Report Diagnostics

Last Modified on 16/04/2019 7:05 pm AEST

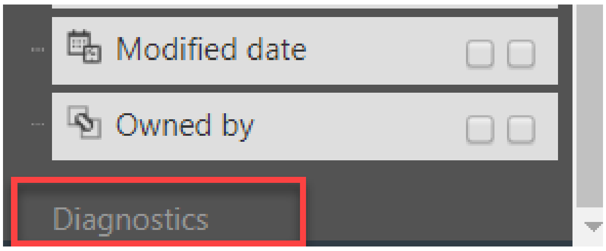
The report diagnostics tool has been designed to diagnose and improve report performance.

In order to improve report performance, it is helpful to understand how the:

- report is structured
- security rules are applied
- data is cached and shared

How to run the report diagnostics

1. Select the required report and go to the report builder
2. Scroll down the left-hand field list to the bottom
3. Clicking on the grey **Diagnostics** link will open the Report Diagnostic tool



4. Select the **User** context for the report analysis
5. Then select **Show Diagnostics**

The tool will only analyse the saved report. If you have unsaved changes, then the report will only show the result as of the last save.

If the user that you are trying the run the report as does not have access to that report, you will receive a *Forbidden* message.

Report Diagnostics Sections

Caching

This areas shows ways a report can cached:

1. **Cachable and shareable between users** - The server will cache the result set, and provide this cached result to other users in the same role until a relevant change is detected. This is most preferable for good report performance.
2. **Data cachable, but user-specific** - The server will cache the result set, but it will only be reserved back to the same user.
3. **Plan and data uncachable** - The server cannot cache the result set. This likely to occur for reports that depend on time.

Referenced Object Types

This area lists all the types of objects that are used on the report. Any object that is potentially accessed in a report is significant, because it determines the access rules that need to be considered.

- **Full grant**
  - If an access rule is found that grants **Read** access to all records of a particular object, then ***full grant*** will be shown.
  - The access rule may also provide create, modify, delete but only *read* is relevant to reports.
  - The access rule may also be applied to a parent or ancestor object but not derived type.
  - Reports will perform fastest when every object is ***full grant***.

- **System rules**

  - In addition to visible access control rules, there are internal system access rules.
  - For most users these do not apply, but for certain system/admin objects they may.
  - If there are any applicable system rules, then ***system rules*** is shown

Nodes

Nodes are arranged in a tree-like structure starting with the object the report is based on, then following relationships to corresponding objects that also exist in the report. Information will also also include nodes when data is summarised or calculations are performed.

- **Relationships**
  - the direction of the relationship is marked with either ***Fwd*** or ***Rev***.

    - the cardinality of the relationship is marked with either ***to-one*** or ***to-many*** *s*hows how many related records may be returned.
    - recursive relationships are also indicated.
- **Summarise operations**
    - appear in the node list as ***Aggregate.***
    - will appear as either ***Ungrouped*** or ***Grouped***, for the later, indicating that some descendant nodes have field values used for grouping
    - if there are two separate paths of relationships that contain 'to-many', then the top node of each path will indicate (crossed). This is because the results of the two separate paths are effectively multiplied out. A message is also shown below the node table indicating that crossed joins are present is not ideal and may affect performance.

Each node is typically is secured in one of the following ways:

- **Secured**
    - access rules are applied in the normal manner.
    - if a node is full grant, then***full-grant*** is shown, meaning this node gets optimised.
- **Implicitly secured**
    - access that has been granted via the relationship means that the security check can be optimised by virtue of the records relationship with its parent.
- **Unsecured**
    - the tenant administrator has used the !unsecured option in a calculated-field to explicitly suppress security checks for this node.
- **Explicit security check (bad!)**
    - access that has been granted via the relationship but in the opposite direction being followed in the report, will mean that the report engine must enter a special mode to evaluate security correctly, which can be *very slow.*

Calculations

All calculations are listed out as either calculated columns, conditions or calculated fields along with the type of calculation.

Calculations can substantially increase the number of nodes in a report.

Inherited/Derived Types

In order to determine what type of security rules apply, it's also helpful to understand inherited and derived objects.

The total set of security access rules that apply to an object include:

- rules applied to the object itself
- rules applied to ancestor objects
- rules applied to derived objects
- rules applied to other ancestor objects of derived objects (if at least one derived type contains multiple ancestor objects)

Objects in (slow) secures flags mode

This section lists any objects used in the report that was necessary to enter the slow mode to evaluate an explicit security check. This means that any objects that have been used that have been granted access via the relationship but in the opposite direction.

The system will add the word ***activated*** to explicitly indicate that the mode was activated. If there are any objects in this list, then it is a good idea to carefully review the structure of security rules, relationship security flags, and the report itself.

Suggested workarounds if you find yourself in the slow secures flag mode:

- Create an access rule that provides full access to the object that to be secured via the flag. For this to work, there must be no conditions applied, otherwise it will fall back into the slow secures flag mode.
- If you are accessing the node via a calculation, you could also 'un-secure' the calculation using the !unsecured function. Use this with caution, as you may need to not be appropriate to 'un-secure' column data.

User Security Roles

This section lists all of the security roles that apply to the current user.

The user may be directly assigned to those roles, or the role may be include other roles (directly or indirectly) that the user is assigned to.

Access Control Rules

This is the list of access control rules that have been found to be relevant, for the current user, to the objects used in the report.

This section includes:

- object that the rule is applied to
- name of the access rule
- name of the role
- details about the rule and how it got used