Troubleshooting a Failed Client Push Installation

Several students have requested assistance with their Client Push Installation. So, I thought it would be helpful to provide a guide to several of the common problems associated with client push.

We will cover the following:

- The lab prerequisites
- Initiating a client installation
- Checking out the Server and Client Logs
- Analyze errors that we find
- Examine the client push requirements
- Fixing the problems
- Take a look at the inbox and the retry folder
- Retry the installation

Lab Prerequisites

- Create an additional Windows 10 Computer in virtual box, (or your VM of choice) use your ISO file to create this VM.
- For Virtual Box, change the network to NAT network
- Assign the VM an available IP address.
- Name the VM ITFWS05
- Join ITFWS05 to the domain

Initiate a Client Installation

- From the Workspace click Assets and Compliance, From the Navigation pane, click Devices. After several minutes, ITFWS05 should appear in the console. Click ITFWS05, and also notice that the client has not been installed.
  Open the needed log files in CMTrace. CMTrace is located on \\itfsccm01\sms_itf\tools\cmtrace.exe, right click on CMTrace and pin to the taskbar on your server.

Server logs

SMSprov.log, SmsAdminUI.log, are Site Server logs that record information about the operation of the Configuration Manager console.
The CCM.log, records client push activities on the Site Server.

- Open CMTrace, click the folder, click ignore existing lines, **double click smsprov.log**
- Open another instance of CMTrace, click the folder, click ignore existing lines, **double click ccm.log**
- Right click on ITFWS05 click install client, click next, click the box that say's install the client software from a specified site. In this case our site is ITF-ITFLEE, click next, click next again, then close.
- Now open SMSprov.log, and we see it is checking to see if the user has rights. The log shows that the machine was able to initiate the install.

- Now let's check the CCM.log in CMTrace. CCM.log will handle the installation requests. Notice there are errors.

Analyzing the errors

Now let's analyze the errors – Now let's take a look at our ccm.log file

- Notice that the process is trying each entry in the SMS Client Remote Installation accounts list. But continues to warn us that no remote client installation account was found.
  Let's take a look and see if there is a client installation account.

  From the **Configuration Manager console** open the Workspace, click Administration, from the Navigation Pane click site configuration, click sites, click Client Installation Settings, select Client push installation. Click accounts, and here we see that there is no account listed. This is a problem that we will fix in a minute. This leads us to the next error.

- The process is trying and fails to connect to the admin$ using the machine account with an error 5.
  Open CMTrace, from tools, click error lookup, type 5 in the error code box, which is access is denied.
  Then the error continues by saying failed to connect to the \\ITFWS05\admin$ share using the 'Machine Account'

This should raise several questions.

- Where did the admin$ share come from? These shares are automatically created by Windows.
- Why is there a $ after the word admin? The $ tells windows to hide the share
- Where is the admin$ share located? It is located on C:\Windows
- What is it used for? It is used to deploy software remotely.
- What permissions do I need to access admin$ share? You need to have local administrator rights on the target computer.

Another question that you may have is what is a **machine account**? The machine account refers to the site server account, which in this case is **ITFSCCM01**.

So, what is this error trying to tell me? The client push process first check's the client push accounts, and if there are no accounts listed, the process automatically tries to use the site server account to access the admin$ share on ITFWS05. But because the site server account is not listed in the local administrators group on ITFWS05 the machine account cannot access the admin$ share and that is why we get a 5 error which is access denied.

Now let's see if I can manually connect to admin$ share.
From the SCCM server, open file explorer, from the search bar type \\itfws05\admin$
We can connect, that is because I am logged into the SCCM server as Domain Admin and the Domain Admin account would have the necessary rights to the ITFWS05 admin$ share.

- Our last issue says, Error: Unable to access target machine for request “2097152008” access denied or invalid network path.
  With the 2008 error, that could possible mean that your firewall settings are not configured correctly, or the invalid network path could indicate a DNS issue.

Now let’s examine the Client Push Requirements – We will use these requirements to fix our problems.

- It is recommended to create a Domain User account in Active directory. Add this account to the local administrators group on the client.
- Add this domain user account to the Client Push installation, accounts.
  This account will give the installation needed permissions to access the admin$ share on the target computer.
- For added security we will verify that our domain user account cannot log on locally.
- Check out the Firewall settings – Inbound and outbound rules must be configured
  For WMI, and file and printer sharing

Fixing the Problems

Creating a Domain User Account in Active directory

- From the Domain Controller in this case ITFDC01, open Server Manager, tools, then open Active Directory Users and Computers.

- Right click the user’s container, then click new, user, for first name type SCCMClientPush, for User logon name type SCCMClientPush, then click next, click password never expires, type a password twice, click next, then click finish. Close Active Directory Users and Computers.

Now we will manually add the account into the local administrators group on the target computer

- From the client machine in this case ITFWS05, from the search bar type lusrmgr.msc
- On the left side click **Groups**, from the right side right click **Administrators,** click **add to group**, click add, then type **SCCMClientPush**, then click **check names**, then click apply, then click **ok**. Close local users and groups.

Add this Domain user account to the Client Push Installation, accounts in Configuration Manager.

- From the ITFSCCM01 server open Configuration Manager, From the Workspace, click Administration, from the Navigation Pane, double click **site configuration**, then click sites.
- From the Ribbon click settings, **Client Installation Settings**, then **click client push installation.**

- Click **general**, uncheck Enable automatic site-wide client push installation. For this lecture we don't want to install the SCCM client on every computer that has been discovered.
- Click **Accounts**, click the **star** and select **New Account**, then from Windows User Account type **SCCMClientPush,** click browse, then type **SCCMClientPush**, then click **check names** click **ok**. Now type in your **Domain Admin account and password,** then click ok.

Check Allow log on locally

- From the windows 10 computer, ITFSW05, from windows search, type secpol.msc, press return.
- Click local policies, click User Rights Assignment, click Allow log on locally. For added security, verify that the client push account is not listed.

Configuring Windows Firewall

- We have gone over this in a previous lecture, so we will just open windows firewall and verify that these rules have been configured.
- From the windows workstation ITFWS05, from windows search, type wf.msc. From the left side click **inbound rules.**
- Scroll down until you see **file and printer sharing**. We see the green checks, this verifies that those settings have all been enabled.
- Scroll down until you see **WMI instrumentation**, we see green checks, so these have been enabled.
- Repeat the same process for the outbound rules. Click outbound rules, scroll down until you see file and **printer sharing**. We see the green checks, this verifies that those settings have all been enabled as well.

Now let's **retry the client installation** – I could just right click on the target computer and select client push again, but instead let's take a look at what is happening here.

- There are two folders that are currently being used during the installation process. Located in C:\program files\Microsoft Configuration Manager\inboxes.
  One folder is the CCR.box, and the other is the ccrretry.box.
- A much quicker method of retrying the installation is to cut the retry file from the ccrretry.box folder and paste that file into the ccr.box folder. Let's go ahead and do that. And now the system will retry the installation again.
- Now go back to the ccm.log on the server. We see that the SCCMClientPush account connected to the admin$ share folder. You can ignore the error. We have created the SCCMsetup folder and now we are copying client files to ccmsetup. Now the request has been completed.

Now let's go over to the **client** and checkout the **CCMsetup.log file**

- From windows file explorer, click network, in the search bar, type \\ITFSCCM01\sms_itf\tools double click cmtrace, click the folder, now click the up arrow, now click windows\ ccmsetup\logs\ now double click ccmsetup.log
  We can see that the installation is progressing,
  at the end of the log, it will say **client.msi installation succeeded.**

- From ITFWS05, open the Control Panel. We should now have configuration Manager installed.
- Now let's go back to the SCCM01 server, open configuration Manager again and now we see ITFWS05, now shows the client installed and active.
- Therefore, our problems have been fixed.

Congratulations you have completed this lecture, thanks for watching and we will see you in the next lecture.