OnTraQ

CAP Server Application Installation

Table of Contents

Server Hardware Notes

The server that hosts the CAP Server and OnTraQ applications requires a second network interface card be installed solely for connecting the server to the switch. This network card should be the 2nd network connection (so that the default connection is the corporate LAN). The IP address is set to 192.0.2.25 for the first CAP Server attached to the switch, 192.0.2.26 for the second, etc. The license file generated by Siemens uses the MAC address of this 2nd NIC.

Note: The server must have an alphanumeric machine name. No blanks, underscores, etc or CAP won't install correctly.

Check for firewall settings between the OnTraQ servers and the Traffic Analyst server as well as between the OnTraQ servers and the OnTraQ clients. It's not always obvious that data is being blocked. For instance, the client may load data, but not be able to update data dynamically.

IIS Settings

For the reporting web service to work, some IIS setting may need to be changed on the server that Traffic Analyst and the database server are running on.

From Administrative Tools (within the control panel), open the Internet Information Services (IIS) Manager. On the tree control at the left, the last option on the 2nd level is "Web Service Extensions". Select that. Then on the right hand side, verify that "Active Server Pages" and "ASP .NET v2.0.50727" are allowed. If not, select each item and then select the "Allow" button. Just close the tool when you are done.

IP Access

The following IP ports are used by default and must be unblocked.

- Port 32001 between OnTraQ clients and OnTraQ servers
- Ports 2638 (or 2639) and 957 between the OnTraQ server and the Traffic Analyst/Database server.
- If using TA clients on a separate PC from the TA server, then port 4001 should be unblocked.

CAP Server Application Installation

Follow the installation directions in the CAP documentation.

Configuring CAP

Create one HiPath 4000 switch connector and one Proxy. The switch connector id usually ends in _scc and the proxy id in _sccp. By default, the switch connector uses IP address 192.0.2.25, and some connection parameters. Don't modify any fields marked as "(optional)".

If this CAP Server is not the only process using a ACL link to the switch, then use the IP address configured above for the 2nd network connection. Also all of the of the connection parameters values on the "CA 4000" tab for the switch connection is increased by the number of other links. So the 5th CAP Server adds 4 to the default values for the switch connection. The switch connector port (default 26535) on the "SCC" tab doesn't need to change in any case.

For now, the proxy always uses the default port of 27535. XML applications cannot share a CAP Server so there should not be a need to change this, but the port is stored in the ACDServerDef record in the TA database.

On the last tab of the switch settings, the IP address of the switch is always 192.0.2.3 unless you are connecting directly to an IPDA. For an IPDA use the IP address of the “CCAADDR” parameter of from the AMO SIPCO for that IPDA (The address of the main processor on the IPDA).

CAP Server Settings

In the file ...\HiPathCTI\data\TelasAdmin\import\ImpAdmData.cfg, make sure there is a line:

```
ExecuteAllChanges=1
```

In the file ...\HiPathCTI\config\<server name>\admin\mgmnt\http-server.props
change all occurances of com.siemens.server.port.maxThreads value from 20 to 400

In the file ...\HiPathCTI\config\<server name>\admin\mgmnt\adminIf.cfg set the line:

```
SysMgmtTimeout=600000
```

Setup the SAT Activated Mode (address translation): In most files, just uncomment the line which has the following data. The SCCP and SCC file directories include the name of the SCC or SCCP entered when setting up CAP. This must be done fore each connector if there are multiple connectors.

In the file named ...\HiPathCTI\config\<server name>\admin\sat_svc\SatServer.cfg, set the line:

```
LEGACY_MODE = false
```

In the files named like ...\HiPathCTI\config\<server name>\sccp_<SCCP name>\Telas.cfg, set the line:

```
CFR_SATLegacyMode = 0
```

and

```
SocketPoolSize = 20
```

In the files named like ...\HiPathCTI\config\<server name>\telasServer_<SCC name>\Telas.cfg, set the lines:

```
SFR_SATLegacyMode = 0
CFR_SATLegacyMode = 0
noMStartSATMode = 1

requestTimeout = 20
rcvSockSize = 256960

adminQueryTimeout = 120
```

On switches with a log of traffic, increase the socket buffer size in Windows.

1. Start regedit, create / modify the following fields in
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
   and add the values as hexadecimal:

   type: DWORD value
   name: TcpWindowSize
   value: 0003EBC0

   type: DWORD value
   name: GlobalMaxTcpWindowSize
   value: 01000000

   type: DWORD value
   name: TcpTimedWaitDelay

value: 1E

type: DWORD value
name: Tcp1323Opts
value: 1

2. Restart the server, so registry entries may take effect.

License

A license file generated specifically for this server by Siemens (using the MAC address of the NIC that connects to the switch) must be installed. The number of licensed devices needed is the number of route control groups plus the number of extensions with the “AGENT” privilege (an ACD agent is allowed to login at the extension).

CAP Users

OnTraQ only needs one user configured in CAP administration. It is an application user. It doesn’t need an assigned device. The convention is user: “ontraq”, password “impact”.

Importing Devices into CAP

Any time RCGs are added or Agent privileges are added to a new or existing extension, “devices” must imported into the CAP Server. This is required for the CAP Server to recognize and report on new devices. Without doing so OnTraQ results will be incomplete and inaccurate.

To begin, you will need to import the CAP Devices file into CAP Management.

- For CAP V3.0 R9 and earlier, you will use **CAPDevicesR9Fmt.txt**
- For CAP V3.0 R10 and later, you will use **CAPDevicesNewFmt.csv**

For earlier editions of Windows, this file is located in the Document and Settings\All Users\OnTraQ folder. Or, if using Windows 2008, it will reside in the Users\All users\OnTraQ folder.

1. Import the CAP Devices file into CAP Management:
    a. Launch CAP Management.
    b. Login to CAP Administration and pick the “Data” option from the top menu bar. Then the “Import” from the vertical list of choices on the left.
    c. For the Data Type field, pick the “Device Data” option.
    d. For Import Mode, pick the “Create data from import file.” option.
    e. For Import File, enter the path and file name created above or use the browse button to select it.
    f. Hit the “Start Transfer” button and let it run. This can be a slow process.

2. When finished, verify that CAP is still working correctly:
    a. List the devices by going to the “Device” choice in the main menu bar of CAP Administration and choose “Search/Modify” option on the left. Just use the default fields in the resulting dialog and hit the “Search” button.
    b. You should see a list of devices that match the list from the file. If you don’t, the CAP management service may need to be restarted or the CAP Server rebooted.