Sicher mit
Microsoft™ SQL Server®?!

Agenda

- Vorstellung
- Kurzüberblick über SQL Server Sicherheit
- Sicherheit von SQL 2000 und 2005 in der Übersicht (Unterschiede in den Editionen)
- Die grafische Oberfläche
- Schemasicherheit oder Rollenkonzept? – oder und?
- Wenn noch Zeit bleibt: Q&A

PASS - The Definitive Community for SQL Server Professionals
Join PASS Today at www.sqlpass.de

Vorstellung

- Ehemann und Vater
- Unternehmer im Sinne von „unternehmen“
- Selbständig im Sinne von „selbst und ständig“
- MCT, MCSE + Security, MCDBA 7.0-2000, MCITP SQL Server (DBA/DBD/BI)
- Kein CLS (Certified License Specialist)

PASS - The Definitive Community for SQL Server Professionals
Join PASS Today at www.sqlpass.de

Agenda

- Vorstellung
- Kurzüberblick über SQL Server Sicherheit
- Sicherheit von SQL 2000 und 2005 in der Übersicht (Unterschiede in den Editionen)
- Die grafische Oberfläche
- Schemasicherheit oder Rollenkonzept? – oder und?
- Wenn noch Zeit bleibt: Q&A

PASS - The Definitive Community for SQL Server Professionals
Join PASS Today at www.sqlpass.de

(Kurz-)Überblick

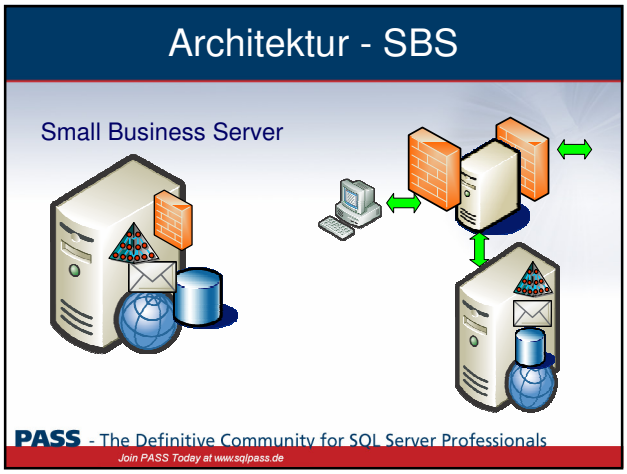
- Warum nur kurz?
- Architektur
  - Client
  - Netzwerk
  - Server

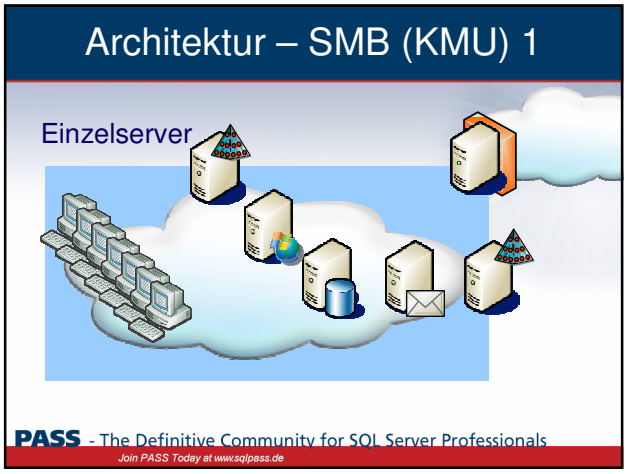
PASS - The Definitive Community for SQL Server Professionals
Join PASS Today at www.sqlpass.de

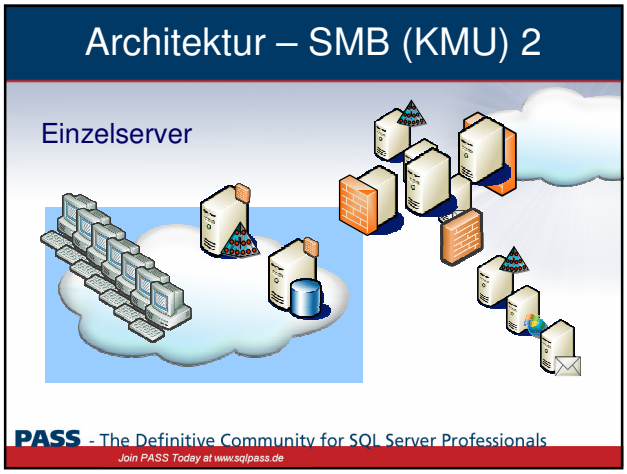
Überblick - Architektur

- Small Business Server
- SMB / KMU 1-3
- Virtualisiert
- High Performance Umgebungen

PASS - The Definitive Community for SQL Server Professionals
Join PASS Today at www.sqlpass.de

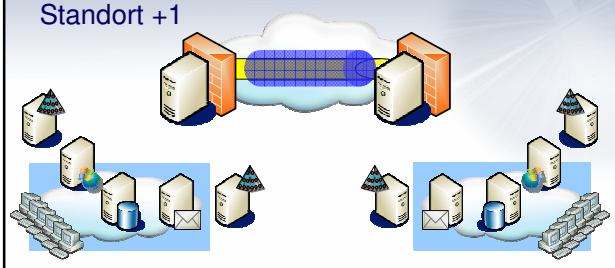

Architektur - SBS
Small Business Server
PASS - The Definitive Community for SQL Server Professionals
Join PASS Today at www.sqlpass.de


Architektur – SMB (KMU) 1
Einzelserver
PASS - The Definitive Community for SQL Server Professionals
Join PASS Today at www.sqlpass.de


Architektur – SMB (KMU) 2
Einzelserver
PASS - The Definitive Community for SQL Server Professionals
Join PASS Today at www.sqlpass.de

Architektur – SMB (KMU) 3

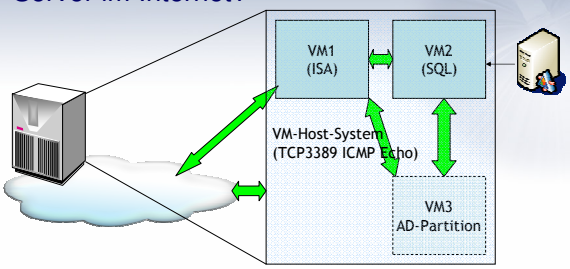
Standort +1



PASS - The Definitive Community for SQL Server Professionals
Join PASS Today at www.sqlpass.de

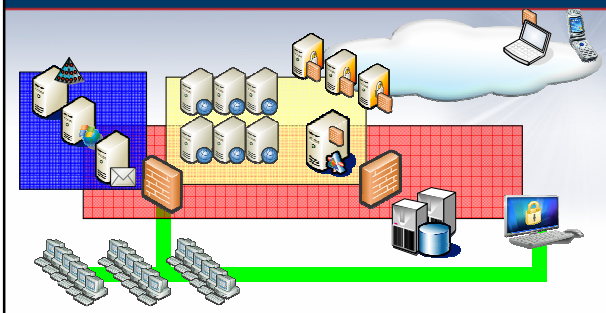
Architektur - virtualisiert

Server im Internet?



PASS - The Definitive Community for SQL Server Professionals
Join PASS Today at www.sqlpass.de

High Performance / Security



PASS - The Definitive Community for SQL Server Professionals
Join PASS Today at www.sqlpass.de

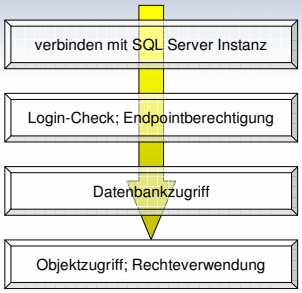
Agenda

- Vorstellung
- Kurzüberblick über SQL Server Sicherheit
- Sicherheit von SQL 2000 und 2005 in der Übersicht
- Die grafische Oberfläche
- Schemasicherheit oder Rollenkonzept? – oder und?
- Wenn noch Zeit bleibt: Q&A

PASS - The Definitive Community for SQL Server Professionals
Join PASS Today at www.sqlpass.de

„Der Weg bis zur (Daten-)Zelle“

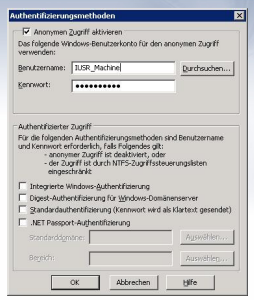
- Optional: Kommunikationseröffnung mit Windows IPC$ (Named Pipes, IPSec)



- Kommunikationseröffnung mit SQL Server
- Authentifizierung
- Authorisierung
- Schemasicherheit
- Authorisierung,
- Kryptografie

PASS - The Definitive Community for SQL Server Professionals
Join PASS Today at www.sqlpass.de

Anmeldung am System



- Lokal am System
- In der Domäne
- Am Webserver

PASS - The Definitive Community for SQL Server Professionals
Join PASS Today at www.sqlpass.de

Anmeldung am System

- Lokal am System („Computer\Benutzer“)
  - Zugriff auf lokale SQLServerinstanzen möglich
  - Nutzung von lokalen Ressourcen mit einem Benutzerkonto
  - Accesstoken besteht aus:
    - SID des Benutzers
    - SID der lokalen Gruppen
  - Sonderfall: durchgreifende Berechtigung
    - Bug? oder Feature!

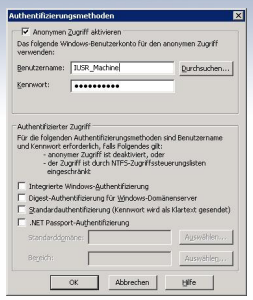
PASS - The Definitive Community for SQL Server Professionals
Join PASS Today at www.sqlpass.de

Anmeldung am System

- In der Domäne („Domäne\Benutzer“)
  - Zugriff auf lokale und entfernte Serverinstanzen möglich
  - Nutzung von vielen Ressourcen mit einem Benutzerkonto
  - Accesstoken besteht aus:
    - SID des Benutzers
    - SID der Domänengruppen
    - SID der lokalen Gruppen
  - Sonderfall: durchgreifende Berechtigung

PASS - The Definitive Community for SQL Server Professionals
Join PASS Today at www.sqlpass.de

Anmeldung am System – Web



- Anonym als
  - IUSR
  - Webserver\User
  - Domäne\User
- Integriert
- Digest
- Basis
- Passport

PASS - The Definitive Community for SQL Server Professionals
Join PASS Today at www.sqlpass.de

Netzwerkbibliotheken

- Shared Memory
- TCP/IP
- Named Pipes

PASS - The Definitive Community for SQL Server Professionals
Join PASS Today at www.sqlpass.de

Netzwerk - Shared Memory

- Kein Zugriff über das Netzwerk möglich
- Default bei neuen MSDE-Installationen
  - (ab SP 3)
- Default bei SQL 2005 Express Edition, Developer Edition, Evaluation Edition

PASS - The Definitive Community for SQL Server Professionals
Join PASS Today at www.sqlpass.de

Netzwerk – Named Pipes

- Zugriff über das Netzwerk möglich
- Primäres Protokoll bei SQL Server 2000 Installationen
- Anmeldung zwingend an IPC$ mit einem Windowskonto!
- → Der Zugriff auf den SQL Server schlägt fehlt, wenn IPC$ nicht den Zugriff auf den Windowscomputer freigibt!

PASS - The Definitive Community for SQL Server Professionals
Join PASS Today at www.sqlpass.de

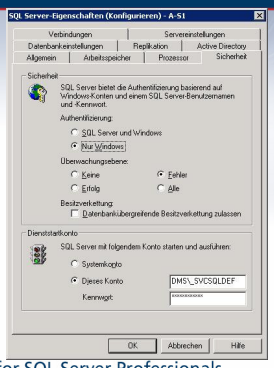
Netzwerk – TCP/IP

- Zugriff über das Netzwerk möglich
- Primäres Protokoll bei SQL Server 2005 Installationen
- Anmeldung „direkt“ am SQL Server über TCP-Port 1433 (oder 0)
- Slammer: UDP Port 1434 (weitere Instanzen) / >= MDAC 2.6
- SQL 2005 Native Client

PASS - The Definitive Community for SQL Server Professionals
Join PASS Today at www.sqlpass.de

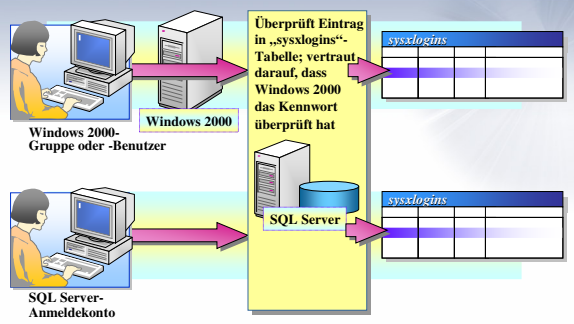
Die Anmeldung am SQL Server

- Windowsbenutzer
- Windowsgruppen
- SQL Server Benutzer
- Serverrollen,
- Datenbankrollen



PASS - The Definitive Community for SQL Server Professionals
Join PASS Today at www.sqlpass.de

Die Anmeldung am SQL Server



PASS - The Definitive Community for SQL Server Professionals
Join PASS Today at www.sqlpass.de

Idealisiertes Zugriffsschema

- Liebe Entwickler, die Datenbankzugriffe funktionieren auch, ohne das man als „sa“ mit dem SQL Server arbeitet!
- Tschüss „sa“! - auch auf Entwicklerservern! (bei SQL 05 sowieso deaktiviert!)
- Mach‘s gut „dbo“ – Erstelle „db_executor“!

☺ Mach‘s besser, Kollege! ☺

PASS - The Definitive Community for SQL Server Professionals
Join PASS Today at www.sqlpass.de

T-SQL Syntax (allgemein)

```
GRANT | REVOKE | DENY

SELECT | INSERT | UPDATE | DELETE |
REFERENCES | EXEC                ALL
| CREATE ----------------------
DATABASE | TABLE | VIEW | PROCEDURE |
FUNCTION | RULE | DEFAULT
| BACKUP ----------------------
DATABASE | LOG

[ ON Objekt ]
TO Benutzer
```

Syntax für SQL 2000!

```
GRANT SELECT ON Plan_Data TO Accounting WITH GRANT OPTION
```

PASS - The Definitive Community for SQL Server Professionals
Join PASS Today at www.sqlpass.de

T-SQL Syntax (allgemein)

- CREATE enthält nicht mehr automatisch auch ALTER und DROP

```
GRANT | REVOKE | DENY

SELECT | INSERT | UPDATE | DELETE |
REFERENCES | EXEC | …
| CREATE | ALTER | DROP ----------------------
DATABASE | TABLE | VIEW | PROCEDURE |
FUNCTION | RULE | DEFAULT | …
| BACKUP | RESTORE ----------------------
DATABASE | LOG …

[ ON ::SCHEMA | Schema.Objekt ]
TO Benutzer | (App.)Rolle
```

PASS - The Definitive Community for SQL Server Professionals
Join PASS Today at www.sqlpass.de

Noch mehr Syntax

- CREATE LOGIN
- CREATE USER
- GRANT EXECUTE ON <Database>
- GRANT SELECT ON <Schema>
- ALTER ANY ‚X' (X = Objekttyp)
- TAKE OWNERSHIP
- ALTER TRACE
- GRANT CONTROL u.v.a.m.

PASS - The Definitive Community for SQL Server Professionals
Join PASS Today at www.sqlpass.de

Ausführungskontext

- EXECUTE AS CALLER
  - Standard, wie SQL 2000 und früher
- EXECUTE AS „xyz"
  - Für „xyz" das Recht IMPERSONATE nötig
  - Wechsel des Benutzerkontextes
- EXECUTE AS SELF
  - Ausgeführt als Benutzer der EXECUTE AS ausführt
  - Der „faule" Entwickler: Ich durfte → du jetzt auch! ☺
- EXECUTE AS OWNER
  - Der „reale" Besitzer des Moduls (FN, P, TR)
  - ACHTUNG! Ändert sich beim Besitzerwechsel!

PASS - The Definitive Community for SQL Server Professionals
Join PASS Today at www.sqlpass.de

Die grafisch(e) Oberfläche(n)

Vorführung

PASS - The Definitive Community for SQL Server Professionals
Join PASS Today at www.sqlpass.de

Agenda

- Vorstellung
- Kurzüberblick über SQL Server Sicherheit
- Sicherheit von SQL 2000 und 2005 in der Übersicht
- Die grafische Oberfläche
- Schemasicherheit oder Rollenkonzept? – oder und?
- Wenn noch Zeit bleibt: Q&A

PASS - The Definitive Community for SQL Server Professionals
Join PASS Today at www.sqlpass.de

Idealisiertes Zugriffsschema

- Domänenbenutzer organisieren in
- Globalen Gruppen (nach Aufgabengebiet) diese wiederum in
- (Domain-) lokale Gruppen, die als Login
- Im SQL-Server (Ressource) auftreten
- Diese DLGs werden in die Datenbank- / Serverrollen aufgenommen, welche nur die nötigsten Rechte an
- SQL Server Objekten u. ä. haben

PASS - The Definitive Community for SQL Server Professionals
Join PASS Today at www.sqlpass.de

Serverrollen

Serverrolle	Berechtigung
sysadmin	Beliebige Aktivität ausführen
dbcreator	Datenbanken erstellen und ändern
diskadmin	Festplattendateien verwalten
processadmin	SQL Server-Prozesse verwalten
serveradmin	Serverübergreifende Einstellungen konfigurieren
setupadmin	Replikation installieren
securityadmin	Serverbenutzernamen verwalten und überwachen
bulkadmin	Anweisung BULK INSERT ausführen

PASS - The Definitive Community for SQL Server Professionals
Join PASS Today at www.sqlpass.de

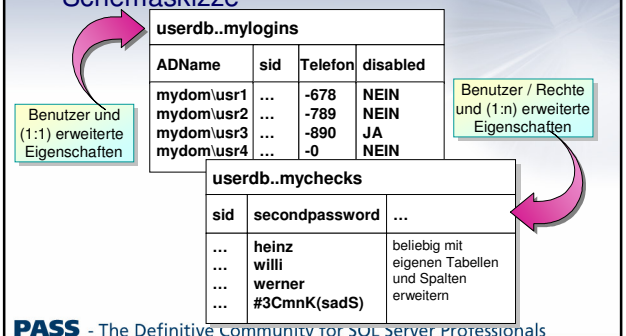
Datenbankrollen (System)

Datenbankrolle	Berechtigung
public	Standardberechtigungen (siehe model-Datenbank)
db_owner	Beliebige Datenbankrollenaktivitäten ausführen
db_accessadmin	Datenbankbenutzer, Gruppen und Rollen hinzufügen oder entfernen
db_securityadmin	Anweisungs- und Objektberechtigungen zuweisen
db_ddladmin	Datenbankobjekte hinzufügen, bearbeiten oder löschen
db_backupoperator	Datenbank sichern und wiederherstellen
db_datareader	Daten aus beliebigen Tabellen lesen
db_datawriter	Daten aus allen Tabellen hinzufügen, ändern oder löschen
db_denydatareader	Daten können aus keiner Tabelle gelesen werden
db_denydatawriter	Daten können in keiner Tabelle geändert werden

PASS - The Definitive Community for SQL Server Professionals
Join PASS Today at www.sqlpass.de

Eigene Login-Tabellen

- Schemaskizze



userdb..mylogins

ADName	sid	Telefon	disabled
mydom\usr1	…	-678	NEIN
mydom\usr2	…	-789	NEIN
mydom\usr3	…	-890	JA
mydom\usr4	…	-0	NEIN

userdb..mychecks

sid	secondpassword	…
…	heinz	
…	willi	
…	werner	
…	#3CmnK(sadS)	

PASS - The Definitive Community for SQL Server Professionals
Join PASS Today at www.sqlpass.de

Eigene Login-Tabellen 2

- Vorteile
  - Beliebig erweiterbar
  - "Mehr-Schlüssel-Zugriff" möglich
  - Schreiben einer UserDB die mit AD und anderen Verzeichnisdiensten synchronisiert werden kann
  - Extensives Logging und differenziertes automatisches Auswerten über Trigger und Prozeduren möglich
- Nachteile
  - Zusätzliche Eingangsprüfung
  - Umgehung bei mangelhafter Programmierung leicht möglich
  - Wird nur durch Anwendung - nicht durch SQL-Server - geprüft
  - Genaueste Berechtigungsplanung bei UserDB nötig

PASS - The Definitive Community for SQL Server Professionals
Join PASS Today at www.sqlpass.de

Diskussion

- SQL Anwendungsbenutzer (hart codiert)
- ein Windows-Benutzer (z. B.: Web)
- SQL-Konten
- Windowskonten
- Rollen vs. Schema

PASS - The Definitive Community for SQL Server Professionals
Join PASS Today at www.sqlpass.de

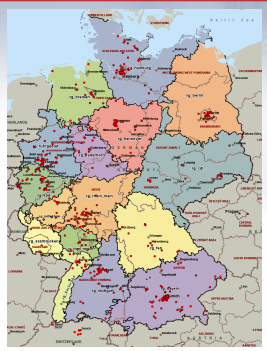
PASS: History & Facts 2007

- gegründet 31.08.2004
- Über **800** PASS'ler, davon >**380** Mitglieder
- mehr als 60 Treffen in 2005, **noch mehr in 2006**
- 1. BI-BootCamp 2005 auf dem Gut Höhne
- 2. BootCamp 2006: **mehr Inhalt, noch intensiver**
- 13 Regionalgruppen in ganz Deutschland
- SIGs für DBA, T-SQL, BI, RS
- Schweiz und Österreich im Aufbau
- Monatlicher Newsletter
- Präsenz auf (fast) jedem relevanten SQL Event sowie auf der CeBit

PASS - The Definitive Community for SQL Server Professionals
Join PASS Today at www.sqlpass.de

Regionalgruppen

- Etablierte Regionalgruppen
  - Bayern
  - Berlin
  - Hamburg
  - Hannover
  - Karlsruhe
  - Köln / Bonn / Düsseldorf
  - Mittelrhein
  - Rhein/Main
  - Rhein/Neckar
  - Ruhrgebiet
  - Sachsen
  - Stuttgart
- Im Aufbau / In Planung
  - Franken
- Unterstützung
  - Österreich
  - Schweiz



PASS - The Definitive Community for SQL Server Professionals
Join PASS Today at www.sqlpass.de

PASS'ler sind...

- ...Idealisten, die fest an den Wert von Networking glauben.
- ...überzeugt, dass es sich lohnt, ein sehr gutes Produkt noch besser zu machen.
- ... SQL Rookies oder SQL Jedis.
- ...bereit einem anderen User jederzeit unter die Arme zu greifen.
- ...wissbegierig!!!

PASS - The Definitive Community for SQL Server Professionals
Join PASS Today at www.sqlpass.de

Was war nicht dran?

- Anwendungsrollen – unbedingt anschauen
- Verschlüsselung von Datenverkehr, Passwörtern, DDL-Code, Daten
- Code-Signaturen
- Sicherheit bei .net-Integration, Service Broker, Reporting, OLAP, etc.pp.
- Mehr Details und Szenarien (Geduld, bitte warten Sie auf mein Buch, wenn ich es denn wirklich noch fertig schreibe)

PASS - The Definitive Community for SQL Server Professionals
Join PASS Today at www.sqlpass.de

Bis später…

Vielen Dank für Ihre Aufmerksamkeit!
Ihr Ralf Dietrich

Fragen an Training@damisys.de
Betreff: 1.SEK 2007

PASS - The Definitive Community for SQL Server Professionals
Join PASS Today at www.sqlpass.de