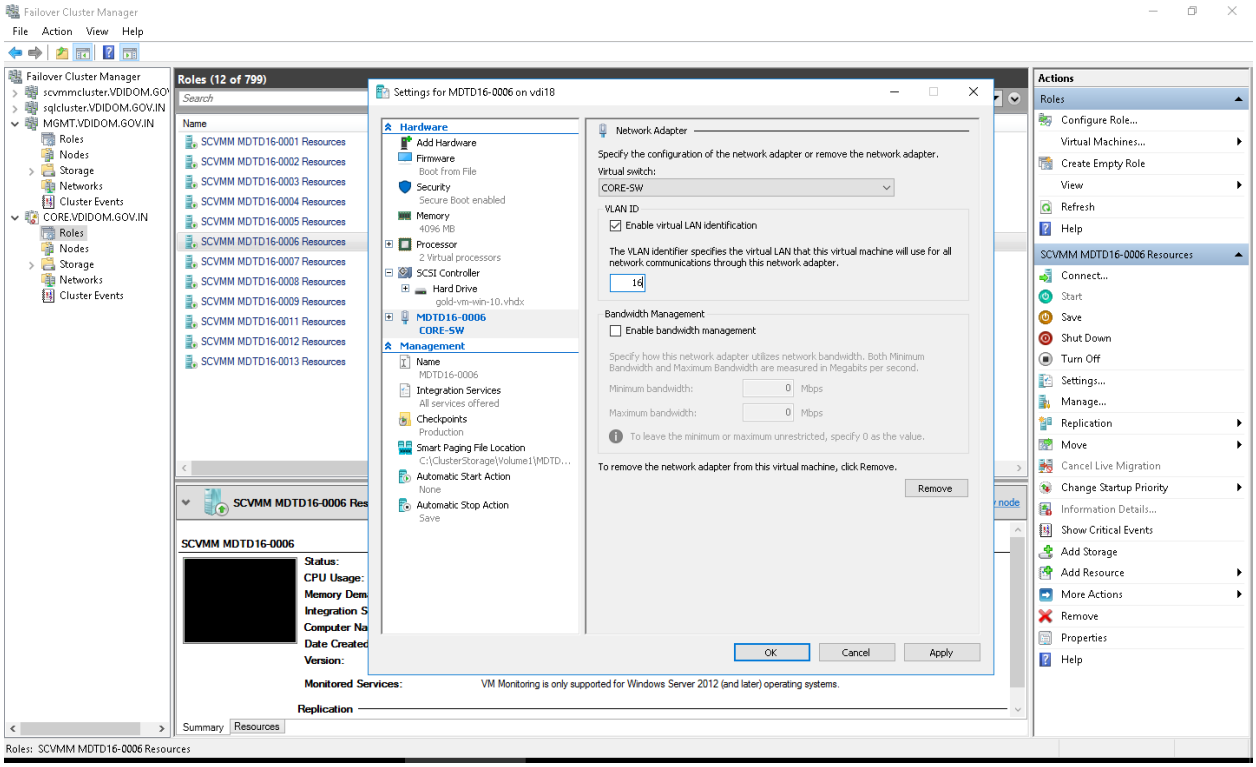

Figure 20: Configuring the VLAN identifier

B) Configuring the IP address for VM

IP address of the VM is configured through console.

- Choose CORE.VDIDOM.GOV.IN from fail over cluster manager
- Select Roles
- Search the VM using desktop name (Desktop name: as per Hyworks web console) from the right side pan
- Choose the required desktop and click connect from the right side menu
- Windows 10 VM console will be displayed
- Login with local administrator privileges (User name: .\admin)
- Go to network settings and configure the IP address as shown in figure 21.

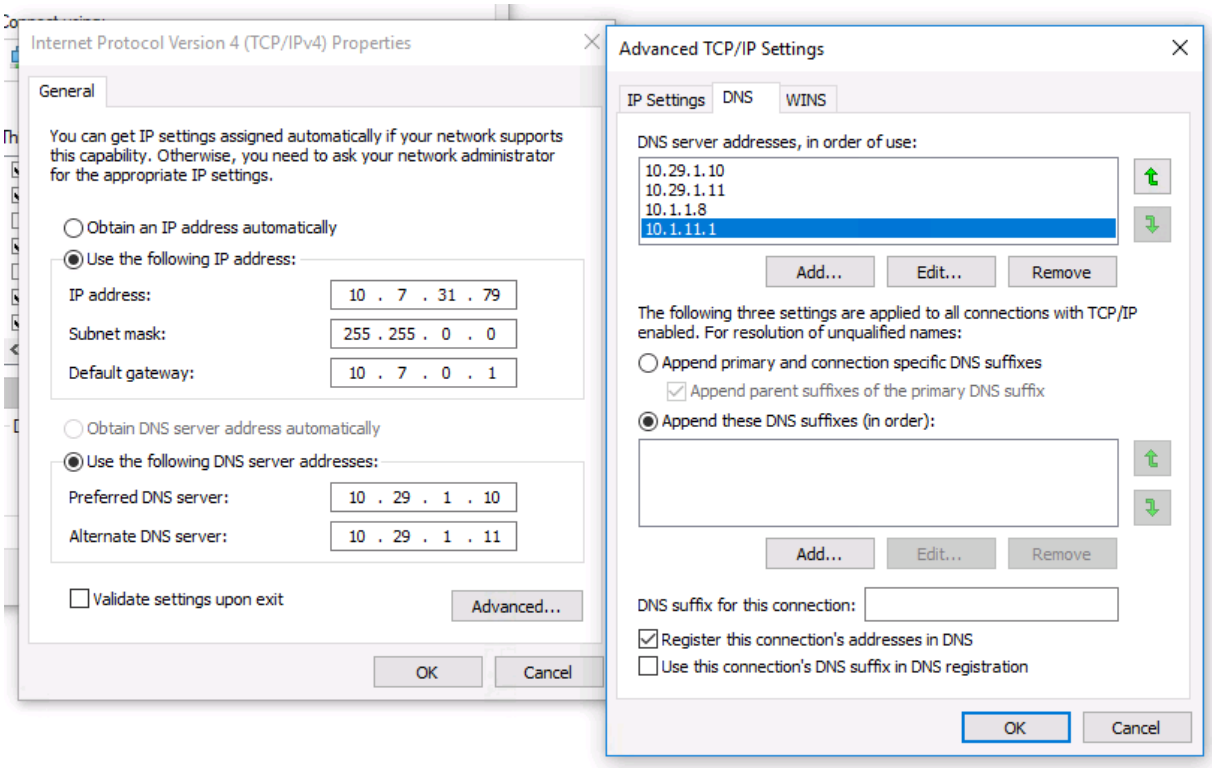

Figure 21: Configuring the IP address of VM

After assigning the proper IP address and DNS entries verify the network connectivity by pinging into file server and intranet server (Eg. ping fileserver, ping iis).

C) Enabling remote desktop users

The assigned user for the particular desktop will be accessible only if the user's logon name is added into the remote desktop users group. This configuration is done inside the user VM with the following steps.

- Open Computer management -> System Tools, local users and group manager
- Select Groups
- Select Remote Desktop Users from the right side pane
- Double click Remote Desktop Users and add the user into the Members of the group to grant the right to logon remotely (Eg. logon name: igcc6775)
- Provide the domain administrator privileges while adding user names
- Click OK. Figure 22 shows the screen shot of adding users to the remote desktop users group.

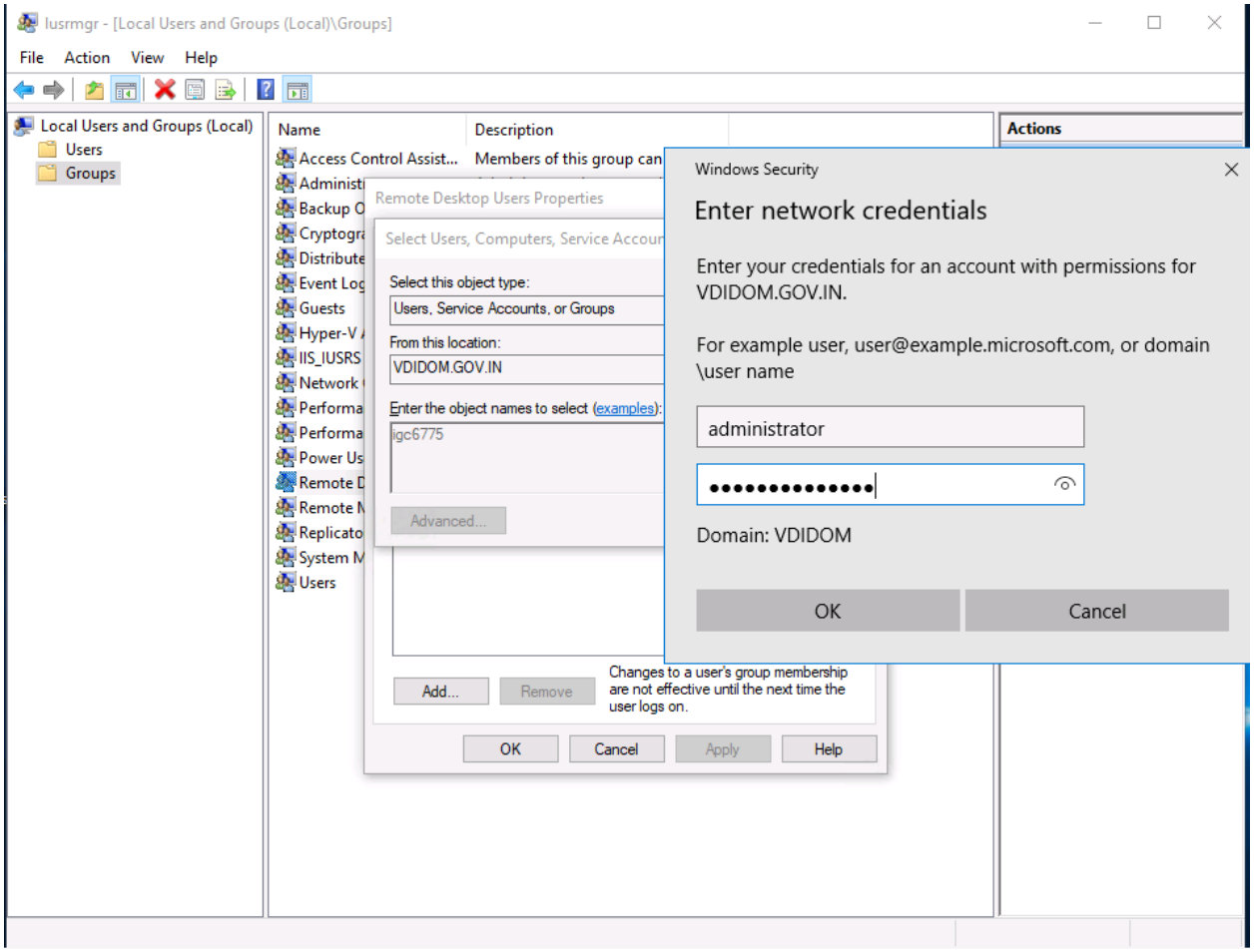

Figure 22: Adding user to the remote desktop users group

D) Invoking VM with user logon name

After adding the user name into remote desktop users, VM is invoked through console from the fail over cluster manager. After providing the logon name and password (Eg. logon name: igc6775) the user VM will be invoked as shown in the figure 23. Windows 10 VM with users profile will be displayed. Ensure the presence of C drive with 50 GB and H drive with 200 GB. With this the VM is ready for the deployment.

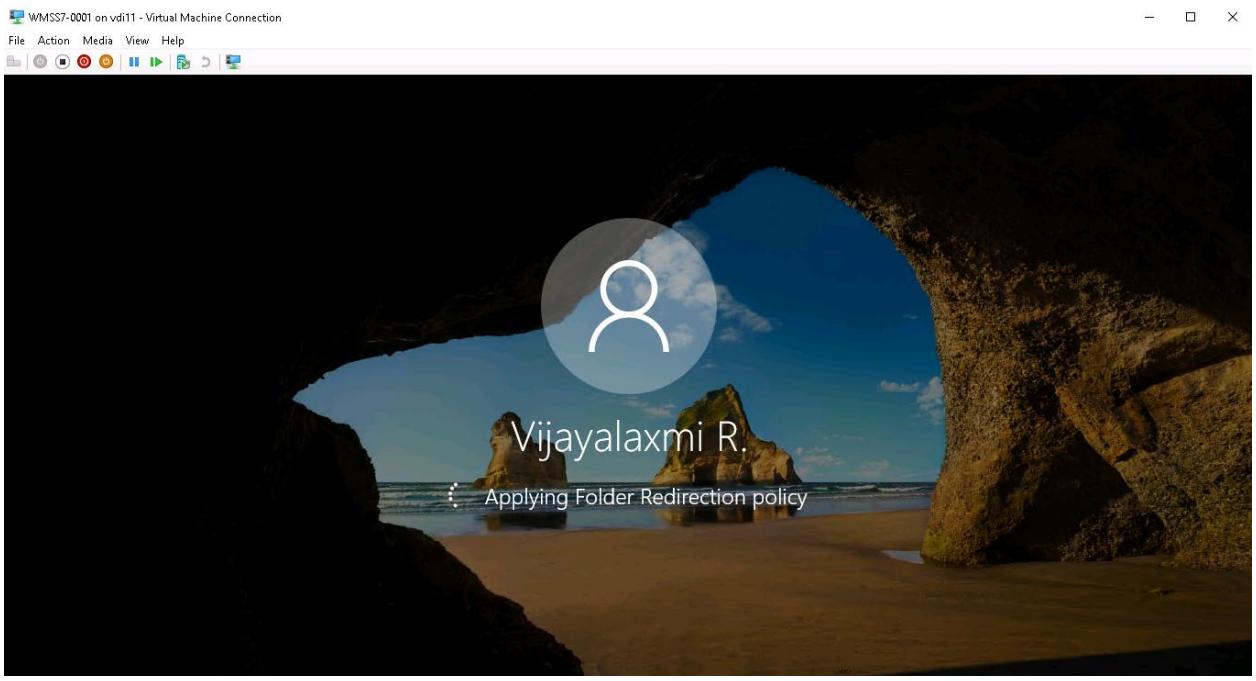

Figure 23: Invoking VM using user's credentials

4. Configuration at thin client

During the deployment the thin clients will be given to the respective user. The following configurations are required at thin client side to invoke the VM.

- Specify the Hyworks controller IP as shown in figure 24
- Configure the network IP address of the thin client with subnet mask and default gate way (As a standard practice Thin-client IP is derived by adding the 20 to the 3rd octet of the VM IP)
- Check the connectivity icon. It should be blinking as green
- Go to log on screen, and provide user logon name and password
- Users desktop will be invoked

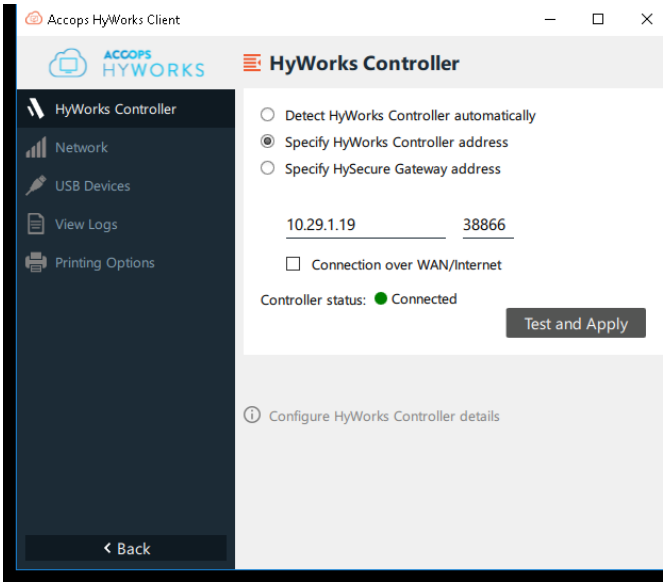

Figure 24: Configuring the Hyworks controller IP address

5. Conclusion

The VDI setup of IGCAR has been commissioned with twenty two high-end servers, unified storage and 10G network supports at the data centre setup of Computer Division. The setup is capable of supporting thousand user virtual desktops through thin-client distributed across the campus. This document describes about the overall configuration of the setup. The document also outlines the procedure involved in the creation and deployment of user virtual machines.