**INFO 2416 : SERVER OPERATING SYSTEMS**

**GROUP PROJECT – Final Report**

**TOPIC 3 – Create a Windows Server 2012 R2- Based Network Using Microsoft Azure**

**By**

**Umair Rashid (100312938)**

**Ammar Albaqshi (100294683)**

**Matthew Haskins (100220599)**

**Ben Laktin (100329657)**

**Our Business Introduction and Purpose**

Our company, Vprovide Accessories, sell smartphone accessories through retail. As a small company with roughly 50-80 users, we require Active Directory to distribute permissions to the different types of users and allocate resources and sharing among the departments. We currently have seven departments: Marketing, Human Resources, IT, Inventory/Merchandise, Accounting and Finance, Customer Service/ Retail and Purchasing. Each department has a hierarchy of users starting with managers, and ending with employees.

The CEO will have full access to everything and the administrators will have the second most amount of access in order to perform their duties for their respective departments. Each of the departments will have access to the files and folders in their own department, but not any others. For example, the users of the Marketing department cannot access the files and folders of the Human Resources department.

We currently have one office in Vancouver downtown where we manage our inventory and offices for other departments. We have two retail stores in major malls that displays our products and sell them.

**Description of the departments**

Marketing

* Marketing deals with promoting the products, running ads on social media, and pricing promotions in store and online.

Human Resources

* Human Resources performs the management of human resources. They deal with recruiting, upholding labor laws, administering benefits, and other aspects of employment.

IT

* IT is responsible for technical support and maintaining the architecture, software, hardware, and networks of computers in the company.

Inventory/Merchandise

* Inventory/Merchandise are responsible for stocking products in the warehouse and shipping to fulfill orders for retail and online

Accounting and Finance

* Accounting and finance deal with the financial elements of the company, such as payroll, financial reports, inventory costs, accounts payable and receivable, among other duties.

Purchasing

* Purchasing is responsible for purchasing products and materials needed from suppliers.

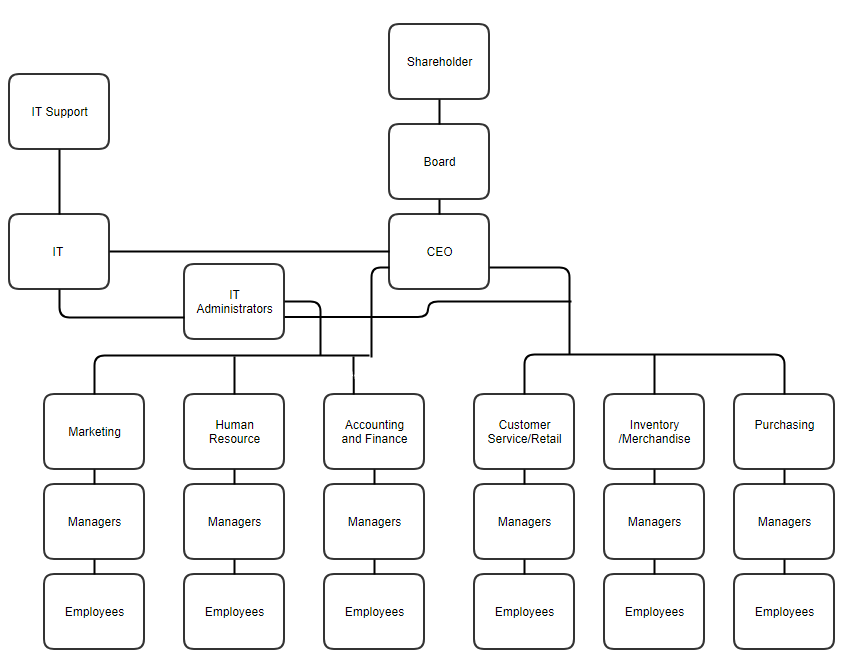
Customer Service /Retail

* Customer Service/Retail provides service to the customers. They sell products to the customer, deal with complaints, and take orders from the customer.

**Business Structure Chart:**

We have created a business structure chart to demonstrate how our departments are structured and how it managed by the management. We have the shareholders, then the board and then an appointed CEO to run the company. Under the CEO, we have department manager that report to the CEO. IT department is divided into two different sub-departments called IT Support and IT admins.

All other departments have a department manager and an assistant manager to help them with managing the department. Customer Service/Retail Department is divided into three categories. We have two stores and online customer services. Each managed by a manager. Each department has different users and will be represented later in a user chart.



**Types of Users and Amount of Users(Chart):**

**CEO:**

A chief executive officer, who is the highest-ranking person in the company. All Department managers report to him about their goals, progress and any issues they can’t solve. CEO is the one with the highest access in the company and can access any part of the company without any restrictions.

**IT Administrators:**

IT administrators are who control and manage the IT infrastructure of the company. They usually include Systems administrator and Network administrator. They have the highest access besides the CEO and they deal with any IT issues that can’t be handled by IT support. They handle security of the systems and make sure the companies data is not compromised. They decide the groups and group policies which must be assigned to the type of users. IT Admin Manager will have access to every Department but IT admins under him will only have access to Departments Assigned.

**Managers:**

Department managers are responsible for their departments performance. They have the highest position in their department and they all usually have assistant managers or other managers (if the department is bigger) to help them manage the department. Assistant Managers are involved with the employees on day to day basis and report to the department manager. They have access to every file or folder in the department.

**IT Support:**

They are responsible for basic IT support. They can reset passwords, help with any software issues the terminals might be having with the employees. They are first line of support for the rest of the employees. If any issues are above them then they must contact one of the admins to look and fix the issue. They also help setup accounts for the users and providing them the credentials when they first join the company. They implement group policies which are assigned by administrators based on the account type.

**Department Employees:**

They are responsible for the daily tasks their department assign to them. They only have access to the files they work with so basically, they have the least amount of access. These include retail as well as department employees that are under their department assistant managers.

**Resources:**

**Terminals:**

There will be 50 terminals in the office and only one of the terminals will be allowed to be accessed by the CEO and the IT manager. The rest terminals can be accessed based on the employee’s user account.

**Folder Sharing:**

There are many folders available to access on our domain controller but only few can be accessed by each department. They will be chosen and assign permission to a certain folder(s) only. Only The CEO of the company and the IT manager will have full access to all the folders available.

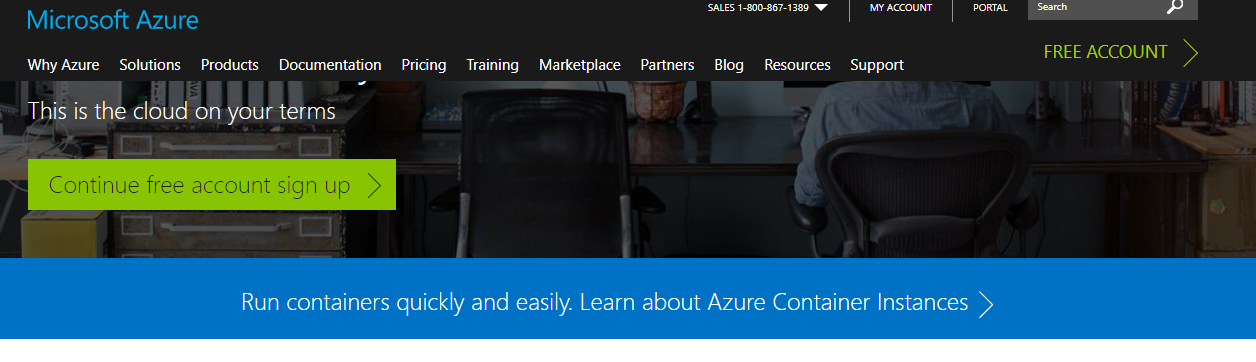
**WINDOWS SERVER NETWORK PLANNING AND IMPLEMENTATION**

The very first step in the planning process is to choose how much power we want in our VMs and how much power we want on our Domain Controller. We decided to allocate more power to the domain controller since it’s the main part of our network and we only assigned enough power in our terminal VMs so they function efficiently.

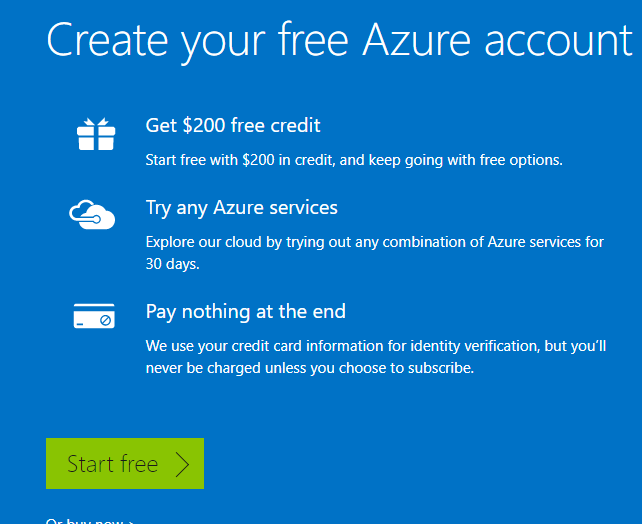
We first created an account to acquire Azure Services.

**Guide to Creating an Account for Azure**

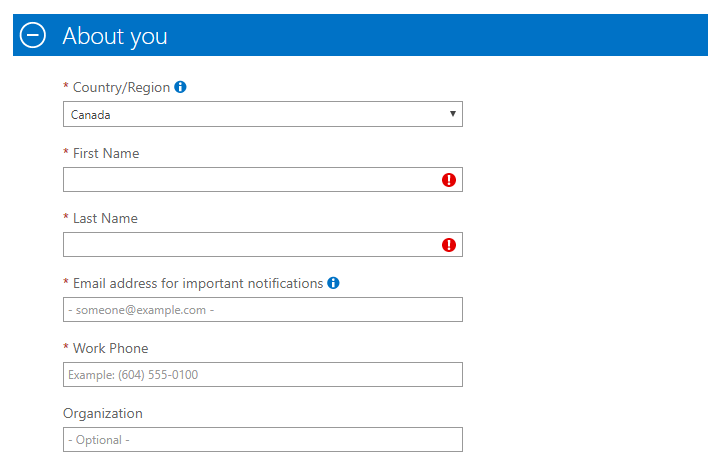
1. Go to azure.microsoft.com



1. Click Free Account
2. Click Start Free



1. Use your Microsoft account to sign in.
2. You will be taken to the step to fill information about you.

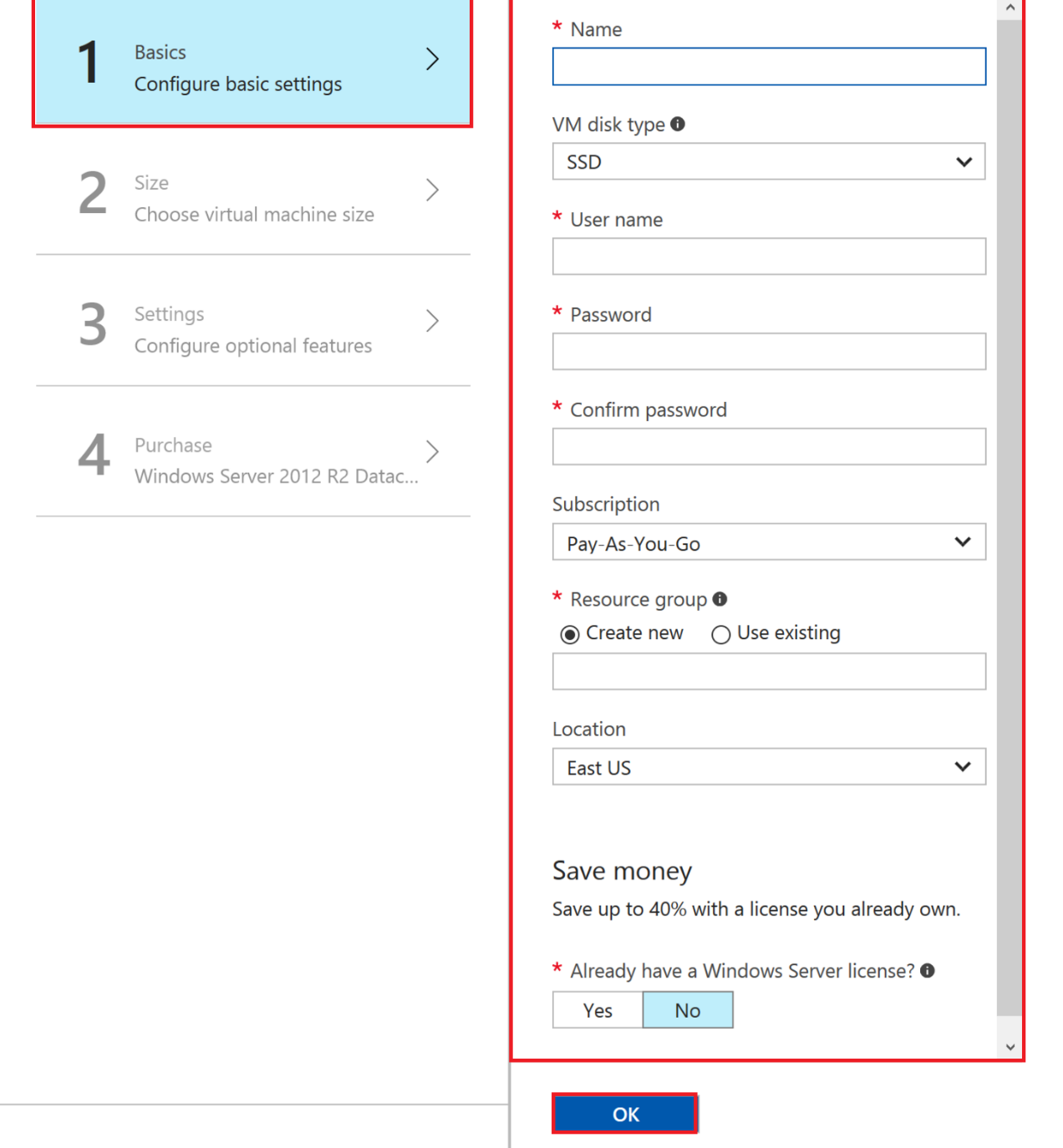


1. Fill up First Name Last Name email address and Work Phone
2. Next step will be identify verification by phone. You must fill the phone number and send a text message to verify your phone.
3. After Verification then you must fill up the credit card details. Your card wont be charged for the free trial but will be charged after the free trial ends.
4. Last step would be the summary and you have to accept terms to finalize the account.

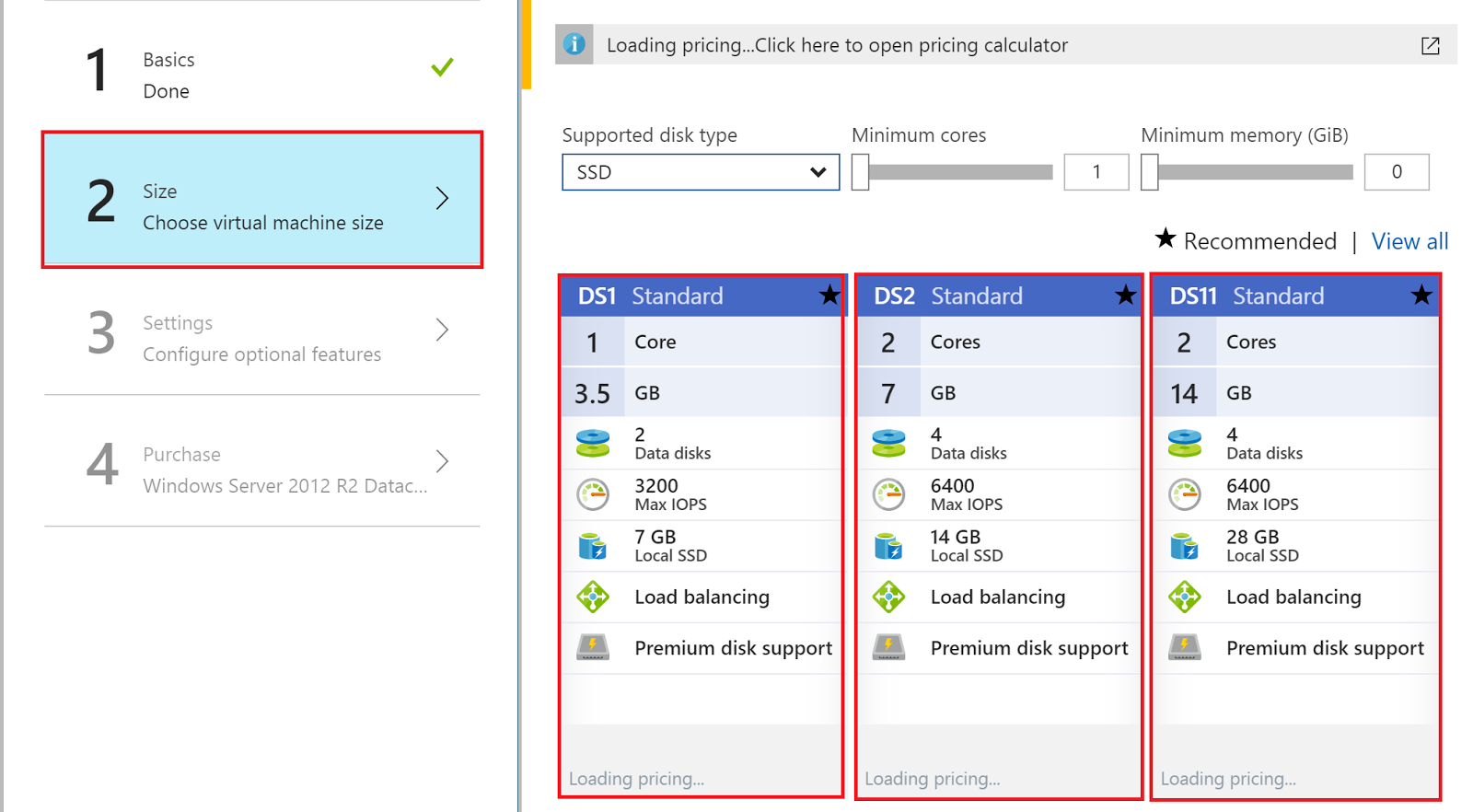
After creating an account, the next step was to create two VMs

**Guide to Creating a VM in Azure**

* 1. Click +New
  2. Select Compute > Windows Server 2012 R2 Datacenter.
  3. In the basic, type the Name, select VM disk type, type the Username, Passwords and resources Group. Type the closest Server Location to you and if you have the Windows Server license already because if you do then the machines will be cheaper since it doesn’t add any licensing cost.

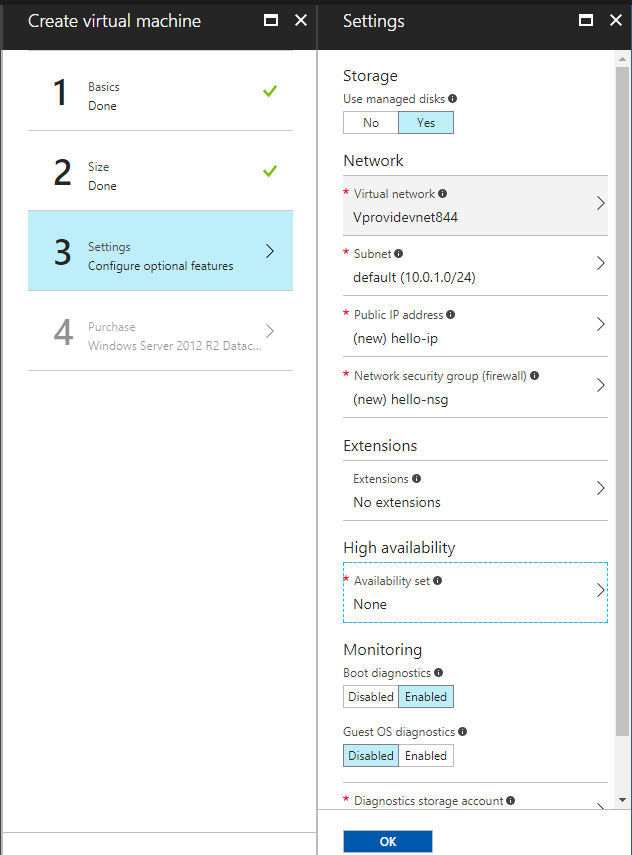


* 1. In the size, Select your machine based on the power you would be using. The more the powerful the machine the higher the cost. There is also an option between SSD and HDD.

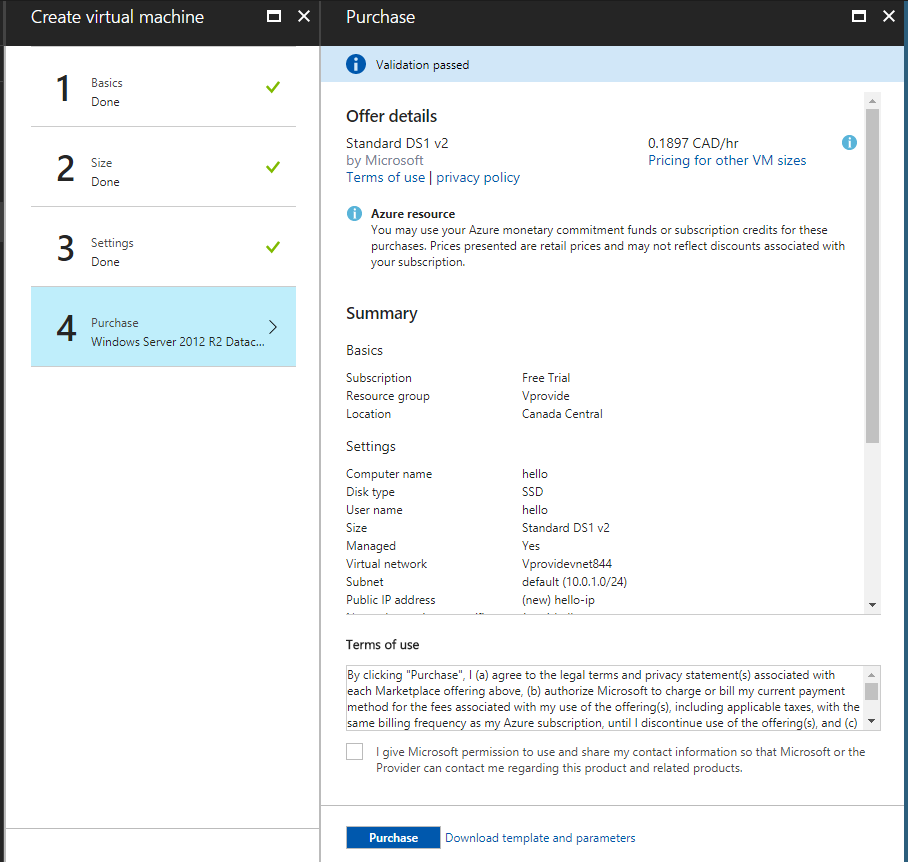


* 1. In the setting, you can configure optional feature.

1. Manage disk options allow you to virtually manage the disk or let azure do the managing of the disk. Things like fault tolerance and data redundancy is managed by azure if click yes.
2. Network options allows you to choose the virtual network you want to put the machine, its subnet, public IP address and network security group. If you want to keep them in a same network then you have to choose the same network for all the machines you want to be in the same network.
3. Extensions allows you to add features such as configuration management or antivirus.
4. High Availability provides redundancy to your application, we recommend that you group two or more virtual machines in an availability set. This configuration ensures that during a planned or unplanned maintenance event, at least one virtual machine will be available and meet the 99.95% Azure SLA. The availability set of a virtual machine can't be changed after it is created.
5. Monitoring allows you to capture boot diagnostics and Guest OS diagnostics.
6. All the metrics are written to a storage account which is called the diagnostic storage account.



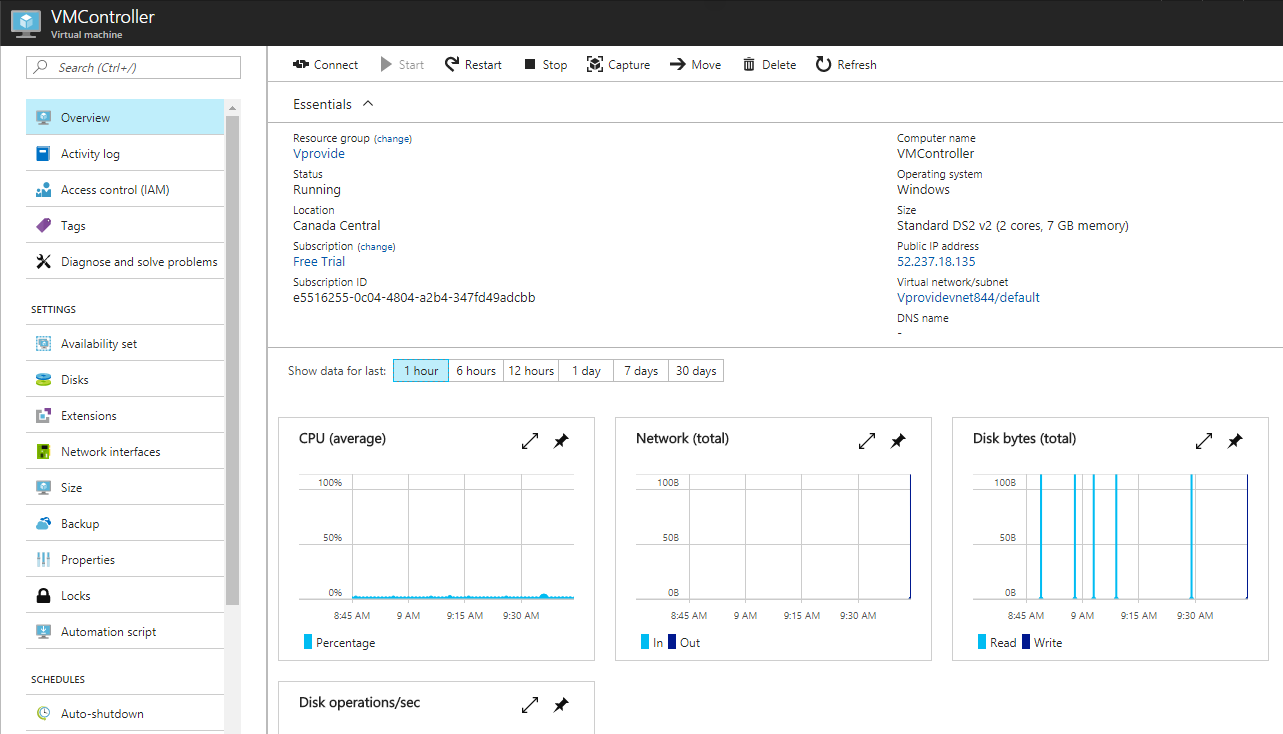
* 1. On the last page, you have to review all the criteria you selected for the vm and agree to azure term and click purchase.



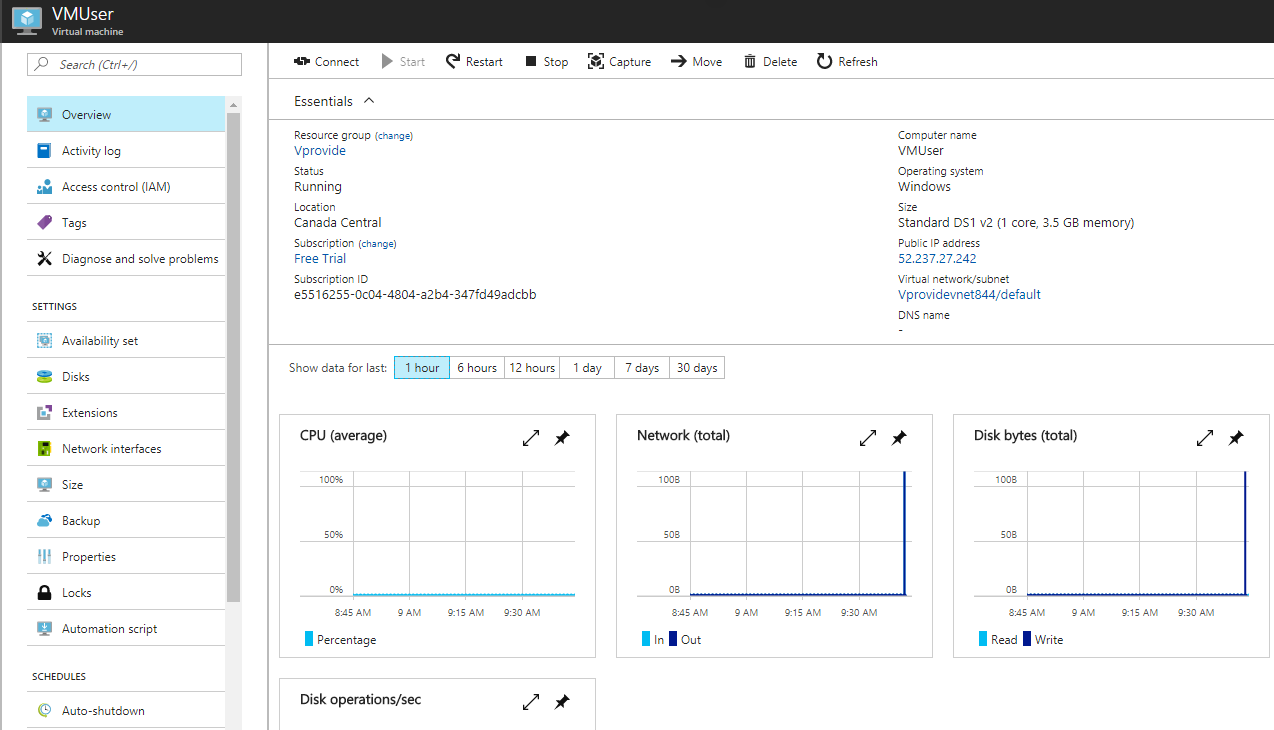
**Overview of our VMs and Virtual Network:**

Both of our VMs was assigned the same network so they can communicate between each other. They both have access to internet as well. Both have SSD hard drives and decent amount of power for what it will be used for. Domain controller Is named VMController and VM for users is called VMUser.

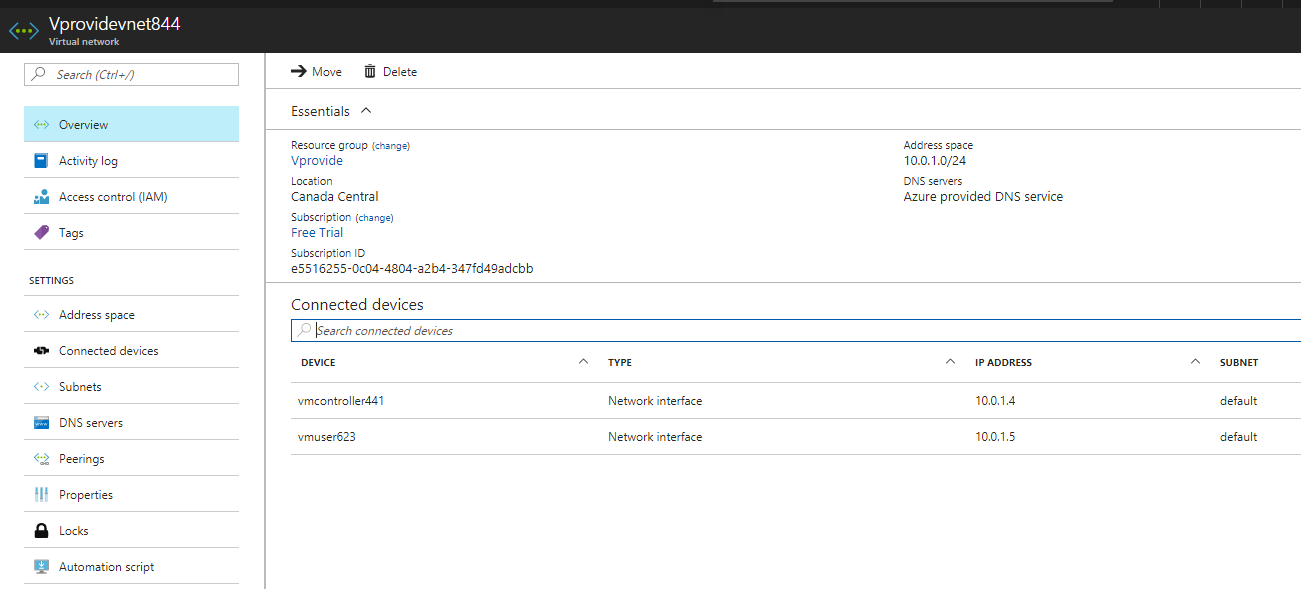
*Overview of VMController*



*Overview of VMuser*



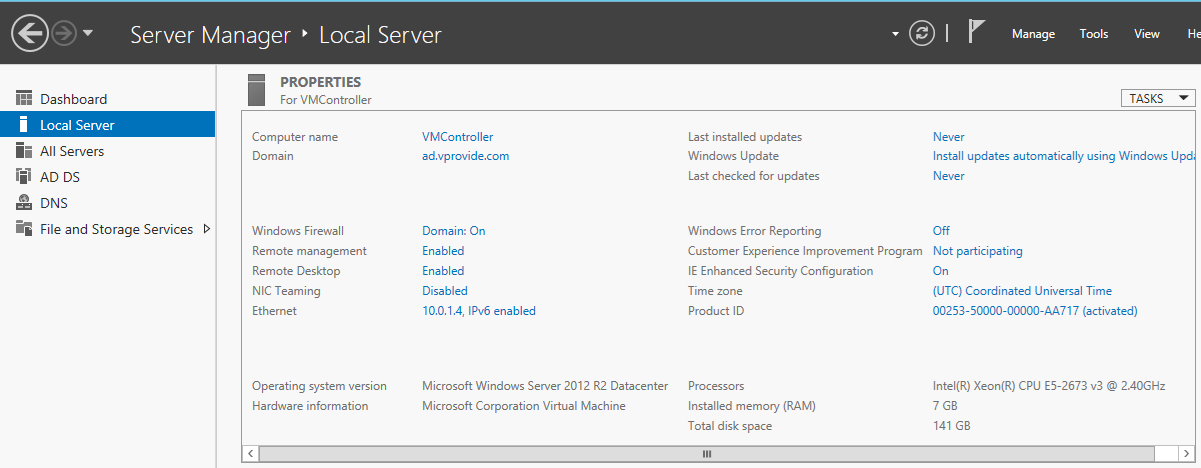
*Overview of Virtual Network*



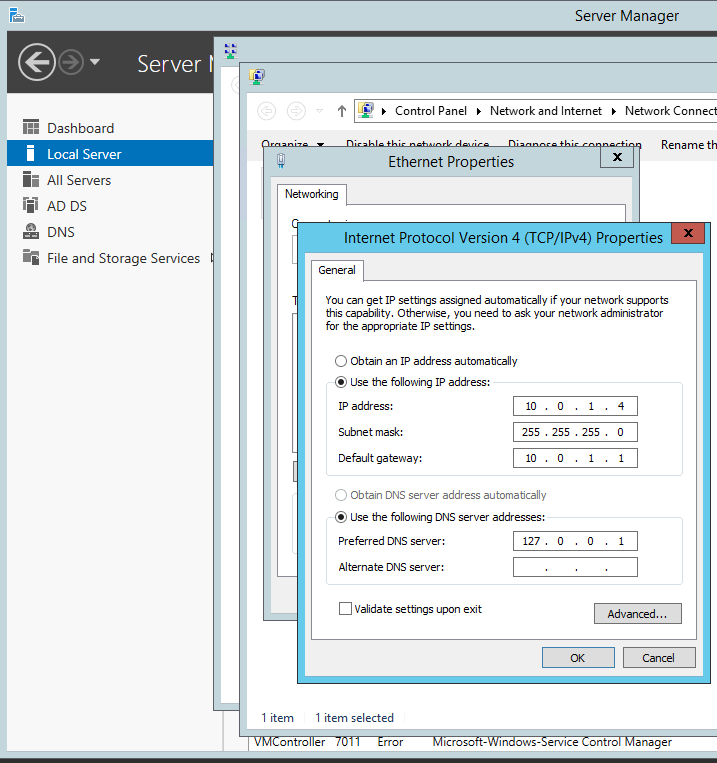
**Domain Controller and Connecting VM to Domain Controller:**

After the creation of both VMs, We first created a domain controller on of the VMs. Our Domain Forest was called ad.vprovide.com. We assigned a static IP for our domain controller so other VM can connect to it. We got this static IP from the command console using ipconfig /all. After changing to static IP the next step was to install Active Directory Services and upgrade the Server to Domain Controller. Once the domain controller was ready we joined the our other VM to the domain controller. We use the static IP of domain controller to be used as Static IP in DNS section of the VM and then joined the VM to the Domain Controller.

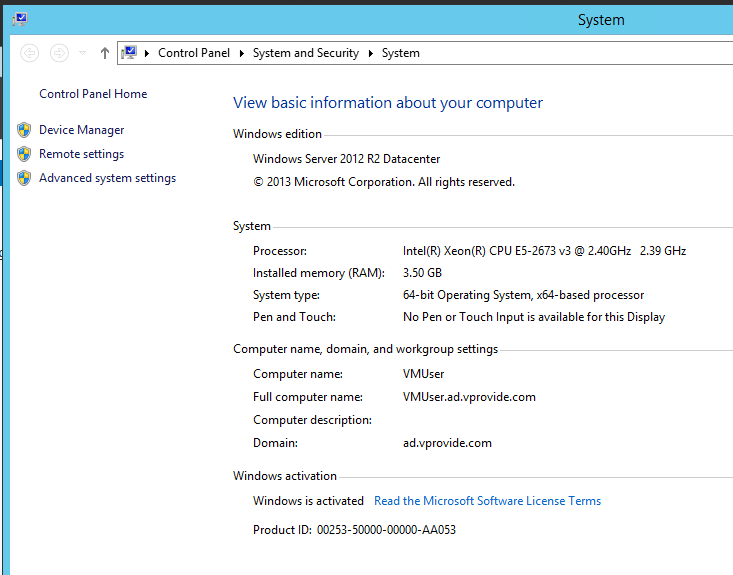
*Domain Controller Properties Window*



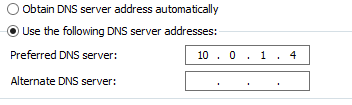
*Static IP Configuration – Domain Controller*



*VMs Computer Properties*



*VM static IP Configuration DNS Server*

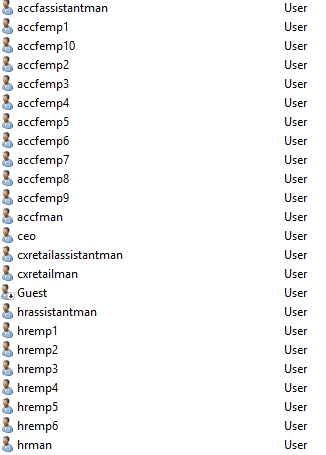


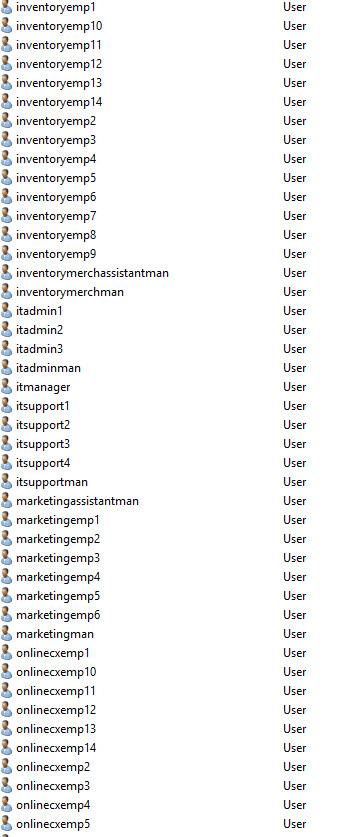
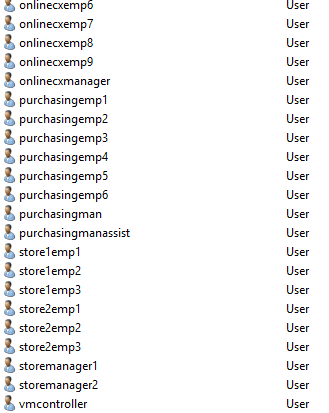
**Creating Users**

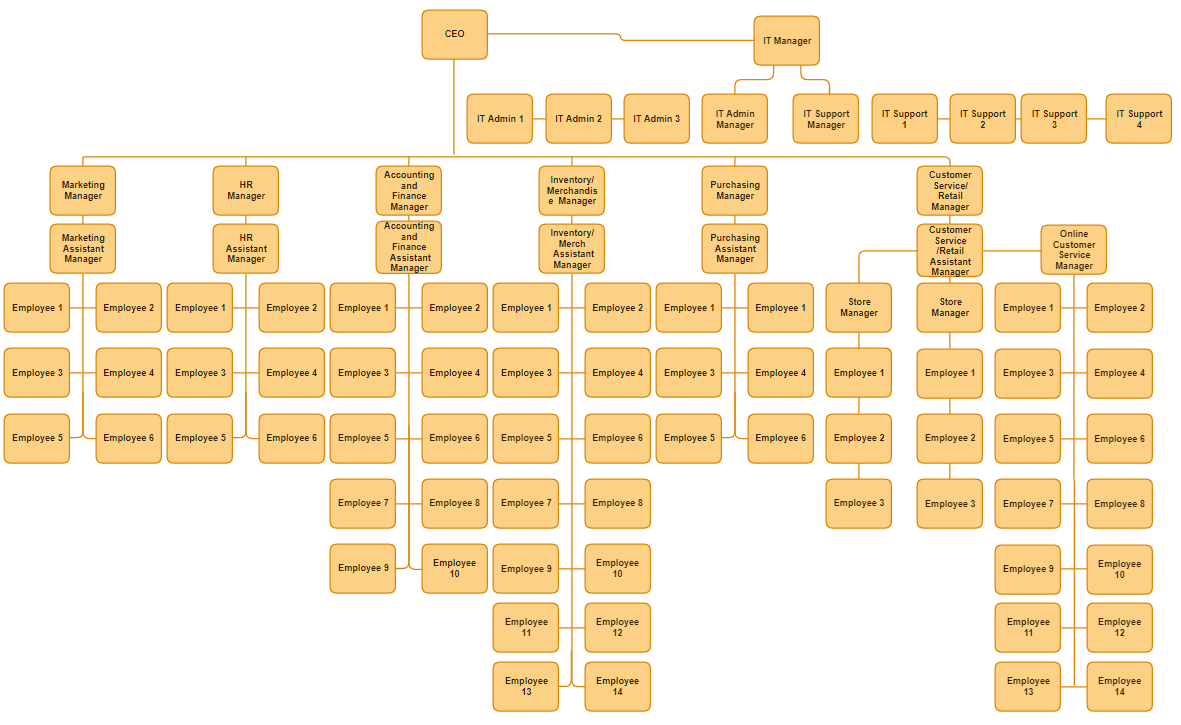
Our Next step was to create users based on our department structure. We decided that each department’s users will vary since the demand for the users of departments such as Inventory and Customer Service is much more compare to HR. We created a user chart to understand the managerial hierarchy and number of users and their roles in our company. We have seven departments as mentioned before and each department has its manager and assistant manager.

IT Department is divided into two sections support and admins. Admins control the infrastructure of the server network and Support provide day to day help to the employees regarding any technical issues. If any issue is above the tech support then they pass it to their admins. Customer Service is also divided into two parts. Customer service online which mean for people who want to chat or call us can do so and these agents would be able to help them about products. Store employees and managers handle the store service and sales.

***Users Created in Domain Controller and The User Chart***





****

**Create Groups, Domain Local Groups and Folders**

After making all the user accounts we turned our attention to the different folders departments will be sharing among them. We made a list of all the data we would need in our business and distributed them among folders. Some departments will have permissions to some folder and sometime a manager in that department will have permissions to more folders or only folder that he or she can access.

Furthermore, we thought about different permissions that are applied to department assigned to the same folder. Such as there is a department which has read only permission to a folder but another department has full access. We created a list of folders that are categorized by who will have access to them and what access they will have on these folders.

List of Folders Containing data:

**FOLDERS: (CEO has access to all folders and IT ADMINS(Domain Admins) have access to all folders except one)**

**ONLY CEO:**

1. Top Secret Company Information

**IT Admin – Manager:**

1. System Infrastructure Access
2. Network Infrastructure Access
3. IT Problem Reports
4. IT Guidelines – Full Access

**IT Admins:**

1. System Infrastructure Read Only
2. Network Infrastructure Read only
3. IT Guidelines – Full Access
4. IT Problem Reports

**IT Support:**

1. IT Guidelines – Read Only
2. IT Problem Reports

**Only Marketing Managers:**

1. Marketing Budget – Write/Read

**Marketing Department:**

1. Product Development

**Only HR Managers:**

1. Employee Information – Full Access

**HR Department:**

1. Removing an employee guideline

**Only Accounting and Finance Managers:**

1. Financial Statements

**Accounting and Finance Department:**

1. Receipts
2. Store Reports – Full Access

**Only Inventory/Merchandise Manager:**

1. Pricing and Inventory – Full Access

**Inventory/Merchandise Department:**

1. Inventory Reports

**Only Purchasing Manager:**

1. Suppliers Full Information

**Purchasing Department:**

1. Purchasing budget
2. Inventory Report – Read Only

**Only Customer Service/ Retail Managers:**

1. Store Reports – Read Only

**Customer Service/ Retail Department:**

1. Receipts – Read Only
2. POS System – Read-only

**All Employees:**

1. Employee Discount – Read Only

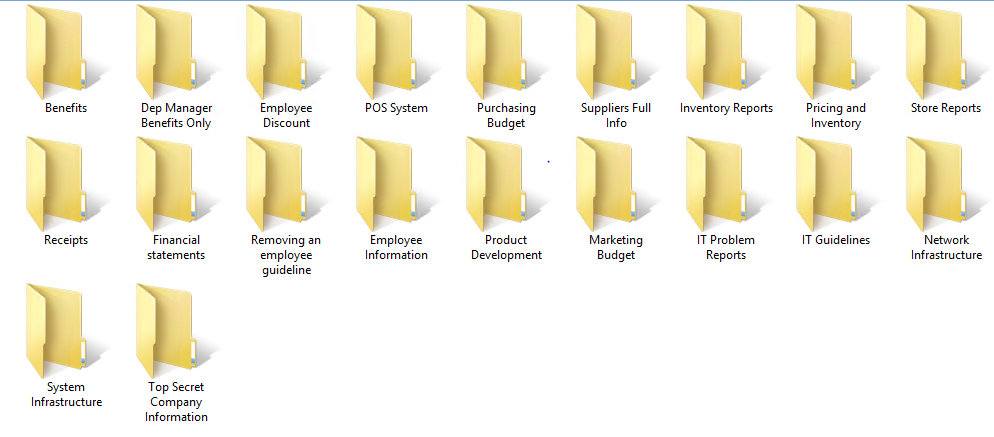
**Department Managers**

1. Department Manager Benefits Only – Read Only

**Assistant and Store Managers**

1. Benefits – Read Only

*Folders Created*

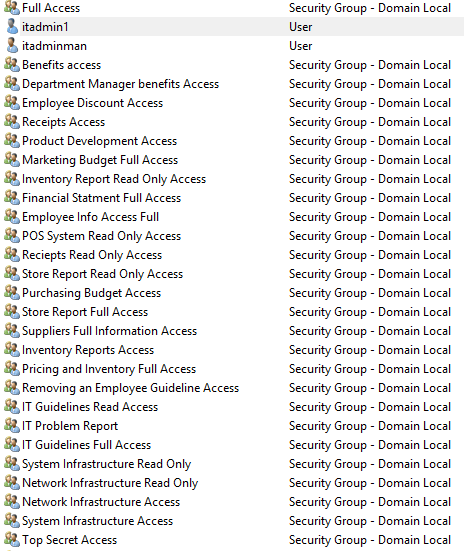


After organizing data in our folders we created groups and domain local groups so we can easily manage permissions to these folders. We created domain local group for each access folder and sometimes when the permissions in each folder have to be divided into read only and full access then for that folder we created domain local groups so we can assign them different permissions based on their criteria. We created groups for all employees, each department, each department managers, it support etc.

**Domain Local Groups:**

1. Full Access – Complete Access(It has permission for full access from every folder)
2. Top Secret Access – Only for CEO
3. System Infrastructure Access
4. IT Guidelines Full Access
5. IT Guidelines Read Access
6. IT Problem Reports
7. Marketing Budget Full Access
8. Product Development Access
9. Employee Info Access Full
10. Removing an employee guideline Access
11. Financial Statements Access
12. Receipts Access
13. Receipts Read Only Access
14. Store Reports Full Access
15. Store Reports Read Only Access
16. Pricing and Inventory Full Access
17. Inventory Reports Access
18. Inventory Reports Read Only Access
19. Suppliers Full Information Access
20. Purchasing Budget Access
21. POS System Read Only Access
22. Employee Discount Access – ALL Employees
23. Dept Manager Benefits Access – Only for Dept Managers
24. Benefits Access – For Only Assistant managers and Store Managers

*Domain Local Groups*



**Groups: (with Users)**

1. Admins – All IT admins
2. Department Managers – ALL Department Managers
3. Assistant Managers and Store Managers – All Department Managers (Assistant) and Store Managers
4. Employees – Every Single Employee
5. IT Support – Only IT Support
6. IT – IT Department – All IT admins and support
7. IT Managers – All IT managers
8. Marketing – Marketing Department
   1. Marketing Managers – Only Marketing Manager and Assistant Manager
9. HR – HR Department
   1. HR Managers – Only HR Manager and Assistant Manager
10. Accounting and Finance – Accounting and Finance Department
    1. Accounting and Finance Managers – Only Accounting and Finance Manager and Assistant Manager
11. Inventory/Merchandise - Inventory/Merchandise Department
    1. Inventory/Merchandise Managers – Only Inventory/Merchandise Manager and Assistant Manager
12. Purchasing – Purchasing Department
    1. Purchasing Managers – Only Purchasing Manager and Assistant Manager
13. Customer Service/ Retail – Retail and Customer Service Department (Three Groups)
    1. Store Managers
    2. Store Employees
    3. Online Customer Service Employees

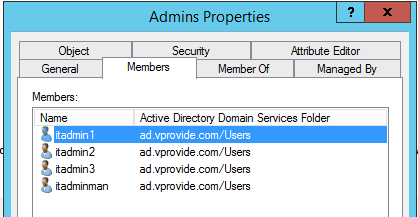
*Groups Created*



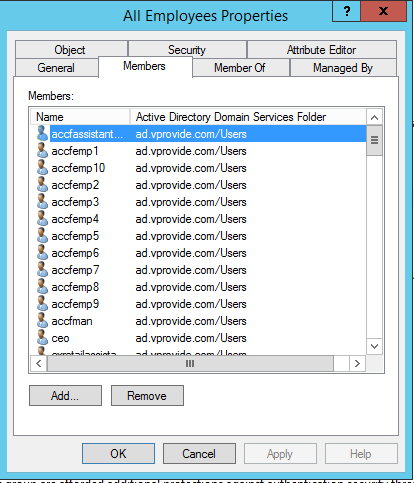
After finishing up all the groups users and domain local groups. We started sorting the users in the groups and groups into domain local groups to provide the right access to the folders created.

***Some example of groups***

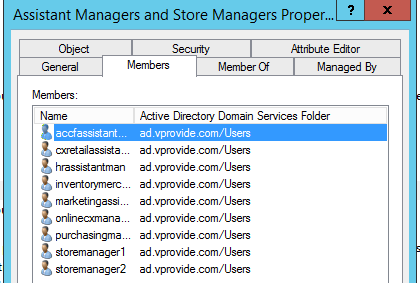
*Admins*



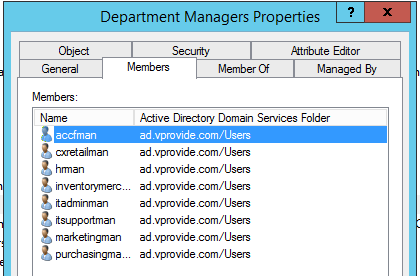
*All Employees*



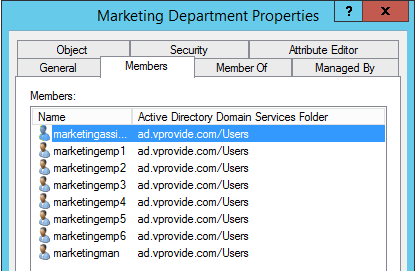
*Assistant and Store Managers*



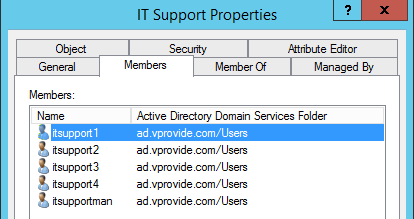
*Department Managers*



*Marketing Department*

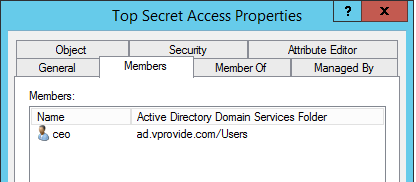


*IT Support*

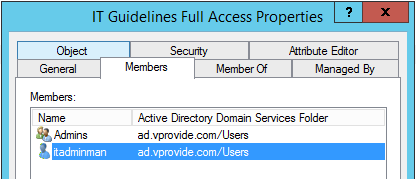


***Some Example of Domain Local Groups***

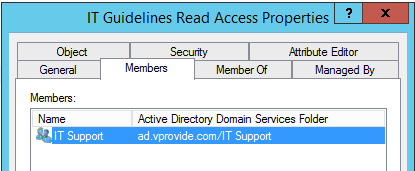
*Top Secret Access*



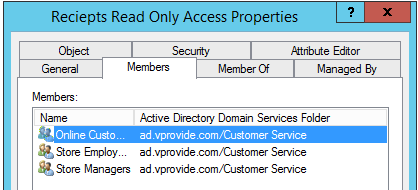
*IT Guidelines Full Access*



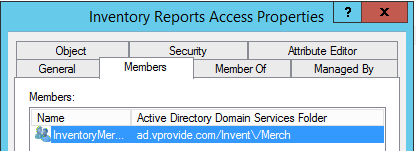
*IT Guidelines Read Access*



*Receipts Read Only Access*

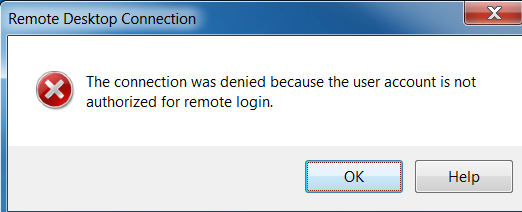


*Inventory Reports Access*



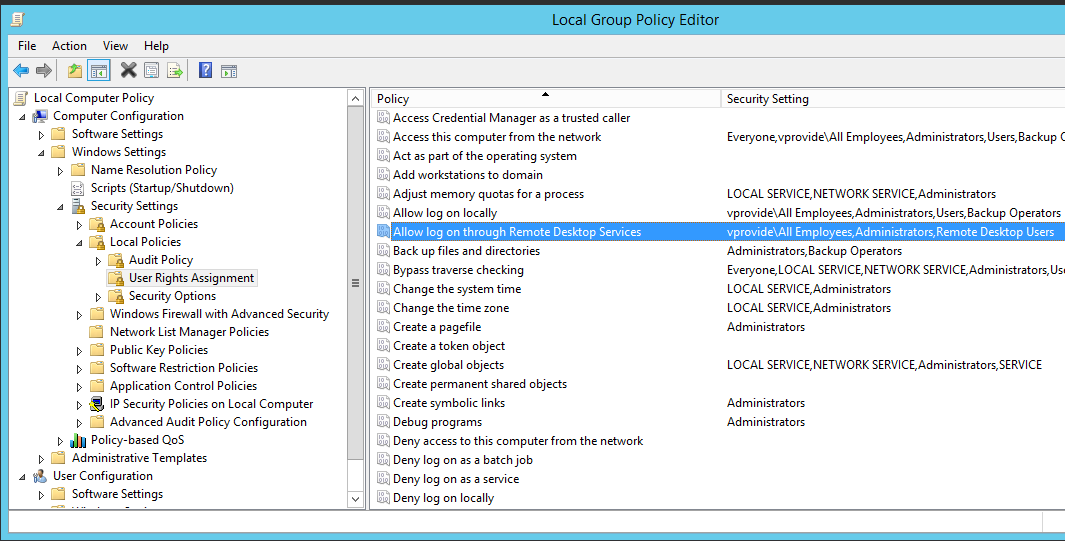
**Connecting the VM to Controller**

After creating the groups our next task was to make sure we could login using our VM to our accounts in controller. We first tried with the account of CEO and it wouldn’t allow us to login it kept giving us this error.

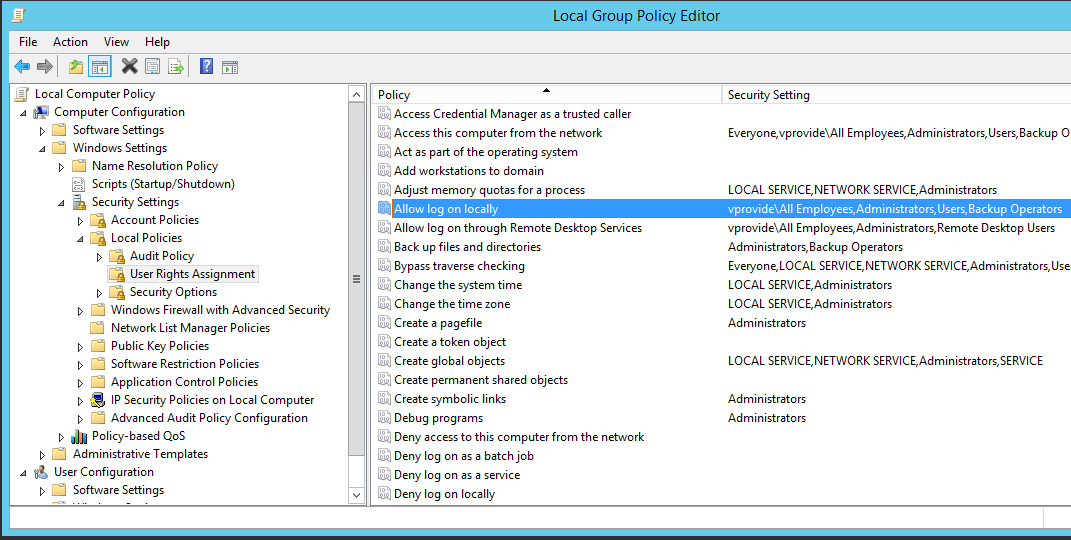


We had to login on our VM as an administrator and make some changes to allow the computer to sign in with any account using a remote connection. The very first thing we did is we went to the local policy settings and change the policy of allowing remote desktop connection by adding all domain users to it. Then we allowed all employees to log on locally. After trying it again with a different user the login was still giving the same error connection denied due to unauthorized account used for login. After searching for a solution we were able to get the solution by going to Control Panel > System and Security > System > Advanced System Setting > Remote > Select Users and add all employees so they can access this machine remotely.

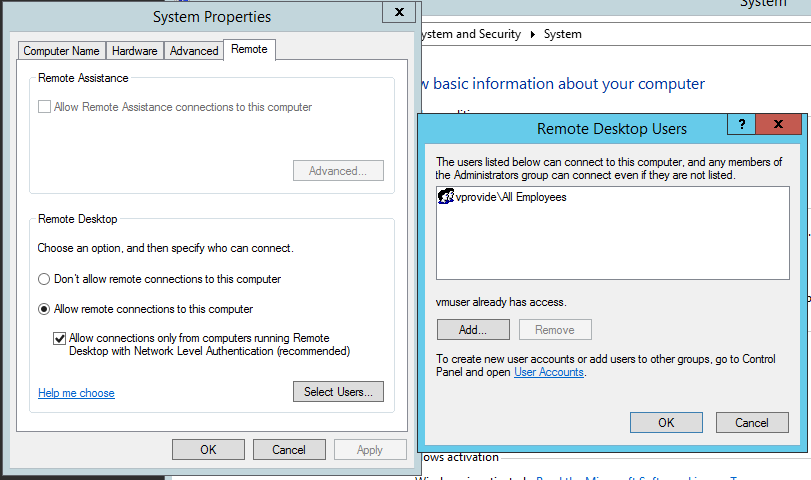
*Allow log on through Remote Desktop Services*



*Allow log on locally*

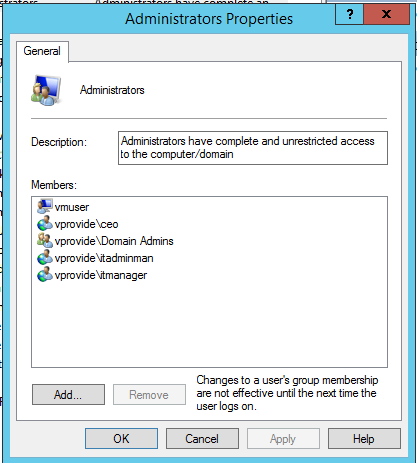


*Add Users for Remote Login*



Next Step was to add CEO, IT Manager, IT Admin Manager as administrators for this VM. We changed that in local users and groups. We went to groups and added administrators.

*Adding Administrators to the VM*

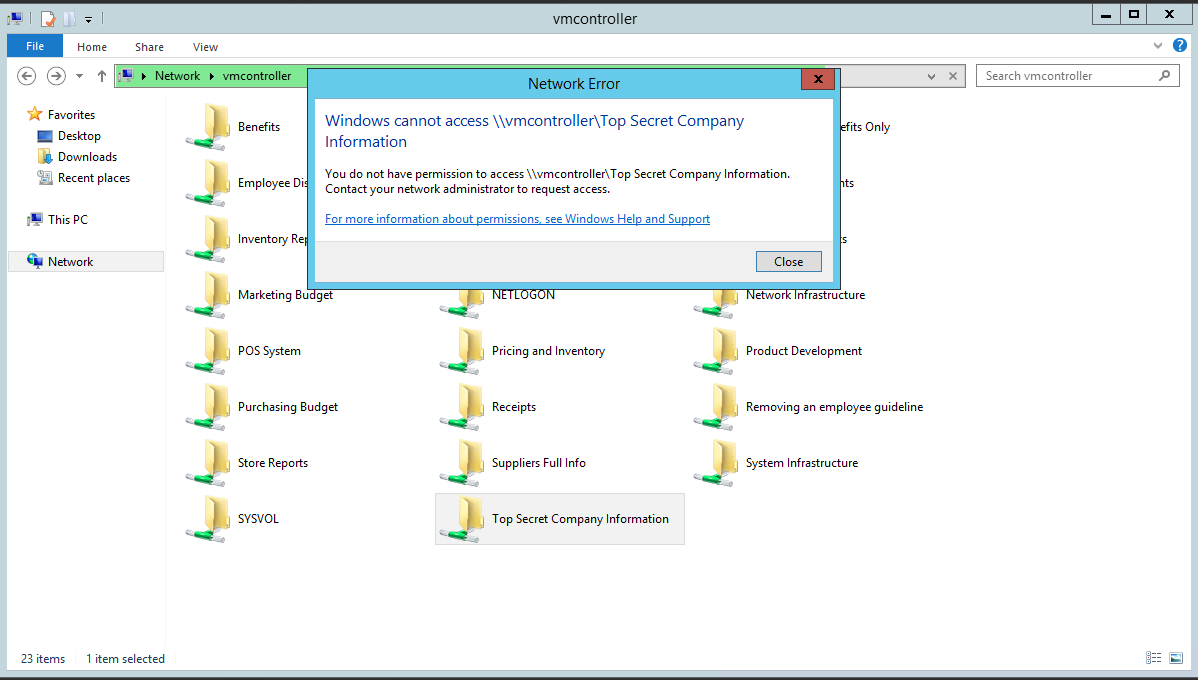


**Folder Access Check:**

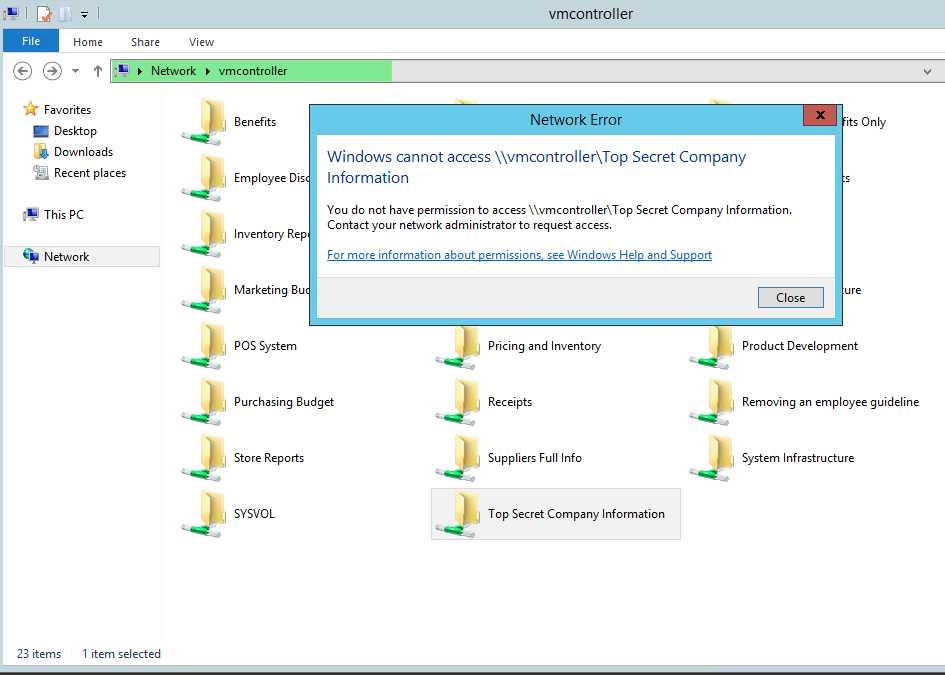
Our next objective is to make sure the folders are shared properly and the certain user has the right access.

*Checking Top Secret Folder with users itadmin itmanager and ceo.(in that order)*

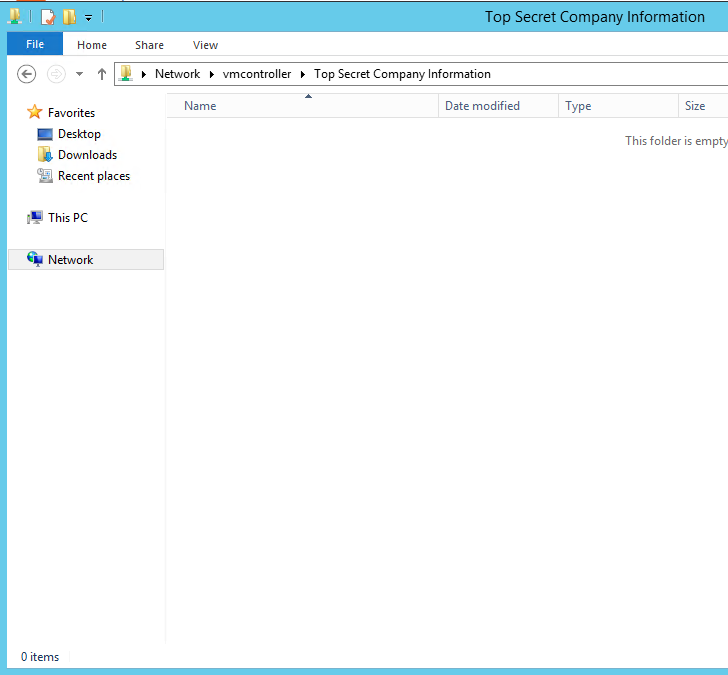
*Logged as itmanager*



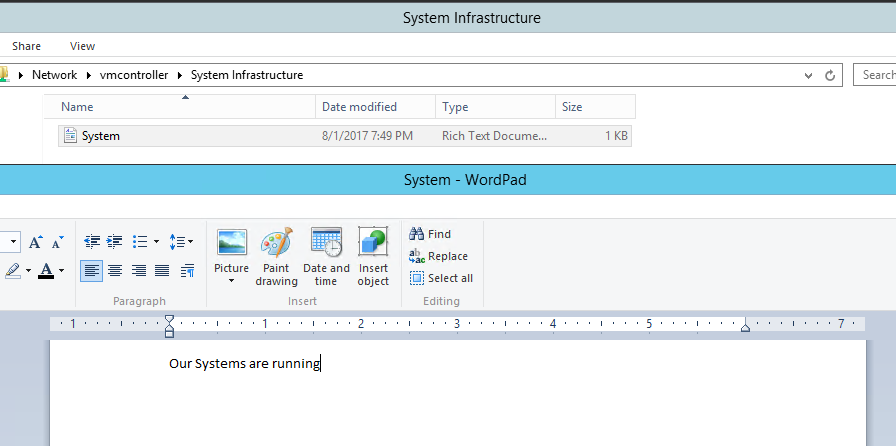
*Logged as it admin*



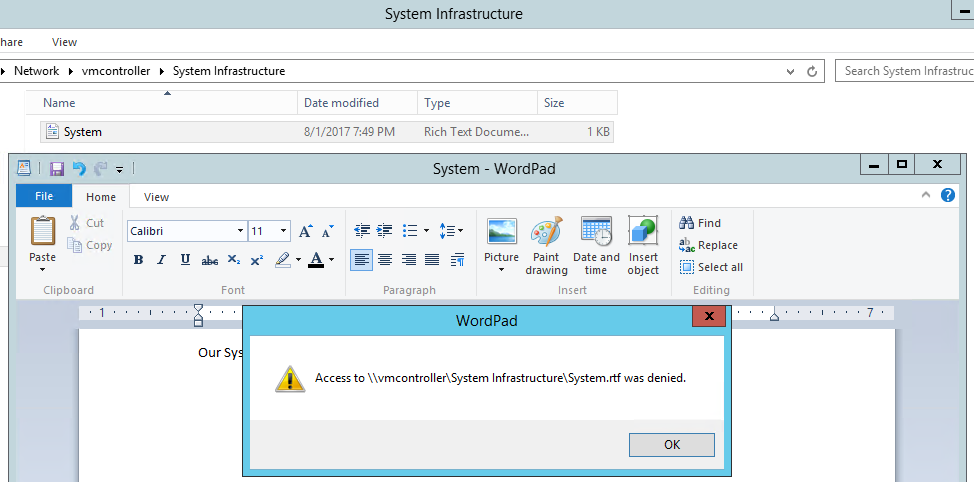
*Logged as ceo*



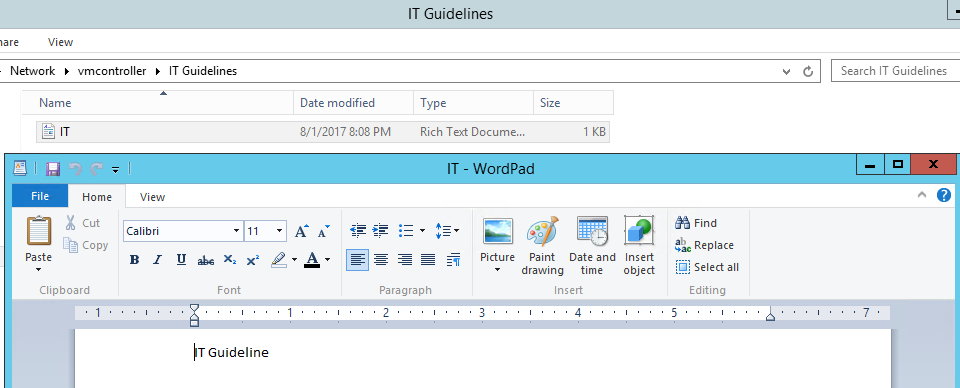
*System infrastructure logged in as IT Manager – Full Access*



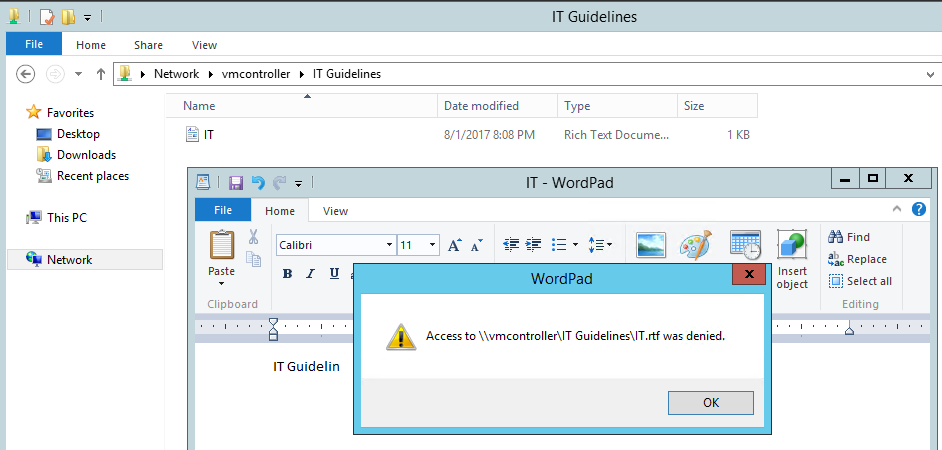
*System infrastructure logged in as IT Admin 2 – Read Only Access*



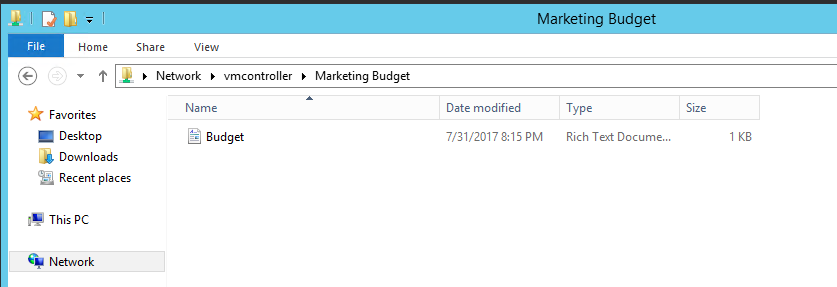
*IT Guidelines logged in as IT admin 2– Full Access*



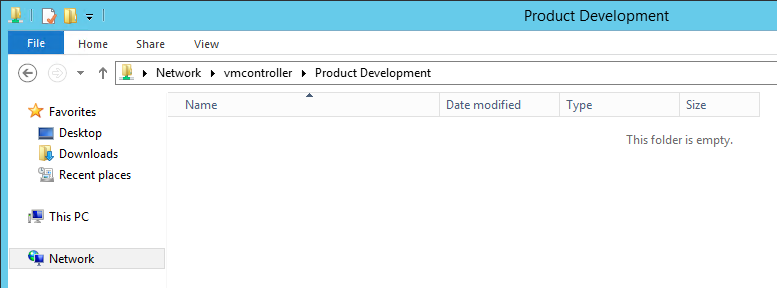
*IT Guidelines logged in as IT Support – Read Only*



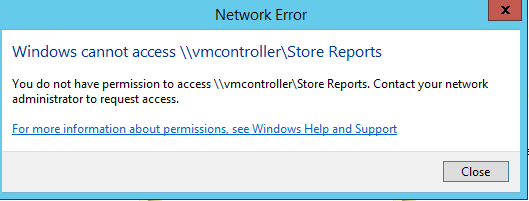
*Marketing Budget logged in as Marketing Manager*



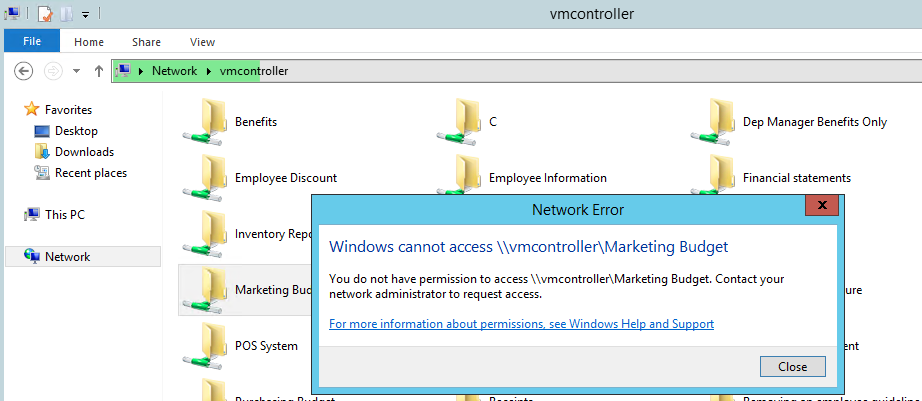
*Product Development logged in as Marketing Manager*



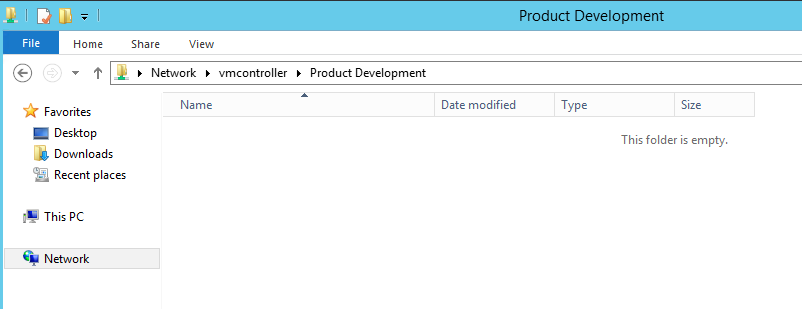
*Store Reports logged in as Marketing Manager*



*Marketing budget logged in as Marketing Employee*



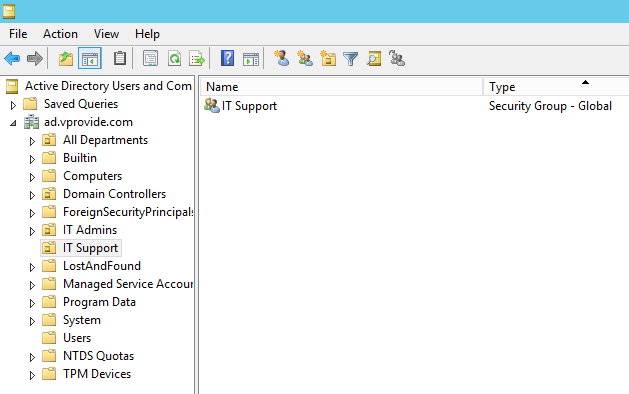
*Product Development logged in as Marketing Employee*

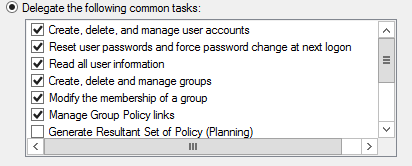


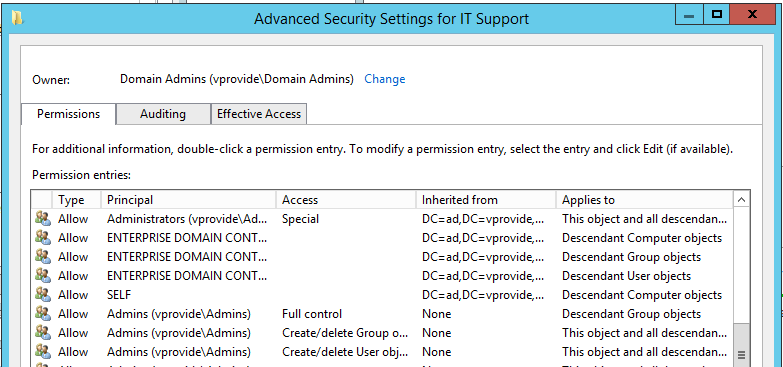
**Organization Units and How it will be administered.**

Since we had IT Admins we wanted them to able to have some control over the department users except IT users. We created three different Organizational Units to delegate control and to apply group policy objects.

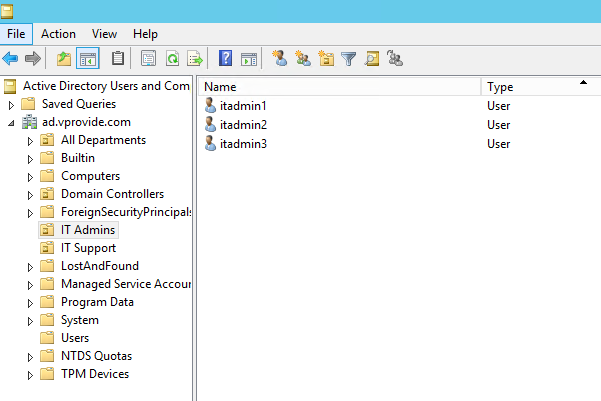
1. IT Support – Administered by Admins

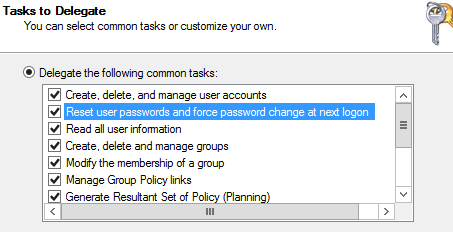


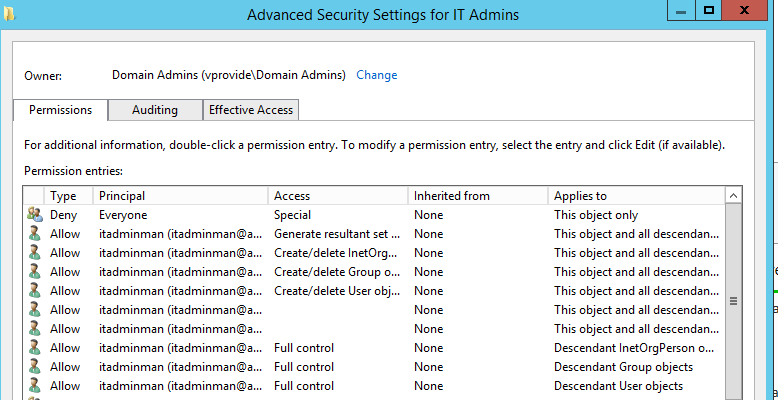




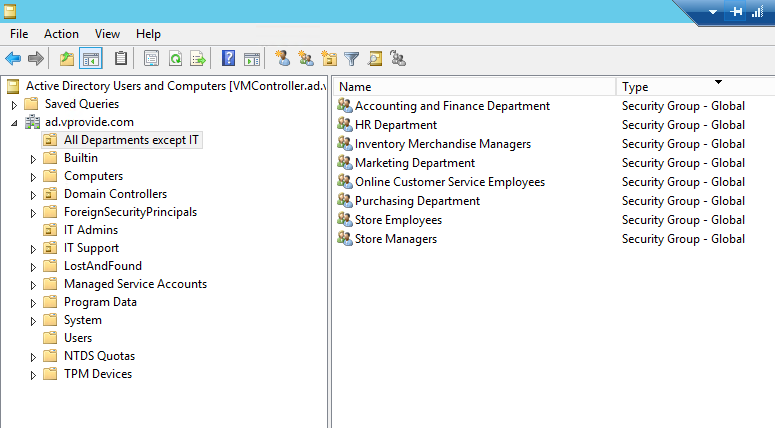
1. IT Admins– Administered by IT Admins Manager



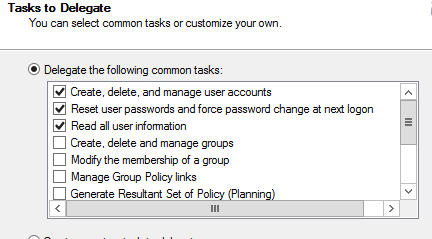




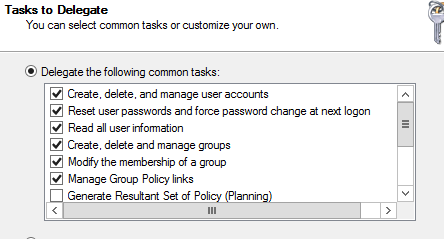
1. ALL Departments except IT Department by IT Admins and IT support



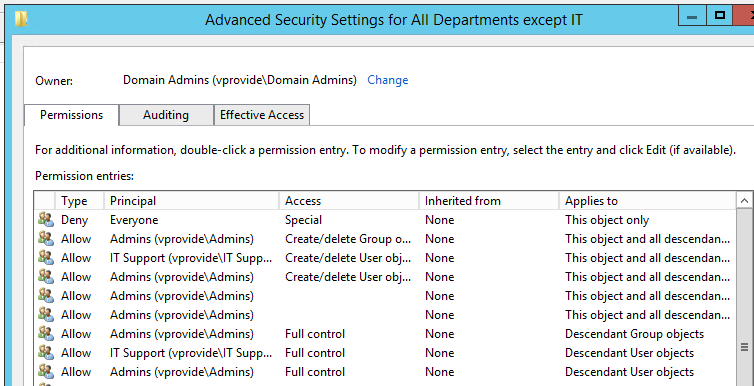
IT Support Control



IT Admin Control



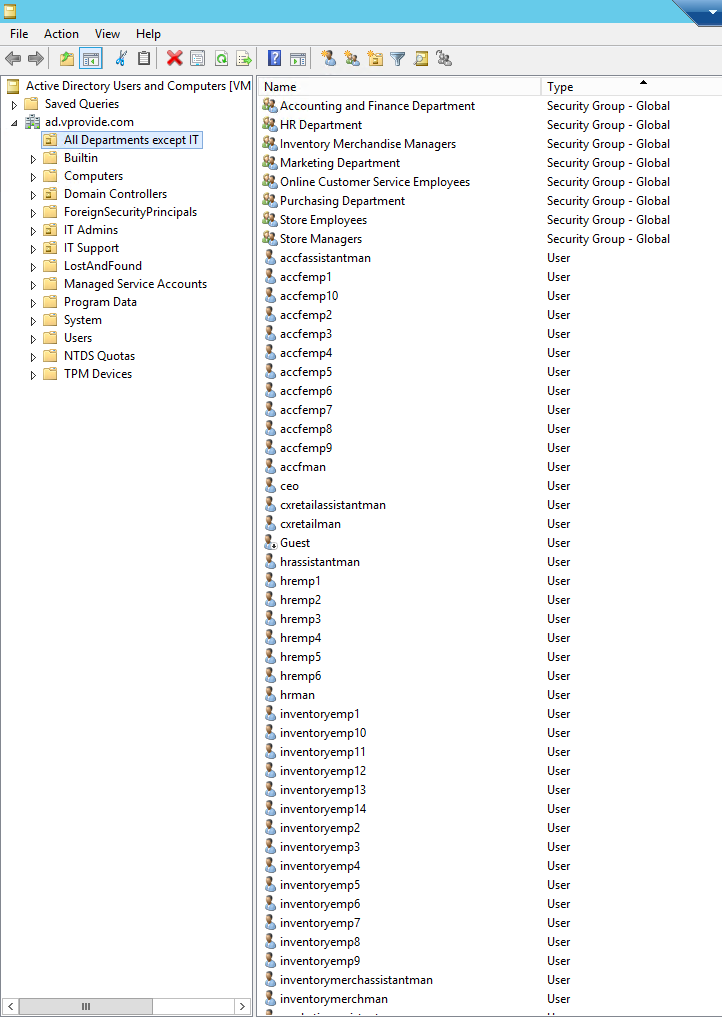
Advanced Security Settings for All Departments except IT



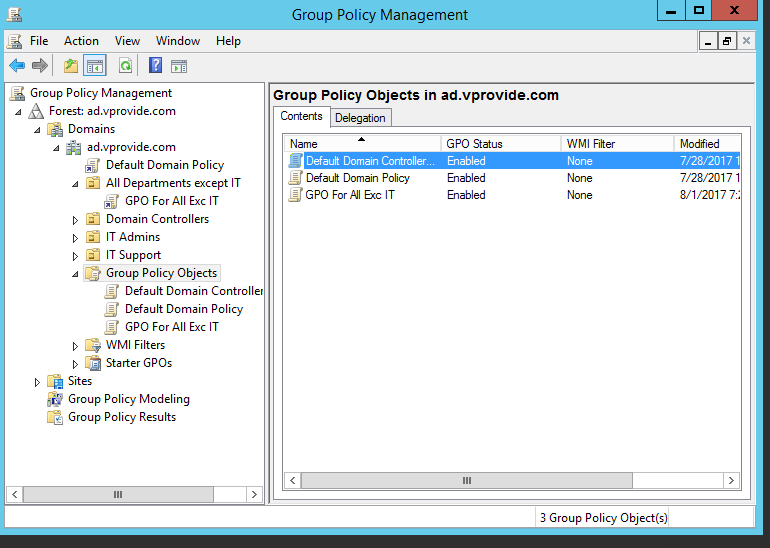
**Group Policy Objects for all departments except IT**

We decided to add group policies for all the employees except the CEO and It department so they can be restricted on their user accounts. When we created the OU (All Departments except IT). We added groups in it so we can assign administrators, but now since we need to apply group policy object we need to add all the users we want this GPO to be applied to.

*Adding all users for GPO*



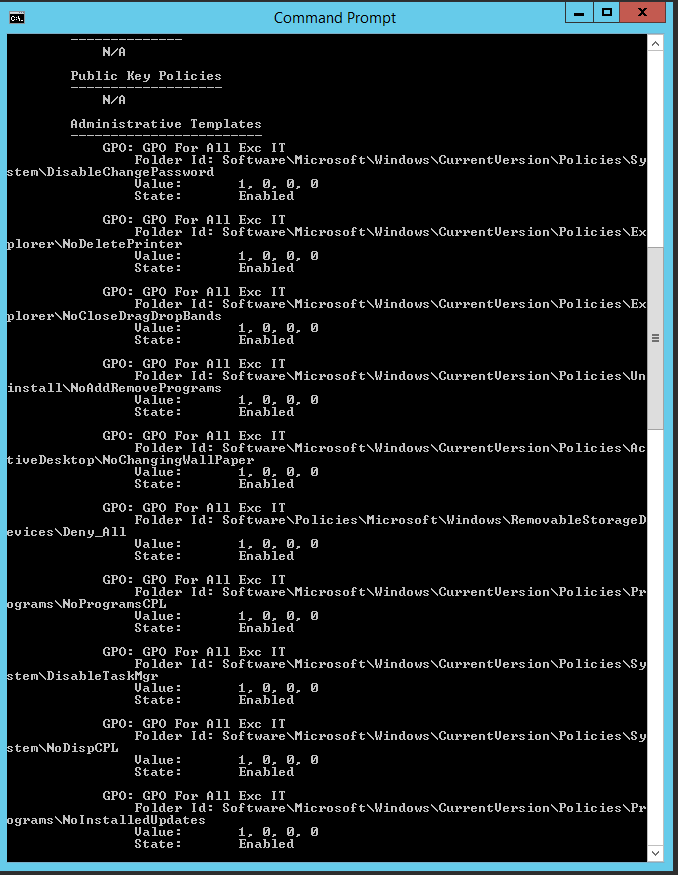
*GPO Created and Linked to the OU*

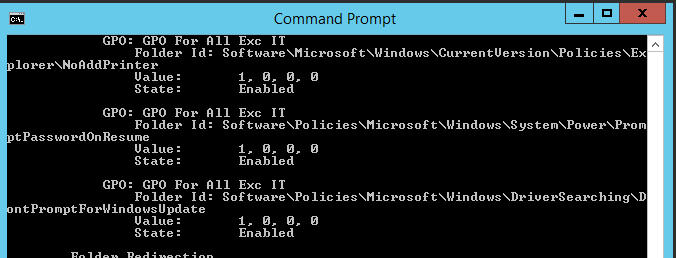


*Group Policies in this OU*

1. Remove Task Manager
2. Remove Change Password
3. All Removable Storage classes: Deny All Access
4. Prompt for Password on resume from hibernate/suspend
5. Disallow changing of georgraphic location
6. Turn off Windows Update device drive search prompt
7. Remove Add or Remove Programs
8. Disable The Display Control Panel
9. Prevent changing desktop background
10. Prevent addition of printers
11. Prevent deleteion of printers
12. Hide Installed Updates
13. Hide Programs Control Panel
14. Prevent adding,dragging,dropping and closing the Taskbar toolbars

*Screenshot of GPO Applied*





**Comparison to Other Cloud Based Services**

**Microsoft Azure**

* **Description**
  + Azure Active Directory is a comprehensive, access management, highly available cloud solution that provides core directory services, advanced identity governance, and application access management. Azure Active Directory also offers a platform that enables developers to deliver access control to their applications, based on a set of policies and rules.
* **Pricing**
  + Basic
    - $1 user/month
  + Premium P1
    - $6 user/month
  + Premium P2
    - $9 user/month
* **Free Trial**
  + One month trial
  + Full access to features for the duration of one month
* **Service**
  + Features
    - Single sign-on to any cloud app, which simplies user access
    - Pre-integrated with Salesforce.com, Office 365, Box and more
    - Enforce Multi-Factor Authentication with SaaS to protect sensitive data and applications
    - Easily extend Active Directory to the cloud
    - Works with multiple platforms and devices
    - Integrate with on-premises Active Directory
    - Use single sign-on to extend Active Directory and any other on-premises directories with Azure AD
    - Enterprise Scale and SLA
    - Enable self-service for your employees by delegating tasks to employees

**Amazon Web Services Directory Service (AWS Microsoft AD)**

* **Description**
  + AWS Microsoft AD enables directory-aware workloads and AWS resources to use managed Active Directory in the AWS Cloud. Since Microsoft AD is built on Microsoft Active Directory, it does not require one to synchronize or replicate any data from an existing Active Directory to the cloud, making it easy to migrate to AWS Microsoft AD.
* **Pricing**
  + AWS Directory Service for Microsoft Active Directory
    - $0.40 per hour
      * Includes two domain controllers for high availability, each billed at $0.20 per hour, totalling $0.40.
    - For each additional domain controller, it is $0.20 per hour.
  + Simple AD
    - Small is $0.05 per hour
    - Large is $0.15 per hour
  + AD Connector
    - Small is $0.05 per hour
    - Large is $0.15 per hour
* **Free Trial**
  + For 30 days, the free trial provides you with 1,500 hours of use across all your Directory Service managed directories. There are certain types of managed directories that are eligible for the AWS Directory Service free trial
    - AWS Directory Service for Microsoft Active Directory
    - Simple AD
    - AD Connector
* **Service**
  + Has the standard Active Directory administration tools as well as built-in Active Directory features such as Group Policy, trusts, and single sign-on.
  + Benefits include:
    - Easily migrate your current AD-dependent, on-premise applications and workloads to the AWS Cloud without synchronizing or replicating data from an existing Active Directory.
    - Use actual Microsoft Active Directory instead of a similar service
    - Share a single directory for cloud workloads
    - Easily extend existing domains
    - Administer on-premises resources, such as computers, laptops, and printers, from the cloud.
    - Simplify administration with a managed service.
      * No more installing software as AWS handles all patching and software updates.
      * Detects and replaces domain controllers that fail.
      * Data replication and automated daily snapshots are configured for you.

**Jumpcloud (Directory-as-a-Service DaaS)**

* **Description**
  + Jumpcloud is an alternative to Microsoft Active Directory.
    - They provide help to clients when migrating from Active Directory to Jumpcloud
  + Jumpcloud’s Directory-as-a-Service (DaaS) is a cloud-based user store that enables IT admins to securely connect and manage users with the applications, devices, and networks users need to access. DaaS uses a variety of protocols to ensure that organizations can control and manage a variety of IT resources.
* **Pricing**
  + Startup
    - Up to 10 users
    - Free forever
  + Professional
    - 11 users and beyond
    - Month-to-month is $10 / user per month
    - Annual billing is $7.50 / user per month
    - Minimum of 10 paying users required for the paid plan
* **Service**
  + Features
    - Mac OS X, Windows, and Linux User and System Management
    - Supports a variety of authentication protocols such as LDAP, SAML, RADIUS, SSH, and JumpCloud’s REST API
    - LDAP-as-a-Service
    - RADIUS-as-a-Service
    - Policy Management and Script Execution
    - REST API
    - End User/Employee Self Service
    - Password Complexity Management
    - One-Click Application Access
    - Microsoft Active Directory Bridge
    - G Suite User Provisioning & Sync
  + Benefits
    - IT resources allow users to be securely connected
    - On-premise IT and cloud resources are supported
    - Users can be systematically provisioned/deprovisioned with a single click
    - Strong hashing algorithms, multi-factor authentication capabilities, and logging allow for more enhanced security
    - End users will never be denied access to applications, systems, or IT resources due to automated load balancing, elastic scaling, and redundancy
    - Zero installation or server configuration and no management overhead
    - Easy compliance and auditing with JumpCloud’s logging system

**Comparison**

* **Pricing**
  + The pricing for Azure Active Directory and Jumpcloud are somewhat similar, though Azure AD has 3 different levels. Azure AD’s Premium P2 is $9 user/month, while Jumpcloud’s Professional is $10 user/month or $7.50 user/month if paying annually. Therefore, it terms of pricing Jumpcloud has the edge, though Jumpcloud is an alternative to Active Directory and may not contain all the same features.
  + Amazon Active Directory is priced based on hourly use of domain controllers ($0.20 per hour), making it difficult to compare to the other two.
* **Free Trial**
  + Both Azure Active Directory and Amazon Active Directory have one month free trials, both with access to the full features. However, Amazon’s is limited to 1,500 hours while Azure’s isn’t.
  + Jumpcloud’s free trial is free forever; however, it is limited to 10 users and under. It’s good for startups, and trying it out, but it’s not as useful for a larger business with many users, as a larger business would not be using Jumpcloud forever with only 10 users.
* **Service**
  + Both Azure Active Directory and Amazon Active Directory share a lot of the same features, emphasizing single sign-on, security, extending Active Directory, cloud services, and remote access. Since they do provide a lot of the same features, it’s best to compare costs instead.
  + Jumpcloud also possess a lot of similar features as well, but it’s not Active Directory. If the business is comfortable with Active Directory and does not want to make the switch, it may be best to stick with Azure Active Directory or Amazon Active Directory. Fortunately, migrating from Active Directory to Jumpcloud is easy for those wanting to try something new, especially since Jumpcloud helps their clients make the switch.