

LA GESTIONE DELLA PROTEZIONE IN:

Mysql 5 community

Oracle 10g XE

MS SQL 2005 express

Introduzione

Le caratteristiche di sicurezza di un software devono essere analizzate sia dal punto di vista tecnico che da considerazioni relative a:

1. Tipologia di mercato a cui il prodotto si rivolge
2. Reali necessità
3. Assistenza e aggiornamenti
4. Rapporto tra costi e benefici

Queste slide si concentrano solamente sull'analisi tecnica: in particolare sulla granularità e la facilità con cui sia possibile definire le policy di sicurezza dopo un'installazione "fresca".

N.B. In queste slide non si analizza il dialetto SQL o i particolari comandi per assegnare privilegi da utilizzare nei vari DBMS ma si descrivono le varie funzionalità messe a disposizione.

Metodologia di lavoro



Il confronto dei tre DBMS è stato fatto su di una macchina virtuale che fungesse da *sandbox* con sistema operativo Windows XP appena installato.

Si è scelta la piattaforma Microsoft e non Linux perchè supportata da tutti e tre i software (vedremo che è anche possibile l'autenticazione tramite il sistema operativo)

Oracle 10g Express Edition

Versione gratuita (*non open source*) del DBMS Oracle, libera anche per uso commerciale.

Con alcune limitazioni (al massimo 4Gb di dati, 1 GB di memoria e altro) non relative alla sicurezza.

Recuperabile all'indirizzo:

<http://www.oracle.com/technology/xe/index.html> (richiede login)

Oracle XE: Introduzione

Datasheet

Versione	Oracle Database 10g Release 2 (10.2.0.1) Express Edition
Piattaforme	- Microsoft Windows (2000 SP4, XP, Server 2003) 32bit - Linux (alcune tra le maggiori distribuzioni)
Prezzo	Gratuito. Le versioni a pagamento (con meno limitazioni) partono da \$5,000 per processore (versione Standard ONE) fino a \$40,000 per processore (versione Enterprise).
Licenza	Libero (non open-source) per uso personale ma anche per uso commerciale e distribuibile all'interno di software proprietario.
Requisiti	Non troppo esigente "sulla carta" (configurazione minima di 512MB di RAM e 2GB di spazio)
Limitazioni	- Supporta al massimo 4GB di dati - Al massimo un'istanza per server - Utilizza un solo processore in sistemi SMP - Utilizza al massimo 1GB di RAM
Funzionalità	Simili (eccetto le limitazioni) alla Standard Edition quindi grande stabilità, storage di ampi tipi di dati e accesso tramite moltissime interfacce standard. Le funzionalità del database sono estremamente evolute (ad es. le stored procedure in diversi linguaggi) e le funzionalità statistiche e di analisi.

Oracle XE: Installazione

Durante l'installazione avvengono tre attività fondamentali dal punto di vista della sicurezza:

- Viene richiesto l'inserimento di una password che verrà utilizzata per **gli account SYS e SYSTEM**
- Viene creato un nuovo gruppo nel sistema chiamato **ORA_DBA** (in LINUX si chiamerebbe **dba**) e al suo interno viene inserito l'utente che effettua l'installazione
- Vengono aggiunti dei servizi di rete che rispondono sulle seguenti **porte TCP**:
 - ▣ Oracle Database Listener: 1521
 - ▣ Oracle Services for Microsoft Transaction Server: 2030
 - ▣ Listener HTTP: 8080

Oracle XE: Utente SYS

E' un utente amministrativo e gestisce il DB e il *data dictionary*, non deve mai essere utilizzato per operazioni normali ma solo per manutenzione.

Un utente quando si connette può voler assumere il privilegio di:

- ▣ SYSDBA

E' il massimo livello di privilegio, opera nello schema SYS e può gestire utenti e impostazioni ed effettuare lo shutdown/startup

- ▣ SYSOPER

Simile a SYSDBA ma non può effettuare operazioni molto delicate come *Incomplete Recovery* e opera nello schema PUBLIC

Oracle XE: Utente SYSTEM



È l'account per le normali operazioni di amministrazione, è proprietario delle tabelle di default di Oracle (escluso il *data dictionary* che gestisce solo SYS), dovrebbe essere **utilizzato da una sola persona** e solo per **operazioni di creazione, modifica utenti o manutenzione** del DB.

Oracle XE: Altri utenti



Oltre a SYS e SYSTEM esistono dei ruoli già predefiniti (ad esempio per agenti snmp, per servizi web, per scheduling, ecc).

N.B. Durante l'installazione vengono creati degli utenti di esempio (bloccati di default) a cui è comunque consigliabile cambiare password.

Vi è anche un utente ANONYMOUS (con tablespace TEMP) da bloccare o a cui cambiare password.

Oracle XE: Ruoli



I ruoli permettono di amministrare facilmente i privilegi di un gran numero di utenti (un concetto simile al raggruppamento di utenti).

E' quindi possibile creare un ruolo e assegnarlo a certi utenti e poi modificare solo esso per amministrare i privilegi di tutti gli utenti.

N.B. I ruoli possono essere applicati **sia ad utenti che ad applicazioni**

Oracle XE: Le tablespaces

- Le tablespaces servono a raggruppare logicamente porzioni del DB (tabelle, indici), sono importanti come **funzionalità di sicurezza** perchè possono essere assegnate ad ogni utente, **consentono quindi l'amministrazione di una porzione limitata** del DB.

Le tablespaces possono essere di diversi tipi (permanent, undo, temporary) e si creano tramite il comando SQL "create tablespace".

Il DBA può creare nuovi utenti e assegnare ad essi privilegi di amministrazione all'interno di certe **tablespace**, ad esempio:

```
SQL> CREATE USER pippo IDENTIFIED BY segreta  
      DEFAULT TABLESPACE utenti  
      TEMPORARY TABLESPACE temporanea;
```

N.B. Esiste sempre una **tablespace di sistema**, denominata SYSTEM.

Oracle XE: Impostazioni utenti

- Quote

Definisce per ogni utente una quota di spazio massimo utilizzabile all'interno della sua tablespace, questo per evitare che un utente possa rallentare il DB o per ragioni commerciali

- Scadenza password

Si impone ad un utente la scadenza della password obbligandolo quindi a cambiarla

- Blocco Utenti

E' possibile bloccare/sbloccare un utente temporaneamente in modo da inibirne, anche solo temporaneamente, l'accesso

- Limiti sull'utilizzo delle risorse

Si può limitare le risorse (cpu, esecuzioni, ecc.) in modo da evitare sovraccarico del sistema

Oracle XE: Privilegi



I privilegi in Oracle possono essere gestiti dall'utente SYSTEM o da un qualsiasi utente a cui siano state a sua volta date le credenziali per poter gestire alcuni oggetti, utenti, ecc.

Si noti che in Oracle è possibile scegliere con **estrema granularità** i privilegi (vi sono centinaia di opzioni).

Ad es. è possibile definire privilegi isolati anche sulla singola colonna di una tabella o sull'esecuzione di procedure, sulle view, ecc.

Oracle XE: Perché granularità?



La granularità nella scelta dei privilegi è necessaria per definire con precisione cosa ogni utente o applicazione può fare.

Oracle è molto avanzato in questo campo: è possibile definire privilegi isolati anche sulla singola colonna di una tabella o sull'esecuzione di procedure, sulle view, ecc.

È anche possibile scrivere delle policy che si comportano in base a determinati valori all'interno del database.

Oracle XE: Privilegi sulle tabelle

Per quanto riguarda le tabelle i privilegi possono essere relativi al:

- DML (data modification language):
comandi che modificano i dati
- DDL (data definition language):
comandi che modificano la struttura delle tabelle

N.B. In modo simile è possibile definire le operazioni sulle **VIEW**

Oracle XE: Privilegi sulle procedure

Le procedure hanno una gestione particolare, due tipi:

- Definer rights

la routine viene eseguita con i diritti del creatore, è utile ad esempio per far accedere a certi dati un utente solo tramite procedura

- Invoker rights

la routine viene eseguita con i diritti dell'esecutore, si impedisce così che usando una routine si facciano operazioni per le quali non si ha il permesso come utenti

N.B. Si può manipolare tramite il privilegio **EXECUTE** chi ha il diritto di eseguire una procedura

Oracle XE: Privilegi di sistema

Alcuni privilegi:

- ▣ Sessioni
- ▣ Tabelle
- ▣ Viste
- ▣ Procedure
- ▣ Privilegi
- ▣ ...

Una buona reference:

http://www.adp-gmbh.ch/ora/admin/system_privileges.html

Oracle XE: Privilegi sugli oggetti

Alcuni privilegi applicabili a tutti gli oggetti (tabelle, indici, viste, funzioni, trigger, ecc.):

- ▣ Alter
- ▣ Select
- ▣ Delete
- ▣ Insert
- ▣ Update
- ▣ ...

Una buona reference:

http://www.adp-gmbh.ch/ora/misc/users_roles_privs.html

Oracle XE: Auditing



In Oracle è anche possibile impostare l'**auditing**: questo permette di controllare nel dettaglio cosa “fanno” gli utenti (i dati vengono salvati all'interno del DB stesso) e analizzare eventuali accessi indesiderati.

La difficoltà è simile a quella degli IDS in cui spesso è difficile distinguere i falsi positivi, la potenza in Oracle però sta proprio nella possibilità di attivare opzioni di Auditing altamente selettive in base alle azioni degli utenti (sempre in linguaggio SQL)

Oracle XE: I tipi di login

- Tramite il sistema operativo (**autenticazione esterna**)
durante l'installazione viene creato il gruppo ORA_DBA, i membri di tale gruppo possono connettersi al DB direttamente senza inserire password
- Tramite password (**autenticazione di database**)
il login viene fatto in modo "classico" inserendo la password del relativo utente
- Tramite LDAP esterno (**autenticazione globale**)
il login viene fatto su un sistema centrale esterno atto a gestire gli utenti (l'accesso su Oracle può avvenire anche tramite proxy)

Oracle XE: Connessione tramite

- Locale

utilizzando SQL*PLUS sulla macchina locale dove è installato il server (questo solitamente non avviene in un ambiente in produzione)

- Rete

si possono configurare dei Listener (alcuni di default vengono creati durante l'installazione) che permettono tramite client TCP/IP la connessione remota (anche da altri software)

Oracle XE: Connessione tramite



- Web

Oracle mette a disposizione un'interfaccia web (che si può aprire anche alla rete esterna e non solo al server locale) che permette di gestire il DBMS in modo più user-friendly rispetto alla console

Oracle XE: Crittografia

La crittografia è necessaria (principalmente) per:

- Difendere i dati memorizzati da attacchi diretti alla macchina (ad esempio una compromissione fisica o un attacco perpetrato tramite un altro servizio)
- Difendere i dati durante la trasmissione da “occhi indiscreti”

Oracle **supporta la crittografia** forte dei dati memorizzati (DES) e la trasmissione TCP/IP con SSL (MD5 e SHA1 per l'integrità)

MS SQL Server 2005 Express

Versione gratuita (*non open source*) del DBMS SQL Server, libera anche per uso commerciale.

Con alcune limitazioni (al massimo 4Gb di dati, 1 GB di memoria e altro) non relative alla sicurezza.

Recuperabile all'indirizzo:

<http://www.microsoft.com/sql/editions/express/default.mspx> (non richiede login)

SQL Express: Introduzione

Datasheet

Versione	SQL Server 2005 Express Edition
Piattaforme	- Microsoft Windows (2000 SP4, XP, Server 2003, Vista) 32bit, richiesto .NET 2.0
Prezzo	Gratuito. Le versioni a pagamento (con meno limitazioni) partono da \$3,700 per processore (versione Workgroup) a \$24,000 per processore (versione Enterprise).
Licenza	Libero (non open-source) per uso personale ma anche per uso commerciale e distribuibile royalty-free previa registrazione con Microsoft.
Requisiti	Non troppo esigente “sulla carta” (configurazione minima di 512MB di RAM e 1GB di spazio)
Limitazioni	- Supporta al massimo 4GB di dati - Utilizza un solo processore in sistemi SMP - Utilizza al massimo 1GB di RAM
Funzionalità	Vedi: http://www.microsoft.com/sql/prodinfo/features/compare-features.msp Supporta funzionalità adatte ad attività di prototipazione o studio oppure per piccole esigenze. Si allinea al prodotto concorrente di Oracle.

SQL Express: Installazione



Durante l'installazione avvengono tre attività fondamentali dal punto di vista della sicurezza:

- Viengono aggiunti dei servizi di sistemi per la partenza di Microsoft SQL
- Si può scegliere di aggiungere l'utente che effettua l'installazione come amministratore del DB
- Si può decidere di utilizzare l'autenticazione del DB e non quella del S.O. (seguendo l'installazione non di default)

SQL Express: Istanze



SQL Express permette l'utilizzo di istanze, **di default durante l'installazione viene creata un'unica istanza** all'interno della quale gestire tutti i DB (questa è la strategia consigliata), è ovviamente necessario gestire i privilegi degli utenti per abilitare l'accesso solo ad alcuni DB.

E' possibile creare più di una istanza (al massimo 15) ma con un forte degrado di prestazione (duplicazione di librerie, ecc.)

SQL Express: Autenticazione



- Tramite l'autenticazione di windows:
SQL Server convalida l'utente in modo predefinito tramite l'autenticazione di Windows (protocollo di protezione Kerberos), si hanno tutte le garanzie relative alla gestione degli account di windows (blocco utenti, scadenza password, ecc.)

SQL Express: Autenticazione



- Modalità mista:

SQL Server convalida l'utente tramite una password, è chiaramente necessario che l'utente sia prima validato dall'autenticazione di windows

N.B. Microsoft **consiglia fortemente** l'utilizzo della prima modalità di autenticazione per garantire migliore sicurezza e capacità di passare più facilmente a SQL Server Standard

SQL Express: Gestione utenti

Esistono due comandi principali per creare gli utenti:

- **CREATE LOGIN**

è il comando base per la creazione di nuovi accessi (la modalità mixed o tramite windows dipende da come è impostato il DBMS)

- **CREATE USER**

serve per associare ad un LOGIN determinate utenze (e quindi relativi privilegi in base agli schemi a cui possono accedere)

SQL Express: Gestione



La gestione del DBMS oltre che da linea di comando può avvenire tramite due tools:

- **Management Studio**

Permette di configurare gli utenti, i ruoli, ecc. e gestire database, tabelle e gli altri oggetti, tutto tramite una GUI molto user-friendly

- **Configuration Manager**

Permette di configurare alcune opzioni di base del server come le istanze, i protocolli di rete, ecc.

SQL Express: Ruoli

Anche in SQL Express (similmente a Oracle) **esistono i ruoli**, ed è quindi possibile mappare i privilegi per un gran numero di utenti tramite di essi.

I ruoli permettono di amministrare facilmente i privilegi di un gran numero di utenti (un concetto simile al raggruppamento di utenti).

E' quindi possibile creare un ruolo e assegnarlo a certi utenti e poi modificare solo esso per amministrare i privilegi di tutti gli utenti.

Esistono dei ruoli predefiniti di default all'installazione di SQL Express, si faccia riferimento alle reference relative:

<http://msdn2.microsoft.com/it-it/library/ms188659.aspx> (ruoli server)

<http://msdn2.microsoft.com/it-it/library/ms189121.aspx> (ruoli database)

SQL Express: Schema e Privilegi

Uno SCHEMA è un oggetto usato per raggruppare più database.

I privilegi degli utenti vengono assegnati non al singolo database ma ad uno SCHEMA, questo permette di gestire più facilmente l'aggiunta di privilegi su determinati oggetti (basta includerli in un certo SCHEMA e definire i permessi su di esso)

E' altresì possibile definire in modo granulare i permessi e vi sono funzioni apposite per visualizzare i permessi di un certo utente.

SQL Express: Privilegi su procedure

In modo simile ad Oracle XE le procedure possono essere eseguite con diverse modalità:

- **AS CALLER**

la procedura viene eseguita con i privilegi di chi la chiama

- **AS 'Utente'**

la procedura viene eseguita con i privilegi dell'utente indicato

- **AS SELF**

la procedura viene eseguita con i privilegi del suo creatore

SQL Express: Connessione al DB

Diverse possibilità sono disponibili per la connessione al DBMS:

- Shared memory

Permette di connettersi solo sullo stesso computer (non via rete)

- Named pipes

Permette l'accesso via rete sfruttando diversi protocolli (anche in base al client) tra cui NetBEUI, TCP/IP e IPX/SPX.

- TCP/IP

Specificando IP e nome dell'istanza tramite connessione TCP

- VIA

Virtual Interface Architecture, si tratta di un protocollo per cluster di server usato per System Area Networks

SQL Express: Porte in ascolto



Interessante notare che in SQL Express è presente un servizio *SQL Browser* che serve a sapere su che porte le varie istanze ascoltano per le connessioni.

Di default questo servizio è arrestato (si utilizza la connessione tramite *shared memory*) ma una volta attivato ascolta sulla porta 1434 UDP

SQL Express: Crittografia

La crittografia è necessaria (principalmente) per:

- Difendere i dati memorizzati da attacchi diretti alla macchina (ad esempio una compromissione fisica o un attacco perpetrato tramite un altro servizio)
- Difendere i dati durante la trasmissione da “occhi indiscreti”

In modo simile a Oracle:

- Supporta la connessione crittografata (SSL)
- Salvataggio dei dati crittografati con specifiche funzioni e definendo anche crittografia automatica di una certa colonna (per cifrare l'intero DB è possibile utilizzare la crittografia del file system NTFS)

MySQL 5 Community Edition

DBMS open source, libero anche per uso commerciale.

Rispetto alla versione enterprise non ci sono limitazioni particolari (si tratta di assistenza e aggiornamenti)

Recuperabile all'indirizzo:

<http://dev.mysql.com/downloads/mysql/5.0.html#downloads> (non richiede login)

MySQL 5: Introduzione

Datasheet

Versione	MySQL Community Server 5.0
Piattaforme	<ul style="list-style-type: none">- Windows (32bit e 64bit, 2000, XP, 2003 Server)- Linux (le maggiori distribuzioni 32bit e 64bit)- Altro: Solaris, FreeBSD, Mac OS X, HP-UX, IBM AIX, QNX, NetWare, SCO OpenServer 6
Prezzo	Gratuito e open source. Le versioni a pagamento includono servizi avanzati (console di amministrazione e altro) e supporto post-vendita (consulenza telefonica/email su problemi di performance, sicurezza, ecc.). Si parte da €500 per macchina/anno a €4000 per macchina/anno.
Licenza	Open Source GNU GPL e MySQL FLOSS, libero utilizzo.
Requisiti	Non troppo esigente, si può configurare per funzionare anche con pochissima memoria (30-40MB ad esempio) e poche centinaia di MB di spazio.
Limitazioni	Rispetto alla versione a pagamento non ci sono grosse limitazioni (il pagamento è soprattutto per il supporto post-vendita e per dei software di amministrazione)
Funzionalità	Vedi: http://dev.mysql.com/doc/refman/5.0/en/what-is-mysql.html Si tratta di un database leggero e veloce, mancano alcune funzionalità avanzate (presenti su Oracle e Microsoft) come la gestione di transazioni, rollback, subqueries, trigger avanzati, update automatici, ecc. Si adatta molto bene a progetti per il web o a piccoli gestionali, supporta anche alcune funzionalità di HA.

MySQL 5: Installazione

L'installazione è *molto* semplice e fa seguire un wizard di prima configurazione dove fare un primo “tuning” del DBMS, a livello di sicurezza:

- ❑ Si decide se aprire la porta TCP/IP (**3306 TCP** di standard) oltre alle named pipes (abilitate di default)
- ❑ Viene installato MySql come servizio di sistema
- ❑ Viene richiesta la password di *root* (l'utente amministratore), di default è disabilitato il suo accesso da macchine remote

MySQL 5: Istanze



E' possibile **avviare più di una istanza** di MySQL, ognuna delle quali ha differenti utenti e database.

Questa funzionalità è direttamente supportata tramite un demone apposito: `mysqld_multi`

Il vantaggio è che quindi si possono fornire (ad esempio a dei clienti) istanze completamente slegate, naturalmente si rischia un degrado di prestazioni.

MySQL 5: Opzioni di avvio

All'avvio di un'istanza è possibile impostare alcuni parametri di sicurezza che hanno la precedenza anche sui file di configurazione.

Questo può essere utile per assicurare il rispetto di alcune cose:

- ❑ `--safe-show-database`: quando si esegue il comando `SHOW DATABASE`, vengono listati solo i DB per i quali si possiede privilegio
- ❑ `--safe-user-create`: permette di inserire utenti tramite il comando `GRANT` solo se si ha il privilegio di `INSERT` all'interno della tabella utenti
- ❑ `--skip-name-resolve`: disabilita la risoluzione dei nomi relativi agli host che si possono connettere al server (tabella utenti), bisogna quindi inserire direttamente gli IP numerici
- ❑ `--skip-networking`: disabilita le connessioni tramite TCP/IP
- ❑ `--skip-show-database`: disabilita l'esecuzione del comando `SHOW DATABASES` a meno che non si abbia il privilegio corrispondente

MySQL 5: Gestione



Oltre alla gestione da command-line sono disponibili gratuitamente dei tool di amministrazione via GUI, che permettono di:

- ▣ creare/modificare i database
- ▣ gestire il DBMS (utenti, backup, ecc.)

MySQL 5: Connessione



La connessione al DB avviene solitamente via rete TCP oppure tramite named pipes.

Esistono per i diversi linguaggi *connector* o *librerie* per facilitare la connessione al server MySQL.

In ogni caso valgono le regole di autenticazione delle prossime slide.

MySQL 5: Autenticazione

A differenza di Oracle XE e Microsoft SQL Express, MySQL **non gestisce l'autenticazione tramite il sistema operativo ma solo all'interno del database.**

Esiste infatti un DB particolare chiamato "mysql" all'interno del quale vengono salvate le impostazioni sugli utenti.

Ogni utente è identificato da una tripletta username/host/password (quest'ultima salvata cifrata).

MySQL 5: Fasi di autenticazione



Durante le fasi di autenticazione viene:

- Verificato l'host da cui viene effettuata la connessione (è possibile specificare IP o netmask da cui è consentito l'accesso)
- Verificata username e password
- Ad ogni operazione viene controllato se vi sono i privilegi per portarla a termine

MySQL 5: Privilegi



La gestione dei privilegi è meno evoluta rispetto a Oracle XE e Microsoft Sql Express.

Si tratta infatti di una gestione meno granulare, non è ad esempio possibile:

- ▣ Bloccare un account (si può fare indirettamente non assegnandogli privilegi)
- ▣ Specificare che un utente possa creare o cancellare tabelle ma non cancellare il DB
- ▣ Non esiste una gestione per ruoli
- ▣ Non esiste una gestione della disk quota (si può fare indirettamente tramite il sistema operativo)

MySQL 5: Specifica dei Privilegi

I privilegi vengono specificati, similarmemente in questo caso agli altri DBMS, tramite istruzioni SQL.

E' **altamente consigliabile** utilizzare sempre le istruzioni **GRANT**, **REVOKE** e **SET PASSWORD** per modificare i privilegi, in questo modo il DBMS li renderà **subito effettivi**.

Se invece si modificano manualmente le tabelle relative ai permessi è necessario eseguire il comando **FLUSH PRIVILEGES** per rendere le modifiche effettive.

MySQL 5: Granularità

Come si diceva in MySQL c'è meno granularità, in particolare all'interno del DB *mysql* si specifica:

- Tabella *user*: privilegi a livello globale sull'autenticazione
- Tabella *db*: privilegi a livello di database
- Tabella *tables_priv*: privilegi a livello di tabella
- Tabella *columns_priv*: privilegi a livello di colonna

N.B. E' anche possibile definire dei privilegi relativi all'utilizzo delle risorse (es. numero di query, ecc.)

MySQL 5: Crittografia

La crittografia è necessaria (principalmente) per:

- Difendere i dati memorizzati da attacchi diretti alla macchina (ad esempio una compromissione fisica o un attacco perpetrato tramite un altro servizio)
- Difendere i dati durante la trasmissione da “occhi indiscreti”

MySQL supporta la crittografia in modo semplificato:

- Può essere ricompilato (non esiste una versione binaria pre-compilata per problemi di licenza) per permettere la connessione SSL (in questo caso la sicurezza è paragonabile a Oracle XE e Sql Express)
- Può salvare i dati in modo cifrato (anche con AES se ricompilato con SSL), l'operazione però avviene richiamando funzioni durante le query di inserimento, non è possibile definire una colonna come sempre cifrata o gestire efficacemente le chiavi (sono stati anche segnalati bug in cui la chiave in chiaro si trovava nel disco di swap!). Non è possibile quindi cifrare un intero database se non sfruttando il S.O.



Per maggiori informazioni visitate www.xelon.it

<http://creativecommons.org/licenses/by-nc-sa/2.5/it/>