

Wer hat Angst vor dem Rechenzentrum

Autor: Uwe Ricken
db berater GmbH

© db Berater GmbH, 64390 Erzhäusen, Mai 2009

Agenda

- Übersicht über Leistungsmerkmale eines Rechenzentrums
 - Organisatorische Aufteilung
 - Räume eines Rechenzentrums
 - Sicherheit in einem Rechenzentrum
 - Backup eines Rechenzentrums
- Prozesse für die Implementierung einer SQL Datenbank in ein Rechenzentrum
 - Einrichtung eines POC (Proof of concept)
 - Einrichtung einer UAT (User Acceptance Test)
 - Einrichtung einer PROD (Production environment)
 - Einrichtung eines BCP (Backup Center Production)



© db Berater GmbH, 64390 Erzhäusen, Mai 2009

Agenda

- Einschränkungen bei der Verwendung von SQL Datenbanken in einem Rechenzentrum
 - Zugriff auf das Dateisystem
 - Verwendung von ActiveX-Komponenten
 - Verwendung von Extended Procedures
 - Mailversand
 - Administrative Aufgaben (Benutzeradministration, Backups, Datenbankmaintenance, ...)

- Workarounds für Sicherheitsbeschränkungen
 - Zugriff auf das Dateisystem
 - Verwendung von ActiveX-Komponenten (sp_OACreate...)
 - Verwendung von Extended Procedures
 - Mailversand (MAPI Mail / Database Mail)



Organisatorische Aufteilung

- Als Rechenzentrum bezeichnet man sowohl das Gebäude bzw. die Räumlichkeiten, in denen die zentrale Rechentechnik (z. B. Rechner aber auch die zum Betrieb notwendige Infrastruktur) einer oder mehrerer Unternehmen bzw. Organisationen untergebracht sind, als auch die Organisation selbst, die sich um diese Computer kümmert. Ihr kommt damit eine zentrale Bedeutung in der Unternehmens-EDV zu.

- Rechenzentren sind einer administrativen Stelle zugeordnet, zum Beispiel der Finanzverwaltung, einer Forschungseinrichtung, einer Hochschule oder einem kommerziellen Betrieb wie einer Bank oder einer Versicherung. Diese administrativen Stellen haben die Anforderung, große Datenmengen zu verarbeiten.



Organisatorische Aufteilung

- Systemtechnik

Die Systemtechnik ist für die Hardware verantwortlich.

- Systemverwaltung

Die Systemverwaltung ist für die Administration der Maschinen zuständig.

- Operating

Das Operating übernimmt eher Hilfsaufgaben, die vom Wechseln des Druckerpapiers, dem Reißen der Ausdrucke und deren Verteilung oder dem Einlegen von Magnetbändern reicht.



Räume und Technik

- Der Maschinenraum eines Rechenzentrums auf dem Stand der Technik ist mit einem geräumigen Doppelboden ausgestattet, durch den nicht nur die Verkabelung, sondern auch kühle Luft von der Klimaanlage zu den Geräten geführt wird. Netzwerkschränke stehen sich in geschlossenen Reihen mit ihren Vorderseiten oder Rückseiten gegenüber



- Die hohe Leistungsdichte und damit einhergehende Wärmeentwicklung erfordert nicht nur aufwendige Maßnahmen zur Kühlung, sondern bewirkt durch den Lärm der in den Geräten enthaltenen Ventilatoren auch, das während des Aufenthalts im Maschinenraum Gehörschutz erforderlich ist.
- Die Anforderung an die Verfügbarkeit von Rechenzentren sind hoch. Sie werden deshalb mit redundanten Klimaanlagen, unterbrechungsfreien Stromversorgungen und Brandmeldeanlagen ausgestattet.

Sicherheit in einem Rechenzentrum

- Abhängig vom administrativen Umfeld gibt es unterschiedlich starke Sicherheitsanforderungen an Rechenzentren. Meist wird lediglich der Zutritt kontrolliert und die Räume sind durch Alarmanlagen gesichert. Einige sind sogar in einem atombombensicheren Bunker untergebracht, der unterirdisch mehrere Stockwerke umfasst. Der Zutritt ist auf jeden Fall strikt reglementiert.
- Dem Brandschutz wird ein besonderer Stellenwert eingeräumt. Neben Brandabschottungen gibt es häufig auch Löschanlagen, die Hardwareschäden minimieren sollen. Wasser kann einem Großrechner mehr Schaden zufügen als ein verschmortes Kabel. Aus diesem Grund wird in modernen Rechenzentren spezielles Gas (meistens das Edelgas Argon oder aber auch noch Kohlenstoffdioxid) zum Löschen des Brandes eingesetzt. Die Archivierung von wichtigen Datensicherungen findet daher auch in dedizierten Brandabschnitten statt.



© db Berater GmbH, 64390 Erzhausen, Mai 2009

Backuprechenzentrum

- Um für Katastrophen gerüstet zu sein, gibt es das sog. Backup-Rechenzentrum. Dabei wird ein vorhandenes Rechenzentrum räumlich vom Originalrechenzentrum deutlich getrennt komplett dupliziert. Die Duplizierung gilt sowohl für die Hardware als auch für die Software und die aktuellen Daten. Sollte das Originalrechenzentrum ausfallen, so kann der Betrieb im Backuprechenzentrum sofort fortgesetzt werden.
- Notfallpläne und Ausstattung sehen oft sogar vor, daß die Arbeitsräume der Mitarbeiter bis auf die Ausstattung des einzelnen Arbeitsplatzes 1:1 kopiert werden, so daß von einem Tag zum nächsten die Arbeit in den Räumlichkeiten des Backup-Rechenzentrums fortgesetzt werden können.
- Der Grund für die großen Investitionen (Zeit und Geld) ist: Der Totalausfall eines Rechenzentrums wird als Unternehmensgefährdung angesehen.

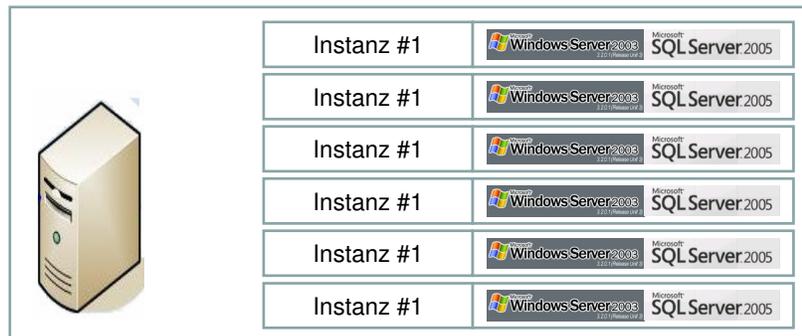
© db Berater GmbH, 64390 Erzhausen, Mai 2009

Gründe für den Betrieb in RZ

- Gehostete Umgebung (Operating)
 - Das Business konzentriert sich auf Kernkompetenzen und lagert die Administration von Hard- und Software aus.
 - Ein physikalischer Server kann entweder mehrere Betriebssysteminstanzen (VM Ware) und / oder mehrere SQL Server Instanzen verwalten.
 - Konsolidierung von Inventar
 - Hard- und Software Sharing
- Kostenreduktion
 - In virtualisierten Umgebungen werden die Kosten für den Betrieb der Hardware und des Operatings von mehreren Abteilungen gemeinsam übernommen.
 - Infrastruktur wird auf ALLE Geschäftsbereiche des Unternehmens kostenmäßig verteilt. Es bedarf keiner individuellen Infrastrukturlösung mehr.
 - Senkung der Energie-, Verwaltungs- und Mietkosten
- Datensicherheit
 - Regelmäßige Überwachung der Datensicherung durch das Operating garantiert eine hohe Ausfallsicherheit
 - Verwendung redundanter Systeme

© db Berater GmbH, 64390 Erzhäusen, Mai 2009

Virtual Servers (VM)



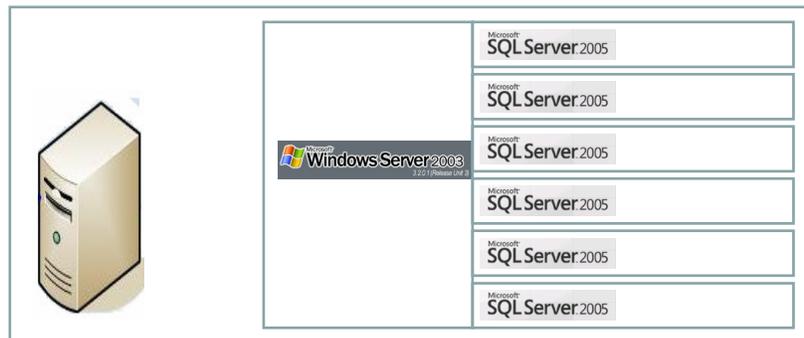
© db Berater GmbH, 64390 Erzhäusen, Mai 2009

Virtual Servers (VM)

Item	Anzahl	Kosten	Summe
Server	1	15.000,00 €	15.000,00 €
VM Ware	1	3.750,00 €	3.750,00 €
Windows 2003 Server	6	4.520,00 €	27.120,00 €
SQL Server 2005 Enterprise	4	19.000,00 €	76.000,00 €
Summe			121.870,00 €
Kosten / PC	40.000		~ 3.00 €

© db Berater GmbH, 64390 Erzhäusen, Mai 2009

Instanzen



© db Berater GmbH, 64390 Erzhäusen, Mai 2009

Instanzen

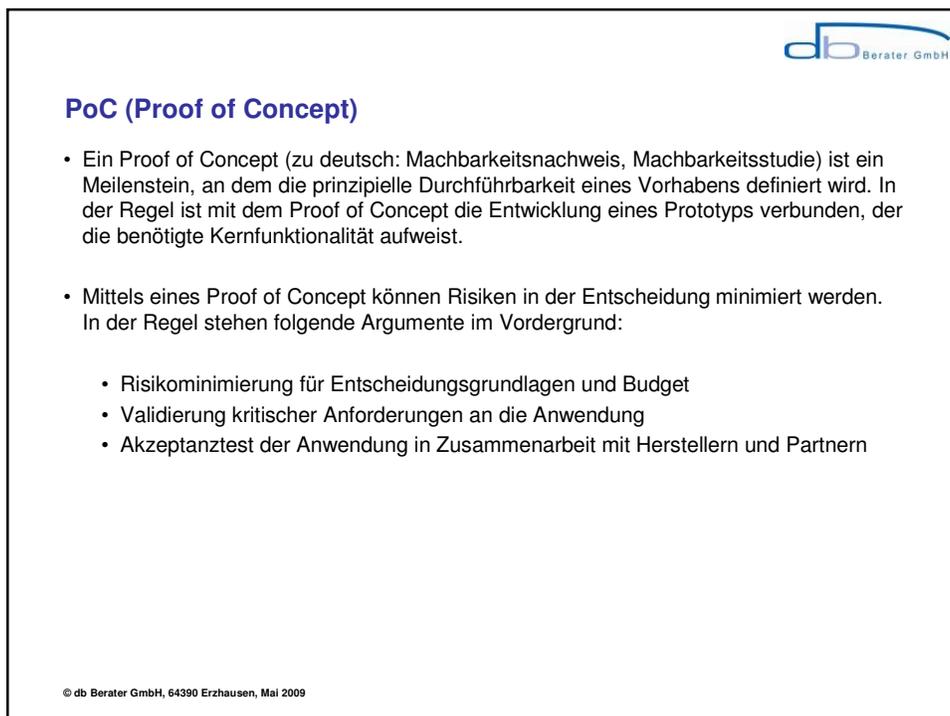
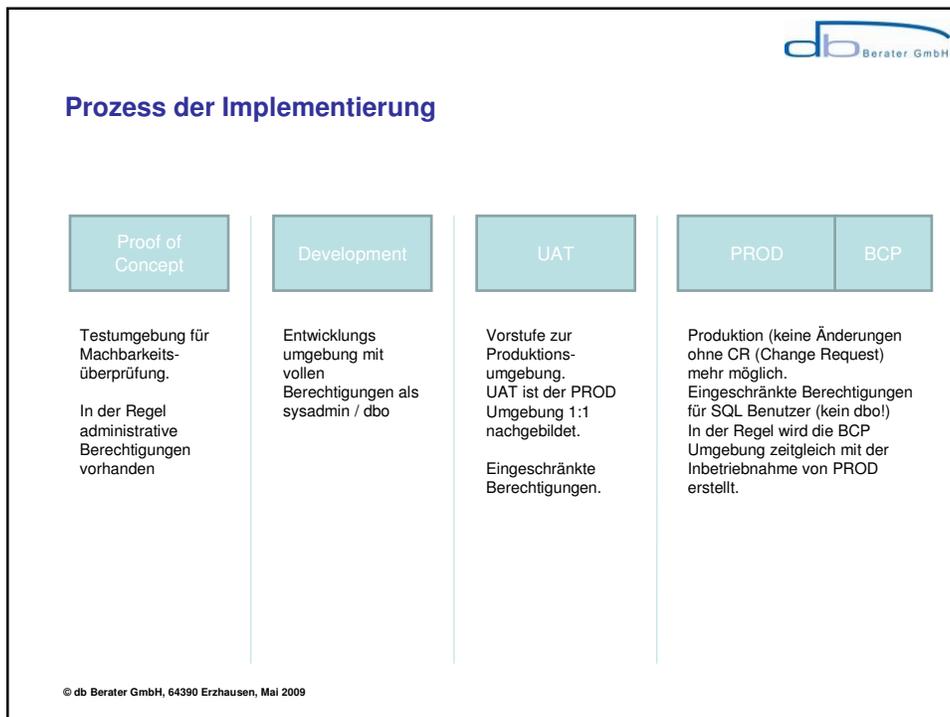
Item	Anzahl	Kosten	Summe
Server	1	15.000,00 €	15.000,00 €
VM Ware	1	3.750,00 €	3.750,00 €
Windows 2003 Server	1	4.520,00 €	4.520,00 €
SQL Server 2005 Enterprise	4	19.000,00 €	76.000,00 €
Summe			99.270,00 €
Kosten / PC	40.000		~ 2,50 €

© db Berater GmbH, 64390 Erzhäusen, Mai 2009

Einschränkungen bei der Verwendung von SQL Datenbanken in einem Rechenzentrum

- Alltägliche Probleme eines Entwicklers
 - 32 Bit vs. 64 Bit (Treiber, BI, IS)
 - Good dba, bad dba (Sicht eines Entwicklers und eines Administrators)
- Berechtigungseinschränkungen
 - Prozesse für die Implementierung einer SQL Datenbank in ein Rechenzentrum
 - Einrichtung einer UAT (User Acceptance Test)
 - Einrichtung einer PROD (Produktionsumgebung)
 - Einrichtung eines BCP (Backup Production)
- Einschränkungen bei der Verwendung von SQL Datenbanken in einem Rechenzentrum
 - Zugriff auf Dateisystem nicht erlaubt (xp_cmdShell)
 - Benutzung von ActiveX Objekten nicht erlaubt (sp_OACreate, ...)
 - Keine Verwendung von MAPI erlaubt (xp_sendmail)
 - Keine Benutzerwaltung erlaubt (xp_addLogin)
 - Keine dbo-Berechtigungen (zu 95% die Probleme, die wir hier haben)

© db Berater GmbH, 64390 Erzhäusen, Mai 2009



Development

- Entwicklungsumgebung
 - Dediziertes System (i. d. R. auf VM-Ware)
 - Volle administrative Kontrolle für Entwicklerstab
 - Eingeschränkte Berechtigungen auf Betriebssystemumgebung
 - Installation von Software ist in der Regel durch Operating möglich.

UAT (Softwaretest)

- Ein Softwaretest ist ein Test während der Softwareentwicklung, um die Funktionalität einer Software an den Anforderungen und ihre Qualität zu messen, und Softwarefehler zu ermitteln
- Der UAT verwendet Sicherheits- und Systemkonfigurationen, wie sie in der Produktion verwendet werden.
 - Verwendung von dedizierter Instanz
 - Minimale Berechtigungen für Entwickler und Anwender
- Entwickler können keine Änderungen mehr unmittelbar durchführen (CR muss erstellt werden)
- Updates werden durch SQL Administratoren eingespielt



PROD (Arbeitsumgebung)

- In der Produktionsumgebung werden verschärfte Sicherheitsvorkehrungen getroffen
 - Verwendung von dedizierter Instanz (Virtualisierung)
 - Minimale Berechtigungen für Entwickler und Anwender
 - SQL Administratoren haben keinen unmittelbaren Zugang mehr zum Server (Segregation of Duty)
- Es dürfen keine ungeprüften „third party“ Produkte auf dem Server installiert werden.
- Entwickler können keine Änderungen mehr unmittelbar durchführen (CR muss erstellt werden)
- Administration des SQL Servers (Sicherheit, Backup, Management) obliegt ausschließlich den SQL Administratoren
- Updates (SQL Scripts) werden durch SQL Administratoren nach ihrer technischen Überprüfung (USE Database, GRANT acl) eingespielt.
- Servicepacks können nur von Systemadministratoren eingespielt werden

© db Berater GmbH, 64390 Erzhäusen, Mai 2009



BCP(Backup of Production)

- Das BCP-System ist identisch mit PROD
- BCP-System kann eine / mehrere Sicherungsstrategien verwenden:
 - Transaction Log Shipping
 - Replication
 - Mirroring

© db Berater GmbH, 64390 Erzhäusen, Mai 2009



Transaction Log Shipping

- Log Shipping erlaubt den automatischen Versand von Transaction Logs von einer Datenbank (Primary Database) zu einer zweiten Datenbank (Secondary Database) auf einem andere Server . Auf dem zweiten Server werden die Transaction Logs nach der Übertragung unmittelbar wiederhergestellt. Ein optionaler dritter Server zeichnet die Historie und den Status von Backup- und Restore Operationen auf und wirft bei Problemen Meldungen aus.
- Vorteile von Log Shipping
 - Geographische Trennung der Server ist möglich
 - Benutzung der Datenbank auf Server #2 ist möglich (Standby-Server)

DEMO

© db Berater GmbH, 64390 Erzhäusen, Mai 2009



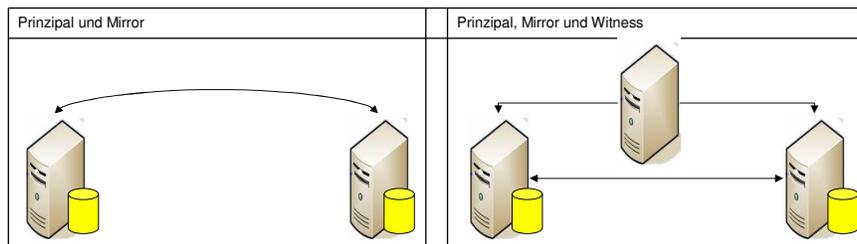
Database Mirroring

- Database Mirroring bietet eine vollständige Redundanz der Daten
- Serverinstanzen kommunizieren über eine direkte Netzwerkanbindung und können sich an unterschiedlichen Standorten befinden.
- Keine besondere Hardware ist erforderlich.
- Der Rollenwechsel geschieht bei einigen Einstellungen „on the fly“.
- Ein SQL Server kann verschiedene Rollen gleichzeitig annehmen
- Database Mirroring unterstützt Volltextkataloge.
- Leicht zu administrierende Alternative zum FailOver Clustering
- Eine Datenbank kann sowohl als Prinzipal in einer Mirror-Umgebung als auch als Lieferant für eine Log Shipping Verfügbarkeit verwendet werden.
- Database Mirroring kann innerhalb einer Replikationsstrategie verwendet werden.
- Nachteile
 - Nur der Prinzipal kann verwendet werden
 - Datenbank im Spiegel befindet sich immer im Recoverymode
 - Automatischer Wechsel (FailOver) kann nur bei synchronen Spiegeln verwendet werden. Asynchrone (Hohe Performance vs. Hochsicherheit) Spiegel müssen wieder komplett neu erstellt werden, wenn der Spiegel zerbrochen ist

© db Berater GmbH, 64390 Erzhäusen, Mai 2009

Database Mirroring

- Szenario 1: principal und mirror
 - FailOver muss manuell initiiert werden
 - Je nach Typus (synchron / asynchron) wird bei einem FailOver der Spiegel zerbrochen
- Szenario 2: principal, witness, mirror
 - FailOver wird automatisch durchgeführt
 - Spiegel wird je nach Typus bei FailOver zerstört



© db Berater GmbH, 64390 Erzhäusen, Mai 2009

Replikation

- SQL Server unterscheidet drei Arten von Replikation
 - Snapshot Replikation
Bei der Snapshot Replikation wird eine Momentaufnahme der Datenbank an die Subscriber geliefert. Der Datenfluss ist unidirektional zum Subscriber und nimmt keine Rücksicht auf Änderungen in dessen Datenbank.
 - Transaktionale Replikation
Setzt man auf die transaktionale Replikation werden alle Änderungen im Publisher möglichst synchron auf den Subscriber übertragen, da dieser ein bestmögliches Abbild des Publishers darstellen soll. Dies erfordert eine zuverlässige Netzwerkverbindung mit ausreichender Bandbreite.
 - Merge Replikation
Die Replikation wird entweder durch den Publisher / Distributor als Push- oder durch den Subscriber als Pull-Mechanismus initiiert. Für eine Pushreplikation ist eine ständige Netzwerkverbindung notwendig!

© db Berater GmbH, 64390 Erzhäusen, Mai 2009



Einschränkungen bei der Verwendung von SQL Datenbanken im Rechenzentrum

- Warum gibt es Einschränkungen in virtuellen Systemen und /oder Instanzenbetrieb?
 - Zugriff auf Betriebssystem darf nur durch Systemoperatoren erfolgen
- Benutzerverwaltung obliegt den Systemoperatoren
- Zugriffe auf Dateiebene bergen Gefahren
 - Import von Virensystemen
 - Import von Trojanern
 - Löschen von Systemdaten
 - Gefahr des Produktionsausfalls
- Unmittelbare Zugriffe sind auf dem Level des Betriebssystems bereits abgesichert
- SQL Server und/oder SQL Agent laufen unter einem Systemaccount, der in der Regel administrative Berechtigungen besitzt – GEFAHR!

© db Berater GmbH, 64390 Erzhausen, Mai 2009



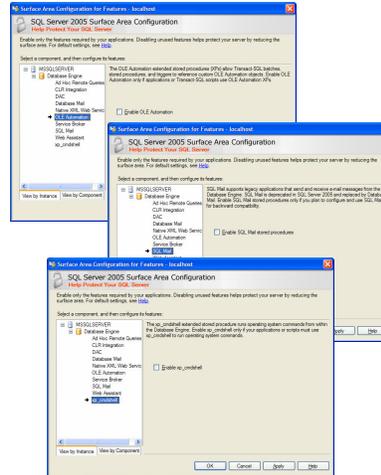
Standardberechtigungen eines dbo (db_owner)

- Hat Zugriff auf ALLE Datenbanken der Instanz, dessen Eigentümer der User ist!
- CONTROL – Berechtigung auf Datenbank
 - Kann Berechtigungen für User erteilen
 - Kann Recovery Modus ändern (Datensicherung!)
 - Kann Schemata verwalten
 - Kann User der Datenbank verwalten
- Alle Verwaltungsaufgaben für eine Datenbank
 - Vergrößern / Verkleinern von Datenbanken (Dateisystem)
 - Durchführen von Datensicherungen (Dateisystem / Sicherheitssystem)
- Verändern von Berechtigungen der Datenbankobjekte
 - Datenintegrität kann geschädigt werden
 - Applikationen können u. U. nicht mehr arbeiten
 - Geschäftsausfälle drohen

© db Berater GmbH, 64390 Erzhausen, Mai 2009

Standardinstallation eines SQL Server im RZ

- Systemaccount „sa“ ist deaktiviert (SQL 2005)
- SQL Server und SQL Agent verwenden einen Service-Account des AD (Active Directory)
- Netzwerkverbindung ausschließlich TCP/IP
- OPENROWSET ist deaktiviert
- CLR Integration ist deaktiviert*
- Database Mail ist deaktiviert
- Native XML Web Service
- OLE Automation ist deaktiviert
- Service Broker ist deaktiviert
- SQL Mail ist deaktiviert
- Web Assistant ist deaktiviert
- xp_cmdShell ist deaktiviert



© db Berater GmbH, 64390 Erzhäusen, Mai 2009

Werden grundsätzlich nicht aktiviert

Können bei Bedarf aktiviert werden

Warum kein xp_cmdShell

- Administratoren fühlen sich wie Götter ;-)
- xp_cmdShell kann unkontrolliert auf das Dateisystem zugreifen wenn der Serviceaccount / Agentaccount entsprechende Berechtigungen besitzt.
 - EXEC xp_cmdShell 'DEL C:\WINDOWS*.*'
- xp_cmdShell hat Berechtigungen des SQL Server Service accounts
- xp_cmdShell arbeitet synchron!
 - Die Kontrolle wird erst nach der Ausführung des Befehls wieder an den Aufrufer zurückgegeben
 - Risiko eines Geschäftsausfalls (Das obige Beispiel wartet auf eine Bestätigung!)

© db Berater GmbH, 64390 Erzhäusen, Mai 2009



Warum kein sp_OA...

- Administratoren fühlen sich wie Götter ;-)
- sp_OA... startet unkontrolliert ActiveX Komponenten
- ActiveX Komponenten müssten auf Server installiert werden – das ist aber nicht erlaubt!
- Um sp_OA... auszuführen, muss der Benutzer Mitglied der Serverrolle „sysadmin“ sein

© db Berater GmbH, 64390 Erzhäusen, Mai 2009



Warum kein SQLMail

- SQL Mail verwendet Extended MAPI als Schnittstelle für den Versand von Mails
 - MAPI muss vor der Verwendung unter dem Service Account des SQL Servers konfiguriert werden
 - Mails werden unter dem Service Account des SQL Servers versendet
 - Mailprogramm (Outlook) muss auf Server installiert werden
- SQL Mail verwendet extended Procedures für den Versand von Mails
 - xp_startmail
 - xp_sendmail, xp_deletemail, xp_readmail, xp_findnextmsg
 - xp_stopmail
- Per Standard haben nur Mitglieder der Serverrolle „sysadmin“ Ausführungsberechtigungen auf die oben genannten Stored Procedures!
- SQL Mail wird in zukünftigen Versionen von Microsoft SQL Server nicht mehr verwendet

© db Berater GmbH, 64390 Erzhäusen, Mai 2009

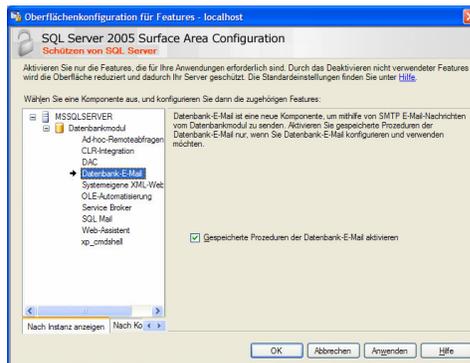
Alternativen gegen Beschränkungen

- Ausführung von bestimmten Funktionen, die auf administrativen Zugriff angewiesen sind, als Job erstellen
 - Jobs laufen unter dem Serviceaccount des SQL Agent
 - Jobs werden durch SQL Administratoren überprüft und implementiert
 - Jobs können abgelehnt werden, wenn sie Einträge aus Tabellen für xp_cmdshell einsetzen (fehlende Kontrolle)
- Verwendung von Database Mail statt SQL Mail
 - Database Mail benötigt weder Microsoft Outlook noch „Extended Mapi“ für den Mailversand
 - Database Mail verwendet Standard SMTP
 - Database Mail wird als ausgelagerter Prozess außerhalb von SQL Server gestartet (Process Isolation)
 - Asynchrone Bearbeitung der Mailjobs (SQL Routine läuft weiter und wartet nicht auf ein Feedback vom Prozess)
 - Mitglieder der Datenbankrolle „DatabaseMailUserRole“ in msdb können Mails versenden! Diese Option wird jedoch in der Regel nicht eingerichtet. Vielmehr sollte ein Job regelmäßig eine „Mailqueue“ in der Applikationsdatenbank überprüfen und ggfls noch nicht versendete Mails abschicken (siehe Beispielscript)

© db Berater GmbH, 64390 Erzhausen, Mai 2009

Database Mail - Besonderheiten

- Database Mail muss explizit aktiviert werden (Surface Configuration)



- Per Standard haben nur Mitglieder der Gruppe „DatabaseMailUser“ in msdb „EXECUTE“ Permissions zum Ausführen von sp_send_dbmail!

© db Berater GmbH, 64390 Erzhausen, Mai 2009



Database Mail aktivieren

- **EXEC** `msdb.dbo.sysmail_start_sp`
Startet Database Mail
- **EXEC** `msdb.dbo.sp_send_dbmail`
Führt Database Mail aus und versendet die Email
- **EXEC** `msdb.dbo.sysmail_stop_sp`
Beendet Database Mail

© db Berater GmbH, 64390 Erzhäusen, Mai 2009

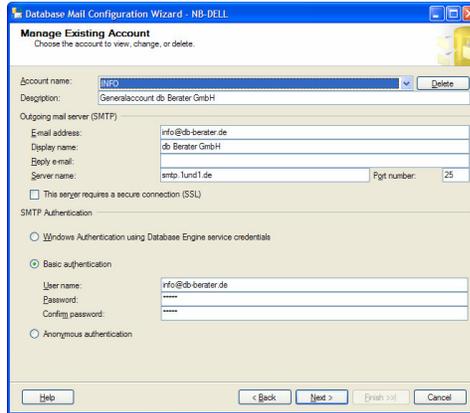


Hinweis

- `sp_send_dbmail` erwartet zwingend „Inhalt“
Der Inhalt kann sein:
 - `@body` Mailbody
 - `@query` Abfrageergebnis
 - `@file_attachments` Dateianhang
 - `@subject` Betreff
- `@recipients`, `@copy_recipients`, `@blind_copy_recipients` müssen durch Semikolon voneinander getrennt werden, wenn es sich um mehr als einen Empfänger handelt
- Database Mail arbeitet IMMER im Kontext des aktuell angemeldeten Benutzers und muss beim Zugriff auf das Filesystem beachtet werden.
- SQL User haben KEINEN Zugriff auf das Filesystem da sie nicht gegen die Sicherheitseinstellungen der des Filesystems überprüft werden können
- Wenn `@query` oder `@file_attachments` angegeben werden und keine Daten gefunden werden, wird `sp_send_dbmail` zwar weiter ausgeführt aber die Mail wird nicht gesendet!

© db Berater GmbH, 64390 Erzhäusen, Mai 2009

Konfiguration



The screenshot shows the 'Manage Existing Account' dialog box in the Database Mail Configuration Wizard. The dialog is titled 'Database Mail Configuration Wizard - MS-DELL' and has a subtitle 'Manage Existing Account'. Below the subtitle, it says 'Choose the account to view, change, or delete.' The dialog contains several fields and options:

- Account name:** A dropdown menu showing 'INFO' and a 'Delete' button.
- Description:** A text box containing 'Generalaccount db Berater GmbH'.
- Outgoing mail server (SMTP):**
 - E-mail address:** 'info@db-berater.de'
 - Display name:** 'db Berater GmbH'
 - Reply e-mail:** (empty)
 - Server name:** 'smtp1.tund1.de' and **Port number:** '25'
 - This server requires a secure connection (SSL)
- SMTP Authentication:**
 - Windows Authentication using Database Engine service credentials
 - Basic authentication
 - Username:** 'info@db-berater.de'
 - Password:** (masked with asterisks)
 - Confirm password:** (masked with asterisks)
 - Anonymous authentication

At the bottom of the dialog, there are buttons for 'Help', '< Back', 'Next >', 'Finish >>', and 'Cancel'.

© db Berater GmbH, 64390 Erzhäusen, Mai 2009