Granular security control with function usage

Function usage provides the ability for more granular security controls

Dawn May

October 17, 2013

Function usage provides the ability to implement granular security controls rather than granting users powerful special authorities such as all object, job control, or service. This article reviews the function usage capability and the basics of how to use it.

Introduction

The ability to use many operating system functions is controlled by special authorities. For example, job control (*JOBCTL), all object (*ALLOBJ), or service (*SERVICE) special authorities may be required to perform certain operating system functions. However, these special authorities are quite powerful. How can you allow certain users, such as system administrators, to access the functions that they need to perform without giving them powerful special authorities?

By implementing function usage!

You can limit access to system functions by registering which users can access which functions. You can allow access or deny access using the functional usage capabilities; depending on the component, you can allow one user to change some settings and allow another user to only view those settings. Many system components support the use of function usage capabilities to provide more granular access to their capabilities. Function usage does not eliminate or replace the need for securing resources on your system; it simply provides an additional way to control the functions that a user can access.

Function usage has three user interfaces:

- A graphical user interface (GUI) that allows you to manage the function usage on the system. The GUI for this capability is under Application Administration within IBM ® Navigator for i and IBM System i ® Navigator (where it is an optionally installable component).
- Commands:
  - Change Function Usage (CHGFCNUSG)

    - Display Function Usage (DSPFCNUSG)
    - Work with Function Usage (WRKFCNUSG)
- A set of application programming interfaces (APIs) in the security category under User Function Registration Facility API.

Configuring function usage

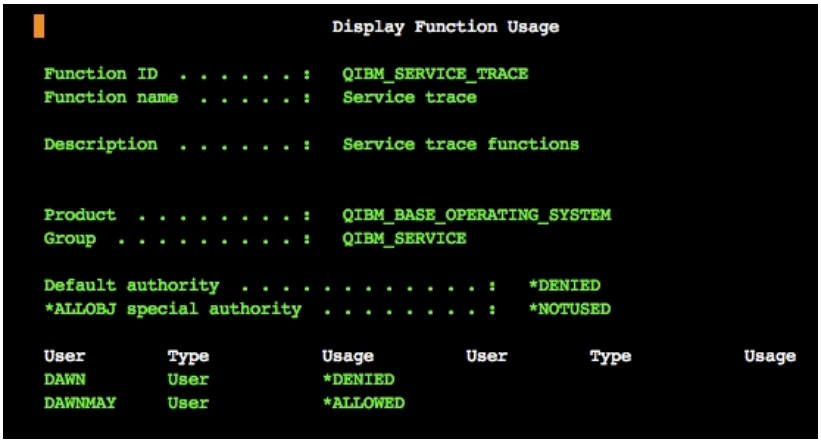
When you need to configure function usage, you can use either the commands or the Application Administration GUI. There are different types of accesses that you can configure:

- You can configure the default access.
  Default access (which is called **default authority** on the command interface) specifies whether users can access the function by default. The shipped setting of the default access can vary by function ID. Possible values are:
    - *ALLOWED – where users are allowed to use the function
    - *DENIED – where users are not allowed to use the function

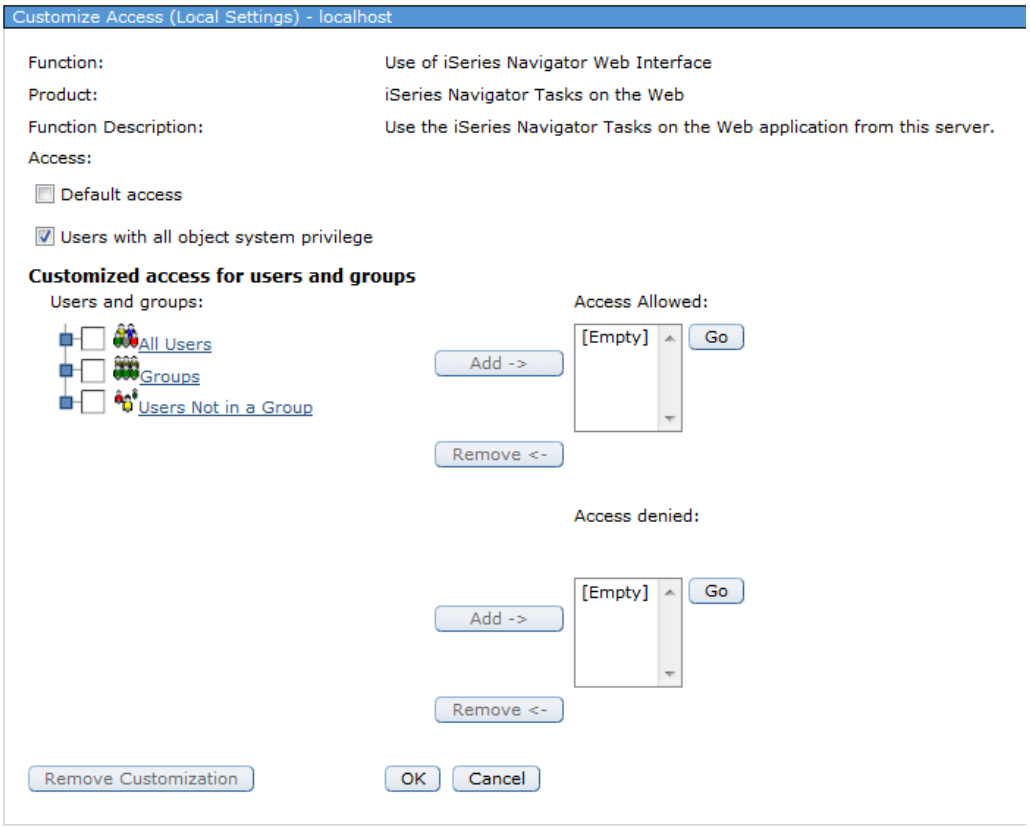
    - You can configure whether you want a user with **all object** access (***ALLOBJ** special authority on the command line) be allowed to access the function. The shipped setting for the all-object access can vary by function ID. Possible values are:
        - *USED – A user with *ALLOBJ authority is always allowed to use the function.
        - *NOTUSED – A user with *ALLOBJ authority must be explicitly allowed to use the function.

        - You can **customize** (**usage** on the command line) the settings for specific users or groups. This allows you to add or remove users or groups in the *Access Allowed* and *Access Denied* lists.

The following screen capture shows an example of the information that you can see with the **Display Function Usage** command. In my example, you can see that I have allowed user DAWNMAY to access trace functions, even though DAWNMAY may not have *SERVICE special authority. User DAWN is not allowed to access trace functions.



The following figure shows the information that is displayed when you customize access for a function ID on the Navigator for i GUI.



Examples

The following sections provide examples of how you can take advantage of this ability to control access in a more granular manner.

Database functions

You can control access to IBM DB2 ® for i administration and monitoring facilities with function usage capabilities; the DB2 for i function usage is available on both IBM i 6.1 and 7.1 releases. The IBM i 7.1 information center topic Authority Options for SQL Analysis and Tuning describes these function usage capabilities.

- Database Administrator - QIBM_DB_SQLADM
  The **Database Administrator** function is needed whenever a user is analyzing and viewing SQL performance data. Some of the more common functions are displaying statements from the SQL plan cache, analyzing SQL performance monitors and SQL plan cache snapshots, and displaying the SQL details of a job other than your own.
- Database Information - QIBM_DB_SYSMON
  The **Database Information** function provides much less authority than Database Administrator. The primary use of this function is to allow a user to examine high-

level database properties. For example, a user who does not have *JOBCTL or QIBM_DB_SQLADM, can be allowed to view the SQL plan cache properties if granted authority to QIBM_DB_SYSMON.
- You can also have more granular control over users who can access the database application server jobs and the DDM/DRDA application server jobs. The Add QIBM_DB_ZDA and QIBM_DB_DDMDRDA function usage IDs article on IBM developerWorks® describes these function usage IDs in much more detail. These function usage IDs were added through program temporary fixes (PTFs). So, be sure to have the DB2 Group PTFs installed.
  - 6.1 - SF99601 - level 25 or later
  - 7.1 - SF99701 - level 16 or later

- Toolbox Application Server Access - ZDA - QIBM_DB_ZDA

This function usage ID allows the ability to restrict access to the optimized server that handles DB2 requests from clients. Server access is used by the Open Database Connectivity (ODBC), OLE DB and .NET providers that is included with IBM i Access for Microsoft ® Windows ® as well as JDBC Toolbox, Run SQL Scripts, and other parts of System i Navigator and Navigator for i web console. It provides an easy alternative (rather than writing an exit program) to control access to these functions from the server side.

- DDM and DRDA Application Server Access - QIBM_DB_DDMDRDA

This function usage ID allows the ability to restrict access to the distributed data management (DDM) and Distributed Relational Database Architecture (DRDA) application server. It provides an easy alternative (rather than writing an exit program) to control access to DDM and DRDA from the server side.

Service functions

The function usage IDs in the service functions category allows more granular access to service functions rather than requiring *SERVICE special authority. *SERVICE special authority and access to many of the system's service tools needs to be managed carefully because incorrect use of certain system tools might cause damage to the system.

There are many types of service functions, and so, there are several function usage IDs associated with the various types of diagnostic work a user may need (such as collecting traces or dumps, or using watches) to allow more granular access to service functions. For example, you can give a user Service Trace usage, which will allow that user to collect traces such as job traces, communications traces, and Licensed Internal Code (LIC) traces, but that user would not have access to any other service tools.

BRMS

Backup, Recovery, and Media Services (BRMS) has implemented extensive use of function usage to control access to specific capabilities. This information is well documented in the IBM i information center.

Auditing

Function usage is audited in the security audit journal. You need to enable auditing and the audit level needs to be configured to record authorization failures. A generic record with type F (function registration operations) (GR-F) audit record is used. This audit record will record the user profile name that the function registration operation was performed against. The audit record also contains the description of the function registration operation that was performed. The possible values are provided in the following table.

Value	Description
*REGISTER	Function has been registered
*REREGISTER	Function has been updated
*DEREGISTER	Function has been de-registered
*CHGUSAGE	Function usage information has been changed
*CHKUSAGE	Function usage was checked for a user and the check passed
*USAGEFAILURE	Function usage was checked for a user and the check failed

A bit of history

The User Function Registration Facility API set was first introduced in V4R3, so this capability has existed for quite some time. The commands were introduced in V5R3, which improved ease of use because a program no longer had to be written to implement the capability.

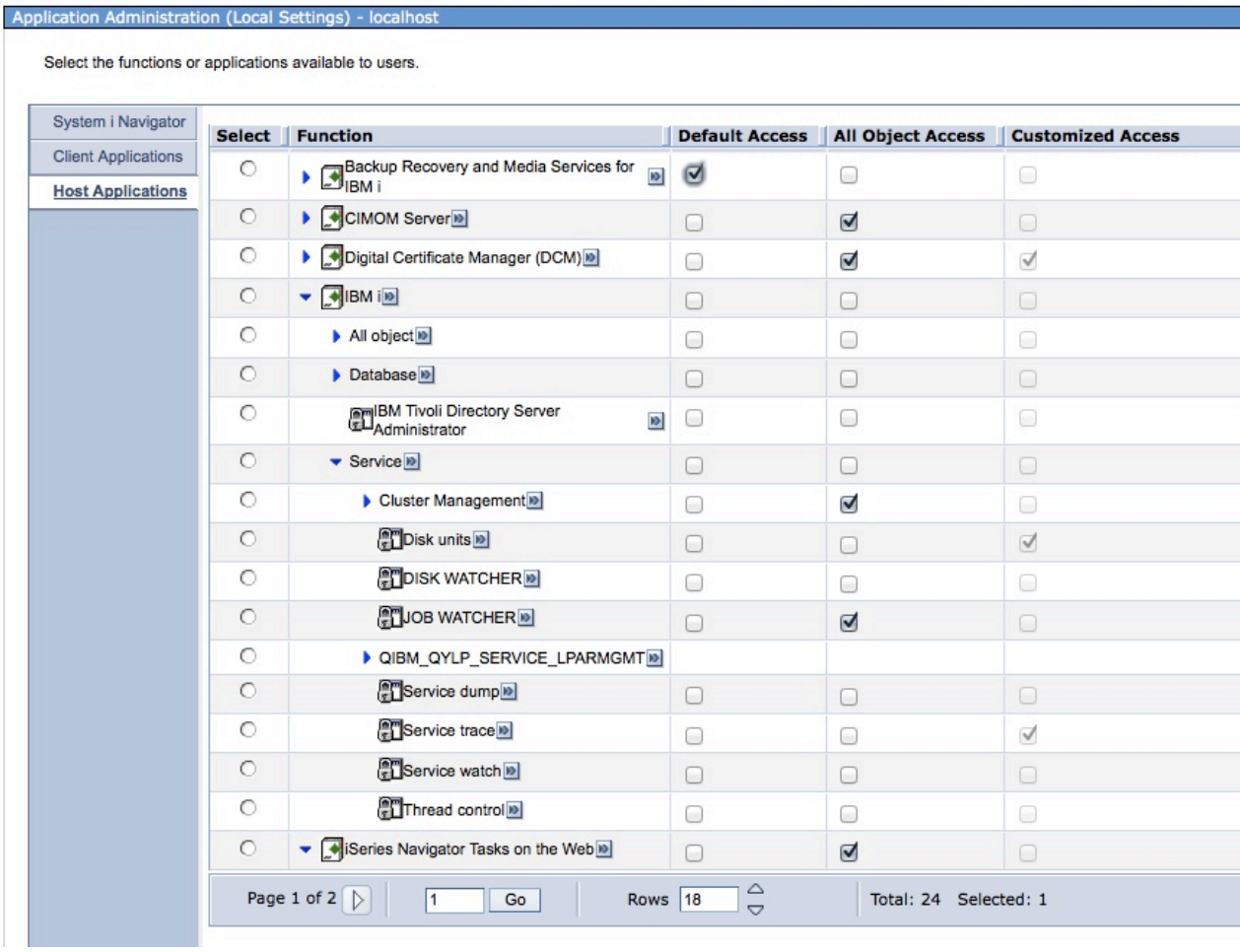
The first use of limiting function access within the operating system was in the V4R5 release when the Trace Connection (TRCCNN) command was introduced. Service commands required *SERVICE special authority; but *SERVICE special authority is quite powerful; you might want to allow someone to collect a dump or a trace, but not want them to have *SERVICE special authority. Today, most of the service commands (traces, dumps, and watches) support customized access through function usage. Since the introduction of TRCCNN, many system components have added support for granular access through function usage.

Documentation

You can use the following options for finding additional documentation on function usage IDs and Application Administration:

1. Use the **Display Function Usage** or **Work with Function Usage** commands.
   The output from these commands displays information about each function usage ID, including the QIBM... function ID string and a description that provides a brief overview of what that function usage ID is for. That description might be sufficient to clue you in as to what that function is for.
2. Use the GUI.
   The Host Applications tab lists the function usage IDs and include a descriptive name that is more meaningful than the QIBM... ID you find on the command-line interface. The following screen capture is an example of what you will see. Many of the

functions are self-describing and you can easily figure out what is controlled from the description.



3. Search for the QIBM... string in the IBM i information center.
   This search returns all the interfaces that check on the specified identifier and this helps to get a good idea of what the function is for. However, it turns out that not all function IDs are documented in the information center, and those that are, generally have information scattered.
4. Search for more information on the Internet.
   Some of the functions have had articles written on them when they were first made available. You can search on the Internet for the QIBM.... string to find additional information beyond what is available in the IBM i information center.
5. Review the reference document on Function usage IDs. This document contains all of the function IDs in one place and includes the information about the functions that are controlled by that ID. This reference is the only place where you can find them all documented at one location.

Conclusion

If you have not been using function usage, you should investigate this feature further. If you have not been using function usage, you might have restricted access to important and useful capabilities of the operating system because you did not want to grant the users the required

special authorities, or you might have given users excess authority that can expose the system to unnecessary risk.

In either case, function usage gives you an alternative security model for a more granular control access to system functions.

Resources

The following references provide additional information on function usage:

- Operations Navigator V5R1 Volume 1: Overview and More has a good chapter on Application Administration. Note that the IBM Redbooks ® documentation is based upon the Operations Navigator client, but the capabilities are the same, even in the browser (IBM Navigator) added in 6.1.
- Functional Usage Capabilities blog.
- Functional Usage Capabilities, Part 2 blog.
- New Function Usage IDs blog.
- Add QIBM_DB_ZDA and QIBM_DB_DDMDRDA function usage IDs article on developerWorks.
- Improved Security Controls Open Door to DB2 for i Tool Usage
- Function usage IDs reference PDF