STEALTHbits Access Library

How-To Guide

Access Rights Reporter for

PostgreSQL Databases

PostgreSQL

Version 1.0

4/1/2019

Table of Contents

Introduction

This document is designed to enable a user to install, configure, and execute the Access Rights Reporting Module (Module) for PostgreSQL Databases in their environment.

This Module will connect to a PostgreSQL instance, collect a list of databases, roles, role members, permissions, and objects, then concatenate that data into a view within the StealthAUDIT® Access Information Center (AIC). This will show the permissions of accounts on individual pieces of content within the PostgreSQL environment.

StealthAUDIT® Overview

STEALTHbits' StealthAUDIT Management Platform helps organizations collect and analyze the data they need to answer their most difficult questions in the management and security of their critical IT infrastructure, data, and applications. Unlike point-products designed to address only a single need, StealthAUDIT is a true framework. With preconfigured solutions to address your most common requirements, as well as an extensive toolset for you to create solutions of your own, StealthAUDIT remains relevant even when your requirements change.

Key Features & Benefits:

- **Preconfigured Solution Sets** – StealthAUDIT contains out-of-the-box, ready to run Solution Sets aligning to Data Access Governance for Unstructured and Structured Data, Active Directory Management and Security, OS-level Auditing and Governance, and more.
- **Process Automation** – StealthAUDIT seamlessly ties together disparate processes, creating fully automated solutions that save time, avoid unnecessary costs, and alleviate burden on IT.
- **Governance** – Not all the data you need can be obtained from a system or application. StealthAUDIT provides both simple and sophisticated methods of retrieving and incorporating end-user feedback into the data analysis and decision-making process, including Entitlement Reviews, Self-Service Access Requests, and more.
- **Technology Integration** – StealthAUDIT can push and pull data to and from dozens of technologies (including home-grown systems) to enhance the value of existing and future technology investments.
- **Consolidated Reporting** – StealthAUDIT can report on any available dataset, enabling organizations to automate a multitude of reporting tasks, as well as view all of their reports in a single pane of glass.

Access Rights Reporter for PostgreSQL Module

This document describes the process for installing and configuring the PostgreSQL Module for the STEALTHbits Access Library into an environment where the StealthAUDIT Management Platform and the AIC are already installed and running.

Prerequisites

Prior to installing the module, please ensure you have administrator rights on the StealthAUDIT console, as well as enough rights to download or copy software to the machine on which it is hosted.

You will need access to an administrator account for the PostgreSQL instance.

Configuration

The following steps can be prepared ahead of time to query for PostgreSQL information.

Creating the Host File

Step 1: Generate a blank text file titled "Hosts.txt".

Step 2: Input into this text file the list of all PostgreSQL databases to query against. This expects IP address, a colon, port number, a comma, and database name. Separate each entry on a different line. An example is below:

- 192.168.37.77:5432,postgres
- 192.168.40.72:5432,postgres

Save this file for later use.

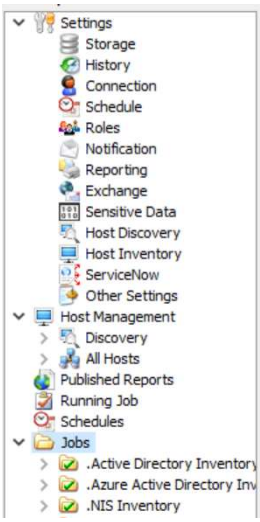
Implementation

This section will walk you through how to extract the package you have downloaded from the STEALTHbits website in the optimal way, as well as configure the information collected in the configuration section appropriately to run this Module.

Extracting the Downloaded Package

Follow the steps below to extract the downloaded package:

Step 1: Create a new Group in the StealthAUDIT Job Hierarchy by right-clicking at the "Jobs" scope and choosing "Create Group". Name the group however you choose.



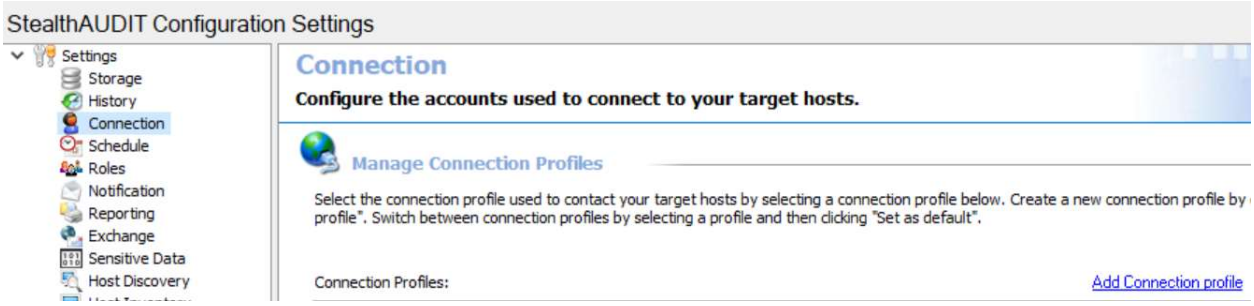
Step 2: Right-click on the new Group and choose Explore Folder. The directory that opens is where the new Job that has been downloaded will be placed. Extract the job to this location.

Step 3: Either relaunch the StealthAUDIT console, or right-click on "Jobs" and choose "Refresh Tree". Your new Module should now be visible.

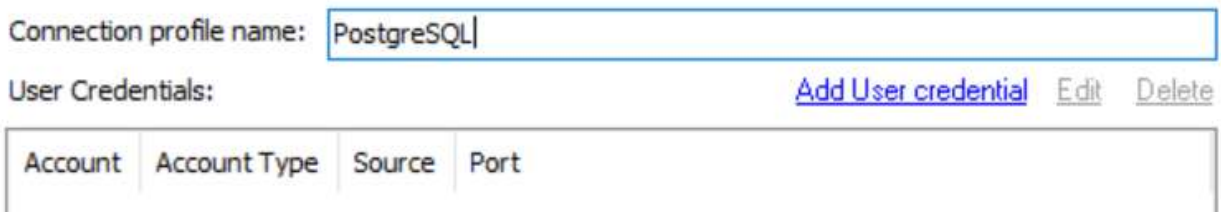
Setting up the Module

Follow the steps below to set up the Module:

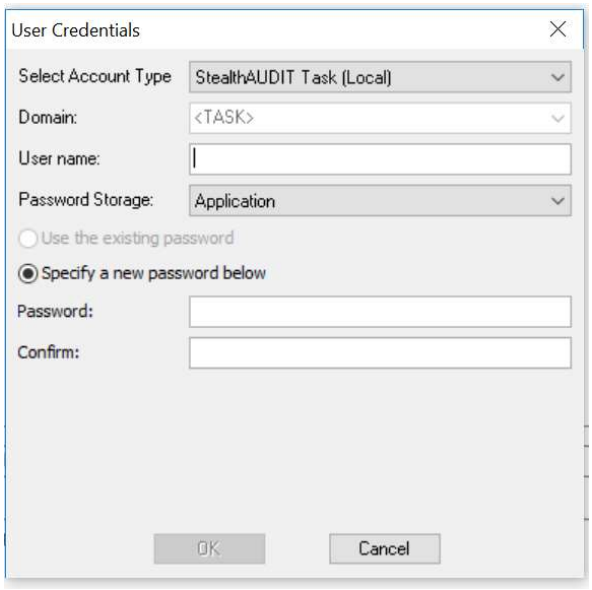
Step 1: Add a new set of credentials by navigating in the StealthAUDIT hierarchy to "Settings" -> "Connection". Click "Add Connection Profile".



Step 2: Name the profile however you choose. Click "Add User credential".



Step 3: For the Account Type choose "StealthAUDIT Task (Local)". The User name will be the login name of the administrative account that will be used. The Password will be the password of that account.



Click "OK" when done, then click "Save".

Step 4: Right-click on the Job in the StealthAUDIT hierarchy and choose "Explore Folder". Replace the Hosts.txt file here from the one in the previous steps.

Execution

Set the Host Assignment to "Local host". To execute, right-click on either the parent folder or job scope. Choose either "Run Group" or "Run Job" respectively. This will allow the Job to collect the necessary information and import it into the AIC.

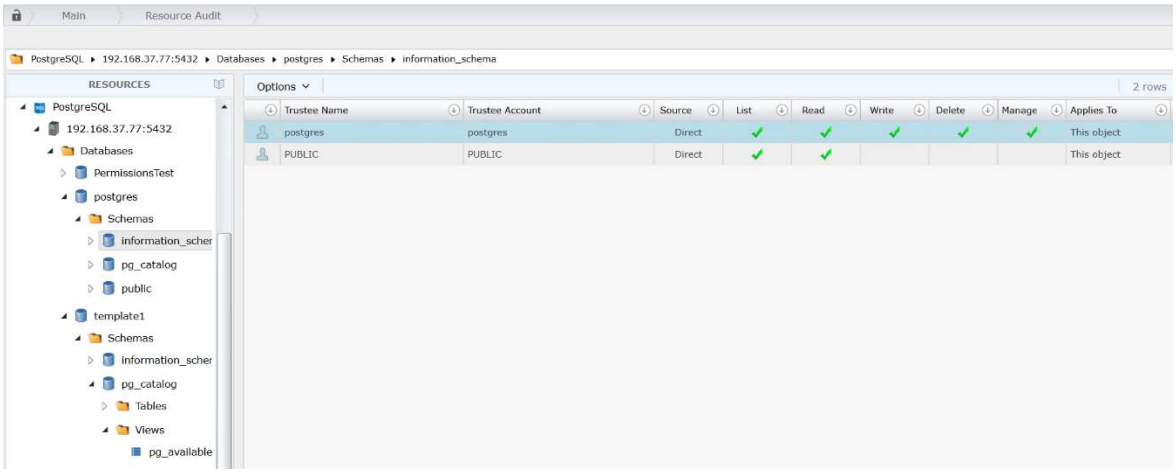
See Results

Identifying in the AIC

Content will be output to the AIC to show access. No reports are included with this Module.

Step 1: Launch the AIC by double-clicking the icon on the desktop, navigating to the direct URL, or accessing it any other way that may be configured. Login as needed.

Step 2: Click on Resource Audit. Navigate to "PostgreSQL" on the left-hand hierarchy. Expand out to see additional details.



Information is broken down in a hierarchal view by PostgreSQL -> Server -> Database Collection -> Individual Databases -> Child scopes. Clicking on a scope shows the permissions on all objects within that container.

Access Library Overview

STEALTHbits' Access Library is a site where STEALTHbits and STEALTHbits' users can post and share data access "connectors" for data repositories not natively supported within StealthAUDIT. Once validated by STEALTHbits, connectors can be posted and shared with the entire STEALTHbits community, whereby licensed StealthAUDIT users can browse and download connectors for free. The connectors and the data they collect are subsequently displayed within StealthAUDIT's Access Information Center (AIC) or used for custom reporting within StealthAUDIT.

Legal Notice

Legal Notice

The information in this publication is provided for information use only, and does not constitute a commitment from STEALTHbits of any features or functions, as this publication may describe features or functionality not applicable to the product release or version you are using. STEALTHbits makes no representations or warranties about the Software beyond what is provided in the License Agreement. STEALTHbits assumes no responsibility or liability for the accuracy of the information presented, which is subject to change without notice. If you believe there is an error in this publication, please report it to us in writing.

The STEALTHbits logo and all other STEALTHbits product or service names and slogans are registered trademarks or trademarks of STEALTHbits Technologies, Inc. Non-STEALTHbits vendors and products referenced in this document are either registered trademarks or trademarks of those organizations in the United States and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

Disclaimers

This document may contain information regarding the use and installation of non-STEALTHbits products. Please note that this information is provided as a courtesy to assist you. While STEALTHbits tries to ensure that this information accurately reflects the information provided by the supplier, please refer to the materials provided with any non-STEALTHbits product and contact the supplier for confirmation. STEALTHbits assumes no responsibility or liability for incorrect or incomplete information provided about non-STEALTHbits products.