Austin Pierce – CITC-2320 PC7

Plan of Action

1. Download and configure **Windows Server 2019**.
2. Initial Server Configuration
   1. Collect and clear logs from event viewer before further configuration.
   2. Set password policy to allow for short password.
   3. Set static IP address.
   4. Continue server specific maintenance and first boot tasks including:
      1. Power scheme settings.
      2. Set correct time zone.
      3. Configure “No Memory dump” on system failure.
      4. Defragmenting drives.
      5. Keyboard settings to allow for Spanish keyboard.
   5. Create local admin account before promotion to domain controller.
3. Promote to DC:
   1. Export list of users and groups into HOHOHO LOGS folder.
   2. Users file should be “HOHOHO-USRS1-B4DC”
   3. Groups file should “HOHOHO-GRPS1-B4DC”
   4. Save event viewer logs.
   5. Finally promote to DC.
4. Configure the server to act as a file server.
5. Add new drives to server per specification.
   1. Create F Drive- 2GB Label “FILES” (Dynamically allocated)
   2. Create H Drive- 3GB Label “HOMES” (Dynamically allocated)
   3. Create N Drive -1GB Label “WORK” (Dynamically allocated)
   4. Create S Drive – 2GB Label “SECURE” (Dynamically allocated)
   5. Create P Drive – 2GB Label “LIMITED” (Dynamically allocated)
6. Create and share requested folders with specified access for each group/user.
   1. In C: create folder DNLDS – Not shared
   2. In F: create folder “HOHOHOCO” – Shared.
      1. Shared with all authenticated users local and remote with full access.
      2. Shared with HOCO-04 name
   3. In F: create folder “Windows NT Compressed Folder” named “HOHO-COMPRESSED.
   4. In F: create NTFS Encrypted folder named “HOHO-SECURE”.
   5. In F: create “Group Common Areas” for each department.
   6. In N: create folder “ WORKING” and share as “work” for all authenticated local and remote users.
      1. Ensure users who create files are the only ones allowed to delete them.
   7. In S: create ensure it is only accessible by managers, executives, and sys-admins.
      1. Managers can ONLY read files.
      2. Log all access to files in folders in S drive.
   8. In P: ensure only managers, executives, and sys-admins can read, write, delete, etc files and folders.
      1. No user is allowed to save more than 50MB of data.
      2. Log any data over 45mb.
7. Create web server and add custom webpage.
   1. Web page must contain company name, address, phone number, and other relevant company information.
   2. IP will be IP of web server and should be accessible via domain name as well.
8. Create Users, Groups, and OUs in active directory.
   1. Active Directory:
      1. Add company information into active directory like phone number, address, etc.
   2. Create groups.
      1. IT, Mgrs, Executives, Finance, Sales, Production, Custodial, Quality, HR, Physical, Café, Marketing, Engineering, Education.
      2. Names must be limited to 12 characters or less.
   3. Create Users from full user list.
      1. Usernames must be 12 characters or less.
      2. LastNameFNx format.
      3. Initial password of “pw”
      4. “Ho Humm”
         1. Must change password at next login
      5. “Ho Uckup” & “Ho Micidel”
         1. Can never change his/her password
   4. OUs
      1. OU\_”Groupname” for each group.
      2. DG\_”department” for each department group.
9. Create user management script to handle automation.
   1. This will be a PowerShell script.
10. Configure Privileged users:
    1. Ho Lottmore & Ho Umpaige & Ho Mee
       1. Can administer accounts with limited functionality.
    2. All IT Staff
       1. Domain Admin
    3. Ho Malone
       1. Backup Admin
    4. Ho Uldme
       1. Printer admin
11. After DC promotion logging:
    1. Capture users, groups, and event view logs.
       1. Add “-AFTERDC” suffix to file names.
12. Configure Active Hours:
    1. Supervisors, Managers, Executives, and IT staff.
       1. Can log-on after 9pm Monday-Friday & weekends.
13. Special rules in regards to login:
    1. Configure server to expire passwords after 120 days post password change.
    2. Users cannot use the same password for 2 iterations.
    3. Lockout after 9 attempts for 1 minute
    4. IT:
       1. Passwords expire after 60 days.
       2. Lockouts after 3 attempts
       3. 3 minute lockout.
       4. This will be configured via group policy.
    5. Setup welcome message.
       1. “We Love HoSPITALITY” is the message.
       2. Title box should be “HOHOHO CO. Message of the Day.”
       3. Applies to all domain members.
14. Configure 2 company printers:
    1. Printer 1.
       1. This will be exclusive for IT employees.
       2. Named “IT PRINTER”
       3. Network printer with IP of 192.168.50.251
       4. HP laserjet M602.
       5. Highest priority.
       6. Shared with name of “IT Rocks”
       7. Does not require a “Separator Page”
    2. Printer 2.
       1. All employees except “Ho Pefully”
       2. Named “HOHOHO PRINTER”
       3. IP will be 192.168.50.251
       4. HP Lasterjet M602
       5. Lowest priority.
       6. Printer is not shared.
       7. Audited access for each department.
       8. Must use a separator page.
          1. Must be adobe postscript.
          2. Will include logo, company name, standard data.
15. Windows Client setup.
    1. Configure 1 Windows 10 client in virtualbox.
    2. Join it to the domain.
    3. Document assigned static (assigned dynamically but configured for static after) ip address.
    4. Documents setup.