SERVICE SUPPORT AND BUSINESS APPLICATIONS
LOGISTICS APPLICATION SERVICES

LOGFAS
User Management Module (UMM)
Roles Management Issue

Table of contents

Document change log			
Version	Comments	Date	Author
1.0	Initial version	03 JUNE 2019	Andras AMANN
1.1	Updates	04 JUNE 2019	Marius ROFEL

Summary

Due to a problem in the UMM "Roles" page, LOGFAS user managers must **not use the UMM "Roles"** page to manage role membership. As workaround, the memberships must be managed via the UMM "Users" page.

1. General

Applicability

- This Knowledge Base Article (KBA) addresses LOGFAS ***user managers***;
- The document is describing roles management on servers with multiple databases;
- Applicable LOGFAS versions: ***6.3*** and ***6.4*** series.

Background

Login roles were introduced starting with LOGFAS 6.3.1 as a security update, in order to secure users authenthication when connecting to databases. As the *login roles* were previously managed at the database engine level outside LOGFAS interface, it was necessary to add certain features to *UMM*, in to enable the user managers to handle access of users to databases. This was implemented in the *Attempts* page, which allows user managers to create *login roles* (if necessary) when approving remote database connections. At this moment, it is important to underline that the *login roles* are not stored in databases, even though they are associated with *user accounts*, which are part of databases. The same *login role* may be associated to an *user account*, which sits in multiple databases of a LOGFAS instance.

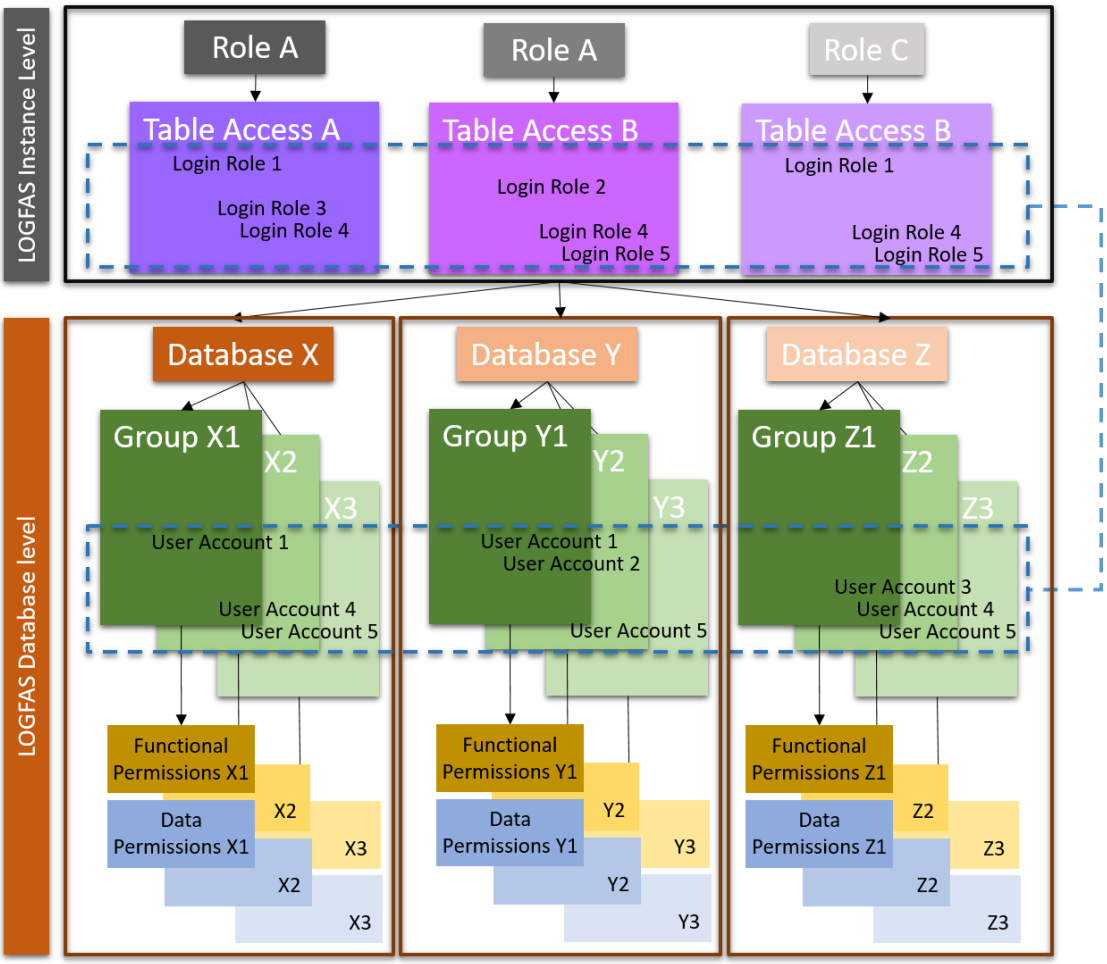
Roles were also introduced together with the *login roles* as an additional feature. The *roles* are directly associated to the *login roles* (indirectly to the *user accounts*), and also managed at the database engine level (not stored in databases). For the same reason of allowing user managers to control the privileges of users, it was necessary to add applicable functionality to *UMM*. This was implemented in the *Users* and *Roles* pages as following:

- Specific table access may be defined for each *role*, referencing standard LOGFAS database structure, therefore applicable throughout all databases:
    - By default, all *roles* have no table access defined, except for:
        - *logfas_user_group*, which comes with complete access rights for all tables in a LOGFAS database structure (*Create*, *Update* and *Delete*);
        - *user_manager*, which enables user managers to control user permissions in UMM over remote connection databases;
    - The *role* table access changes will be reflected in UMM when connecting to different databases, as the *role* is applicable across all databases;
    - Database exports do not include the customized table access per role (the *roles* are not changed in the LOGFAS instance where the database backup is imported to);
- *Role* membership may be set for *login roles* associated to *user accounts* in the active database:
    - *logfas_user_group* role is assigned by default when creating a new *login role* for a *user account*;
    - *UMM* is limited to handling *user accounts* in the active database only, which is why user managers should be aware of the following:
        - A *login role* may be associated to an *user account* stored in multiple databases (the *role* membership changes to a *login role* will be reflected for the associated *user account* throughout all databases whom is part of);

- The *role* membership may include *login roles* associated to *user accounts* in databases other than the active one (the *role* membership changes should affect the *login roles* associated to the *user accounts* in the active database only – ***the following sections include details of an unexpected behaviour for this use case***);
- If a *login role* is deleted then re-created (for an *user account*), any previously assigned *role* membership is lost;
- Database exports do not include *role* membership details (nor *login roles*), therefore the target LOGFAS instance will not include such details following the database backup import).

All *roles* are pre-defined and there is no LOGFAS tool for creating, editing or deleting *roles*, nor options to customize access to tables outside LOGFAS database structure. The following *roles* are available:

- pg_monitor;
- pg_read_all_settings;
- pg_read_all_stats;
- pg_stat_scan_tables;
- pg_signal_backend;
- data_updater;
- eve_manager;
- eve_power_user;
- eve_user;
- guest;
- ldm_manager;
- ldm_power_user;
- ldm_user;
- logfas_user_group;
- user_manager.



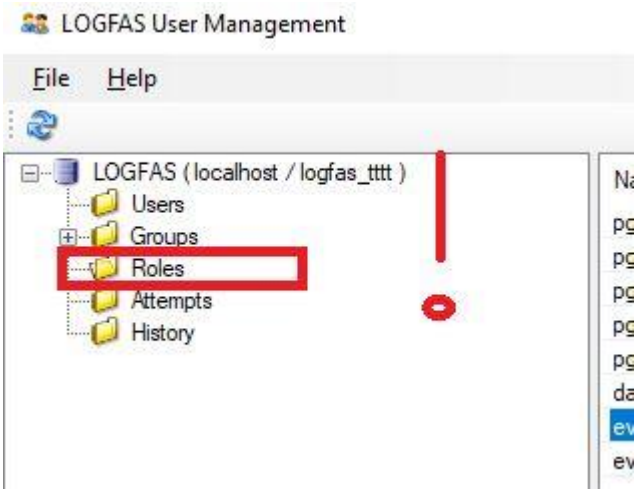
Roles and Permissions Managment in UMM 1

2. Bug Description

As described in the previous sections, UMM should allow *role* membership changes for the *login roles* associated to the *user accounts* in the active database only. While this works correctly in the *Users* page, unexpected results occur when using the *Roles* page.

Problem Details

The *users_for_role…* window in UMM displays the *user accounts* of the active database only. Nevertheless, *user accounts* from different databases may be also assigned to the *role*, but they are not visible in UMM. When removing an *user account* from the *role*, it is expected that no *user account* is affected if not present in the active database. Actually, UMM incorrectly removes from the *role* membership all *user accounts* from other databases, unless present in the active database also. UMM unexpectedly overwrites the *Members/Non-Members* list of *user accounts* in all databases with the current listing, which displays *user accounts* in the active database only.

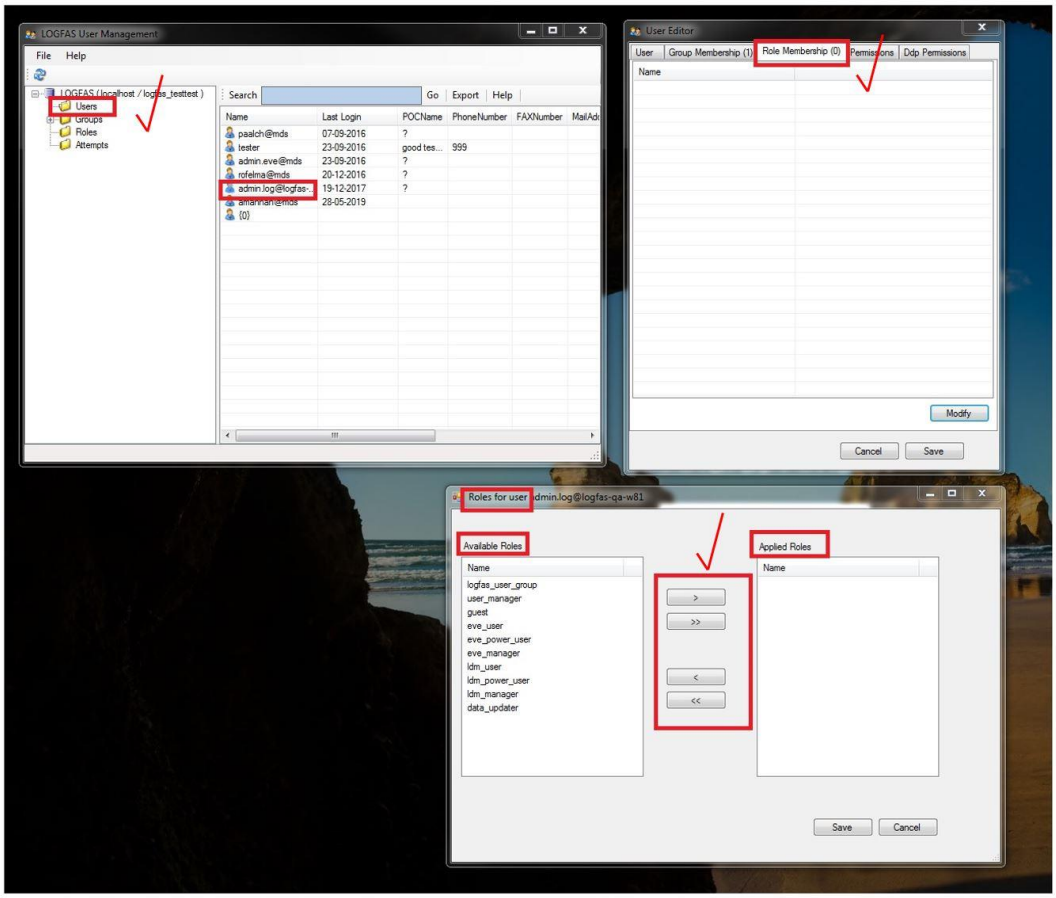


Explanation:
UMM is not aware of *user accounts* in database other than the active one, therefore the above mentioned unintended consequences occur when *role* memberships are changed using *Roles* page.

3. Proposed workaround

Do not assign *user accounts* to a specific *role*, ***assign roles to a specific user*** instead, as described below:

a) Select *UMM Users* page and double-click an *user account* from the list, in order to open the *User Editor* window;
b) Click the *Role Membership* tab, then click on *Modify* button, in order to open the *roles for user…* window:
   - *Available Roles* are listed in the left section;
   - *Applied Roles* are listed in the right section.
c) Use arrow buttons to assign or remove *Available Roles* to the *user account* and click the *Save* button.



If the change is done for a *login role* with an associated *user account* in multiple databases, the *roles* membership updates will be visible in *UMM* for all applicable databases.