The chain reaction started when a customer's line of business application doesn't work with UNCs

devblogs.microsoft.com/oldnewthing/20160531-00

May 31, 2016

Raymond Chen

A customer (via their customer liaison) reported that they use Folder Redirection to put various folders on a network share, but they discovered that one of their line of business applications doesn't work when the application's Data Directory is set to a UNC. The customer is working with the vendor to address the problem, but in the meantime, they need to deploy a temporary fix. What they've found is that they can change the Data Directory for the application in the registry and point it to a local directory.

This works, except that some other unknown line of business application is going in and resetting the registry key back to the network location.

One thing they could try is ask the vendor of the original line of business application if there is a Group Policy that they can use to force the Data Directory to be a specific location. Standard group policy registry keys are kept in a registry key that grants write access only to administrators, which means that the rogue line of business application will not be able to write to it.

Our suspicion was that this avenue of exploration was likely to lead to a dead end, so we had to try some other ideas.

Another idea is to use a Group Policy to deploy a script that sets the registry key for the Data Directory to the local directory. (It appears that there's also a special type of Group Policy setting just for registry entries.) The customer had thought of this, but realized that the rogue line of business application will eventually come along and stomp on the value, so any relief would be short-lived.

To work around this, the customer could mark the registry entry as Process Even If The Group Policy Objects Have Not Changed. The registry key will be set back to the policy value each time Group Policy refreshes.

This is still not great, because it means that when the rogue line of business appliation changes the registry key, it'll take up to 90 or 120 minutes for the policy to refresh and reset the value. The customer could change their refresh interval to lower the size of this window, but it increases the cost of group policy processing across their entire network.

What they can do is set a security audit on the registry key that triggers when a write to the key occurs. That will generate an entry in the security event log which will identify the program that is writing to the key. That will at least let them identify the rogue line of business application, and then they can work with the vendor of that other rogue program to see if they can disable the rogue behavior.[1]

If they cannot disable the rogue behavior, then as a final desperation measure, they could set the key value to the desired value, and then make the registry key read-only. That way, when the rogue line of business application tries to reset the value, it will fail. This does assume two things:

1. The original program can cope with one of its configuration registry keys being read-only.
2. The rogue program doesn't respond to the inability to reset the key by going double-rogue.

[1] Given that the registry key in question is custom to the original line of business application, it's possible that the rogue line of business that is resetting the registry key comes from the same vendor as the original program! But maybe if they're lucky, it's some custom in-house program that they can modify.

Raymond Chen

Follow