

Application Server Runtime issues due to users logging in to Galaxy nodes using ArchestrA Network Account

Download as PDF

Application Server Runtime issues due to users logging in to Galaxy nodes using ArchestrA Network Account

PROBLEM

Title

Application Server Runtime issues due to users logging in to Galaxy nodes using ArchestrA Network Account

SOLUTION

Summary

This *Tech Note* describes runtime issues that can arise when users log in to the Galaxy nodes using the ArchestrA Network Account. It also explains the possible local security policy changes that can be done to prevent the same.

Situation

Application Versions

- Applicable for any version of Application Server

Symptoms

CAUSE

The ArchestrA Network Account is used for node-to-node communication between the Platform nodes in the Galaxy. This account must be the same across all Galaxy Platform nodes for the runtime communications to work. The ArchestrA Application Engines (aaEngine.exe) and other processes run under the context of this ArchestrA Network Account all the time.

This account is configured during the installation. The **Change Network Account** application allows you to make changes to this account after the installation.

If users log in to the Galaxy Platform nodes using this ArchestrA Network Account, there can be runtime issues after the user logs out of the session.

The Windows Operating System unloads the profile and marks certain registry entries for deletion after logging out of the session. Because of this, the Application Engines (aaEngine.exe) can throw random errors when the components running under these processes access the same registry keys that are marked for deletion.

Figure 1 (below) shows an Application Engine that has thrown the errors.

Warning	RedundantIDObjectRuntime2	RedundantIDObject experiencing connection problems with Mx.
Warning	Lmx	MxConnection::SuspendReference - Invalid hRef 0
Warning	RedundantIDObjectRuntime2	RedundantIDObject experiencing connection problems with Mx.
Error	Lmx	Illegal operation attempted on a registry key that has been marked for deletion. (800703fa) raised at line 45 in IMxReferencePtr.h (in D:\BldSrc\9\Ext\Interfaces\Lmx\).
Error	BaseRuntimeComponentServer	CPrimitiveProxy::Execute - The execute method on primitive id 137 threw an exception.
Error	BRO	IngrHFCS0204SP - CBaseRuntimeObject::Execute - Execute on primitive id 137 failed. hr = 80001f4c
Error	BRO	IngrHFCS0204SP - CBaseRuntimeObject::Execute - Going off scan due to error.
Error	IngrHFCS0204SP	- CBaseRuntimeObject::AddError - Going off scan due to error.
Error	Lmx	Illegal operation attempted on a registry key that has been marked for deletion. (800703fa) raised at line 45 in IMxReferencePtr.h (in D:\BldSrc\9\Ext\Interfaces\Lmx\).
Error	BaseRuntimeComponentServer	CPrimitiveProxy::Execute - The execute method on primitive id 140 threw an exception.
Error	BRO	IngrHFCS0204SP - CBaseRuntimeObject::Execute - Execute on primitive id 140 failed. hr = 80001f4c
Error	BRO	IngrHFCS0204SP - CBaseRuntimeObject::Execute - Going off scan due to error.
Error	BRO	IngrHFCS0204SP - CBaseRuntimeObject::AddError - Going off scan due to error.

Figure 1: Application Engine errors

Moreover, there can be other variations of the same problem. In some situations, these errors can appear randomly, even several hours after the ArchestrA Network Account session was logged out.

Action

RESOLUTION

- Do not login to the ArchestrA Galaxy Nodes using the ArchestrA Network Account.
- Currently there is a known issue where the Application Server installation or the Change Network Account application does not add a domain account or any **pre-existing** local account that is used as ArchestrA Network Account to the local security policies **Deny log on locally** and **Deny log on through Remote Desktop Services**.

Application Server can ONLY add a newly-created local account (for ArchestrA Network Account), either during the installation or by running the Change Network Account application to these policies.

- To prevent users from logging on to Galaxy nodes with the ArchestrA Network Account, manually add this account to the **Deny log on locally** and **Deny log on through Remote Desktop Services** policies shown in Figure 2 (below).
- Tech Note 482 (https://softwaresupportsp.aveva.com/#!/knowledgebase/details/000022811?lang=en_US) also recommends for the ArchestrA Network Account to be a member of the above-mentioned local security policies.

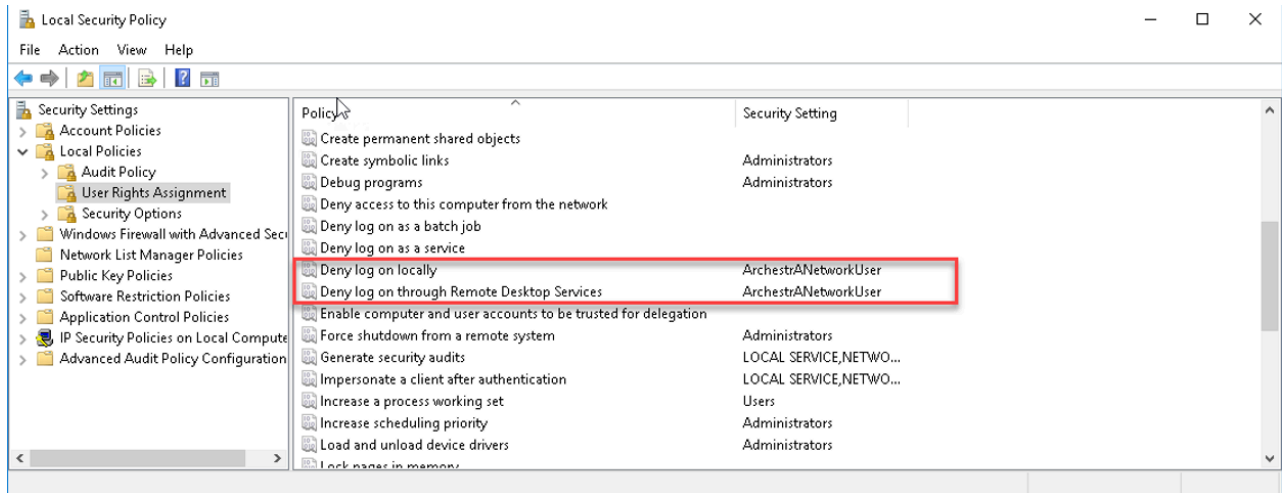


Figure 2: Local Security Policies include ArchestrANetworkUser account

Supporting Information

REFERENCES

Tech Note 482: Troubleshooting Wonderware Application Server Bootstrap Communications (https://softwaresupportsp.aveva.com/#!/knowledgebase/details/000022811?lang=en_US)

Support Article Information

Article

000032631

Subscribe

Legacy Id

TN10542

Article Type

Support Article

Subscribe

Confidence

Expert Reviewed



Published On

Dec 1, 2020

Products

Application Server

Subscribe

