Trusted Cyber Technologies

THALES

Protecting sensitive data in and around SAP HANA

White Paper

Contents

Audience

This technical document is intended to provide insight into where sensitive data resides in and around SAP HANA database. This document assumes some knowledge of Thales' data encryption and key management technology and its associated vocabulary.

Overview

On the surface, encrypting the database instance using SAP native encryption would appear to be sufficient to protect data at rest within the SAP HANA database. But, enterprises storing sensitive data in an SAP HANA database need to consider exactly where in and around the database sensitive data might reside -- even outside the direct control of the Database Administrators (DBAs). To give an example, an SAP HANA database might encounter an error causing it to send information with sensitive data into a trace file or an alert log.

While SAP HANA's native encryption is designed to secure data inside the database, it does not secure potentially sensitive data surrounding the database.

Following is a description of the SAP HANA database with a table that includes a list of all types of files, sub-types, their functions, their locations, and why protecting these files might make sense. This material assumes sufficient understanding of SAP HANA databases so that terms like "redo logs", "tablespaces" or "alert logs" are understood.

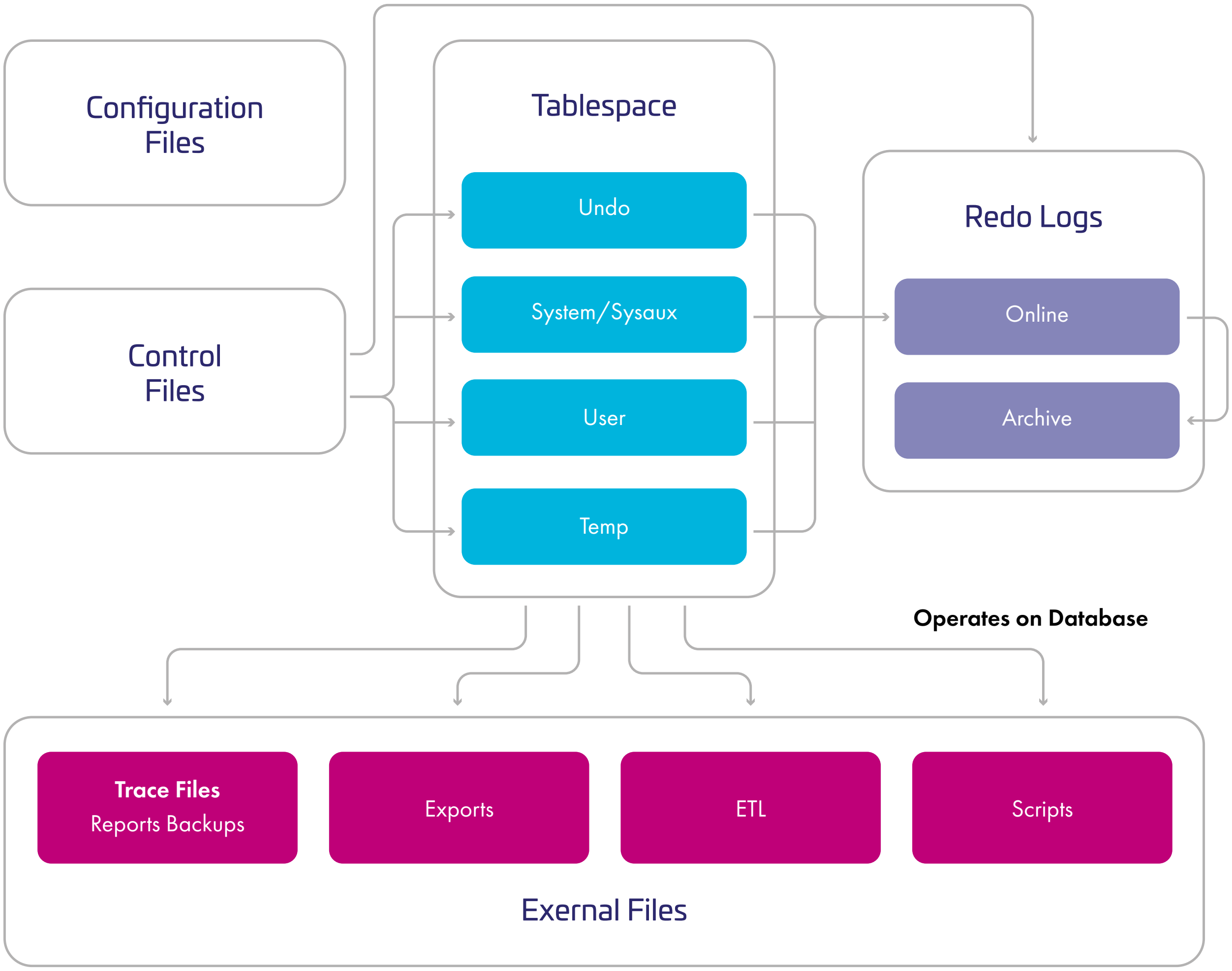

Figure 1. Detailed List of Files Associated with the SAP HANA Database

Type	Sub-type (if applicable)	Function	Why protect this data
Control Files		Control Files know the location of Tablespace Files and Online and Archive Redo Logs.	Guard if configuration information is considered sensitive.
Configuration Files		In general, configuration files define the SAP HANA initialization parameters associated with the database. It includes information like database name, amount of memory associated with the buffer cache(s) and so on.	
	SPFILE	Internally formatted file; easily read via the "strings" command.	
	SPFILE	Plain text version.	
Redo Logs		• In general, redo logs contain information about every change made to the database This includes Data Manipulation Language (DML) changes like INSERTs, UPDATEs or DELETEs, as well as Data Definition Language (DDL) or structural changes like table DROPs, CREATEs, ALTERs and so on. • Under certain specific conditions, changes are not logged, but these are typically exceptions, not the rule.	Redo logs contain copies of sensitive data.
	Online	Always associated with a database.	Sensitive data would reside temporarily in the Online Redo Logs.
	Archive	• Only get created if a database is said to be in "archive-log mode". • When an online redo log fills, it is copied to an archive log to be backed up later. This is known as a "log switch" and is a notoriously expensive operation.	If the database is in archive-log and archive logs get cre-ated, sensitive data will reside in these logs both on disk and in backups, possibly for an extended period of time.

Type	Sub-type (if applicable)	Function	Why protect this data
Tablespace Files		In general, contains the objects associated with a database, like TABLEs, INDEXes, STORED PROCEDUREs and so on.	
	Data Dictionary	Like the control files that "know" where the physical manifestations of the database are located, the Data Dictionary "knows" where the logical manifestations are located, like USERs, TABLEs, INDEXes, and so on. (SYSTEM & SYSAUX tablespaces)	Guard if configuration information is considered sensitive.
	User Objects ("the data")	• These are the TABLEs, INDEXes and so on where User or "Application" data is stored. • The data may or may not be "sensitive" Sensitive data may be isolated by "tablespace"	This is "the data" so it will contain sensitive data.
	UNDO/ Rollback	Used by SAP HANA to maintain a read consistent image of the data when it is being modified by DML.	Sensitive data is very likely to have a transient existence through these tablespaces.
	Temporary	Used internally by SAP HANA for sorting, merging and other activities.	
Recovery Area			
Backups			
Trace files/ Alert Logs		SAP HANA uses trace files to report errors and users can use them to provide information about what the database is doing when retrieving their data.	• In either case, sensitive data can appear in trace files both unintentionally, as when SAP HANA is reporting an error or intentionally if a user is using a trace file to speed up a report. • For example, a report can run a series of SQ statement that could include SSN or PAN to retrieve other data, so the SSN or PAN doesn't end up in the report, but it would be in a trace file that contains intermediate results.
Scripts		Used to execute functions against the database. Could be a one-time job or repeating function.	Frequently contain passwords to database users in clear text.

Type	Sub-type (if applicable)	Function	Why protect this data
Reports		Could be anything from the results of running a SQL*Plus script to a PDF or HTML page that is created on demand.	Like any other unstructured data that might contain sensitive data.
Exports/ Imports	Datapump export	In general, they are files either in internal- SAP HANA format or other format that are used to load data into or extract data from a database.	
	Conventional export	Internally-formatted files that need datapump import to intepret them. SAP HANA provides both a program and stored procedures to interpret these files.	
	SQL*Loader or Extraction, Transformation and Load (ETL) files	Files can be in any of a variety of formats, depending on the tool used (SQL*Loader, ETL tool). ETL data is typically extracted from a production database, transformed to fit operational needs, and loaded into target system (typically a data warehouse).	

Summary

When securing sensitive data in an SAP HANA database, enterprises need to anticipate that sensitive data may reside outside the database itself. Data which could surface vulnerabilities if not protected. Simply encrypting the database using SAP native encryption may be inadequate. Robust data security includes considering how to secure sensitive data not only in, but also around the SAP HANA database.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., is a trusted, U.S. provider of cybersecurity solutions dedicated to U.S. Government. We protect the government's most vital data from the core to the cloud to the edge with a unified approach to data protection. Our solutions reduce the risks associated with the most critical attack vectors and address the government's most stringent encryption, key management, and access control requirements. For more information, visit www.thalestct.com

Protecting sensitive data in and around SAP HANA White Paper

THALES

Contact us

www.thalestct.com