McAfee
An Intel Company

Database Activity Monitoring Best Practices

Table of Contents

This document contains recommendations from McAfee for creating custom rules and rule objects. It should serve both as a starting point for the implementation of McAfee® Database Activity Monitoring and as an example of the ease of rule creation and management.

Recommended Object Groups

Object groups are groups of elements that can be used as replacement variables inside rules with the $groupname notation. It allows you to decouple the rules from the actual parameters that the rules apply to so that changing those parameters will affect all rules using the group without the need to actually change the rules themselves.

Generic groups

The generic groups are groups relevant to all applications and databases. Those groups will be later used in generic rules as well as in application related rules.

admin_ips

object type = IP

Create a group that will contain either a list of IPs for administrator machines or an administrative subnet (if it exists).

Example: 192.168.1.1, 192.168.1.2, 192.168.0.0/255.255.0.0

suspect_programs

object type = application

This pre-populated group contains a list of programs that allow you to directly manipulate database content without the restrictions of an application. You can edit this group to add various applications used in your organization that should be restricted.

Example—'sqlplus', 'toad','DbVisualizer', 'SQL Developer', 'SQL Server Management Studio', 'osql', 'Microsoft Office', 'sqlcmd', 'plsqldeveloper', 'sqlplusw','sqlnavigator', 'dbartisan', 'tora' , 'rapidsql'

suspect_modules

object type = module

This group is essentially the same as the above suspect_programs group but contains a list of suspect modules such as 'SQL*Plus'. Modules are harder to fake than applications.

Example—'SQL*Plus', 'T.O.A.D'

work_day

object type = weekday

This pre-populated group contains the list of working days for your organization.

Example: MONDAY, TUESDAY, WEDNESDAY, THURSDAY, FRIDAY

work_hours

object type = hour

This group should contain a list of regular working hours.

Example—07, 08, 09, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19

admin_db_usernames
object type = user

This group should contain the list of database administrator usernames.

The group can be populated by running McAfee Vulnerability Manager scans and collecting the list of all administrative accounts.

Example—'sys', 'system', 'dbsnmp', 'sysman', 'sa'

admin_os_usernames
object type = osuser

This group should contain the list of administrator usernames.

The group can be populated by integrating with Microsoft Active Directory or LDAP and pointing to the security group the DBAs are part of.

Example—'oracle', 'joe', 'john', 'jane'

Application-specific groups

The following groups are groups that should be specified per application. The <app> notation in the group name should be replaced with a TLA representing the actual application such as CRM, ERP, or others.

<app>_allowed_programs
object type = application

This group should contain a list of application names that the given application consists of.

Please review "application mapping" to see the actual application names connecting to the database.

Example—'apps.exe', 'console'

<app>_allowed_module
object type = module

This group should contain a list of modules that the application uses. If the application passes the module to the database, you can use this group. Alternatively, you can take advantage of the McAfee Database Activity Monitoring Identifier application plug-in to propagate application modules into the database.

Please review "application mapping" to see the actual module names connecting to the database.

Example—'admin', 'customer', 'account'

<app>_allowed_ips
object type = IP

This group should contain the list of IPs that are allowed to access the application databases. You can also use subnets.

Example—192.168.0.0/255.255.0.0

<app>_db_users
object type = user

This list should contain the database users that own or access the application data. Usually, an application will use a single central database user to own all application tables.

Please review "application mapping" to see the actual users connecting to the database.

Example—'apps'

<app>_os_users
object type = osuser

This group should contain the list of OS users that the application server is running with (in the case of a three-tier application) or a list of allowed OS users in client server architecture.

Please review "application mapping" to see the actual users connecting to the database.

Example—'local_system', 'oracle_ias'

<app>_db_admins
object type = user

This group should contain application-specific administrative accounts in the database.

Example—'apps_admin'

<app>_os_admins
object type = osuser

This group should contain application-specific OS users that have administrative privileges in the database.

The group can be populated by integrating with Active Directory or LDAP and pointing to the security group the application DBAs are part of.

Example—'oracle', 'joe', 'john', 'jane'

<app>_sensitive_objects
object type = object

This group should contain the list of sensitive objects that should be given extra protection. Such objects are usually either tables containing sensitive data (PII, CC) or stored program units used for encryption/decryption of sensitive data.

The group can be populated by running vulnerability manager scans and performing data discovery.

Example—'customers', 'cc_table', 'encryption_pkg'

<app>_end_user_administrators
object type = clientid

This group should contain a list of end-user application administrative accounts. It can be used either if the application is setting the client_identifier database field or by taking advantage of the McAfee Database Activity Monitoring Identifier application plug-in to propagate application end users into the database.

Example—'joe', 'john', 'jane'

<app>_admin_module
object type = module

This group should contain a list of administrative modules in the application. If the application passes the module to the database, you can use this group. Alternatively, you can take advantage of the Database Activity Monitoring Identifier application plug-in to propagate application modules into the database.

Example—'admin', 'account'

Recommended Rules

The following paragraph will specify custom rules that an organization is advised to create to protect its databases. It is recommended that several database groups be created and that the rules be applied to the relevant groups. Examples for such groups are test, staging, and production so that rules will first be applied to the test databases then to staging and then to production. Also, if there are several databases for specific applications, it is recommended that groups be created for them as well. Please note that the following rules should be viewed as recommendations and will probably require refinement for each organization. It is also recommended that rules be created with an initially lower alert level than what's specified below for the first three months (as you are learning about all the applications that connect to the database) and then tighten app the configuration with higher level alerts after the initial refinement.

For each rule, we specify rule name in the title, the actual rule text in quotes and the recommended level of alert.

Generic rules

The following rules should be applied across all the databases (starting from the test group and gradually moving to production). They contain recommended generic protections to restrict access to administrative accounts and to alert on unusual activities in the database.

Restrict admin access

Rule = "user = $admin_db_usernames and (ip not in $admin_ips or osuser not in $admin_os_usernames)"

Alert = High

Alert on suspect programs

Rule = "application contains $suspect_programs or module contains $suspect_modules"

Alert = Medium

Alert on suspect activity

Rule = "weekday not in $work_days or hour not in $work_hours"

Alert = Low

DDL/DCL activity

Rule = "cmdtype contains $ddl_cmdtypes and cmdtype <> 'alter session' or cmdtype contains $dcl_cmdtypes"

Alert = Low

Suspicious activities

The rule will catch access to dictionary views to help catch someone doing reconnaissance. Syntax here is Oracle-specific, but similar rules can be applied to other databases.

Rule = "object in ('user_users', 'user_tables', 'user_tab_cols', 'user_sys_privs', 'user_role_privs', 'user_tab_privs', 'all_users', 'all_tables', 'all_tab_cols', 'all_sys_privs', 'all_role_privs', 'all_tab_privs', 'dba_users', 'dba_tables', 'dba_tab_cols', 'dba_sys_privs', 'dba_role_privs', 'dba_tab_privs')"

Alert = Low

Application-specific rules

The following rules should be applied per application. As with the previous section, it is recommended to apply them to the test databases first and move gradually to the production.

Restrict access to <app>

Rule = "user in $app_db_users and (application not in $<app>_allowed_programs or module not in $<app>_allowed_modules or ip not in $<app>_allowed_ips or osuser not in $<app>_os_users)"

Alert = Medium

Protect <app> sensitive objects

Rule = "object in $<app>_sensitive_objects and (user not in $<app>_db_users or application not in $<app>_allowed_programs or module not in $<app>_allowed_modules or ip not in $<app>_allowed_ips or osuser not in $<app>_os_users)"

Alert = High

Restrict <app> administrators

Rule = "user in $app_db_admins and osuser not in $app_os_admins"

Alert = High

Restrict <app> admin modules

Rule = "module in $<app>_admin_modules and clientid not in $<app>_end_user_administrators"

Alert = High

Restrict <app> sensitive table access

Rule = "object in $<app>_sensitive_objects and statement not contains 'where'"

Alert = High

Summary

Need more information? For technical support and detailed product documentation, please visit the McAfee Support Service Portal.

In addition, you can find valuable knowledge posted by members of McAfee's user community here.

Disclaimer: These recommendations for rule objects and rules will require some refinement for each implementation of McAfee Database Activity Monitoring.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

51500gde_dam_0912_fnl_ETMG