Managing Snowflake Roles, Grants, and Privileges with the Snowflake Grant Report Tool

Overview

Snowflake Role-based Access Control (RBAC) offers customers powerful tools to configure authorization to secure their systems, including the ability to build a hierarchy of roles and assign a mix of granular permissions for combined effective permissions.

Snowflake Grant Report extracts Roles and Grants data from Snowflake and provides tabular and visual reports on the Role hierarchy and Grant assignments, reducing the cognitive effort necessary for a full understanding of customer's security posture.

RBAC Design

Snowflake's RBAC features define who can access and perform operations on specific objects (tables, views, schemas, etc.) within an account.

Snowflake Professional Services QuickStart, Best Practices, and Security Consultation offerings help customers plan their Snowflake deployment, including help with appropriate RBAC architecture and Role structure.

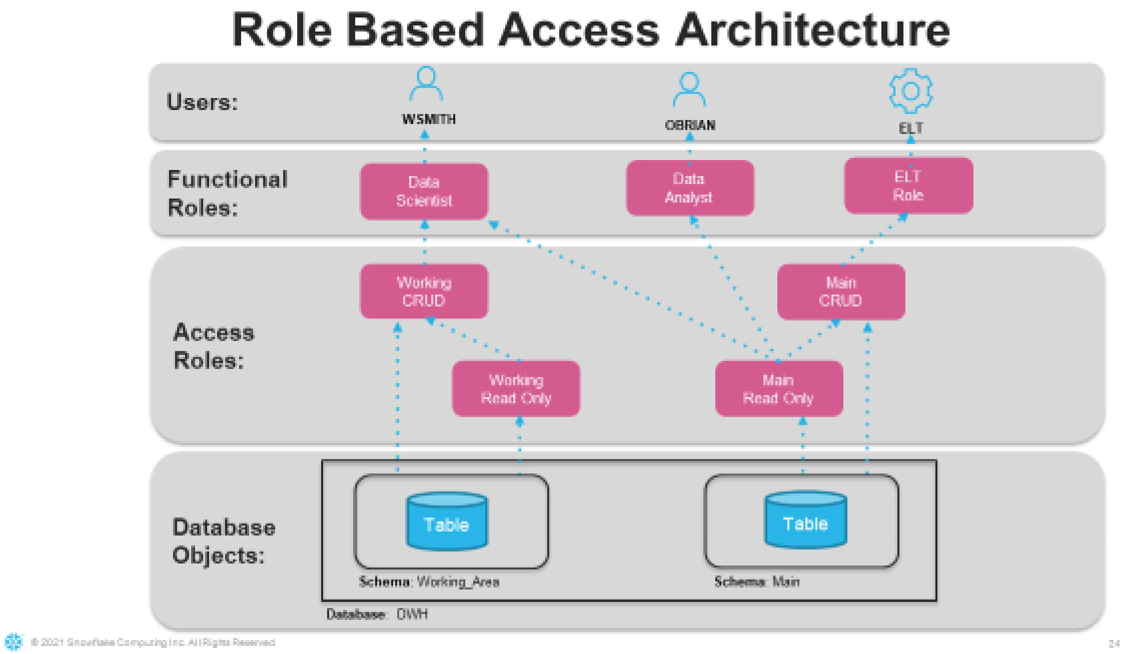
On other hand, many customers experience RBAC configuration in a more organic way. A customer can choose a very flat Role or an exceedingly deep hierarchy. Some customers even take on a heavy administrative burden of managing thousands of individual Roles for each user, including dealing with tens of thousands of unique grant permutations.

As a result of organic or unplanned growth, customers can have unintended holes in their Snowflake security, lock users out of essential resources, and have an unnecessarily high level of administrative burden, potentially leading to dissatisfaction and poor business outcomes.

Functional and Access Roles

One of the core recommendations customers hear from Snowflake Professional Services consultations focused on RBAC design is use of Functional and Access Roles. The fundamental idea is that Access Roles can only contain Privileges, while Functional Roles can only contain other Roles.

In this example, there are 3 Functional Roles (Data Scientist, Data Analyst, and ELT Role) that represent personas doing specific job function. Access to databases is granted to those personas by including Access Roles (Working CRUD, Working Read Only, Main CRUD, Main Read Only) in the Functional Roles, and assigning specific permissions to those Access Roles.



Example of RBAC Functional and Access Roles

When Snowflake Roles include other Roles, they can form POLYarchy instead of straightforward hierarchy, which means that there can be multiple "roots" that are not related to each other.

For more about Functional and Access roles, take a look at "A Functional Approach For Snowflake's Role-Based Access Controls" article.

Reviewing Grants and Role Privileges

With any deployment of meaningful size, customers begin asking questions like this:

- How can I review and manage all privileges assigned to my database objects and compute resources?
- How can I document access levels for regular audits?
- Who has access to what and why?
- How can I understand which Roles are included in other Roles?

Snowflake provides data dictionary object metadata, as well as historical usage data via a shared database named SNOWFLAKE. Specifically, the GRANTS_TO_ROLES and GRANTS_TO_USERS views provide all the data necessary to answer the questions mentioned above.

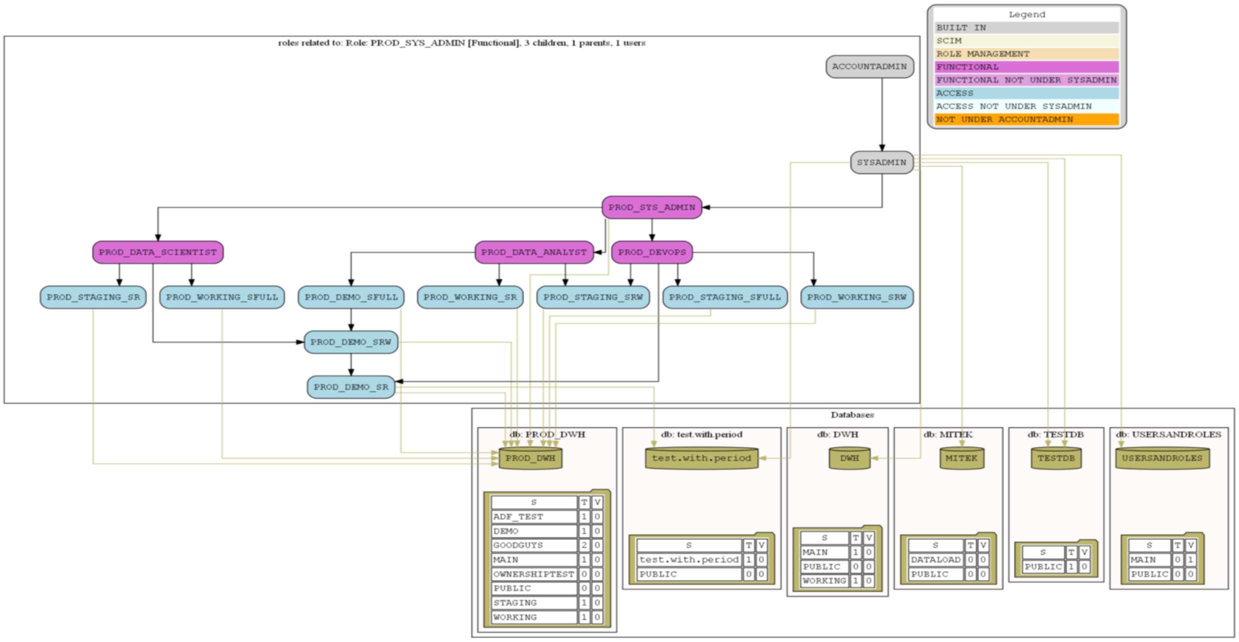
However, depending on the number of Roles and Grants in play, the dataset in GRANTS_TO_ROLES can be quite large and can require significant cognitive effort to interpret. Additionally, the Role structure visualization is not yet available in the Snowflake console.

Snowflake Grant Report

Hoping to address the aforementioned challenges of discovery and documentation of current privileges and understanding of Role polyarchy, I built Snowflake Grant Report, a tool that offers a way of visualizing role structure and helps with rapid diagnosis of as-is permissions.

Snowflake Grant Report retrieves list of Roles, Grants and Users from Snowflake and creates tabular reports in universally accessible Excel and CSV formats with tables and pivots. Role polyarchy is visualized in SVG, PNG and PDF formats, easily displayed in your web browsers.

Here is an example of visual representation of Role structure and Databases used by those Roles, color-coded to Role Functional/Access type:



S	T	V
ADF_TEST	1	0
DEMO	1	0
GOODGUYS	2	0
MAIN	1	0
OWNERSHIPTEST	0	0
PUBLIC	0	0
STAGING	1	0
WORKING	1	0

S	T	V
test.with.period	1	0
PUBLIC	0	0

S	T	V
MAIN	1	0
PUBLIC	0	0
WORKING	1	0

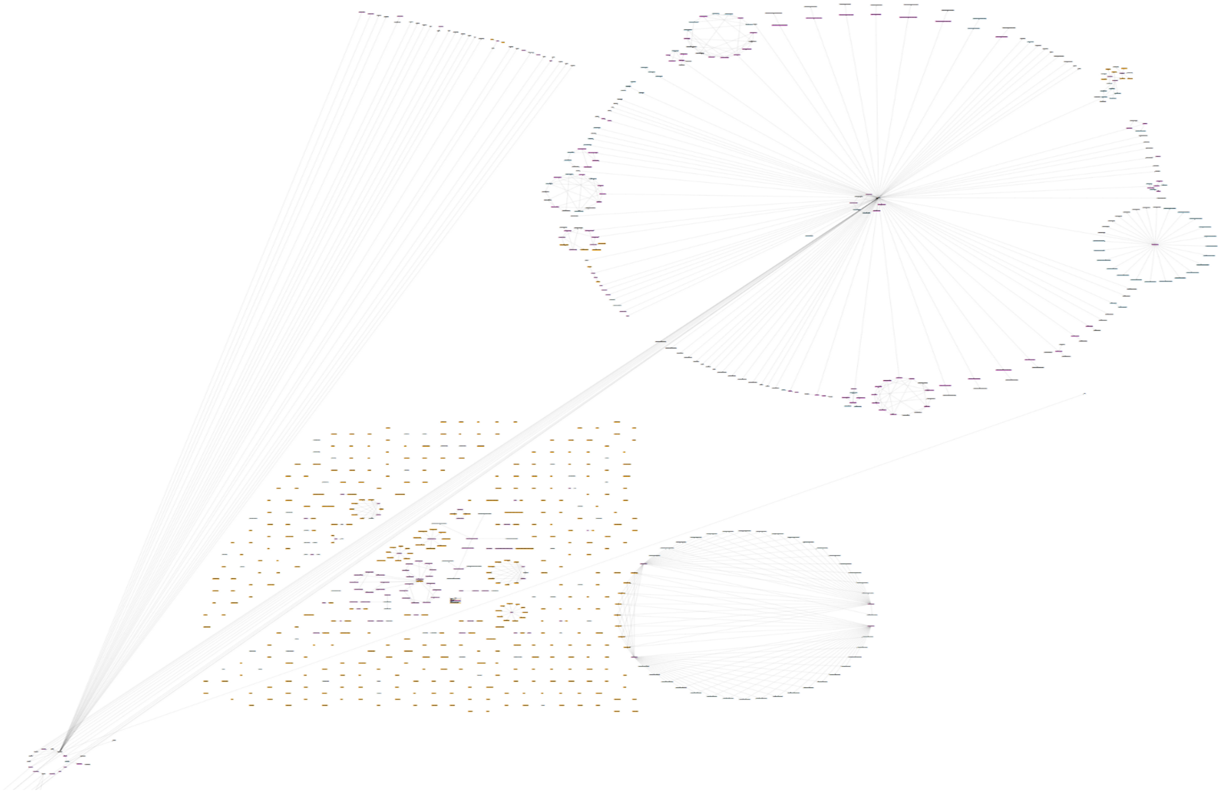
S	T	V
DATALOAD	0	0
PUBLIC	0	0

S	T	V
PUBLIC	1	0

S	T	V
MAIN	0	1
PUBLIC	0	0

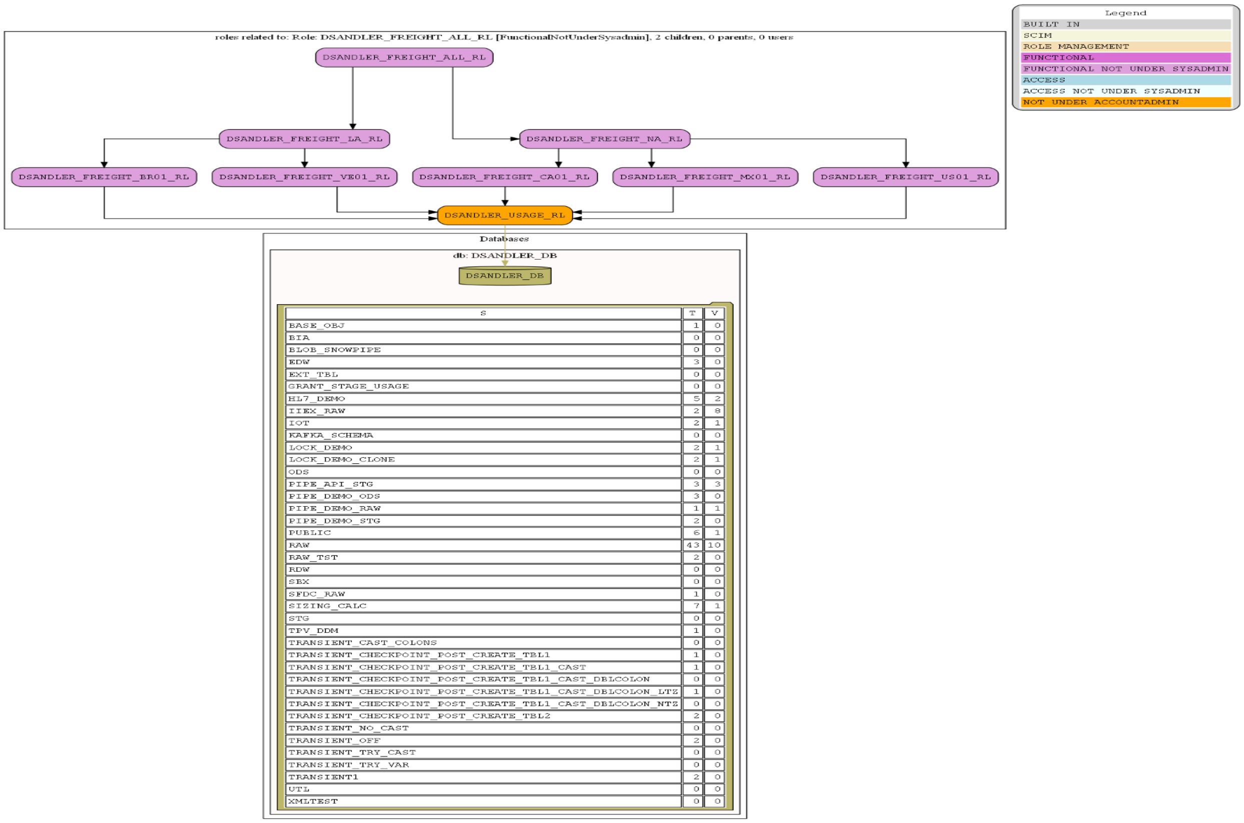
An example of visual display of Role Polyarchy from Snowflake Grant Report output

Many customers have hundreds or even thousands of Roles. Building a single graph with all of them present can result in overwhelming number of objects that can be unreadable. That is a problem common to many complex graph visualizations. Here is a visualization of close to a thousand roles of RBAC hierarchies where no control or planning was done whatsoever:



Role structure without any control or planning can produce T-Shirt-worthy designs

While admittingly neat looking, above visualization is not helpful for understanding of what relates to what. Snowflake Grant Report solves this by preparing a graph for every Role that includes only that Role’s direct relations, and by prerendering SVG, PNG and PDF files for quick display. Drilling deeper, we can see a Role structure for one of the areas of the organizational structure that is easily understood:



S	T	V
BASE_OBJ	1	0
BIA	0	0
BLOB_SNOWPIPE	0	0
EDW	3	0
EXT_TBL	0	0
GRANT_STAGE_USAGE	0	0
HL7_DEMO	5	2
IIEX_RAW	2	8
IOT	2	1
KAFKA_SCHEMA	0	0
LOCK_DEMO	2	1
LOCK_DEMO_CLONE	2	1
ODS	0	0
PIPE_API_STG	3	3
PIPE_DEMO_ODS	3	0
PIPE_DEMO_RAW	1	1
PIPE_DEMO_STG	2	0
PUBLIC	6	1
RAW	43	10
RAW_TST	2	0
RDW	0	0
SBX	0	0
SFDC_RAW	1	0
SIZING_CALC	7	1
STG	0	0
TPV_DDM	1	0
TRANSIENT_CAST_COLONS	0	0
TRANSIENT_CHECKPOINT_POST_CREATE_TBL1	1	0
TRANSIENT_CHECKPOINT_POST_CREATE_TBL1_CAST	1	0
TRANSIENT_CHECKPOINT_POST_CREATE_TBL1_CAST_DBLCOLON	0	0
TRANSIENT_CHECKPOINT_POST_CREATE_TBL1_CAST_DBLCOLON_LTZ	1	0
TRANSIENT_CHECKPOINT_POST_CREATE_TBL1_CAST_DBLCOLON_NTZ	0	0
TRANSIENT_CHECKPOINT_POST_CREATE_TBL2	2	0
TRANSIENT_NO_CAST	0	0
TRANSIENT_OFF	2	0
TRANSIENT_TRY_CAST	0	0
TRANSIENT_TRY_VAR	0	0
TRANSIENT1	2	0
UTL	0	0
XMLTEST	0	0

Subset of the organizational Role structure focusing on just one Role and its relationships

The visualizations are made using GraphViz, a popular open source graph visualization software package (https://graphviz.org/). Customers wanting to make changes to the existing Role polyarchy can take a Role graph and modify it in an online editor without any additional programming to model desired results and see if they fit the business needs.One of the useful tabular reports is list of all Grants for the TABLE Object Type. Similar tables exist for all other object types:

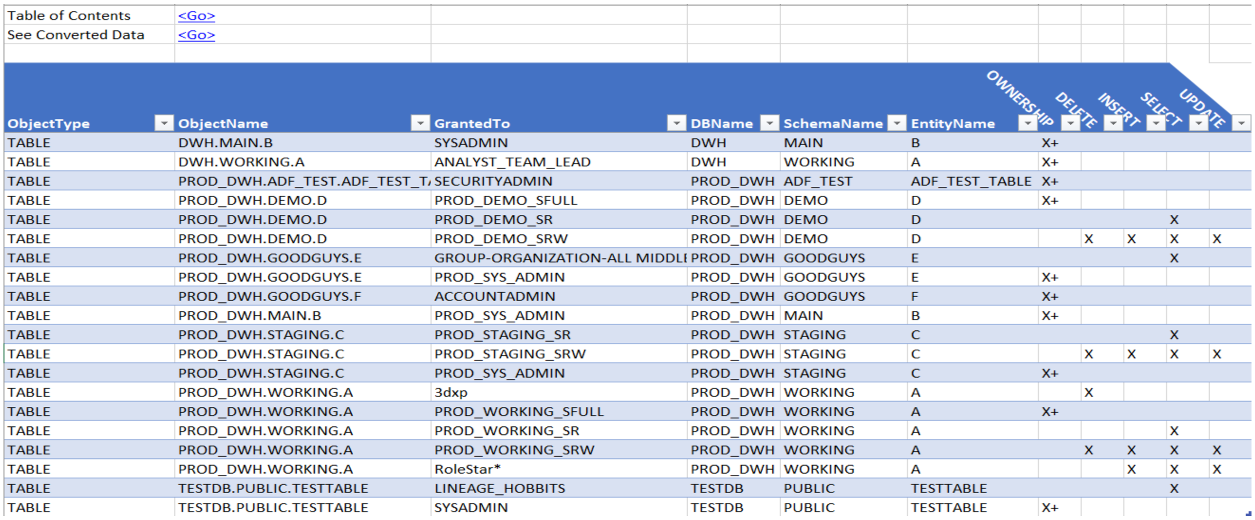
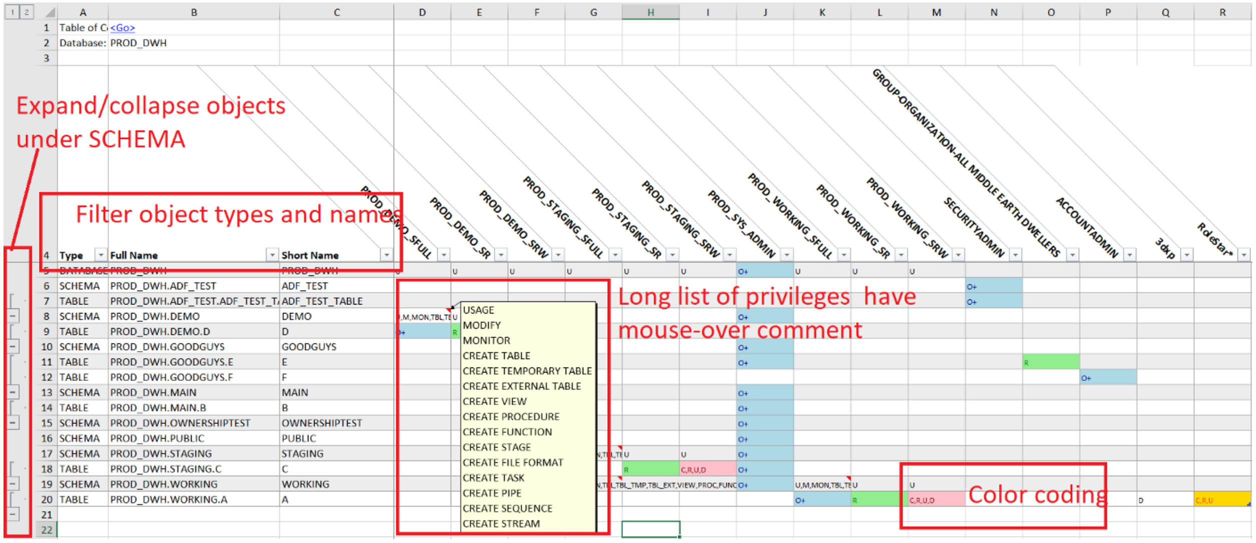


Table of Contents <Go>
See Converted Data <Go>

ObjectType	ObjectName	GrantedTo	DBName	SchemaName	EntityName	OWNERSHIP	DELETE	INSERT	SELECT	UPDATE
TABLE	DWH.MAIN.B	SYSADMIN	DWH	MAIN	B	X+				
TABLE	DWH.WORKING.A	ANALYST_TEAM_LEAD	DWH	WORKING	A	X+				
TABLE	PROD_DWH.ADF_TEST.ADF_TEST_T/	SECURITYADMIN	PROD_DWH	ADF_TEST	ADF_TEST_TABLE	X+				
TABLE	PROD_DWH.DEMO.D	PROD_DEMO_SFULL	PROD_DWH	DEMO	D	X+				
TABLE	PROD_DWH.DEMO.D	PROD_DEMO_SR	PROD_DWH	DEMO	D				X	
TABLE	PROD_DWH.DEMO.D	PROD_DEMO_SRW	PROD_DWH	DEMO	D		X	X	X	X
TABLE	PROD_DWH.GOODGUYS.E	GROUP-ORGANIZATION-ALL MIDDLI	PROD_DWH	GOODGUYS	E				X	
TABLE	PROD_DWH.GOODGUYS.E	PROD_SYS_ADMIN	PROD_DWH	GOODGUYS	E	X+				
TABLE	PROD_DWH.GOODGUYS.F	ACCOUNTADMIN	PROD_DWH	GOODGUYS	F	X+				
TABLE	PROD_DWH.MAIN.B	PROD_SYS_ADMIN	PROD_DWH	MAIN	B	X+				
TABLE	PROD_DWH.STAGING.C	PROD_STAGING_SR	PROD_DWH	STAGING	C				X	
TABLE	PROD_DWH.STAGING.C	PROD_STAGING_SRW	PROD_DWH	STAGING	C		X	X	X	X
TABLE	PROD_DWH.STAGING.C	PROD_SYS_ADMIN	PROD_DWH	STAGING	C	X+				
TABLE	PROD_DWH.WORKING.A	3dxp	PROD_DWH	WORKING	A		X			
TABLE	PROD_DWH.WORKING.A	PROD_WORKING_SFULL	PROD_DWH	WORKING	A	X+				
TABLE	PROD_DWH.WORKING.A	PROD_WORKING_SR	PROD_DWH	WORKING	A				X	
TABLE	PROD_DWH.WORKING.A	PROD_WORKING_SRW	PROD_DWH	WORKING	A		X	X	X	X
TABLE	PROD_DWH.WORKING.A	RoleStar*	PROD_DWH	WORKING	A			X	X	X
TABLE	TESTDB.PUBLIC.TESTTABLE	LINEAGE_HOBBITS	TESTDB	PUBLIC	TESTTABLE				X	
TABLE	TESTDB.PUBLIC.TESTTABLE	SYSADMIN	TESTDB	PUBLIC	TESTTABLE	X+				

All Grants for TABLE objects in multiple databases, by Grant Type

Focusing on auditing of specific Databases, here is a view of all Grants for Schema, Table and View objects in a Database, referenced for each Role that is involved. Similar reports are provided for every Database in your Snowflake deployment:



Expand/collapse objects under SCHEMA

Filter object types and names

Long list of privileges have mouse-over comment

Color coding

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
1	Table of C	<Go>																
2	Database:	PROD_DWH																
3																		
4	Type	Full Name	Short Name	PROD_DEMO_SFULL	PROD_DEMO_SR	PROD_DEMO_SRW	PROD_STAGING_SFULL	PROD_STAGING_SR	PROD_STAGING_SRW	PROD_SYS_ADMIN	PROD_WORKING_SFULL	PROD_WORKING_SR	PROD_WORKING_SRW	SECURITYADMIN	GROUP-ORGANIZATION-ALL MIDDLE EARTH DWELLERS	ACCOUNTADMIN	3dxp	RoleStar*
5	DATABASE	PROD_DWH	PROD_DWH	U	U	U	U	U	U	O+	U	U	U					
6	SCHEMA	PROD_DWH.ADF_TEST	ADF_TEST											O+				
7	TABLE	PROD_DWH.ADF_TEST.ADF_TEST_T/	ADF_TEST_TABLE											O+				
8	SCHEMA	PROD_DWH.DEMO	DEMO	,M,MON,TBL,TE	U					O+								
9	TABLE	PROD_DWH.DEMO.D	D	O+	R													
10	SCHEMA	PROD_DWH.GOODGUYS	GOODGUYS							O+								
11	TABLE	PROD_DWH.GOODGUYS.E	E							O+					R			
12	TABLE	PROD_DWH.GOODGUYS.F	F													O+		
13	SCHEMA	PROD_DWH.MAIN	MAIN							O+								
14	TABLE	PROD_DWH.MAIN.B	B							O+								
15	SCHEMA	PROD_DWH.OWNERSHIPTEST	OWNERSHIPTEST							O+								
16	SCHEMA	PROD_DWH.PUBLIC	PUBLIC							O+								
17	SCHEMA	PROD_DWH.STAGING	STAGING				N,TBL,TE	U	U	O+								
18	TABLE	PROD_DWH.STAGING.C	C					R	C,R,U,D	O+								
19	SCHEMA	PROD_DWH.WORKING	WORKING				N,TBL,TBL_TMP,TBL_EXT,VIEW,PROC,FUNC			O+	U,M,MON,TBL,TE	U	U					
20	TABLE	PROD_DWH.WORKING.A	A								O+	R	C,R,U,D				D	C,R,U
21																		
22																		

USAGE
MODIFY
MONITOR
CREATE TABLE
CREATE TEMPORARY TABLE
CREATE EXTERNAL TABLE
CREATE VIEW
CREATE PROCEDURE
CREATE FUNCTION
CREATE STAGE
CREATE FILE FORMAT
CREATE TASK
CREATE PIPE
CREATE SEQUENCE
CREATE STREAM

Per Database view of all Grants for all Roles in SCHEMA, TABLE and VIEW objects

The tabular reports format data in a more user-friendly way that can be useful in discovering what permissions are present and offer a more portable way of exchanging data with your auditing team than just a big CSV file.