Clearwater

Memo

To: Clearwater Executives

From: Luiza Nascimento

cc: Bill Cunningham

Date: 12/13/18

Re: Inventory Control Data Security Audit

This memo contains my analysis and recommendation for the implementation of a database in the library.

Existing System

Clearwater has three main business processes. In this document, the focus will be on the inventory control, that store data from the inbound shipments received and the outbound orders to keep track of the stock available at Clearwater. The warehouse goons currently do not input data to the inventory database.

Statement of Requirements

I will highlight possible data security issues in the inventory control business unit and recommend solutions to mitigate the risk of data breach.

Analysis

The analysis will be break into three sections: Physical Security of Data, Logical Security of Data, and Data Application Security.

Physical Security of Data

The physical security of data consists on safeguarding the files where data stored. All data from the inventory control is in the file users01.dbf in the oradata/itdb folder.

- Alternatively, data from inventory control could be stored in two files in different disks to improve performance. Separating tables that would be accessed concurrently would avoid that operations of read and write from one table delay operations of the other table.
- The file or files should contain only data from the inventory control. Data from other business units should be stored in different physical files to mitigate performance issues.
- It is recommended to back up the file (or files) in a secure location, preferably in another disk or another server. If anything corrupts the original file, data can be recovered and the loss for the company is minimized.
- The file should be backed up frequently to include recent changes in the data. Considering the volume of transaction in this business unit, it would be good to have this file backed up daily.

Logical Security of Data

The logical security of data consists of using tablespaces and schemas to limit access on the data.

- Data from inventory control should be stored in an exclusive schema where all objects in it are relevant to inventory control. This would make it easier to manage the objects in the inventory control and avoid performance issues.
- The tablespace selected to store the tables should have enough storage to accommodate the current data and future growth. If the size allocate to this schema in the tablespace is insufficient, the users would encounter issues to perform their jobs.
- To mitigate risks of corrupting data, it is good practice to create a view with read only of the look up tables, tables that don't change frequently. In the inventory control, those tables would be category, item and color. This would prevent unwanted changes in these tables.

Data Application Security

The data application security consists of enforcing only the necessary privileges to the users of the database. A good practice is to create database roles according to the privilege needs of each group of employees. This would mitigate risks of excessive permissions that could compromise the integrity of the data or lack of permissions that could be prevent users of performing their jobs. In the inventory control, it would be necessary the creation of three roles: warehouse goons, warehouse manager and company leadership. The roles would have the following privileges:

ROLES	SELECT	INSERT	UPDATE
GOONS	Category, Item, Color, Inventory, Shipment and Shipment-line	-	Shipment and Shipment_Line
MANAGERS	Category, Item, Color, Inventory, Shipment and Shipment-line	Shipment and Shipment_Line	Shipment and Shipment_Line
LEADERSHIP	Category, Item, Color, Inventory, Shipment, Shipment_line, Order and Order_line	-	-

Recommendations

Considering physical data security, I would recommend creating two files - users01.dbf and users02.dbf. These files would be stored in separated disks and daily backed up in the end of the day in an alternative server.

Considering logical data security, I would recommend the creation of a separated schema to own all the objects relevant to inventory control and give enough space in the tablespace Users for this schema. I would also create a view with read only option of the tables category, item and color.

Considering data application security, I would recommend the creation of three roles with the privileges described in the analysis section. To guarantee that the users have the correct access to the tables they and only to the tables they need, I would recommend the following test plan:

ITERATION	TEST	EXPECTED RESULT	ACTUAL RESULT	ACTION REQUIRED
1	Grant manager's role to a user with no previous permissions or roles, connect to the db with this user and insert data to the tables Shipment and Shipment-line	The user should be able to insert data into these tables	The user does not have enough privileges to insert the tablespace.	Grant quota on the tablespace to that user.
2	Repeat the test of iteration 1, after grant quota on the tablespace Users	The user should be able to insert data into these tables	Data was inserted in both tables.	None
3	Grant goon's role to a user with no previous permissions or roles, connect to the db with this user and select data from the tables Category, Item, Color, Inventory, Shipment and Shipment-line	The user should be able to select data from all those tables.	The user could access all tables.	None
4	Grant goon's role to a user with no previous permissions or roles, connect to the db with this user and select data from the tables Order and Order_line	The user should not be able to select data from all those tables.	No data came up.	None
5	Grant manager's role to a user with no previous permissions or	The user should not be able to select data from all those tables.	No data came up.	None

ITERATION	TEST	EXPECTED RESULT	ACTUAL RESULT	ACTION REQUIRED
	roles, connect to the db with this user and select data from the tables Order and Order_line			
6	Grant manager's role to a user with no previous permissions or roles, connect to the db with this user and select data from the tables Category, Item, Color, Inventory, Shipment and Shipment-line	The user should be able to select data from all those tables.	The user could access all tables.	None

Appendix

```
/*****************************************************************
* Script for creating objects for the Inventory Control DB, according to my
* recommendations in the memo
* Author: Luiza Nascimento
* Created on 12/13/2018
*****************************************************************/

-- Enable saving the outputs into a file
SPOOL /home/oracle/data_security/logs/orcl_cr_clearwater.lst append;

-- Save both command and output to the file
SET echo ON;
SET serveroutput ON;

-- Create user (schema) that will own all tables.
CREATE USER cw_inventory
      IDENTIFIED BY library
      DEFAULT TABLESPACE USERS;
GRANT connect TO cw_inventory;
GRANT resource TO cw_inventory;

-- Connect to the db with cw_inventory and create the tables with the existing script

conn sys/ as sysdba

-- Create goons, managers and leadership roles with all the permissions the users
need.
CREATE ROLE goons_role;
GRANT CREATE SESSION TO goons_role;
GRANT SELECT, UPDATE ON cw_inventory.shipment TO goons_role;
GRANT SELECT, UPDATE ON cw_inventory.shipment_line TO goons_role;
GRANT SELECT ON cw_inventory.category TO goons_role;
GRANT SELECT ON cw_inventory.color TO goons_role;
GRANT SELECT ON cw_inventory.inventory TO goons_role;
GRANT SELECT ON cw_inventory.item TO goons_role;

CREATE ROLE managers_role;
```

```
GRANT SELECT, INSERT, UPDATE ON cw_inventory.shipment TO
managers_role;
GRANT SELECT, INSERT, UPDATE ON cw_inventory.shipment_line TO
managers_role;
GRANT SELECT ON cw_inventory.category TO managers_role;
GRANT SELECT ON cw_inventory.color TO managers_role;
GRANT SELECT ON cw_inventory.inventory TO managers_role;
GRANT SELECT ON cw_inventory.item TO managers_role;

CREATE ROLE leadership_role;
GRANT CREATE SESSION TO leadership_role;
GRANT SELECT ON cw_inventory.shipment TO leadership_role;
GRANT SELECT ON cw_inventory.shipment_line TO leadership_role;
GRANT SELECT ON cw_inventory.category TO leadership_role;
GRANT SELECT ON cw_inventory.color TO leadership_role;
GRANT SELECT ON cw_inventory.inventory TO leadership_role;
GRANT SELECT ON cw_inventory.item TO leadership_role;
GRANT SELECT ON cw_inventory.order TO leadership_role;
GRANT SELECT ON cw_inventory.order_line TO leadership_role;
```