RSA ECAT: ECAT 4.0 - Machines not showing/updating in the UI

Posted by Richard Paquin Mar 30, 2015

Index

Summary

"My machines don't appear in the UI" is probably the trickiest question you can ask about ECAT.
It is very similar to "My machines don't update in the UI".
Let's see why.

Here is the path followed by a scan:
ECAT Agent > ConsoleServer > ECAT Database > ECAT UI

For each of the elements involved in a scan, you can get a transmission error in both direction, or an internal error.

Why will lead to the following questions:

1. Is the Agent able to create the scan (aka Internal Agent)
2. Is the Agent able to create a connection to the Server (aka From Agent -- *common*)
3. Is the Server able to receive connections from the Agent (aka To Server -- *common*)
4. Is the Server able to decrypt the scans (aka Internal Server)
5. Is the Server able to write give the scans to the Database (aka From Server)
6. Is the Database able to read the scans (aka To Database -- *extremely common*)
7. Is the Database able to parse the scans and insert them in the right tables (aka Internal Database - *common*)
8. Is the Database able to receive connections from the UI (aka From Database)
9. Is the UI able to create a connection to the Database (aka To UI)
10. Is the UI able to display the received data (aka Internal UI -- *uncommon*)

Now if we add the transmission protocols to the chain, we get:

ECAT Agent > [**HTTPS Connection**] > ConsoleServer > [**File in QueuedData**] > ECAT Database > [**SQL Connection**] > ECAT UI

1. Is the Agent able to create the scan?

Is the Agent installed and started:
> sc query EcatService

2. Is the Agent able to create a connection to the Server

This goes hand in hand with point 3.

Verify connectivity / port connection with SysInternal's psping.exe
> psping [hostname/ip]:443

In addition, open the webpage: http://[hostname/ip]:443
If you see: "There is a problem with this website's security certificate." this is OK. It means the HTTP server is responding with a certificate.
If the HTTP server (ConsoleServer) is not reachable, you will get an Error 404. Therefore the certificate error is a good sign.

If not, verify:

- Is ConsoleServer actually listening on port 443, or another port.
- Check if the value port in the packager corresponds to the values in ConsoleServer.exe.config

As a great but complex last resort, use Wireshark on Agent machine to see the packets leaving, as this will confirm which ports are used.

3. Is the Server able to receive connections from the Agent?

This goes hand in hand with point 2.
Can the Packager connect properly in a test connection?

ConsoleServer will be listening on the port set in ConsoleServer.exe.config:
<add key="LocalHttpsServerPort" value="443"></add>

- Is ConsoleServer started ?
- Is the firewall open ?

Can the Packager connect properly in a test connection?

---

5. Is the Server able to write give the scans to the Database?

Be sure to fully understand the following sentences points:
Once the scans are received by the server, 2 actions are made:

- Write files in the QueuedData
- Insert scan notification in DB

The database will consume the scans.

5.1: ACTION Verify that the scan files are being written in QueuedData

The QueuedData folder is set in ConsoleServer.exe.config
In an environment where the Database is installed on a different machine, both ConsoleServer and the Database must access the **same path**.

Config when the DB is local:
<add key="QueuedDataPath" value="C:\ECAT\server\QueuedData"></add>

Config when the DB is remote:
<add key="QueuedDataPath" value="\\EcatServer\QueuedData"></add>

If the machines appear in the UI, try to start a quick scan with Advanced options > Processes.
Monitor with Procmon to see activity in that folder.

A quick scan with only the Processes checkbox is about the quickest way to communicate and see the response from an Agent.

5.1: ACTION Verify that the scan notifications are in the DB

SQL command to see if the Agent scans are inserted:

SELECT TOP(100) [as].[PK_AgentScans] , [as].[BatchTimeStamp] , [as].[FileName] , [as].[ErrorMessage] FROM

---

6. Is the Database able to read the scans ? *(Very common issue)*

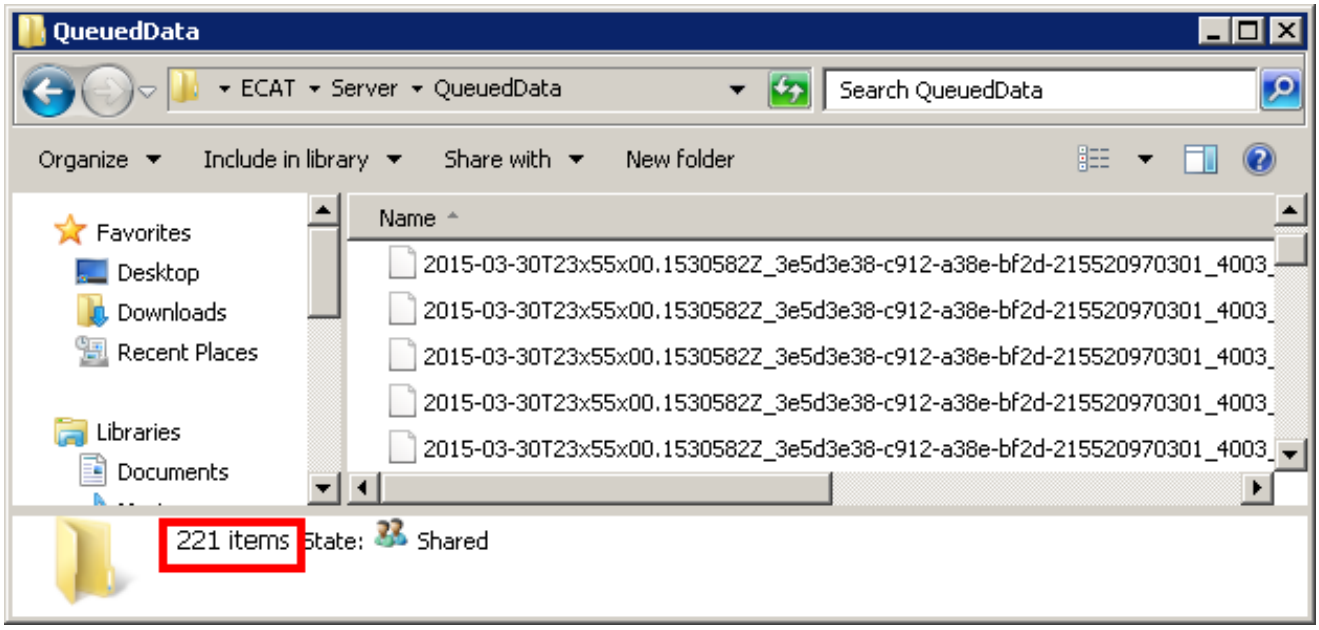
Important: Begin by fully understanding step 5 before investigating step 6.

Once notified that a scan has entered, the Database will do the following steps:

- Read the scan files from the path found in AgentScans

SQL command to see if the Agent scans are consumed:
SELECT TOP(50) [as].[FileName] , [ab].[PK_AgentBatches] -- A batch is a group of files for 1 scan , [ab].[BatchTimeSta
The following error means that the Database might not be able to resolve the path:
Error [usp_StageWithBulkInsert]: Category(2), CSV File is missing , CSV File C:\ECAT\server\QueuedData
\2015-03-30T16x12x09.7017133Z_3e5d3e38-c912-a38e-bf2d-215520970301_4003_0002.scan4

Quick and dirty trick: check the files count in the QueuedData folder:



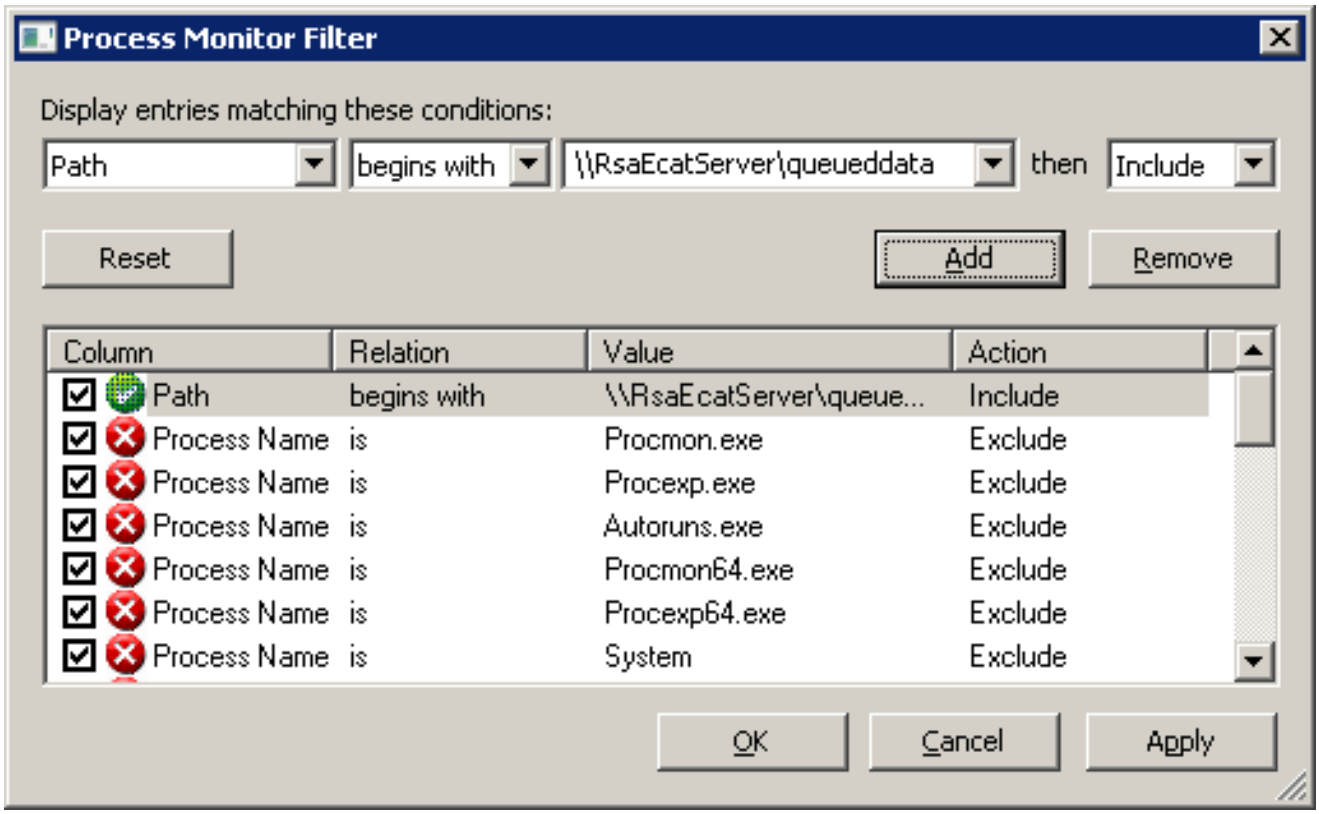
This folder should in 90% of cases automatically empty itself. A situation such as the one shown here might be an indicator of an issue.

6.1 If the Database is on a remote computer

- Verify that the folder is shared: \\[HOSTNAME]\QueuedData
- Verify that ConsoleServer.exe.config has the same value
- Verify that the Database has the permission to access the QueuedData folder

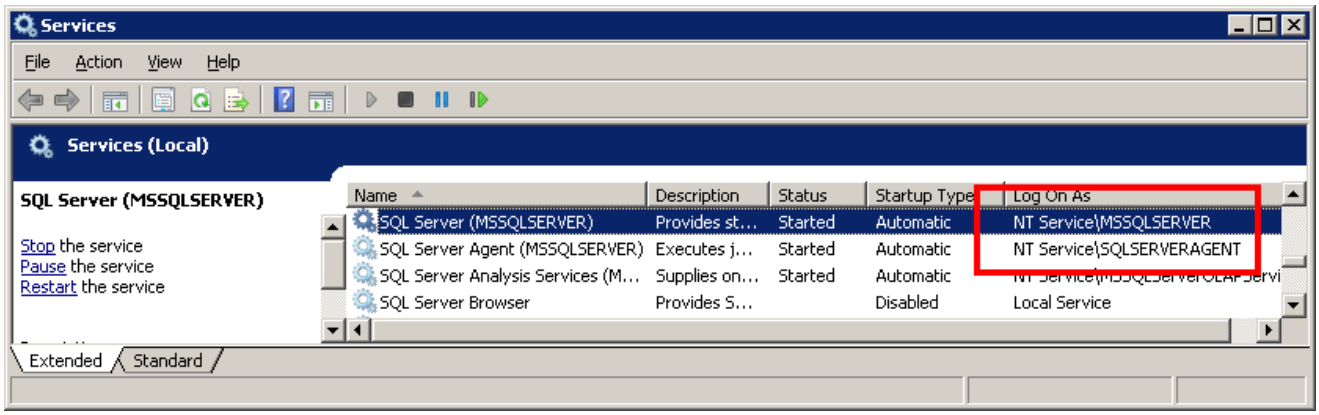
If the QueuedData folder is remote to ConsoleServer, verify that the ConsoleServer user has access to it.
ConsoleServer-error.log can contain the following exception:
30-03-2015 19:27:55
[5] System.NotSupportedException:
The directory "\\RsaEcatServer\QueuedData" does not exist or is not writable. Please review its access rights or those of the parent directory.
  at a.a.c.X . (String A_0)
  at a.b.X ..ctor(String A_0, String A_1, Boolean A_2)
  at a.b.X . ()
Inner-Exception:
[5] System.NotSupportedException:
Logon failure: unknown user name or bad password.

Using Procmon on the **Database** machine can help the diagnosis of Permission issues:



Here is the CSV of this type of filtering:
"19:55:00,8821663","sqlservr.exe","1524","CreateFile","\\RsaEcatServer\QueuedData\2015-03-30T23x55x00.1530582Z_3e5
It shows 3 entries. On the 3rd, we can clearly see that **NT SERVICE\MSSQLSERVER** has denied access the folder **\\RsaEcatServer\QueuedData**.

The users of **both** SQL Server and SQL Server Agent need to access the Shared folder.



Changing the users to domain accounts that have access to the network share and restarting the services is usually the best way to solve this.
Note / reminder: don't restart the services if SQL Server is used for other products in the company ! Ask their DBA to do that work.
112 Views Tags: ecat, ecat 4.0, ecat troubleshooting, ecat faq

There are no comments on this post