Welcome to the CMTrace Overview

The purpose of this lecture is not to fix problems. This is an overview of CMTrace.

In this lecture we will checkout the capabilities of CMTrace and hopefully learn some of the tricks that every SCCM administrator should know.

- **What is CMTrace?**
  CMTrace is a real time Log viewing tool for configuration manager

- **Configuring logging options in Configuration Manager**

  From the ITSCCM01 server, open Configuration Manager

  From the Workspace, click **Monitoring**, from the Navigation Pane double click **System Status or Component Status, in this case click Component Status**

  From the Ribbon**, click start,** then **click Configuration Manager Service Manager.** Click the site you want to manage, in this case ITF is already selected

- **Here we will merge** three log files into one log file – In this example we will merge the three discovery logs into one log file, and **increase the size** of the log to 10 MB. This can be useful if you are having problems with some users or computers not getting discovered from Active Directory.

  Click the **+** next to **ITF**, then **click components**. From component name (on the right) click **Security Group discover agent**, hold down the **shift key** and select **User Discovery Agent**. With **all three** selected **right click** and select **logging**. Type a file name, in this case **Discovery.log** and type 10 in the log size box, then click ok. Now all three files can be accessed as one file, with a file size of 10MB, before that file will be overwritten. The **location of the discovery.log file is C:\program files\Microsoft Configuration Manager\Logs**

- Now let's open the **CMTrace** log file viewer. This program can be located in our SCCM installation folder as indicated.

  Right click on CMTrace.exe and choose pin to task bar. Click the CMTrace icon. The first time CMTrace opens click yes to make this program the default viewer.

  Now click the folder, there are two options.

- **Ignore existing lines** – This selection is great for troubleshooting, it opens the log file with an empty screen. All lines that are added to the file after opening it, will be shown in CMTrace.

  I can demonstrate this by clicking **Ignore existing lines**. Then clicking discovery.log, then click open.

  From Configuration Manager, from the workspace click Administration, from the Navigation Pane double click Hierarchy configuration, then click Discovery Methods, right click on Active Directory Group Discover and select Run Full Discovery Now.

  Now go back to CMTrace and notice that the merged discovery log file now reports the results of a full group discovery.

- **Merge selected files** – This will allow you to select more than one log file and merge the contents, just as we did using **Service Manager.** But here you **can't change the file size.**

- **Filtering**

  Menu/Tools/Filter

  How can we use filtering? For example, let's say we have a computer named Minint, that is not receiving the SCCM client. We could open the CCM.log.

  This log file records client push installation activities. Notice that when we open this file there is a lot of data.

  From menu/tools/filter

  Check **Filter when the Entry Text**, select **contains**, Type Minint, the computer account is displayed.

  There are some errors displayed here. Unable to access target machine, failed to connect.

- **Highlight lines with certain keywords**

  From Tools/highlight – Type the 67 - CMTrace will search and highlight the lines with that number.

  Now go back to **/Tools/highlight** – and type 2097152006. CMTrace highlights that number.

  Now type failed, click ok

  Now the word failed is highlighted in yellow.

- **Error lookup**

  Menu/Tool/Error Lookup

  Type 67 – The network name cannot be found

  Now type 2097152006 – As you can see Error Lookup cannot help us with this error. Let's take a look on the internet and see if we can type in the error code and try and acquire more information on this error.

  From Internet explorer, type CCM log, then type 2097152006

  Choose a web site

  This admin, suggests that the **client push installation account** is missing from the the local administrators built-in group on the computer

  This means that the account that you are using for client push installation should be the local administrator on the client machines or domain administrator for the domain itflee.com.

- **So far from the logs we have determined the following:**

  We failed to connect to the Minint admin$ using the machine account. This means that SCCM is trying to use the site server's machine account and it does not have access.

You may also see a # 5 error (access denied)

Error 67, indicates that the Network name cannot be found – Here Client may not have a DNS entry, or an invalid DNS entry.

2097152006 – Possibly no administrator account has been specified in Client Push accounts.

- Now let me show you where these client push accounts reside.

  From Configuration Manager, from the Workspace, click Administration, double click Site Configuration, Sites, Settings, Client Installation Settings, Client Push Installation, Accounts. **The Client push account must be a member of the local administrators group on the client computers.**

Congratulations for completing this lecture, thanks for watching and I will see you in the next lecture.