Multi-Galaxy Security: OS Group Security Model

SUMMARY

Reliable security is fundamental to operations spanning the Multi-Galaxy environment. As such, the User Authentication Service (UA

Currently, the UAS only supports OS User and OS Group security modes under a domain controller-based environment.
This document expands on the following two rules of OS Group security mode in a Multi-Galaxy environment.

Rule 1: All domain accounts associated with the target Galaxy must be added explicitly to the Roles on the Galaxy where the Cross G
Rule 2: The specific user account must have established at least one successful login on both the source Galaxy and the target Galaxy

We navigate this topic via the following sections:

1. OS Group Security
2. Analysis and Demonstration for Multi-Galaxy Security Rule 1
3. Analysis and Demonstration for Multi-Galaxy Security Rule 2
4. Demonstration for Verified Write in Multi-Galaxy

Note: Multi-Galaxy is referred to as Paired Multi-Galaxy throughout this *Tech Note*.

SITUATION

Application Versions

- Wonderware Application Server 2012 R2 and 2014

OS Group Security

When an OS user attempts to log into a galaxy, the galaxy security system checks the security global cached data for the OS group(s)
If the OS group(s) is found, all assigned galaxy roles for the OS group(s) will be applied to this logged OS user. Figure 1 illustrates th

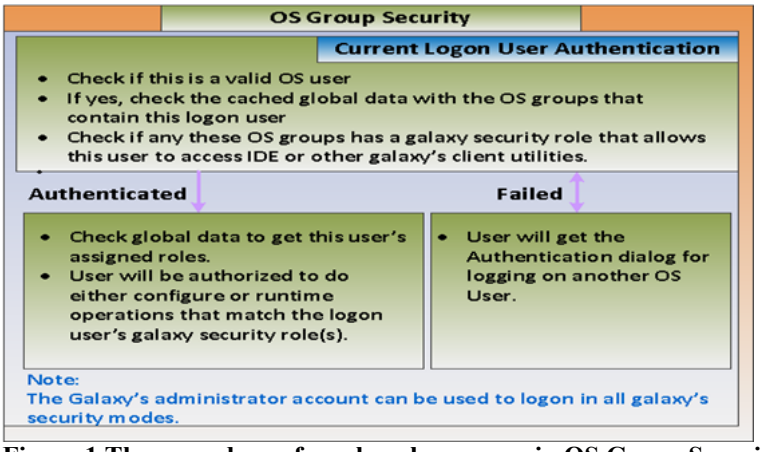

Figure 1 The procedure of a galaxy logon user in OS Group Security mode

Note: The ArchestrA IDE login dialog will not appear if the current logged on OS user is authenticated in either OS User or OS Grou
permission to use the IDE.

ACTION

How to set up OS Group Security including working principles:

1. Initial setup of OS Group Security for a new galaxy:

a. In the IDE log on to the new galaxy as the administrator.

b. Add the Windows group that will be used for OS Group logon in the IDE's "Roles" page, shown in the "Roles" page.
c. Notice that none of the TestGroup1 users (wwuser10 or wwuser11) are shown on the "User" page.

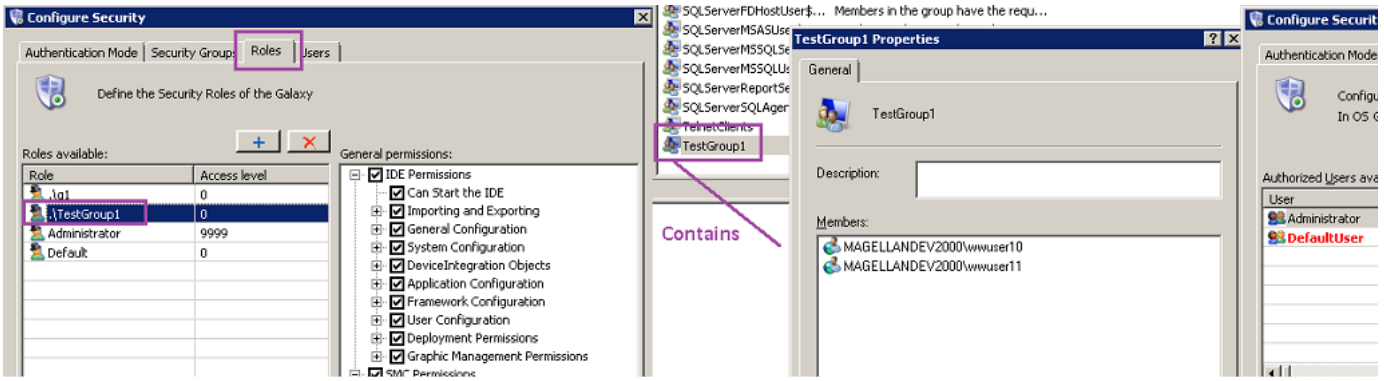

Figure 2 Preparation for OS Group logon

2. Logon to the OS with a user from the OS Group you added in #1 above, wwuser11 in our example, and connect to your gala

Since we added the OS Group (TestGroup1 in our example) which contains this user (wwuser11 in our example) in the Roles pa
authenticated user.

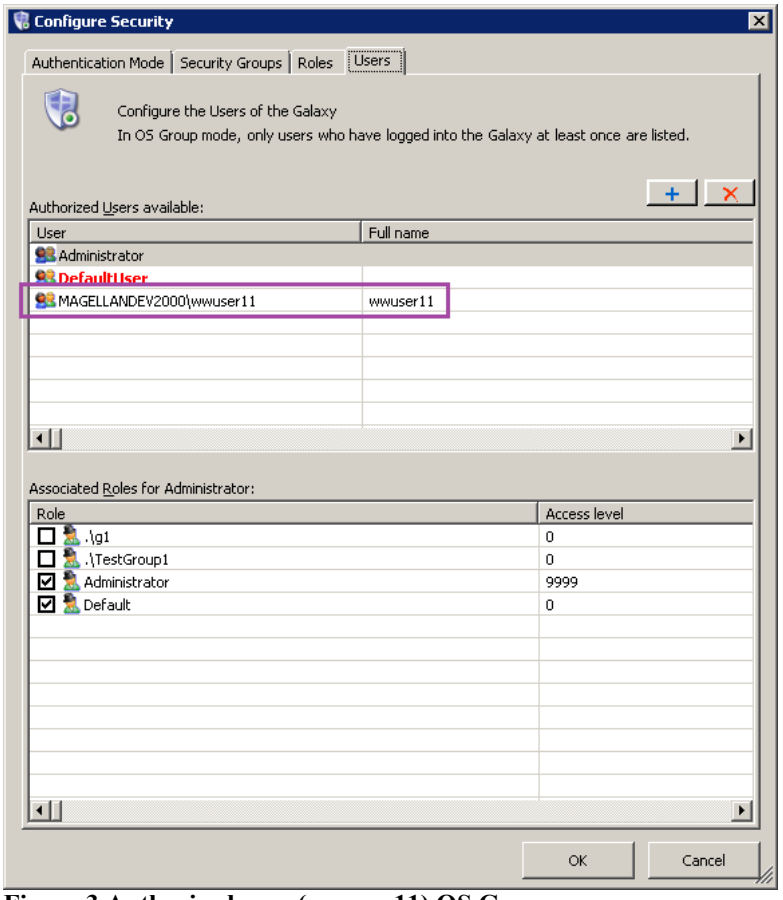

Figure 3 Authorized user (wwuser11) OS Group

**3. At the time of accessing Authentication Mode, the Synchronize process will sync the current logged on user in the OS Grou
platforms' Security Global Cached Data (SGCD).**

The **SGCD** is used by the "ArchestrA User Validator" service for the "Platform Manager" and ArchestrA runtime for attribute s

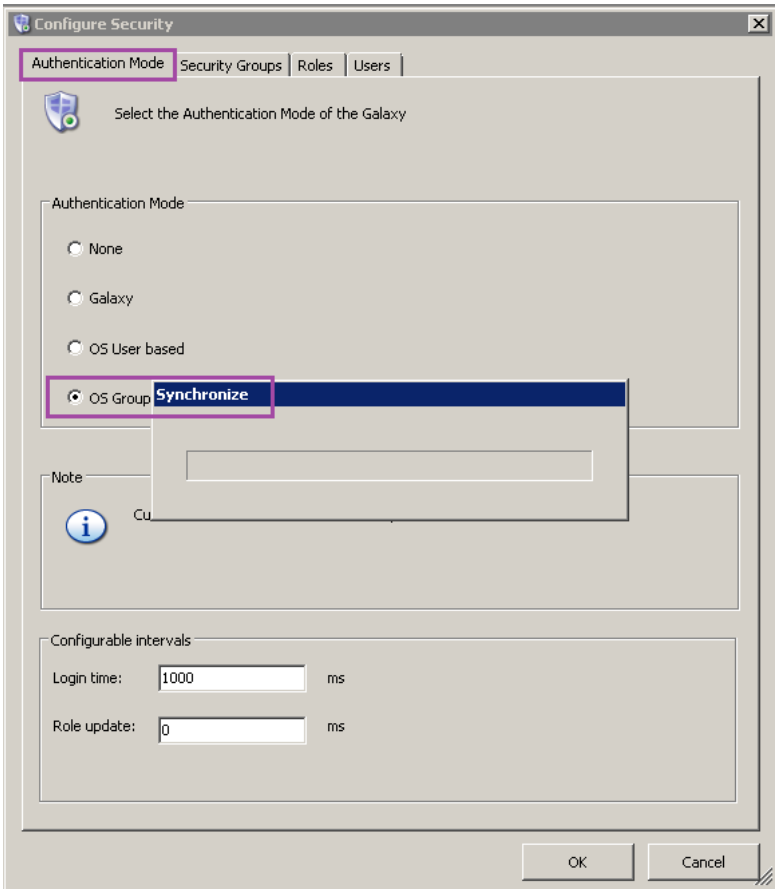

Figure 4 The Synchronize process will initiate when you access the IDE's Configure Security Tool

Note: If the Authentication Mode is "None", Synchronization does not occur.

4. Removal of an authorized user from the Windows user group:

a. Remove the user account (wwuser11 in our example) from the OS group (TestGroup1) as shown in Figure 2.
b. Log out of Windows and log into Windows with the removed user (wwuser11) again.
c. Access the galaxy via the IDE with the removed user account, you will be asked to provide authentication credentials.
d. Once your removed user attempts to log in to the galaxy, your user (wwuser11) is then no longer an authorized user.

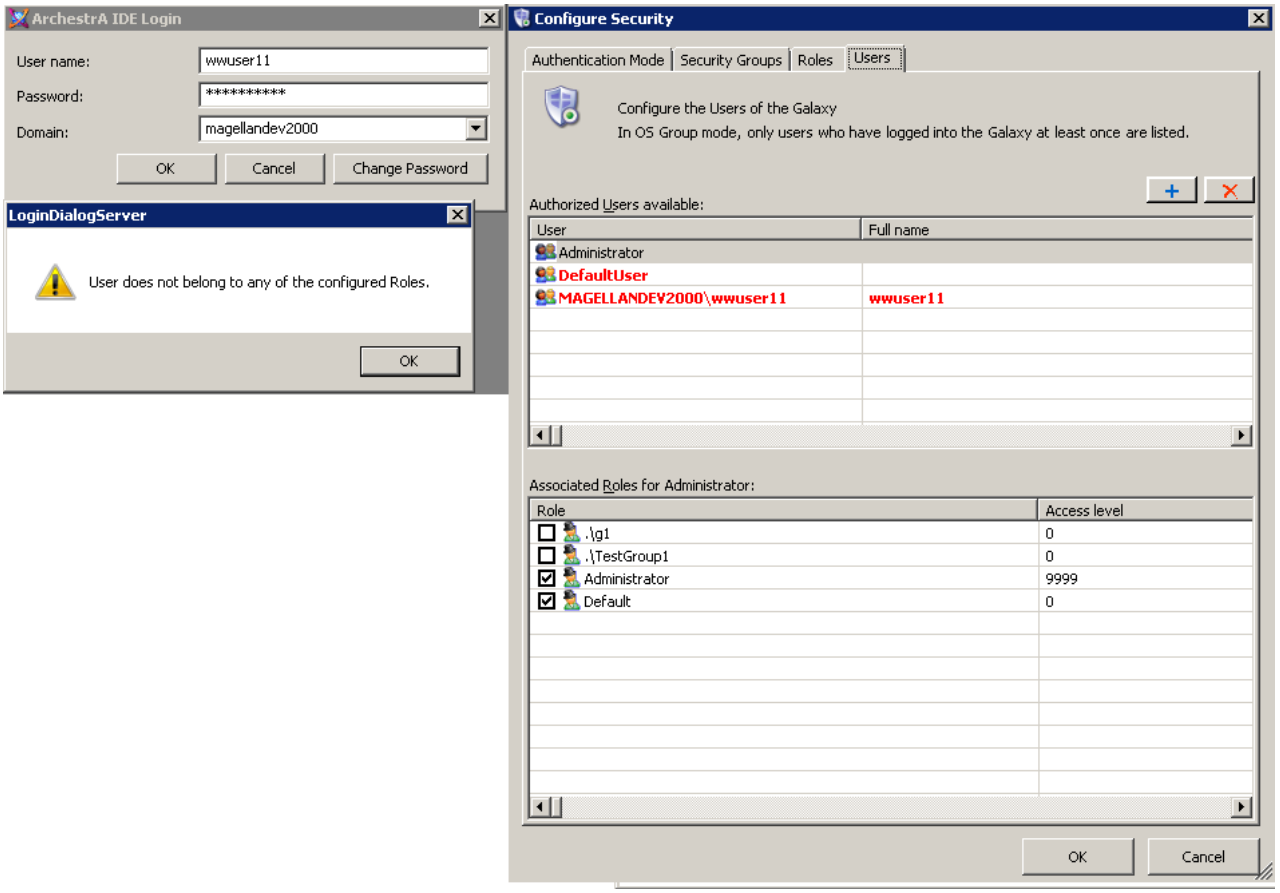

Figure 5 After removing an OS user from the Windows group, the user (wwuser11) will become un-authorized user.

Analysis and Demonstration for Multi-Galaxy Security Rule 1

The User Authentication Service (**UAS**), one of the core ArchestrA Services, builds a security bridge between a paired Multi-Galaxy.

When it comes time to update a value of one of the target galaxy's attributes, the local galaxy will call the ArchestrA Service Bus (**AS** (**WCF**) 4.0 contract, **IData**. Then,

- **IData** will carry the current authorized logged on OS Group user's security token to the target galaxy.
- The target galaxy's **ASB** will check the passed-in security token which contains the domain user from the source galaxy.
- If this domain user is an authorized OS Group user in the target galaxy and has the same security role(s), the permission to updat

For these steps in the Multi-Galaxy Security Model to work properly, we must follow the two rules mentioned in the beginning of this

Rule 1: All domain accounts associated with the target galaxy must be added explicitly to the Roles of the galaxy where the paired ga

Demonstration Setup: OS Groups' setup in the paired galaxies

Galaxy Name	GR Node IP	OS Group Name
MGalaxy1	10.13.18.210	G1 • wwuser13 • wwuser20
Galaxy2	10.13.18.248	G2 • wwuser13 • wwuser20

Table 1 OS Groups' setup in the paired galaxies

Note: The OS Group Names in the Multi-Galaxy can be different. However, they have to contain at least one common domain user w the Multi-Galaxy.

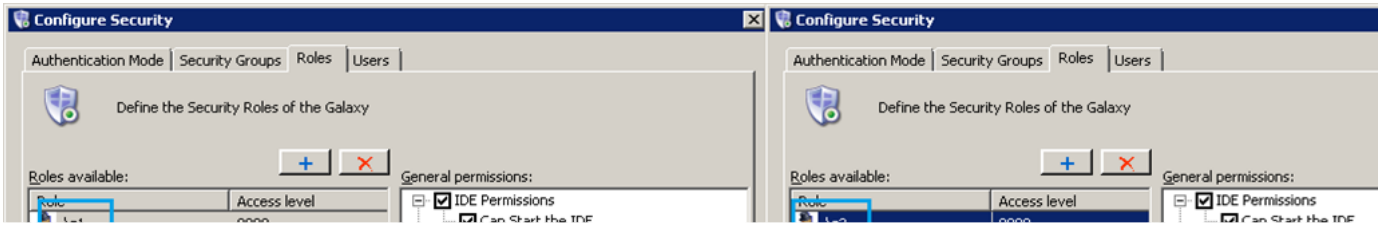

Figure 6 The OS G1 and G2 are added in each Multi-Galaxy's Roles page

Figure 6 illustrates OS Groups G1 and G2 added into the Roles page in MGalaxy1 and Galaxy2 respectively.
In this demonstration, the Role .\G1 and Role .\G2 have the exact same General and Operational permissions. As a result, the OS Gro
the paired Multi-Galaxy.

Note: You can also provide different permission settings in .\G1 and .\G2 Roles, but it will be difficult to troubleshoot if something se

Analysis and Demonstration for Multi-Galaxy Security Rule 2

As previously noted, the Security Global Cached Data (SGCD) plays a vital role in the management of the galaxy security token for b
SGCD for any new or removed OS Group user are done in the IDE's Configure Security interface. The Synchronize process will upd
deployed platforms. The first time that a new OS Group user logs on to the galaxy is important, because this first logon will leave a re
environment, Rule 2 below must be followed.

Rule 2: The specific User account must have established at least one successful Login to both the source Galaxy and the target Galax

Demonstration Setup: Login with two identified domain users into two paired galaxies. After the login is successful, the domain users
authorized users in both MGalaxy1 and Galaxy2.

Galaxy Name	GR Node IP	OS Group Name
MGalaxy1	10.13.18.210	G1 • wwuser13 • wwuser20
Galaxy2	10.13.18.248	G2 • wwuser13 • wwuser20

Table 2 Login with two identified domain users into the paired galaxies

Figure 7 Two same domain users have logged in the MGalaxy1 and Galaxy2

Demonstration for Verified Write in Multi-Galaxy

Demonstration Setup: Verified Write in the Multi-Galaxy. The Verified Write Classification requires two user accounts and these acc paired galaxies.

Galaxy Name	Remote Platform	OS Group Name	
MGalaxy1			
Galaxy2	10.13.18	**UDA**	**G2UDA1**
		Classification	Verified Write

Table 3 The Verified Write Classification requires two user accounts

Note: The full attribute reference in Multi-Galaxy is Galaxy_Name:Platform_Name.URA_Name. In our demonstration, the full refere galaxy2:G2PlatformUDO1.G2UDA1

Figure 8 Do Verified Write on an attribute across Multi-Galaxy

Figure 9 Verified Write is successful

SUPPORTING INFORMATION

References

• Wonderware Application Server 2014 – IDE.PDF
• Celestial Navigation Multi-Galaxy.docx

MORE INFORMATION

Created: January 2015

Authors: E Xu, A. Rantos

Tech Notes Information

Doc ID:	TN765 Subscribe
Doc Type	Tech Note Unsubscribe
Version:	1.0
Status:	Published
Last Modified:	April 22, 2015
Product	• Application Server Subscribe