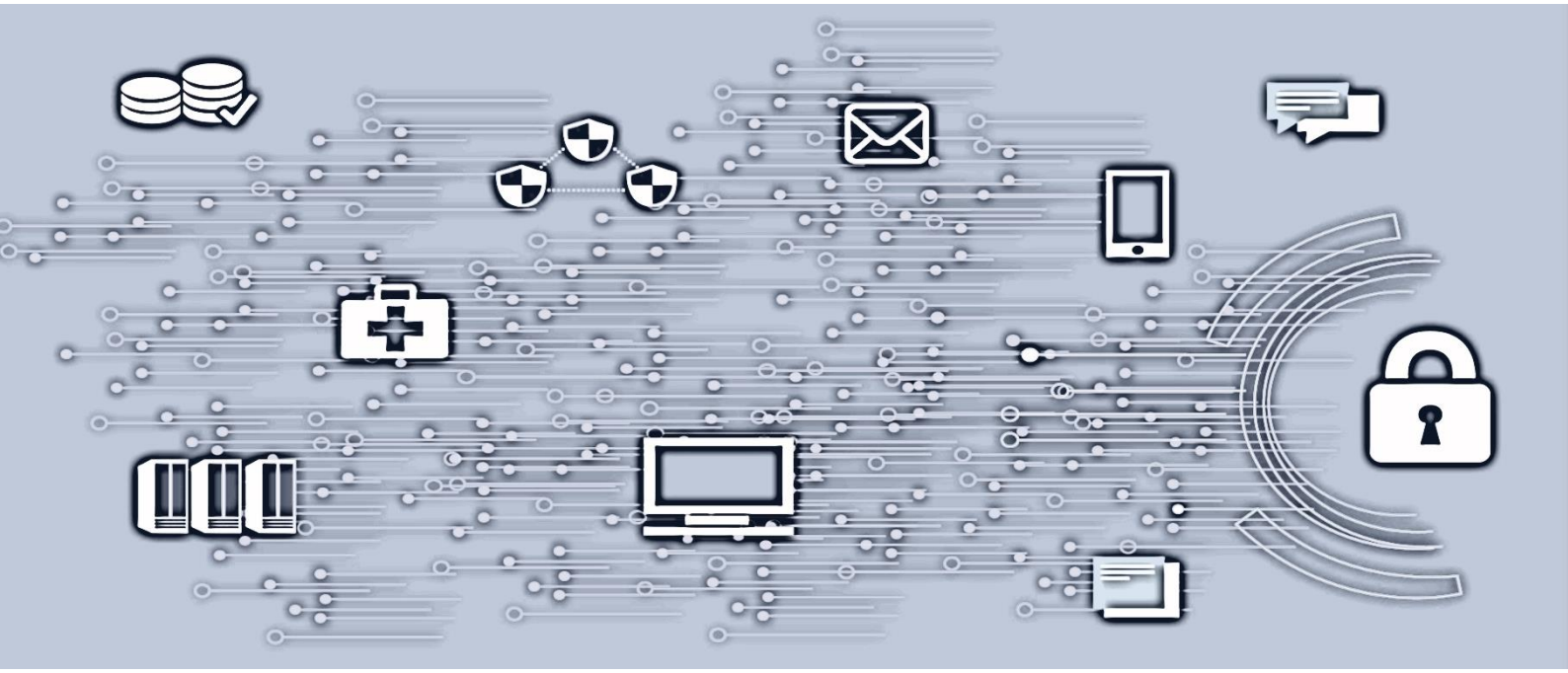
SYKEHUSPARTNER

Sikring av Oracle-databaser



Innhold

Versjon	Dato	Godkjent av
1.0	2022.03.04	Christian Jacobsen

1. Hvordan bruke dokumentet

Retningslinjer for Oracle-databaser kan brukes som sjekkliste sammen med et løsningsdesign i forbindelse med etablering av tjeneste, endring av tjenester, eller i forbindelse med revisjoner og internkontroll av tjenester som benytter Oracle database. Dokumentet brukes også som grunnlag ved anskaffelser av tjenester som skal benytte Oracle database.

Nye applikasjoner må benytte en versjon av Oracle-database som har offisiell support i minimum et år fram i tid, og leverandøren må tillate oppgradering av Oracle til en versjon som til enhver tid er supportert.

2. Unntak fra sikkerhetsprinsippene

Unntak fra sikkerhetsprinsippene skal dokumenteres i risikovurderingen av løsningen.

3. Oracle database

Dette kapittelet gjelder kravstilling til applikasjoner som skal benytte Oracle-database.

Database System Settings		Etterlevd?		
		JA	NEI	I/R
	Ensure audit_sys_operations is reset to default ('TRUE').			
	Ensure audit_trail is set to 'DB'.			
	Ensure compatible is set to '11.2.0.4', '18.1.0' or '19.1.0'.			
	Ensure db_block_size is set to 8192.			
	Ensure db_create_file_dest is set to '+DATA'.			
	Ensure db_create_online_log_dest_1 is set to '+DATA'.			
	Ensure db_create_online_log_dest_2 is set to '+FRA'.			
	Ensure db_recovery_file_dest is set to '+FRA'.			
	Ensure db_securefile is set to 'ALWAYS'.			
	Ensure global_names is set to 'TRUE'.			
	Ensure local_listener er reset to default.			
	Ensure log_archive_dest is set to 'LOCATION=USE_DB_RECOVERY_FILE_DEST'.			
	Ensure o7_dictionary_accessibility is reset to default ('FALSE').			
	Ensure optimizer_features_enable is set to '11.2.0.4', '18.1.0' or '19.1.0'.			
	Ensure os_roles is reset to default ('FALSE').			
	Ensure remote_login_passwordfile is reset to default ('EXCLUSIVE').			
	Ensure remote_os_authent is reset to default ('FALSE').			
	Ensure remote_os_roles is reset to default ('FALSE').			
	Ensure sec_case_sensitive_logon is reset to default ('TRUE').			
	Ensure sec_max_failed_login_attempts is reset to default ('3').			
	Ensure sec_protocol_error_further_action is reset to default ('DROP,3').			
	Ensure sec_protocol_error_trace_action is set to 'LOG'.			

	Ensure sec_return_server_release_banner is reset to default ('FALSE').			
	Ensure sql92_security is reset to default ('TRUE').			
	Ensure resource_limit is reset to default ('TRUE').			

Database Settings		Etterlevd?		
		JA	NEI	I/R
	All databases are created using Oracle Automatic Storage Management (ASM).			
	All databases are created using AL32UTF8 database character set.			
	All databases are created using AL16UTF16 or UTF8 national character set.			
	All tablespaces are created as bigfile tablespaces.			
	All LOBs are created as SecureFiles LOBs.			
	All application data must be stored in separate tablespaces, and not in any of the system tablespaces.			
	All application data tablespaces must support encryption.			

Oracle Connetction and Login Restriction		Etterlevd?		
		JA	NEI	I/R
	Ensure 'FAILED_LOGIN_ATTEMPTS' is less than or equal to '5'			
	Ensure 'PASSWORD_LOCK_TIME' is greater than or equal to '1'			
	Ensure 'PASSWORD_LIFE_TIME' is less than or equal to '90'			
	Ensure 'PASSWORD_REUSE_MAX' is greater than or equal to '20'			
	Ensure 'PASSWORD_REUSE_TIME' is greater than or equal to '365'			
	Ensure 'PASSWORD_GRACE_TIME' is less than or equal to '5'			
	Ensure 'DBA_USERS.PASSWORD' is not set to 'EXTERNAL' for any user			
	Ensure 'PASSWORD_VERIFY_FUNCTION' is set for all profiles			
	Ensure 'SESSIONS_PER_USER' is less than or equal to '10'			
	Ensure no users are assigned the 'DEFAULT' profile			

Oracle User Access and Autorization Restrictions		Etterlevd?		
		JA	NEI	I/R
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_ADVISOR'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_CRYPTO'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_JAVA'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_JAVA_TEST'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_JOB'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_LDAP'			

	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_LOB'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_OBFUSCATION_TOOLKIT'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_RANDOM'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_SCHEDULER'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_SQL'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_XMLGEN'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_XMLQUERY'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'UTL_FILE'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'UTL_INADDR'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'UTL_TCP'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'UTL_MAIL'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'UTL_SMTP'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'UTL_DBWS'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'UTL_ORAMTS'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'UTL_HTTP'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'HTTPURITYPE'			

Oracle Connetction and Login Restriction		Etterlevd?		
		JA	NEI	I/R
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_ADVISOR'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_CRYPTO'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_JAVA'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_JAVA_TEST'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_JOB'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_LDAP'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_LOB'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_OBFUSCATION_TOOLKIT'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_RANDOM'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_SCHEDULER'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_SQL'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_XMLGEN'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_XMLQUERY'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'UTL_FILE'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'UTL_INADDR'			

	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'UTL_TCP'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'UTL_MAIL'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'UTL_SMTP'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'UTL_DBWS'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'UTL_ORAMTS'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'UTL_HTTP'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'HTTPURITYPE'			

Revoke NON-Default Privileges for Packages and Object Types		Etterlevd?		
		JA	NEI	I/R
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_SYS_SQL'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_BACKUP_RESTORE'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_AQADM_SYSCALLS'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_REPCAT_SQL_UTL'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'INITJVMAUX'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_STREAMS_ADM_UTL'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_AQADM_SYS'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_STREAMS_RPC'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_PRVTAQIM'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'LTADM'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'WWV_DBMS_SQL'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'WWV_EXECUTE_IMMEDIATE'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_IJOB'			
	Ensure 'EXECUTE' is revoked from 'PUBLIC' on 'DBMS_FILE_TRANSFER'			

Revoke Excessive System Privileges		Etterlevd?		
		JA	NEI	I/R
	Ensure 'SELECT_ANY_DICTIONARY' is revoked from all application users			
	Ensure 'SELECT ANY TABLE' is revoked from all application users			
	Ensure 'AUDIT SYSTEM' is revoked from all application users			
	Ensure 'EXEMPT ACCESS POLICY' is revoked from all application users			
	Ensure 'BECOME USER' is revoked from all application users			

	Ensure 'CREATE_PROCEDURE' is revoked from all application users			
	Ensure 'ALTER SYSTEM' is revoked from all application users			
	Ensure 'CREATE ANY LIBRARY' is revoked from all application users			
	Ensure 'CREATE LIBRARY' is revoked from all application users			
	Ensure 'GRANT ANY OBJECT PRIVILEGE' is revoked from all application users			
	Ensure 'GRANT ANY ROLE' is revoked from all application users			
	Ensure 'GRANT ANY PRIVILEGE' is revoked from all application users			

Revoke Role Privileges		Etterlevd?		
		JA	NEI	I/R
	Ensure 'DELETE_CATALOG_ROLE' is revoked from all application users			
	Ensure 'SELECT_CATALOG_ROLE' is revoked from all application users			
	Ensure 'EXECUTE_CATALOG_ROLE' is revoked from all application users			
	Ensure 'DBA' is revoked from all application users			

Revoke Excessive Table and View Privileges		Etterlevd?		
		JA	NEI	I/R
	Ensure 'ALL' is revoked from all application users on 'AUD$'			
	Ensure 'ALL' is revoked from all application users on 'USER_HISTORY$'			
	Ensure 'ALL' is revoked from all application users on 'LINK$'			
	Ensure 'ALL' is revoked from all application users on 'SYS.USER$'			
	Ensure 'ALL' is revoked from all application users on 'DBA_%'			
	Ensure 'ALL' is revoked from all application users on 'SYS.SCHEDULER$_CREDENTIAL'			
	Ensure '%ANY%' is revoked from all application users			
	Ensure 'DBA_SYS_PRIVS.%' is revoked from all application users with 'ADMIN_OPTION' Set to 'YES'			
	Ensure 'EXECUTE ANY PROCEDURE' is revoked from 'OUTLN'			
	Ensure 'EXECUTE ANY PROCEDURE' is revoked from 'DBSNMP'			

Audit/Logging Policies and Procedures		Etterlevd?		
		JA	NEI	I/R
	Enable 'USER' audit option			
	Enable 'ALTER USER' audit option			
	Enable 'DROP USER' audit option			
	Enable 'ROLE' audit option			

	Enable 'SYSTEM GRANT' audit option			
	Enable 'PROFILE' audit option			
	Enable 'ALTER PROFILE' audit option			
	Enable 'DROP PROFILE' audit option			
	Enable 'DATABASE LINK' audit option			
	Enable 'PUBLIC DATABASE LINK' audit option			
	Enable 'PUBLIC SYNONYM' audit option			
	Enable 'SYNONYM' audit option			
	Enable 'GRANT DIRECTORY' audit option			
	Enable 'SELECT ANY DICTIONARY' audit option			
	Enable 'GRANT ANY OBJECT PRIVILEGE' audit option			
	Enable 'GRANT ANY PRIVILEGE' audit option			
	Enable 'DROP ANY PROCEDURE' audit option			
	Enable 'PROCEDURE' audit option			
	Enable 'ALTER SYSTEM' audit option			
	Enable 'TRIGGER' audit option			
	Enable 'CREATE SESSION' audit option			

Annet

Fyll inn annen relevant informasjon om systemet/tjenesten:
