Network/System Processes

# Server Roles

**Nagios** – System Monitoring

**NTP** – Network Time Server

**Exchange** – Email/Calendaring

**Sharepoint** – Internal IT forms (new user forms)

**Backup** – System backups

**Storage** – email archive location and home directory archive

**KMS** – Licensing server for Microsoft operating systems and Microsoft Office

**Sccm** – Computer Imaging and application deployment

**WSUS** – Windows update server

**Fileserver1** – File server, print server

**Xserve3** – Open Directory Master, Profile Manager, OSX VPN, Caching, 10.7+ Update server, munki

**helpdesk** – IT and Maintenance ticketing system/IT inventory system

**Directaccess** – Microsoft DirectAccess / VPN

**Radius**- NPS

**HyperV1** – hypervisor

**HyperV2** – Hypervisor

**HyperV3** - hypervisor

**DC1** – ADDS, DNS, Certificate authority

**DC2** – ADDS, DNS

**ADSYNC** – Office 365 sync, GADS, GAPS

# Server/Network Information

### **IT Documentation**

**The IT Admin folder is found a \\fileserver\IT Admin**

**In that folder you will find IT staff directories, documentation, utilities, and scripts**

### **Application Installers**

**Windows**

**The majority of the application installers are located at:**

[\\fileserver\sources\Apps](file:///\\fileserver\sources\Apps)

**OSX**

**The majority of application installers are located at:**

**oneidaxserve /Apps**

### **Wireless**

**There are 2 wireless networks in use**

**SECURE - Used by staff and students**

**GUEST - Used by guests whose accounts have been provisioned by IT**

### **Printing**

**For all HP printers we use ABC vendor to service them and to get the toner supplied for them.**

**We use print server to handle print services**

**The printer spool folder has been changed to the D: drive on the server**

**There is a Nagios alert that will check if that drive is full. If it gets full no more print jobs can be sent. You will need to use Print Management and connect to Fileserver1 and delete out the large print jobs.**

**Printers are typically deployed through a login script on Windows computers. The “deployprinters” GPO runs the “AllPrinterInstalls.vbs” script that runs a check if the printer should be installed or not**

### **Licenses**

**Serial numbers and where they should be installed are located:**

[\\filesserver1\licensing Info\](file:///\\filesserver1\licensing%20Info\)

**The location of the Windows server licensing spreadsheet is located at:**

**\\fileserver1\Licenses\Server Licenses.xlsx**

### **Digital Signage**

**The digital sign server is in the upstairs switch closet.**

**There are 3 displays in the building**

**Next to the room 101, 201 and 301**

### **Laptop Cart Combos**

**The current cart combo is 1234**

**Older combos have been 1111, 2222, 3333**

### **Passwords**

**The staff password policy is:**

**Maximum password age: 90 days**

**Minimum length: 8**

**Password history length: 5**

**Complexity enabled: true**

**We send out a notification email to warn users when their AD password is set to expire. This is a scheduled talk on the exchange server that runs a powershell script**

### **Computer Naming Scheme**

* **For Desktop, Laptop and Tablets (Windows or OSX) that will be joining Active Directory or ChromeBooks use the following guidelines:**
  + **For all desktop computers (including All In Ones) start the computers with a “D”**
  + **For all mobile devices including laptops and tablets start the computer name with a “L”**
  + **After the D or L enter the serial number of the computer**
  + **If the serial number is 15 characters or longer you will need to truncate**
* **For iOS devices use the following:**
  + **For individual assigned devices:**
    - **Building-UserName**
    - **Ex. HS-JSmith**
  + **For shared devices**
    - **BuildingAbbreviation-RMNumber-Devicenumber**
    - **Ex. HS-RM101-01 / HS-CART01-01**

### **Web Filter**

**We currently use XYZ as our internal web filter**

**To access XYZ go to filter.domain.org**

**Login with the username/password in the Network Documentation.**

**Once you are given permission you should be using your AD account for tracking purposes**

### **NTP (Network Time Protocol)**

### **System Monitoring**

**We utilize Nagios as our server/switch monitoring system.**

**Nagios.domain.org\nagios**

**Nagios.domain.org\nagvis**

**Nagvis is the visual front end to nagios that can be left up on a monitor for viewing**

**To add or edit hosts that are monitored you will need to have some Linux experience. The majority of the Nagios configuration files are in /usr/local/nagios/etc/objects but depending on what you are doing you may need to check out /usr/local/nagios/libexec and /usr/local/nagios/etc**

### **Security**

**The security server is at the room 1234. This is the computer that security assignments are given. The changes made here are then propagated out to each building. Badge cards and key fobs are programmed and/or printed from this computer.**

**We has DVR units in every building with cameras that are hard wired back directly to the DVR unit. These are XYZ units.**

**XYZ handles the software maintenance on this machine**

### **Administrative Accounts**

**All users who log into computers should be using non administrative accounts. This includes IT staff. This is to help mitigate the risk of virus/malware proliferation on admin accounts. Each IT staff member should be given a second account which would have the appropriate level of permissions for their job roles. The format for the second account should be the first initial and full last name of the user with a 2 appended to it. ex. jsmith2**

**There should be very few reasons to have to ever login to a workstation as the second account. The suggestion should be to monitor the windows workstation login log to check if users are logging in under their second account.**

### **Login Logs**

**All Windows workstations logins are logged to \\fileserver1\\Logs\Logins This log is broken down by User or PC. Every year an archive is created to keep the file size of each user down to a minimum. This log runs at login and logoff. While it isn’t 100% foolproof it will catch the majority of login/logoff activity. If a user shuts down a computer without logging out properly the user will not show as logging out of the computer.**

### **Updates**

**All Windows workstations are using our internal WSUS server for updates. Define your Update policy here.**

### **Microsoft Volume Licensing**

[**https://www.microsoft.com/licensing/servicecenter/default.aspx**](https://www.microsoft.com/licensing/servicecenter/default.aspx)

**an account will need to be setup to give you access to the volume license account.**

**for all Windows desktops we are using the KMS server to activate them. MAK keys should only be used if it will not activate using KMS for some reason.**

**For all Windows server we use individual MAK keys.**

### **Inventory**

**The district supply of computers/parts are kept in the RM 1234 closet, HS RM132 room/closet.**

**The excess pile is located in the RM555 Computer lab.**

### **Phones**

**XYZ handles the maintenance on the phone system. Minor changes are handled internally but programming of phones, creating extensions, etc are typically handled by XYZ.**

### **IP Addresses**

**Hard coded IP address lists are stored in \\fileserver1\Misc\ipaddresses**

### **Door Key Computer**

**The key making computer is located in the maintenance building**

### **Certificates**

**You should monitor the** [**xyz@domain.org**](mailto:tech@oneidacsd.org) **email address as this address is where the notifications for application certificates. They expire every year. The internal OSX servers also need to be renewed yearly even though they are internal.**

### **Backups**

**We have the backup server running at the Building 123 which backs up most critical servers with important data on them. The backup is run every night and then a backup is done offsite for disaster recovery scenarios. XYZ is responsible for backup and restore jobs.**

### **Service Notifications**

**We use the email account domainit to send out email notifications. For instance, for scheduled maintenance, outages and information about what happened during an outage. For consistency I try to use the following Subjects:**

**IT Service Issue**

**IT Service Notification**

**IT Service Maintenance Notification**

**IT Service Maintenance Alert**

**IT Service Issue Resolved**

**IT Security Notification**

**The following is the format that should be used for consistency. You can also look in the domainit email address send folder to copy and paste to have the formatting:**

**The Quick Explanation:**

What is Happening?  Brief one line explanation as to what is happening

When? Date and Time

Who Will Be Affected? List affected users

Anticipated Time of Services Restored? Date and Time

**Details:**

Here are the specific details for those interested

**Services Impacted:**

List what systems are impacted and who will be

# Processes

### **Application Management**

**Windows**

**We currently us SCCM 2012 for our Windows Application deployment and application updates. This is NOT including Windows updates. Those are deployed from the WSUS server. You will need to use the SCCM console to connect to the server. .**

**OSX**

**We currently use Munki to deploy OSX applications and patches to the OSX clients.**

**Add new Application or package to deploy**

**Download the package to xserver1 (local munki server)**

**Make sure the package is a .app, .pkg, .mpkg, .dmg**

**Open Terminal**

**Type: munkiimport /Users/admin/Desktop/libreoffice.pkg**

**(obviously replace the path to your actual path)**

**I typically name the item the full app name and version number (i.e. Adobe Flash Player 17.0.0.134)**

**Put that name in the Item Name, Display name and the Description field.**

**Put the version number in (put in the entire version including point revisions if possible)**

**Add it to the “all” catalog**

**Import the item**

**Leave “Upload item to subdirectory path” blank**

**Once “vim” opens there is typically nothing that needs to be done so you can just quit out of it. type :q (the actual command is :q , so make sure you are actually typing the colon) and hit enter**

**Choose y to rebuild the catalogs**

**Type: manifestutil**

**Type add-pkg “packagename” --manifest all**

**Replace packagename with the Item Name given above. Make sure to leave the quotes in in case you have spaces in the package name. Also note there are two dashes before manifest.**

**If it was successful you should see that the package was added to the manifest**

**Type exit to quit out of manifestutil**

**The package should be available immediately for testing on clients**

**Run Managed Software Update from terminal**

**Typically, you will run Managed Software Update from the Utilities folder but if you want to see what is happening is it helpful to run it from terminal. To do so open terminal and run the following command.**

**sudo /usr/local/munki/managedsoftwareupdate**

### **Temporary Workstation Administrators**

**There are times when staff need to be local administrators of their computers. Typically, this is to install home printers on their computers. To grant temporary rights go to ADUC and find the user and add them as a member of the “TempAdministrators” group. Then move their AD account to the “Users > Admin > TemporaryLocalAdmins” OU. Make sure the user logs out and back in to have the changes take effect.**

### **Computer Imaging**

**Windows**

* **We utilize System Center Configuration Manager as our Windows Imaging system**
  + **To accomplish this we use PXE to network boot the clients**
  + **This is different on different models but typically you hit the F12 key to network boot**
  + **You will come to a prompt about password protected media. The password is XYZ**
  + **Then will need to pick an image to pull down**
    - **Currently we support**
      * **Windows 7 Enterprise x64**
      * **Windows 7 Enterprise x86**
      * **Windows 8.1 Enterprise x64**
    - **All images will use x64 except the XYZ model. They need to use the x86 image. All Windows 7 images use the same base image regardless of the model. So the only difference is the drivers that get injected. The same goes for the Windows 8.1 images.**
    - **If you do not see a specific model for the computer you are imaging choose the location based on the end location of the computer you are imaging.**
    - **If there is a specific model make sure to choose it, otherwise the machine drivers will not install properly.**
    - **You will be prompted to reboot**
      * **For the computername follow the following guidelines in the Naming Scheme section of this document.**
      * **You will need to choose a workstation OU to place the imaged computer into. Choose the appropriate one based on the computers end location**
      * **You will need to authenticate using your domain admin credentials. In the user name field type domain\yourusername** 
        + **You need to put in the domain\ or it will not work**
      * **At this point the computer should image and go to the login window when it is completed.**

**OSX**

* **Turn on Mac and hold down “N” key to net boot**
* **Authenticate with the xserver2 admin user/password found in the network documentation**
* **From there you can select the image that you want**
* **For 1.6 restores**
  + **Choose “Restore a master on a volume AD/OD Bind”**
  + **Choose the appropriate image**
  + **Once it gets to the login window it should be ready to use.**
* **For 1.7+ restores**
  + **Choose “Restore Master AD/OD Bind PM Enrollment”**
  + **Enroll in PM**

### N**ew Staff**

* + **Add AD account**
    - **Go to the appropriate OU in Active Directory**
    - **Right click the user template and click copy**
    - **Fill in first and last name**
    - **Fill in “User Logon Name” – typically first initial of first name + full last**

**name**

* + - **If there is a duplicate, choose first initial of first name + first initial of middle name + full last name**
    - **Put in the default password of XYZ**
    - **Open the properties of the user AD**
      * **General Tab**
        + **Enter their phone extension if they have one**
      * **Organization Tab**
        + **Enter Job Title, Department, and Company (Compare another staff member to view the pattern**
      * **Member Of Tab**

**Compare another staff member to see what group memberships they probably should have.**

**These need to be in or they will not get the proper permissions on the File Server.**

* + **Add Office 365 Account**
  + **Add exchange account**
    - **Open Exchange Management Console**
    - **Recipient Configuration > Mailbox > Right Click Mailbox > New Mailbox > User Mailbox > Existing User > Click the Add button and find the user**
    - **Check “Specify the mailbox database…” For teachers choose “Staff”. For admin and office users choose “Office”**
    - **Click New**
  + **Add phone extension / voicemail**
    - **TODO**

### **Staff Room Change**

**Change their Department name (Room number) and Telephone Number in ADUC**

**Generally it is best to delete out the current voicemailbox and recreate a new one. Confirm with the previous staff member that they don’t need any current messages. They will be deleted and unrecoverable.**

**Follow the steps in the section “Create New Voicemail Box” in this document.**

**You should also make the appropriate change in XYZ**

**Open XYZ**

**Make the changes**

### **Bulk Add New USers**

* **Refer to the file** [**\\fileserver1\Scripts\New User Creation\Bulk Create Users PowershellReadME.txt**](file:///\\fs1\homes$\Admin\IT%20Admin\All\Scripts\New%20User%20Creation\Bulk%20Create%20Users%20KG%20Students%20PowershellReadME.txt)

### **Adding Printers to Print Server**

**When adding new printer drivers to the print server make sure to add x86 and x64 drivers in so you don’t have to worry about what architecture is connecting in the future.**

**Follow the format already in the print server**

**RM103-HP-LaserJet 4000N – UPD**

**Room 103**

**Make sure to go to the sharing tab of the printer and check “list in the directory” so users can browse and install the printers themselves.**

**When adding printers that do not have specific drivers append “- UPD” to the end of the printer name to signify it is using the HP Universal Print Driver.**

### **Create a New Voicemail box**

* + **Login to the voicemail system (xxx.xxx.xxx.xxx) credentials in “Network Documentation**
  + **Enter the desired extension and click “add or edit”**  
    **Follow the template to create a new voicemail box**

### **Manually force Office 365 Directory Sync**

* + **Log onto your MS Directory Synchronization Server.**
  + **Browse to the following location: C:\Program Files\Windows Azure Active Directory Sync**
  + **Locate the DirSyncConfigShell.psc1 file and Double-click**
  + **When the Powershell module opens, input the following command:**

**Start-OnlineCoexistenceSync and press “Enter”.**

### **Connect to VRTX**

**Open a web brower and go to x.x.x.x and login using the credentials in the Network Documentation document**

**To login to the console of the blades click on the blade you want and under the properties tab click “Launch Remote Console”. This relies on Java so you may need to make changes to Java to allow the applet to install and run and if you are using IE you may need to add the iDRAC IP into the compatibility list**