

Monday, September 23, 2013 8:00 AM - 4:30 PM (8.5 hours)

I met with Greg Whipple and we discussed what was expected from Guidance Software, Inc. this week. He indicated that the Legal Hold training was a priority and any extra time I had should be spent training his IT staff on how to more effectively use ECC. I proceeded to do an ECC walk-through of the system prior to the initial Legal Hold training to ensure there were no issues with ECC.

I started the Legal Hold training at 2PM. Greg and his two IT staff members along with two City Attorneys and one Legal Assistant attended the training. The training session lasted for 1.5 hours and was used by the City Attorneys as a way to determine how to structure the remaining training sessions for the remainder of the week.

After the training session was complete, Greg and I discussed the software issues/limitations that were encountered last week with ECC v5.2.2, and asked about the release date for ECC v5.3 since Outlook 365 would be supported in the v5.3 release. Greg explained that ensuring Outlook 365 worked with EnCase eDiscovery is crucial to them because they will be migrating to that platform soon. In addition, the new release would address their previous request, which was for additional Active Directory fields when importing custodians in Legal Hold. I told him I'd follow up with him about the release date for ECC v5.3, but in the meantime we would proceed with Legal Hold training and internal IT training as planned. At this time the training schedule for the IT Staff was set for Tuesday, and the training schedule for the City Attorneys was set for Wednesday, Thursday, and Friday.

After leaving the site, I received an email indicating ECC v5.3 was released and I began to download the installation and review the documentation files.

Tuesday, September 24, 2013 8:00 AM - 3:30 AM (20.5 hours)

I informed Greg that ECC v5.3 was released and sent him the release notes, administration, and users guide for him to review prior to performing the upgrade. After reviewing the documentation and transferring the installation software over to the systems, and writing down the current ECC configuration settings, Greg decided we should move forward with the upgrade to ECC v5.3.

Prior to beginning the upgrade to ECC v5.3 on their production systems, I ran a test upgrade on a VMWare image that had ECC 5.2.2. The upgrade to ECC v5.3 completed successfully and took two hours. The primary focus of the upgrade test was to ensure that Legal Hold would work properly since the City Attorneys were set to attend Legal Hold training on Wednesday. Testing Exchange or 365 connectors was not done because the VMWare image did not have those features installed on it. After verifying that the core components of ECC were functioning properly, Greg decided we should proceed with the upgrade to ECC v5.3 on the production systems.

The upgrade process began at 11:00AM. I received an error message that indicated their SMS had expired. Greg emailed Ed Schandlbauer about extending the expiration so we could proceed with the upgrade. Debbie Wall approved an extension to the client's SMS expiration date. The new SMS expiration date was now set for 10/01/13 02:00:00 AM. Since we hadn't received the new Cert files reflecting the new expiration date, I emailed Belle Cook who first validated the Certs/Licenses had been updated in the database, then referred me over to Aman Lama to assist me in getting the updated Certs. Aman emailed the updated Cert, License, and SC2002677_R20130924_104052.cert files to Greg. The updated Certs/Licenses were copied into onto each of the client's systems, and at 7PM we began the ECC v5.3 upgrade process on all three systems.

During the upgrade process, Greg informed me that the City Attorneys pushed the Legal Hold training back to Thursday and Friday, so he decided to have his IT staff training on Wednesday. Since his IT staff training included live cases, we had to ensure the upgrade to ECC v5.3 was completed and ready for use by Wednesday afternoon. There was an issue with the Examiner Service install due to a corrupt EXE file during the first installation, which slowed the process down, but I was able to resolve it and finished the entire ECC v5.3 upgrade across all three systems.

This is a breakdown of what was done during upgrade to EnCase eDiscovery v5.3.0

- **APEDS02**
 - o SAFE – Upgraded from v7g to v7h and updated the SAFE service logon account information.
 - o Database Utility – Installed v5.3.0
 - o Database – Upgraded all v5.2.2 active and reserved databases to v5.3.0
 - o Web Components – Upgraded to v5.3.0
 - o ECC Web Server (x64) – Upgraded to v5.3.0 and reconfigured ECC Web configuration settings.
 - o Examiner Service – Upgraded to v5.3.0
 - o EnCase Examiner – Installed v7.08.01
 - o ECC Desktop – Installed v5.3.0 and updated all locations with the new Certs/Licenses.
- **APEDS01**
 - o ECC Desktop – Installed v5.3.0 and updated all locations with the new Certs/Licenses.
 - o Examiner Service – Upgraded to v5.3.0
- **APEDS-FRED**
 - o ECC Desktop – Installed v5.3.0 and updated all locations with the new Certs/Licenses.
 - o Examiner Service – Upgraded to v5.3.0

Wednesday, September 25, 2013 11:00 AM - 2:00 AM (15 hours)

We started creating the Exchange and 365 Sources in ECC v5.3 and a couple of issues. When adding Exchange 2003 Sources, we would get the following error: *MapiError – 80040115h Exchange store – Could not connect to the server – network error*. I recall trying to help Coy Potts resolve that same issue a few weeks before, so I sent him an email requesting assistance. After a few hours of troubleshooting, I found out that the Exchange service account (CITY\encase.examiner) & mailbox was created on one of the Exchange servers (EXCTY05) only, so even though we could view all mailboxes across all Storage Groups on both Exchange servers, we would only get an error when trying to use the CITY\ecase.examiner service account to connect to a custodian's mailbox that resided on the EXCTY00 server.

The solution was to create a second Exchange service account (CITY\encase.examiner00) and mailbox on the second Exchange Server (EXCTY00) and create two separate Exchange Sources in ECC for EXCTY00 and EXCTY05 that used their respective service account to log on with in the “Authenticate User by\Specifying Credentials” section on the Mail Server Source window in ECC.

IT staff training commenced at 1:30PM. The following items were covered in the EnCase eDiscovery v5.3 training:

- Difference between Enterprise and ECC
- Overview of Enterprise basic concepts (SAFE, EnScripts, Evidence files, NAS Licensing)
- Creating Databases
- Editing Case Settings
- Importing Custodians
- Creating Targets
- Defining Sources (SAFE, Home/Group Shares, Exchange)
- Assigning Targets
- Creating a Collection Job
- Advanced Criteria Writing
- Exporting and Importing Criteria Sets
- Creating and Editing Conditions
- Exporting and Importing Conditions
- Importing Evidence Files
- Importing files into Imported Data Set (PST, NSF, & Evidence Files)
- Managing Jobs (queue, cancel, on-hold)
- Monitor Examiner status and number of Examiners available via the web
- Troubleshooting the Examiner service
- Email de-duplication
- Creating a customized Criteria list for the department to use
- Best practice suggestions for Forensic and eDiscovery cases

In addition to the items listed above, I walked through an actual case with them. Due to time limitations we were only able to create the case, custodians, targets, and define sources. Job collections, processing, and data output would be covered on Thursday.

After training, Greg notified me that the City Attorneys had decided not to go forward with the Legal Hold training after all, so our efforts were now entirely focused on ensuring the IT staff was adequately trained and the 365 connector issues were resolved.

After spending a few hours researching and troubleshooting the 365 connectivity issues, we discovered that the CITY\encase.examiner service account needed to have a mailbox on the 365 server in order for ECC v5.3 to execute the collection jobs properly.

My next task was to ensure that the SAFE servlet deployment feature was configured and working properly. I was able to successfully deploy the servlet to the FRED system as well at Greg's PC.

Before leaving for the day, we ran some test collections on SAFE, Share, Exchange 2003 targets and applied the custom criteria templates we created earlier. All tests collection jobs completed successfully.

Thursday, September 26, 2013 9:00 AM - 5:30 PM (8.5 hours)

Greg and I documented a summary of what had been accomplished over the last few days, and he submitted an internal IT request to have their Exchange administrator create a mailbox on the 365 server for the CITY\encase.examiner service account.

Greg and I had a conference call with Atul Jain at 11:00AM to discuss the status of the project. I indicated that for the most part the upgrade to ECC v5.3 was complete. The only item pending was testing the 365 connector, but we would have to wait until the Exchange admin completed the work request Greg had just submitted.

IT staff training continued after the conference call. During this training session we accomplished the following on actual casework:

- EnCase eDiscovery v5.3
 - o Creating a new Case database, Custodians, and Targets
 - o Creating Global Criteria templates using the Advanced method
 - o Importing Global Criteria templates into their live cases
 - o Exporting Global Criteria templates for future import
 - o Creating a Collection Job
 - o Creating a Collection Job (Report Only)
 - o Duplicating Collection Jobs
 - o Monitoring a job with both ECC Desktop & ECC Web
 - o Reviewing Collection Job logs

The only pending items left at this point were to configure and test the 365 connector, and to cover a few more eDiscovery topics with the IT staff.

Friday, September 27, 2013 8:00 AM - 2:00 PM (6 hours)

Greg confirmed that the 365 mailbox for the CITY\encase.examiner service account had been created by their Exchange administrator, so I proceeded with the 365 Source creation in ECC v5.3 and was able to successfully connect to the 365 online server. We created a test collection job against one mailbox and it ran successfully.

Now that the 365 connector issue was resolved, I continued with the IT staff training session. During this session I walked the staff through their live casework and covered the following items:

- EnCase Enterprise v7.08.1
 - o Overview of SAFE keymaster and user accounts
 - o SAFE account logon permissions
 - o Manually updating Keys and SAFE locations
 - o Troubleshooting SAFE logon issues
 - o Servlet deployment via Sweep Enterprise
 - o Servlet deployment via SAFE Network Preview
 - o In-depth review of how the Servlet is installed on the remote system
 - o Triaging a remote system using Sweep Enterprise
 - o Overview of Best Practices when using EE v 7.08.1 in a Forensic Investigation
 - o Importing Evidence Files and Logical Evidence Files into EE v7.08.1

- EnCase eDiscovery v5.3
 - o Creating a Processing Job
 - o Manually Queuing, Stopping, and Restarting Jobs in ECC Desktop & ECC Web
 - o Manually assigning a specific Examiner to a Queued Job
 - o Importing from a Global Condition Template
 - o Customizing a Global Condition Template import using the Advanced method
 - o Reviewing the Processing Job LEF's and logs
 - o Creating a Deliverable Job & understanding the various types of output that can be generated by ECC
 - o Legal Hold Overview
 - o Creating a Legal Hold Templates
 - o Creating a Questionnaire Template
 - o Creating a Case from Legal Hold
 - o Importing Custodians into a Case via Legal Hold
 - o Placing a Custodian on Legal Hold & Sending Legal Hold Notice/Questionnaire
 - o Reviewing a Custodians Questionnaire Responses
 - o Escalating a Legal Hold Notice to a Custodian's Supervisor
 - o Scheduling Legal Hold Reminders
 - o Releasing a Custodian from a Legal Hold

Prior to my departure from the client site, Greg, Ed, and I met with Tony (Greg's Supervisor) to report on the status of the upgrade and training. The client was very happy with the end result and said they would definitely recommend Guidance Software to others. I had a final meeting the Greg and his IT staff to address any last questions/concerns they had before leaving the client site.