ORACLE DATENBANK SICHERHEITSÜBERPRÜFUNG

Checkliste

Autor: Carsten Mützlitz

Erstelldatum: 03.02.98

Letzte Änderung: 30.09.99

Kontrollnummer: CHECK/IT-Grundschutz/001

Version: 1

ORACLE®

Dokumentenkontrolle

Änderungshistorie

Datum	Autor	Version	Änderungsreferenz
03.02.98	Carsten Mützlitz	1	Kein vorheriges Dokument

Reviewer

Name	Position

Verteiler

Kopie-Nr.	Name	Ablage
1		
2		
3		
4		

Inhalt

Checklisten

Die Checkliste zur Durchführung eines kompletten Sicherheitsreview, bezogen auf eine Oracle Datenbank, ist in 3 Kapitel unterteilt:

- Checkliste zur Überprüfung der Installation und Gewinnung von Information, die für eine spätere Auswertung notwendig sind.
- Checkliste zur Überprüfung des Servers
- Checkliste zur Überprüfung der Sicherheit der Datenbank

Die Checklisten geben dem Anwender dieser Listen nach Beendigung einen vollständigen Überblick des gesamten Systems. Auf Basis des Überblicks wird ein On-Site Check der Datenbank durchgeführt.

Beide Ergebnisse, die des Checks und die Ergebnisse der Checklisten, werden von einem erfahreren DBA ausgewertet. Ziel dieser Auswertung ist es, ein Urteil über die Sicherheitsanforderungen und den bereits umgesetzten Sicherheitsmaßnahmen abgeben zu können. Des weiteren werden zusätzliche Sicherheits-Maßnahmen empfohlen, um eventuelle Sicherheitslöcher zu stopfen.

Checkliste Installation

Installations-Vorbereitungs-Checkliste

Die Vorbereitungs-Checkliste überprüft, ob alle Anforderungen an die Datenbank-Installation erfüllt wurden.

Für die genau geforderten Anforderungen bezüglich Hardware und Software ist unbedingt das Installations-Handbuch der entsprechenden Datenbank-Version mit der dazugehörigen Plattform zu beachten.

Ja	Nein	Frage/Anmerkung	Kommentar / Daten
		Weist die installierte Datenbankversion Konflikte mit anderen Applikationen / Betriebssystem / Filesystem auf?	
		Welche Datenbank Optionen sind installiert?	■
		Hat der Kunde die Installationsanforderungen für die Datenbank mit den entsprechenden Optionen erfüllt? (siehe auch Installation Guide „Software and Hardware requirements“)	
		Hat der Kunde die richtigen Levels von:	
		■ Betriebssystem mit den dazugehörigen bekannten Patches? Mit ***showrev -p*** werden alle Patches angezeigt. Wichtig: Der letzte Kernel Patch muß eingespielt sein!	
		■ Netzwerk Protokolle?	
		■ Compiler?	
		■ Andere abhängige Software?	
		Sind alle Betriebssystem Parameter den Anforderungen entsprechend gesetzt? ■ Unix Environment Parameter (PATH, ORACLE_HOME,etc.) ■ Unix Kernel Parameters(Shared Memory: mindestens Minimum abchecken)? ■ umask ■ ulimit	

Installations-Datenbank-Umgebungs-Checkliste

Diese Checkliste zeigt die wesentlichen Einstellungen einer Oracle Datenbank Umgebung auf. Von Interesse sind die Umgebungsvaribalen, init.ora Parameter, Installationsmethode (Oracle File Architecture OFA), etc..

Ja	Nein	Fragen/Anregungen	Kommentare / Daten
		Name des Oracle Software Eigentümers auf dem Unixsystem?	
		Privilegien des Oracle Software Eigentümers?	
		Init.ora Parameter ■ db_block_size ■ shared_pool_size ■ db_block_buffers ■ log_buffer ■ sort_area_size ■ db_name ■ user_dump_dest ■ background_dump_dest	
		Größe der Redo Log Dateien?	
		OFA Installation? RAID level?	
		■ Hostname ■ db_name ■ ORACLE_SID	
		ORACLE_HOME?	
		ORA_NLS, ORA_NLS32, ORA_NLS33, ... ?	
		Characterset für Datenbank?	
		NLS_LANG im Login Profile des Oracle Eigentümers?	

Ja	Nein	Fragen/Anregungen	Kommentare / Daten
		Keine-Default NLS Environment Variablen gesetzt?	
		Relinked alle installierten Oracle-Produkte?	
		Überprüfung der Log-Dateien die während der Erstellung des Database Dictionary enstanden sind (catalog, catproc)?	
		Manuellen Startup der Datenbank erfolgreich?	
		Manuellen Shutdown der Datenbank erfolgreich?	
		Alert Log überprüft?	
		Mehr als ein Controlfile?	
		Folgende Tablespaces erstellt?	
		■ System – size	
		■ Tools - size	
		■ Temp - size	
		■ Users - Size = 1,7GB	
		■ Rollback - size	
		■ andere Tablespaces	
		Zusätzliche rollback segments erstellt und eingeschaltet?	
		Sql*Net auf dem Server installiert und konfiguriert?	

Installations-Anpassungs-Checkliste

Diese Checkliste überprüft die durchgeführten POST-Aktivitäten einer Installation.

Ja	Nein	Fragen / Anregungen	Kommentare / Daten
		Patch Set Installiert?	
		Installation der Optionen auf Korrektheit geprüft?	
		Zusätzliche Members zu den Redo Log Groups hinzugefügt?	
		Archive Log mode eingeschaltet und geprüft?	
		Datenbank Start / Stop beim Maschinen Start / Stop konfiguriert?	
		TNS Listener / Names Server Start / Stop beim Maschinen Start / Stop konfiguriert?	
		Connect zum Server als NICHT-Oracle Benutzer?	
		Andere POST-Installations-Aktivitäten dokumentiert	
		Vorhandensein von invaliden Objekten geprüft?	
		Standard Kennwörter angepaßt?	
		Konfiguration des TNS Listener durchgeführt und geprüft?	
		„Backup Controlfile to Trace“ (DB Struktur Dokumentation)?	

Checkliste Server

System und Datenbank Verfügbarkeit

Die Verfügbarkeit der Systeme ist die Voraussetzung für einen reibungslosen Ablauf. Verfügbarkeit behandelt die Bereiche Hardware und Software.

Nr.	Fragen/Antworten
1.	**Backup-Methode?**
2.	**Wie oft wird ein Backup gefahren?**
3.	**Wie oft werden Netzwerk Konfigurationsdateien gesichert (tnsnames.ora, tnsnav.ora,etc.)?**
4.	**Werden Backups durch Skripte automatisiert?**
5.	**Wie wird die Datenbank vor einem kalten Backup runtergefahren (Abort, immediate, normal)?**
6.	**Interne Datenbank Struktur der Verzeichnisse (Standard, wie z.B. OFA)?**
7.	**Werden irgendwelche Files oder Tablespaces nicht gesichert?**
8.	**Wie wird die Richtigkeit der Sicherung überprüft?**
9.	**Werden die Controlfiles nach jedem HOT BACKUP gesichert?**
10.	**Führen Sie einen Switch Log nach jedem HOT BACKUP durch (empfohlen)?**
11.	**Werden alle Archive Logs gesichert?**
12.	**Wie stellen Sie sicher, daß genügend Platz im Bereich der Ablage für Archive Logs?**
13.	**Wie oft wird überprüft, daß die Backups OK sind (Recovery)?**
14.	**Tape Rotation Policy?**
15.	**Setzen Sie RAID Technology ein?**
16.	**Wie oft führen Sie ein FULL RECOVERY durch?**
17.	**Wie schnell reagiert der Hardware Support bei Problemen?**
18.	**Werden die Recovery Prozeduren mittels Skripte gesteuert?**
19.	**Sind die System Management, Backup und Recovery Prozeduren dokumentiert?**
20.	**Sind die System Management, Backup und Recovery Prozeduren für neue Administratoren leicht zugreifbar?**
21.	**Setzen Sie Oracle Techniken zur Verfügbarkeitssteigerung ein (Partionierung, Failover, Parallel-Server)?**
22.	**Werden Daten archiviert (Online, Offline)?**

Rechenzentrum

Das Rechenzentrum spielt keine wesentliche Rolle bei einer Sicherheitsüberprüfung der Oracle Datenbank. Es ist aber von wesentlichem Interesse, ob der Datenbank Server in einer sicheren Umgebung eingebettet ist.

Nr.	Fragen/Antworten
1.	**Wo ist der Produktionsserver lokalisiert?**
2.	**Wurde die Administration der Rechner einer Fremdfirma überlassen?**
3.	**Ist das Rechnenzentrum für einen professionellen Betrieb ausgelegt (USV, Klima, etc.)?**
4.	**Wie ist die Zugangskontrolle realisiert?**
5.	**Sind die Namen der Ansprechpartner für die Meldung von Problemen bekannt?**
6.	**Sind die Help Desk Anruf Aktivitäten, sowie die Produktionszeiträume aller Systeme, Netzwerke und Datenbanken den Anwendern bekannt?**
7.	**Bereitschaftsdienst, Remote-Help?**

System Monitoring

Zur Erkennung und Identifizierung von Fehlern, Problemen und fremden unerlaubten Zugriff auf Systemressourcen ist es notwendig, entsprechende Monitorwerkzeuge einzusetzen. Darüber hinaus müssen Aussagen über Verfügbarkeit und Performanz definiert sein (Grundbedrohung: Verlust der Verfügbarkeit).

Nr.	Fragen/Antworten
1.	**Monitor für die Database Administration?** **Automatische Erkennung?** **Listen/Alerts/Reports?** **Wer überprüft die Reports, Logs?**
2.	**Monitor für die System Administration?**
3.	**Gibt es eine zentrale Konsole zur Administration von Systemen, Netzwerken, Datenbanken?**
4.	**Gibt es eine sofortige Meldung der verantwortlichen Parteien bei kritischen Fehlern?**
5.	**Wie ist die Verfügbarkeit des Systems definiert?**
6.	**Wie ist die Performanz des Systems definiert?**

System und Datenbank Integrität

Die Integrität der Daten spielt in der IT-Sicherheit eine weitere Rolle. Eine Grundbedrohung „Verlust der Integrität“ zeigt die Wichtigkeit dieser Thematik.

Nr.	Fragen/Antworten
1.	**Sind System Logins eindeutig, d.h. werden diese nur von einer Person benutzt?**
2.	**Sind die Datenbank Logins eindeutig?**
3.	**Wie oft wird das „ROOT“ Kennwort geändert?**
4.	**Wie oft wird das Kennwort für den „ORACLE“ Account gewechselt?**

Nr.	Fragen/Antworten
5.	**Wie oft werden die Kennwörter der „SYSTEM“ und „SYS“ Datenbank Accounts geändert?**
6.	**Gibt es eine „Muß“-Kennwort-Änderungsprozedur für Benutzer?**
7.	**Gibt es einen designierten Sicherheits-Administrator?**
8.	**Wird der Account für das Betriebssystem zum Datenbanklogin genutzt (OPS$)?**
9.	**Gibt es ein Sicherheitsdokument, daß die Sensibilität der Daten beschreibt?**
10.	**Wird der Zugriff von außerhalb in das Datenbanksystem gewährt? Wenn ja, wie sehen die Sicherheitsvorkehrungen aus?**
11.	**Wer hat Zugang zum „ROOT“ Kennwort?**
12.	**Wer hat Zugang zum „ORACLE“ Unix-Account?**
13.	**Wer hat Zugang zu den Datenbank-Benutzern „SYSTEM“ und „SYS“?**
14.	**Sind Datenbankzugriffsregeln über Datenbank-Roles geregelt?**
15.	**Wie sieht der Mechanismus zum Entfernen der Logins aus, wenn Mitarbeitern das Unternehmen verlassen?**
16.	**Werden die gleichen Kennwörter für die Test-, Entwicklungs- und Produktionsumgebung genutzt?**
17.	**Werden Vorkehrungen getroffen Daten aus dem Produktionssystem, die für Test- und Entwicklungssysteme zur Verfügung gestellt werden, zu entfernen?**
18.	**Wird die Integrität aller Dateien auf dem Filesystem gesichert?**
19.	**Werden regelmäßige Heathchecks durchgeführt?**

Konfiguration Management

Bei Änderungen an einem Produktionssystem muß vorher genau geprüft werden, oft Änderungen nicht eventuell das System lahmlegen können. Aus diesem Grund muß genau validiert werden, was notwendig und was nicht notwendig erscheint.

Änderungen sollten immer nur durchgeführt werden, wenn sie vorher auf einem Abnahme-Server getestet wurden. „Never touch a running system“.

Nr.	Fragen/Antworten
1.	**Validierungs- und Approvalprozeß für Hardware- und Software-Änderungen?**
2.	**Wie werden eventuelle Hardware- und Softwareänderungen geplant?**
3.	**Wie oft werden interne Audit durchgeführt, die sich mit der Überprüfung des gutes Zustandes der eingesetzten Hard- und Software auf beschäftigen?**
4.	**Wird eine Versionskontrolle eingesetzt?**
5.	**Beschreibung der im Einsatz befindlichen Policies zur Durchführung von Änderungen in der Datenbank-Struktur?**
6.	**Wie werden Notfall bzw. Ad-Hoc Änderungen durchgeführt?**
7.	**Welche Qualitätstests werden durchgeführt?**
8.	**Wie wird die Applikation verteilt (CD, etc.)?**

Nr.	Fragen/Antworten
9.	**Werden neue Patches oder Versionen von Software sofort in das Produktionssystem eingespielt?**

Datenintegrität

Datenintegrität ist für den Nutzer von wichtiger Bedeutung. Datenbank Administration und Development müssen garantieren, daß die Daten vollständig und aktuell sind.

Nr.	Fragen/Antworten
1.	**Setzen sie datenbankgestützte Integrität ein? Constraints, Trigger, Stored Procedures?**
2.	**Datenintegrität auf Applikationebene eingesetzt?**
3.	**Benutzen Sie nur lesbare Views (mit der READ ONLY Option)?**
4.	**Benutzen Sie beschreibare Views (WITH CHECK Option)?**

System und Datenbank Performanz

Die Performanz und somit die Präsentation des Systems nach außen zum Anwender ist wichtig auch in Bezug auf Akzeptanz.

Das Layout und der Aufbau einer Datenbank kann erheblichen Einfluß auf die Performanz haben (sind die init.ora Parameter richtig genutzt, ist der Shared Memory des Betriebssystem richtig gesetzt, werden bstat / estat Auswertung regelmäßig durchgeführt, etc.).

Nr.	Fragen/Antworten
1.	**Wie oft wird Applikationstuning durchgeführt?**
2.	**Wie oft wird ein Datenbanktuning durchgeführt?**
3.	**Regelbasierte oder Kostenbasierter Optimizer?**
4.	**Wie oft re-analyse der Indices?**
5.	**Werden Stored Procedure genutzt und die damit verbundenen Vorteile (Reduzierung des Netzwerk-Traffics, weniger Shared Memory Verbrauch, etc.)?**
6.	**Setzen Sie die Shared Pool Parameter ein, um eine Fragmentierung und besseres Flushing durchführen zu können (SHARED_POOL_RESERVED_SIZE und SHARED_POOL_RESERVED_MIN_ALLOC)?**

Checkliste Datenbank Sicherheit

Fragenkatalog zur internen Sicherheit der Datenbank.

Server Information

Eine grobe Beschreibung des Systems. Liste der „trusted“ Personen.

Nr.	Fragen/Antworten
1.	**Wie sieht die System Umgebung aus ?**
2.	**Wie sieht die Oracle Umgebung aus ?**

Filesystem

Es wird hier kein Review des Filesytems durchgeführt, die Informationen sind für einen vollständigen Überblick notwendig.

Nr.	Fragen/Antworten
1.	**Ist die ORACLE Software in einem extra Filesystem abgelegt, wenn ja welches?**
2.	**Filesharing (z.B. NFS)?**
3.	**Netzwerk Access auf die Datenbankmaschine (FTP, WEB, etc.)?**
4.	**Welches Filesystem wird genutzt?**

Raw Devices

Raw devices werden von einigen Datenbank Optionen gefordert (z.B. Video Server Option). Darüber hinaus macht es Sinn verschiedene Teile einer Datenbank auf BASIS von Raw devices abzuspeichern. Den Vorteil den man mit Raw devices erzielen kann, ist vor allen Dingen Performanz (bis zu 20%).

Nr.	Fragen/Antworten
1.	**Existieren RAW devices?**
2.	**Wenn ja, welches Zugriffsschutz haben sie auf Filesystem Ebene?**
3.	**Aus welchem Grund wurden die RAW Devices angelegt (Gefordert z.B. Video Server, Performanz,etc.)?**

SQL*Net

Der Einsatz von SQL*Net ist bei einer Datenbankanwendung über mehrere Schichten (Client / Server oder Internet Computing) notwendig. Das Sicherheitsmodell von SQL*Net ist konfigurierbar.

Nr.	Fragen/Antworten
1.	**Welche Version von SQL*Net ist im Einsatz?**
2.	**Ist ein OPS$LOGON eingerichtet?**
3.	**Filterlisten definiert (Connect Manager, oder Workarounds)?**
4.	**Werden die Kennwörter verschlüsselt (ab 2.1 Standard in SQL*Net)?**
5.	**Haben Sie sensible Daten, die über öffentliche Leitung kommuniziert werden?**
6.	**Wird Advanced Networking Option (ANO) angewendet?**
7.	**Wie wurde ANO konfiguriert?**
8.	**Ist der Listener mit dem PASSWORD-Feature eingerichtet?**
9.	**Zusätzliche Sicherheitsvorkehrungen getroffen (z.B. Eigenentwicklungen)?**

Infrastruktur

Dieser Abschnitt soll einen Überblick vermitteln, wie offen das System ist.

Nr.	Fragen/Antworten
1.	**Wird der Zugriff der Clients über das Internet/WAN geregelt?**
2.	**Wenn ja, haben Sie Firewalls im Einsatz?**
3.	**Haben Sie sensible Daten?**
4.	**Wenn ja, setzen Sie ANO ein (siehe oben)?**
5.	**Haben Sie nur ein Server Environment (dann kein SQL*NET empfohlen)?**

Netzwerkzugriff auf den Datenbank-Server

Es wird kein direkter Betriebssystem- oder Netzwerk Review durchgeführt, aber es wird in Form von den nachfolgend aufgeführten Fragen auf Sicherheitsrisiken hingewiesen.

Nr.	Fragen/Antworten
1.	**Wie wird Telnet und FTP Zugriff protokolliert (Monitored)?**
2.	**Werden Berkley R-Utilites genutzt (Wenn ja, hohes Sicherheitsrisiko, ausschalten)?**
3.	**Dateisharing eingestellt (Wenn ja, kein ROOT ACCESS)?**
4.	**Welche Art der Clients werden eingesetzt (Wenn NT, dann NTFS aktivieren)?**

Oracle Software Installation

Bei der Installation der Oracle Software beginnt die Sicherheit. In diesem Stadium sollte man sich bewußt sein, was man tut. Eventuelle falsche Einstellungen können mögliche Türen öffnen, die dem Installateur vielleicht gar nicht bekannt sind.

Nr.	Fragen/Antworten
1.	**Beschreiben des Vorgehens einer Oracle Installation?**
2.	**Oracle Software in einem Extra-Verzeichnis?**
3.	**Installieren sie in eine definierte Filesystem Struktur (OFA)?** Ja, eigene OFA ähnliche Struktur
4.	**Existiert ein Logbuch für durchgeführte Änderungen?**
5.	**Überprüfen Sie die Installation anhand der mitgeführten Log-Dateien (orinst.log)?**
6.	**Archivieren Sie die Log-Dateien außerhalb des Produktionssystems?**
7.	**Wie behandeln Sie die „root.sh“?**
8.	**Löschen oder archivieren Sie den „root.sh“?**

Oracle Instance

Um welche zu untersuchende Oracle Instance handelt es sich?

Nr.	Fragen/Antworten
1.	**Hostname der zu untersuchenden Instance?**
2.	**Datenbankname der zu untersuchenden Instance?**
3.	**SID der zu untersuchenden Instance?**
4.	**DB Domain der zu untersuchenden Instance?**
5.	**Global Names gesetzt?**

Security Policy Implementierung

Das Ziel dieser Fragen in diesem Abschnitt ist die Informationssammlung mit dem Fokus auf Sicherheit des Kunden.

Nr.	Fragen/Antworten
1.	**Gibt es einen verantwortlichen Sicherheitsbeauftragten?**
2.	**Ist die Rolle formal in dem Unternehmen definiert?**
3.	**Gibt es eine Kennwort-Management/Änderungs Policy?**
4.	**Kennwort-Social-Hacking?**

Nr.	Fragen/Antworten
5.	**Wer ist „trusted“, um die ROOT Kennwörter zu bekommen?**
6.	**Hat der Kunde formale Reviews auf System Security Logs oder Oracle Audit Logs?**
7.	**Gib es definierte Security Policies, wie z.B. Level der Sicherheitseinstufen für Applikation, Datenbanken, etc.?**
8.	**Wurde in der Vergangenheit ein unerlaubter Zugriff auf das System erkannt?**
9.	**Haben die Oracle Benutzer entsprechende Quotas eingerichtet?**
10.	**Werden die Trace und Alert Files der Datenbank regelmäßig überprüft?**

Client

An einem Client soll beispielhaft aufgezeigt werden, ob die Einstellungen der Objekte richtig konfiguriert wurden.

Nr.	Fragen/Antworten
1.	**Welche Software ist auf Clientseite installiert (Prinzipiell gilt, alles was nicht benötigt wird, muß weg)?**
2.	**Wurde die Netzwerkverbindung richtig konfiguriert (SQL*NET)?**
3.	**Ist die Applikation lokal beim Client installiert?**
4.	**Gibt es besondere Mechanismen, die den Verbindungsaufbau zu verschiedenen Datenbank steuern (Test, Development, Produktion)?**

On-Site Check

Zweck

Dieses Dokument beinhaltet Informationen der durchgeführten Prüfungen. Die Prüfungen sind unterteilt in folgende Sektionen:

- Bewertung des Oracle Software Owners
- Bewertung der Dateizugriffsrechte auf dem Server
- Bewertung der SQL*NET Konfiguration
- Bewertung des Objekt-Schutzes
- Bewertung der Auditing Konfiguration

Die Überprüfung fokusiert sich auf die Aspekte Sicherheits Policy / Implementierung, und deckt die nachfolgend aufgeführten Bewertungen zu den entsprechenden Bereichen ab:

- Unauthorisierte Offenlegung von Daten
- Authentifikation Schema
- Unauthorisierte Änderung und Löschung von Daten
- Unauthorisierte Netz-Abhörung und in diesem Zusammenhang Änderung, Löschung von Daten.

Betriebssystem Level Überprüfung

Oracle Software Owner

Allgemein:

Userid:_____

Oracle Software Owner Password Policy: ☐

ORACLE_BASE: _____

ORACLE_HOME: _____

ORACLE_SID: _____

Password geprüft: ☐

Unix Servers:

Privilegierte Group ID: _____

Root Password Policy: ☐

Mitglieder der privilegierten Gruppe:

_____

_____

_____

NT Servers

Userid Oracle Services läuft unter: _____

Wert des Registry key DBA_AUTHORIZATION: _____

(HKEY_LOCALMACHINE / SOFTWARE / ORACLE)

Serverseitiger Datei-Zugriffsschutz

Dateien, die zu untersuchen sind:

- Datenbank-Dateien
- Oracle Software
- UTL_FILE
- Configuration files
- Dump / trace directories
- Audit trail
- BFILE (ab Oracle Version 8)

Database files

Die Directories der verschiedenen Datenbank Dateien weisen den Zugriffsschutz _____ auf.

(select * from v$datafile)

Datenbank-Dateiname (inklusive Pfad)	Zugriffsschutz

Logfiles

Das Verzeichnis der Log Dateien wurde mit folgendem Zugriffsschutz versehen _____.

(select * from v$logfile)

Path	Zugriffsschutz

Controlfiles

Das Verzeichnis der Control-Dateien wurde mit folgendem Zugriffsschutz versehen _____. Es existieren __ Control-Dateien, die über __ Platten verteilt sind.

(show parameter controlfiles)

Controlfile Name (inklusive Pfad)	Zugriffsschutz
1	

Dump Verzeichnisse

Verzeichnisse in denen Trace und Alert Informationen abgespeichert sind, werden nachfolgend aufgeführt:

(show parameter dump_dest)

Dump directory	Path	Zugriffsschutz
user_dump_dest		
background_dump_dest		
core_dump_dest		

Archive log

Archive Log wurde für die _____ Datenbank Instance aktiviert.

(show parameter archive_log_dest)

archive_log_dest: _____

Das Verzeichnis der Archive Log Dateien (Endung arc) hat einen Zugriffsschutz mit den Einstellungen _____. Die darin beinhalteten Archive Log Dateien haben einen Zugriffsschutz mit den Einstellungen _____.

Remote Password File

Der INIT.ORA Parameter REMOTE_LOGIN_PASSWORDFILE hat den Wert _____, d.h. dieser File steht nur der lokalen Datenbank zur Verfügung.

Remote Password Datei Pfad	Zugriffsschutz

Andere Backup Verzeichnisse

Datei Backup Verzeichnis: _____

Export Backup Verzeichnis: _____

In dem Backupverzeichnis werden _____
_____ abgespeichert.

SQL*NET

SQL*NET trace directory:_____

SQL*NET log directory: _____

TNS_ADMIN: _____

Trace / log enabled: ☐

TRACE_DIRECTORY_LISTENER:_____

Listener PASSWORD: ☐

Intelligent Agent (smnp.ora). Password im Klartext: ☐

Intelligent Agent (ano.ora). Für Advanced Networking Option ☐

Oracle Names: ☐

Oracle Names (names.ora), Passwort im Klartext: ☐

UTL_FILE

(show parameter UTL_FILE_DIR)

UTL_FILE_DIRECTORY:_____

BFILE ***(nur Oracle 8)***

Dieses Oracle 8 Feature erlaubt das Abspeichern von LOB Dateien in das Filesystem. Es werden File Access Rechte von den Directories abgeleitet.

Benutzer mit dem CREATE_DIRECTORY / CREATE_ANY_DIRECTORY Recht:

_____

Auflistung eingestellter Verzeichnisse (select * from dba_directories)

_____

Datei Zugriffsschutz unter Windows NT

DateiTyp (FAT, NTFS): _____

ACL's auf Oracle Software:_____

ACL's auf Oracle Datenbank Dateien: _____

Datei-Sharing auf Oracle Dateien: _____

Datei Zugriffsschutz unter Unix:

Filesystem type:_____

Fileshares / NFS: _____

Raw Partitionen

Es sind keine Raw Partitionen eingerichtet.

Raw Partitionen Name/und Link Name	Zweck

Dateien mit speziellem Zugriffsschutz:

Filetype	Name	Path	Zugriffsschutz
Oracle kernel	$ORACLE_HOME / bin / oracle		
SQL*NET V1 listeners	$ORACLE_HOME / orasrv $ORACLE_HOME / bin / tlisrv $ORACLE_HOME / bin / spxsrv others		
Ulimit push	$ORACLE_HOME / bin / osh		

SQL*NET

SQL*NET Version auf Server:_____

SQL*NET Version auf Client: _____

Überprüfen der Kennwortverschlüsselung: ☐

OPS$LOGON eingeschaltet (SQL*NET V1): ☐

OPS$LOGON eingeschaltet (SQL*NET V2): ☐

Advance Networking Option eingeschaltet: ☐

ANO nötig: ☐

Intelligent Agent in Gebrauch: ☐

Wenn, Pfad der snmp.ora: _____(Kennwort im Klartext enthalten)_

Zugriffsschutz auf snmp.ora : _____

Oracle Names: ☐

Wenn, Pfad der names.ora: _____(Kennwort im Klartext enthalten)_

Zugriffsschutz auf names.ora : _____

Datenbank Level Überprüfung

Datenbank Kennwörter

Überprüfung von SYS: ☐

Überprüfung von INTERNAL: ☐

Überprüfung von SYSTEM: ☐

Auflistung anderer priviligierter Benutzer

Oracle Userid	Kennwort-Überprüfung
DBSNMP	
NAMES	
SCOTT	
APPS	
OULN	
MTSSYS	
ORDSYS	
OAS_PUBLIC	
APPLPUBSYS	
WEBDB	
DEMO	
PO8	
CTXSYS	

Kennwort Änderungs Policy vorhanden: ☐

Oracle 8

Kennwort Änderungskontrolle und Überprüfung eingebaut:

(select profile from DBA_PROFILES where resource_type = 'PASSWORD')

Profile	Kennwort Kontroll Routine

Andere Kennwort Überprüfungseinstellungen:

Profile	Parameter	Wert

Auditing

Auditing eingeschaltet: ☐

Audit Trail Review Policy: ☐

Failed Logon Reviewed ☐

Auditing Action	Eingeschaltet/Review Policy

Gesperrte Accounts: (select username from dba_users WHERE account_status= ’’):
(nur für *Oracle 8 RDBMS*)

Account name

Roles und Role Grants

Ausführen des Scripts d_roles.sql ☐

Ausführen des Scripts g_roles.sql ☐

Ausführen des Scripts def_roles.sql ☐

System Privilegien

Ausführen des Scripts sysprivs.sql ☐

Ausführen des Scripts sysprivs1.sql ☐

Object Privilegien

Name der Applikation: _____

Oracle Userid, die das Applikationsystem besitzt:_____

Ausführen des Scripts d_grants.sql : ☐

Ausführen des Scripts r_grants.sql : ☐

Ausführen des Scripts grantopt.sql : ☐

Externe Repositories

Repositories, die in der Datenbank installiert sind:

Repository Name	Oracle version	Genutzt? (J/N)	SID	Server
Enterprise Manager	Oracle7 und 8			
Recovery Manager	Oracle8			
Intelligent Agent	Oracle 7 und 8			
Oracle Backup Utility	Oracle7			

Datenbank Links

(select * from dba_db_links)

Datenbank Link	Privat/Öffentlich