

---

# INTERSYSTEMS

# SYMPOSIUM 2005

## Vyspělá bezpečnost a databáze Caché



Tomáš Vaverka  
Support Advisor

---

# Agenda



- Tématem přednášky bude hlubší pohled na „Vyspělou bezpečnost Caché“ (Caché Advanced Security).
- Autentizace
- System Management Portal
- Autorizace, zdroje, role, práva
- Audit a Bezpečnostní poradce
- Šifrování databáze

# „Vyspělá bezpečnost Caché“ - souhrn



*Ve verzi 5.1 InterSystems představuje „Vyspělou bezpečnost Caché“ (Caché Advanced Security). Tato funkčnost poskytuje jednoduchou, unifikovanou bezpečnostní architekturu s následujícími prvky:*

## Caché Advanced Security

- Silnou, důslednou a vysoce-výkonnou bezpečnostní infrastrukturu pro aplikace.
- Vývojářům umožňuje snadno zabudovat bezpečnostní prvky do aplikací.
- Minimálně zatěžuje výkonnost a provoz.
- Zajišťuje, že Caché umí efektivně fungovat jako součást bezpečného prostředí a hladce komunikovat s ostatními aplikacemi.
- Umožňuje vynucovat bezpečnostní pravidla a audit.
- Splňuje bezpečnostní certifikační standardy.

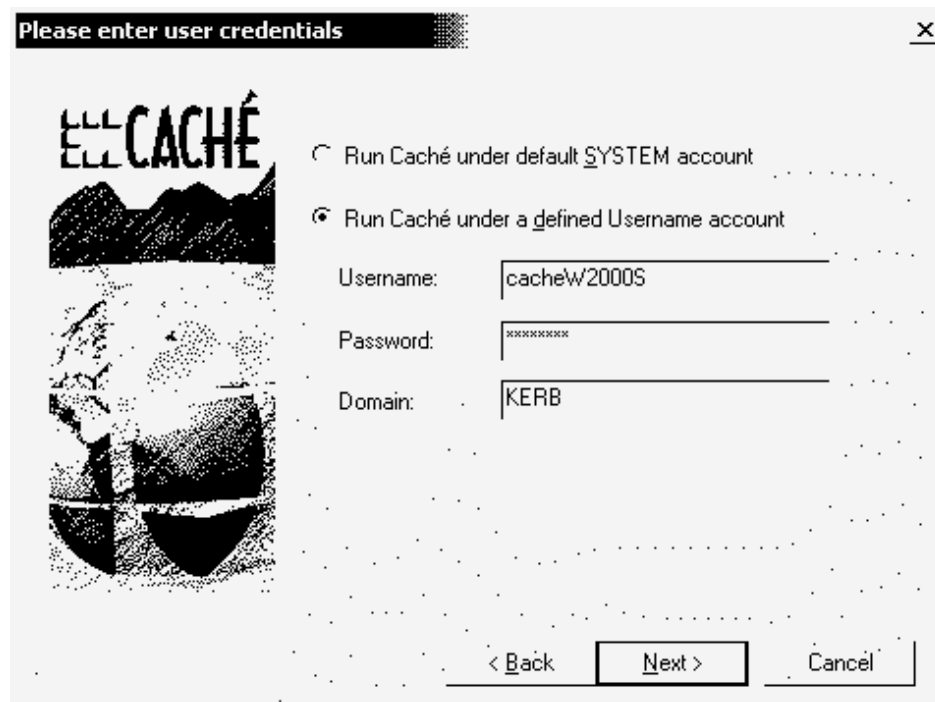
# Komponenty...



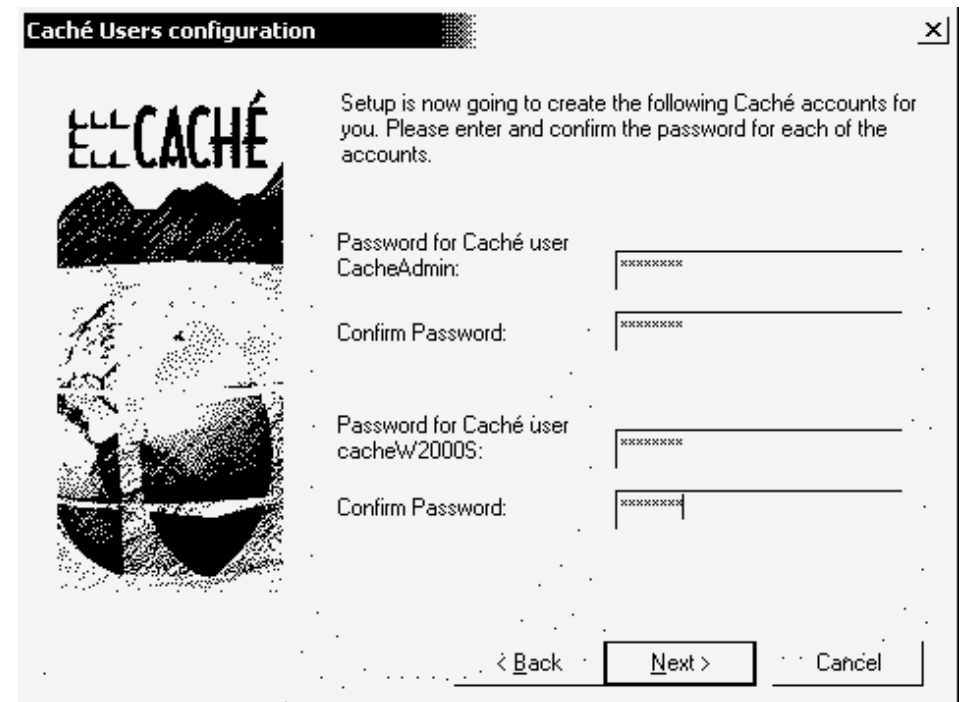
- **Autentizace** zajišťuje ověření identity všech uživatelů.
- **Autorizace** zajistí, že uživatelé mají přístup jen a pouze k těm zdrojům, které potřebují.
- **Audit** udržuje záznamy - buď předdefinované systémem nebo speciální události aplikace.
- **Ochrana integrity dat** zabraňuje útokům na data přenášená po síti.
- **Ochrana důvěrnosti dat**, aby např. žádný spyware nemohl získat užitečná data.

# Co budeme používat?

- Caché 5.1 FT1 (build 715) přednastavená na VMware Windows 2000 Server pod uživatelem “**cacheW2000S**” na portu **1973**



The screenshot shows a dialog box titled "Please enter user credentials" with the Caché logo on the left. It contains two radio buttons: "Run Caché under default SYSTEM account" (unselected) and "Run Caché under a defined Username account" (selected). Below the radio buttons are three text input fields: "Username:" containing "cacheW2000S", "Password:" containing "\*\*\*\*\*", and "Domain:" containing "KERB". At the bottom are three buttons: "< Back", "Next >", and "Cancel".



The screenshot shows a dialog box titled "Caché Users configuration" with the Caché logo on the left. The text reads: "Setup is now going to create the following Caché accounts for you. Please enter and confirm the password for each of the accounts." There are four password input fields: "Password for Caché user CacheAdmin:" (\*\*\*\*\*), "Confirm Password:" (\*\*\*\*\*), "Password for Caché user cacheW2000S:" (\*\*\*\*\*), and "Confirm Password:" (\*\*\*\*\*). At the bottom are three buttons: "< Back", "Next >", and "Cancel".

## Co budeme používat? II.



- Windows Server + Windows Active Directory
- Kerberos Realm (předkonfigurovaný a obsažený v Windows Active Directory Domain)
- Uživatel Windows „CacheAdmin” v doméně „KERB”
- Cache 5.1 FT1 instalované do domény „KERB”
- Administrátorské účty Caché – „CacheAdmin”

---

INTERSYSTEMS

SYMPOSIUM 2005

Autentizace



# Autentizace: Ověření totožnosti



- Vyspělá bezpečnost Caché nabízí několik mechanismů k ověření totožnosti:
  - **Kerberos**: Nejbezpečnější cesta autentizace. Dostupná na všech platformách.
  - **Operační systém**: Dostupný pro Windows, UNIX a OpenVMS, autentizace založená na OS používá identifikaci uživatele v operačním systému pro identifikaci uživatele v Caché.
  - **Caché Login**: Caché si udržuje tabulku kódovaných hodnot hesla pro každý uživatelský účet.
  - **Bez ověření**

# Kerberos

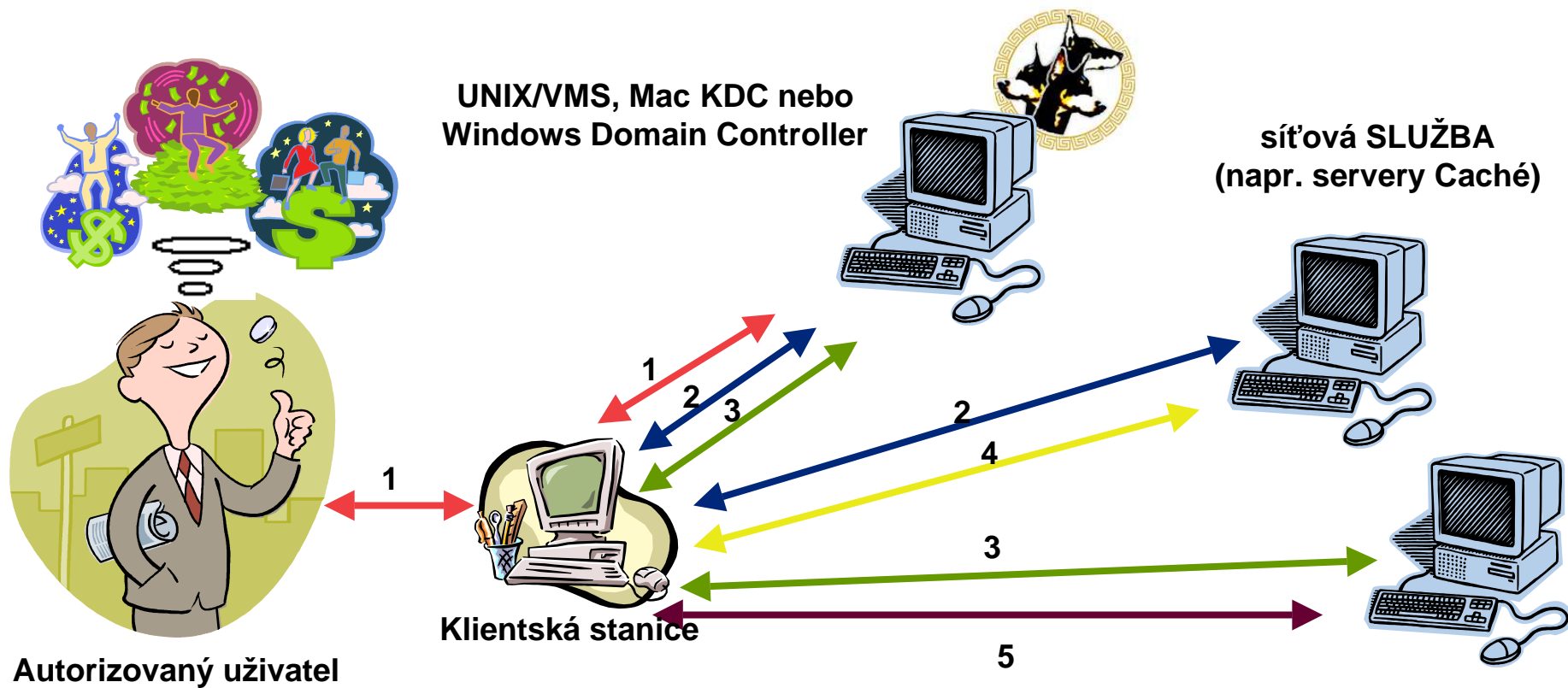


## Prvky:

- Silná autentizace
- Vyzkoušený, ověřený proces
- Dostupný pro všechny platformy
- Snadno použitelný s flexibilní konfigurací
- Rychlý a přizpůsobitelný
- Jediné přihlášení



# Kerberos - přehled...



1: Prihlášení k systému.

2, 3: Počáteční připojení k serveru (uživatel se na chvíli zasní).

4, 5: Následná připojení k serveru.

# Přihlášení



- Uživatel je **přihlášen** do Caché:
  - pro aplikace připojené pomocí ODBC, JDBC, Caché Direct, Caché Objects, Java nebo Call-In, když aplikace volá příslušnou funkci pro spojení.
  - pro uživatele připojení pomocí terminálu či konzoly PC, když Caché vyzve k zadání uživatelského jména a hesla.
  - Při použití autentizace pomocí operačního systému, když se identita uživatele na úrovni operačního systému shoduje s uživatelským jménem zadaným v Caché.
  - Pro nástroje Caché, když je vytvořeno připojení na server Caché.
- Po úspěšném přihlášení s využitím jakéhokoliv shora uvedeného způsobu :
  - systémová proměnná **\$USERNAME** obsahuje uživatelské jméno.
  - **\$ROLES** obsahuje seznam rolí držených uživatelem.

# Cvičení 1: Přihlášení

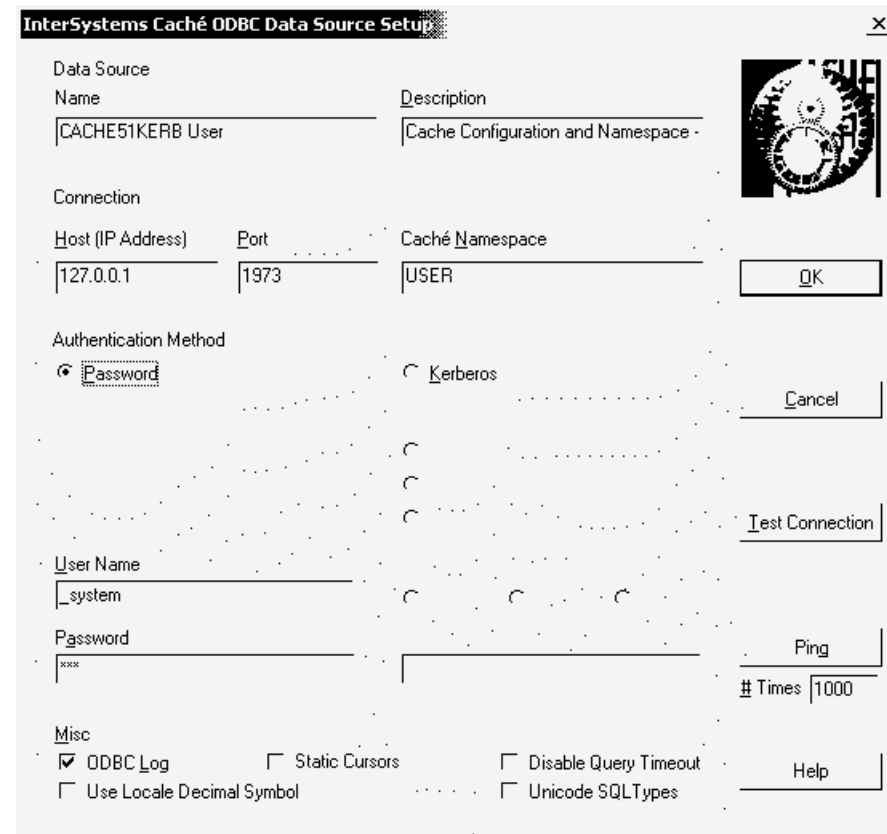


- Spustíte **Terminal** z kostky Caché.
- Zadejte následující příkaz:
- SECURITY> **write \$USERNAME**
- Měli bychom vidět: **CacheAdmin**
- Zadejte následující příkaz:
- SECURITY> **write \$ROLES**
- Měli bychom vidět: **%All**
- **Zavřete** terminál.

# Vyspělá bezpečnost pro ODBC



- Volba **Caché Advanced Security** přidána do ovladače ODBC.
- Autentizace je konfigurovatelná **jednotlivě** pro každé DSN.
- Umožňuje buď zvolit metodu **Caché Login** nebo **Kerberos**



# Úrovně bezpečnosti spojení



- Volba „Clear“ aktivuje protokol Kerberos a...
- Kerberos je použit jen ke kontrole, že **identita je platná**.
- Následné zprávy jsou posílány **bez** kontroly integrity a bez šifrování.

**InterSystems Caché ODBC Data Source Setup**

| Name             | Description                         |
|------------------|-------------------------------------|
| CACHE51KERB User | Cache Configuration and Namespace - |

Connection

| Host (IP Address) | Port | Caché Namespace |
|-------------------|------|-----------------|
| 127.0.0.1         | 1973 | USER            |

Authentication Method

Password  Kerberos

Connection Security Level

Kerberos  
 Kerberos with Package Integrity  
 Kerberos with Encryption

Server Type

Windows  Unix  VMS

Service Principal Name

cacheW2000S

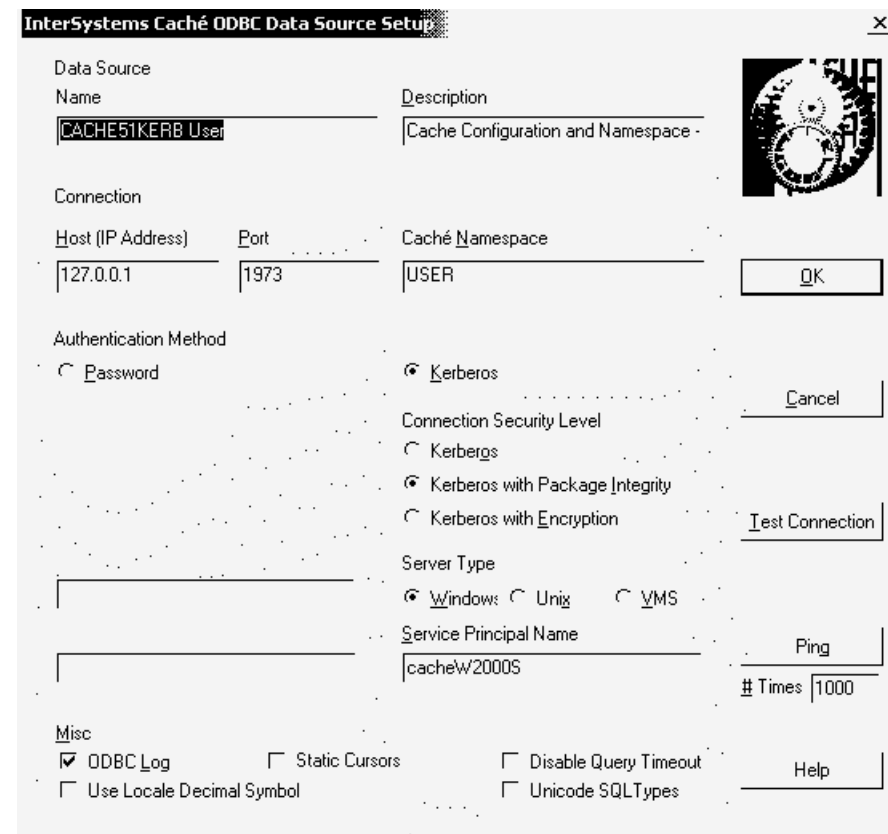
Misc

ODBC Log  Static Cursors  Disable Query Timeout  
 Use Locale Decimal Symbol  Unicode SQLTypes

Buttons: OK, Cancel, Test Connection, Ping, Help

# Úrovně bezpečnosti spojení

- Volba „**Package Integrity**“ aktivuje protokol Kerberos a...
- Zajišťuje **autentizaci**.
- Zajišťuje validaci „**obsahu**“ a „**zdroje**“.
- Data posílána **nešifrována**.



# Úrovně bezpečnosti spojení



- Volba „**Encryption**” aktivuje protokol Kerberos a...
- Zajišťuje počáteční **autentizaci**.
- Zajišťuje **integritu dat**.
- **Všechny** transakce jsou **šifrovány**.
- Zajišťuje ověření platnosti „**obsahu**” a „**zdroje**” a ochranu „**obsahu**”.

InterSystems Caché ODBC Data Source Setup

Data Source  
Name: CACHE51KERB User Description: Cache Configuration and Namespace

Connection  
Host (IP Address): 127.0.0.1 Port: 1973 Caché Namespace: USER

Authentication Method  
 Password  Kerberos  
 Kerberos with Package Integrity  Kerberos with Encryption

Connection Security Level  
 Kerberos  
 Kerberos with Package Integrity  
 Kerberos with Encryption

Server Type  
 Windows  Unix  VMS

Service Principal Name: cacheW2000S

Misc  
 ODBC Log  Static Cursors  Disable Query Timeout  
 Use Locale Decimal Symbol  Unicode SQL types

Buttons: OK, Cancel, Test Connection, Ping, Help

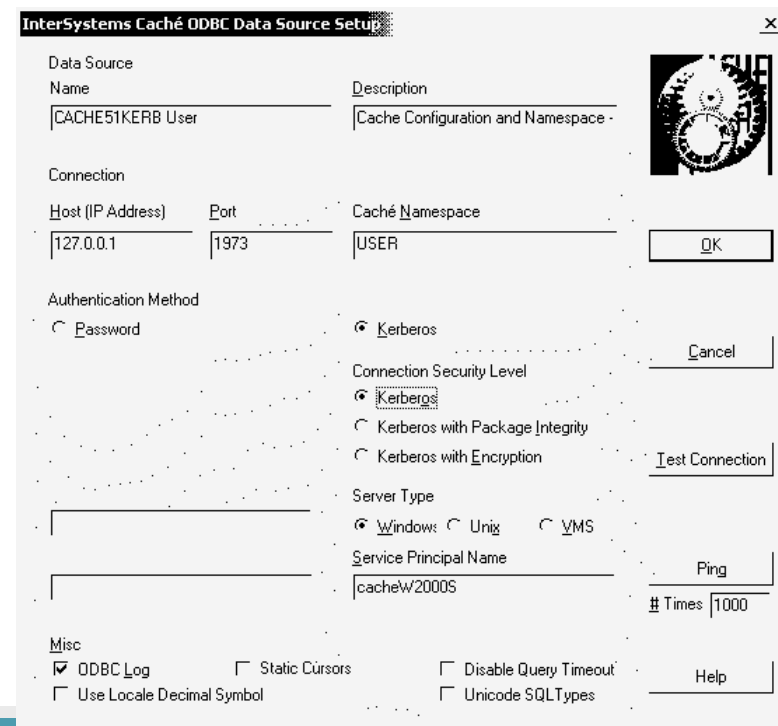
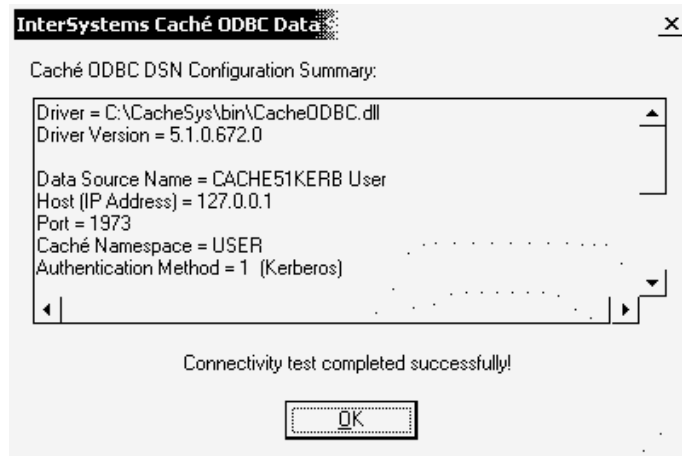
## Cvičení 2: Autentizace



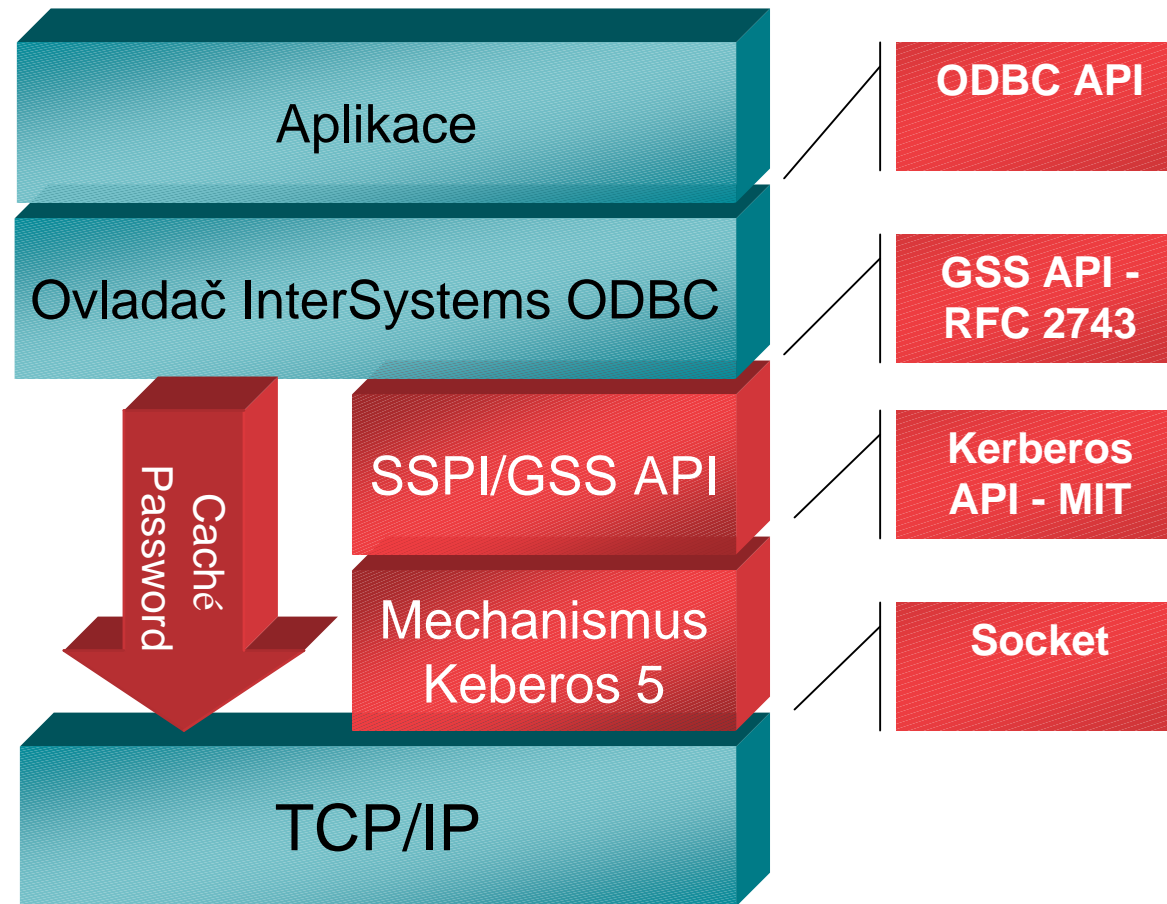
- Otevřete **ODBC Driver Manager**.
- Vyberte záložku **System DSN**, v ní DSN **CACHE Samples**.
- Nastavte **metodu autentizace** na **Password**
- Zadejte **User Name** jako **\_SYSTEM**.
- Zadejte **Password** jako **SYS**.
- Klikněte na tlačítko **Test Connection...** test by měl úspěšně proběhnout.
- Všimněte si zprávy **Authentication Method = 0 (Caché)**

# Cvičení 2: Autentizace - pokrač.

- Změňte **metodu autentizace** na **Kerberos**.
- Klikněte na tlačítko **Test Connection** ... test by měl úspěšně proběhnout.
- Všimněte si zprávy Authentication Method = 1 (Kerberos)
- Ovladač ODBC **si vyžádal** vaše **ověření Windows** pro **autentizaci Kerberos** za **Vás!**



# Nová architektura ovladače ODBC



---

# INTERSYSTEMS

# SYMPOSIUM 2005

System Management Portal



# System Management Portal



- Nové rozhraní **založené na webovém prohlížeči**.
- Umožňuje **vzdálenou správu** systémů přes internet **bez** nutnosti instalace klientské části.
- **Minimalizuje** problémy s kompatibilitou mezi verzemi/platformami.
- Toto nové rozhraní **konsoliduje** funkčnost obsluhovanou dříve pomocí nástrojů:
  - Explorer, SQL Manager, Configuration Manager a Control Panel.

## Cvičení 3: Používání portálu - Databáze



- Otevřete **Systems Management Portal** z kostky **Caché**.
- Všimněte si, že funkčnost je nyní rozdělena na části **System Administration**, **Data Management** a **Operations**.
- Zvolte volbu **System Configuration / Local Databases** z menu **System Administration**.
- Zvolte volbu **Properties** databáze **SECURITY** a zkontrolujte nastavení.

## Cvičení 3: Používání portálu - Uživatel



- Otevřete **Systems Management Portal** z kostky **Caché**.
- Všimněte si, že funkčnost je nyní rozdělena na části **System Administration**, **Data Management** a **Operations**.
- Zvolte volbu **Security Management** z menu **System Administration**.
- Zvolte volbu **Users** z menu **Security Definitions**.
- Zvolte volbu **Create New User**.

## Cvičení 3: Používání portálu - Uživatel



- Zadejte „Bob” jako jméno, „Test User Account” jako popis a „test” jako heslo („Bob“ je účet jen pro Caché).
- Změňte „Default Namespace“ na db SECURITY a klikněte na Save.
- Zvolte [Roles] a přidejte roli %DB\_SECURITY do seznamu Selected a klikněte na tlačítko Assign.
- Zvolte [Users] z horního menu a všimněte si, že nový účet byl přidán do seznamu.

---

# INTERSYSTEMS

# SYMPOSIUM 2005

**Autorizace**



# Autorizace: Aktiva a zdroje



## Autorizace určuje, **co** je uživateli **povoleno** dělat!

- **Aktivum (asset)** je cokoliv, co je chráněno:
  - databáze Caché je aktivum.
  - schopnost se připojit do Caché pomocí SQL je aktivum
  - způsobilost spustit backup je aktivum.
- **Aktiva** jsou zabezpečena pomocí **zdrojů**.
- Caché definuje sadu zdrojů k aktivům, která **chrání**.
  - např. the Samples Database is protected a resource called %DB\_SAMPLES.
- Vývojáři aplikací si mohou rovněž **definovat** své vlastní zdroje.

# Autorizace



- **Oprávnění (privilege) dává povolení (permission) něco dělat s jedním nebo více aktivy (assets) chráněnými pomocí zdroje (resource):**
  - např. být schopen **číst** databázi příkladů - SAMPLES.
- **Oprávnění je zapsáno jako zdroj následovaný povolením, které je odděleno dvojtečkou:**
  - %DB\_SAMPLES:Read
- **Caché definuje následující povolení:**
  - **Read (R)**: Vidět (ale nezměnit) obsah zdroje.
  - **Write (W)**: Vidět nebo změnit obsah zdroje.
  - **Use (U)**: Použít zdroj, např. aplikaci nebo službu

# Názvové prostory - Namespaces



- Uživatelé a aplikace **komunikují** s databázemi Caché přes **názvové prostory**.
- Přístup k nim je přidělen nebo zamítnut podle **povolení** přiřazenému k příslušné **základní databázi**.
- Tento požadavek je kontrolován, když:
  - Proces se pokusí přiřadit názvový prostor jako svůj vlastní (např. funkcí \$ZU(5), příkazem ZNSPACE nebo použitím programu %CD).
  - Při pokusu se připojit do Caché s použitím nějaké služby, která se napojuje do daného názvového prostoru (např. Caché Direct, spojení SQL nebo pomocí objektů).

# Zdroje - Služby



- Zdroje služeb a jejich oprávnění **řídí** schopnost se **připojit** do Caché s využitím rozličných technologií pro připojení.
- Podporované služby jsou:

## Oprávnění služeb

### Zdroj:

%Service\_CallIn  
%Service\_ComPort  
%Service\_Console  
%Service\_CSP  
%Service\_CacheDirect  
%Service\_LAT  
%Service\_Object  
%Service\_SQL  
%Service\_Telnet  
%Service\_Terminal

### Umožňuje:

Connection to Caché via call-in  
Connection to Caché via Windows COM ports  
Connection to Caché on Windows systems via CSESSION or CSS  
Connection to Caché via Caché Server Pages  
Connection to Caché via Caché Direct  
Connection to Caché via the Caché LAT service for Windows  
Connection to Caché via Caché object or SQL client and execute object requests  
Connection to Caché via Caché object or SQL client and execute SQL requests  
Connection to Caché via the Caché Telnet service for Windows  
Connection to Caché via terminal on non-Windows systems

# Správa služeb Caché



- Služby Caché jsou **hlavní** cestou, kterou se uživatelé a počítače **připojují** do Caché, proto jejich správa je **základní** součástí bezpečnostního nastavení.
- Služba může být konfigurována:
  - Zda je služba **aktivována**
  - Zda služba vyžaduje oprávnění **Use**.
  - Jaký typ **autentizace** je povolen / vyžadován.

# Client System Security and Client Application Security



- **Client System Security:** Řídí, které systémy se mohou připojit pomocí dané služby.
  - Není vhodné při velkém počtu klientů (což může být případ architektury „tenkého klienta“).
  - Velmi vhodné při vícevrstvé konfiguraci. Např. při použití služby CSP může být nastavena limitovaná sada webserverů, které se mohou napojit do Caché.
- **Client Application Security:** Řídí, zda přístup ke službě je limitován na vymezení seznam klientských aplikací.
  - Např. pro Caché Direct, použití může být omezeno na konkrétní aplikaci Windows, identifikovanou kritérii jako název, velikost a časovou značku kompilace.

# Aplikační zdroje



- V mnoha případech může být uživateli povoleno dělat různé věci – **používat aktiva chráněná zdroji** – pouze v rámci dané aplikace.
- Caché umožňuje:
  - Vytvořit definici aplikace a **přiřadit** jí roli, kde jsou stanovena všechna oprávnění požadovaná aplikací.
  - Přidělit uživateli **oprávnění** k používání dané aplikace.
- Tři typy aplikací:
  - CSP, privilegované rutiny, klientské aplikace.

# Role



- **Role** je také nazývána jako **soubor oprávnění**.
- Role jsou užitečné, protože **více uživatelů** *typicky* potřebuje **stejnou sadu oprávnění**.
- Taková sada oprávnění je **vytvořena najednou** (což značně usnadňuje pozdější modifikaci) a **sdílěna** odpovídajícími uživateli.
- **Uživatel** může mít **více než jednu roli**.
- Ve Vyspělé bezpečnosti Caché, oprávnění jsou přidělena **pouze rolím**, ne přímo jednotlivým uživatelům.
- Pokud potřebujete přidělit oprávnění jedinému uživateli, můžete vytvořit **roli** jen pro tento účel.
- Máme **předdefinované** a **uživatelsky definované** role.

# Předdefinované role



- Caché obsahuje množství předdefinovaných rolí.
- Tyto definice jsou nastaveny při nové instalaci Caché a nejsou modifikovány v průběhu přeinstalace (upgrade).
- Role **%Public** mají automaticky přiděleni všichni uživatelé.
- Tuto roli nelze smazat, ale její definice může být modifikována.
- S výjimkou role **%All**, používání předdefinovaných rolí je nepovinné.

## Role %All



- Speciální předdefinovaná role.
- Vždy obsahuje všechna oprávnění ke všem zdrojům systému.
- Tato role nemůže být smazána ani upravena a vždy musí existovat nejméně jeden uživatelský účet s rolí %All.
- Pokud je zde pouze jeden takový účet, nemůže být smazán nebo zablokován.
- Což (doufejme) pomůže ochránit správce systému Caché před „zamčení klíčů v autě“.

# Oprávnění a povolení



- **Oprávnění k administraci:** dovoluje uživateli vykonávat určené úlohy systémové administrace Caché.
- **Oprávnění k vývoji:** řídí přístup k vývojovým prostředkům Caché. Ve spojení s oprávněními k databázím řídí přístup vývojářů do Caché.
- **Oprávnění veřejné (Public):** každý zdroj může mít oprávnění Public. Je to ekvivalent, jako kdyby všichni uživatelé měli oprávnění k tomuto zdroji.
- Caché nabízí funkce ke kontrole oprávnění daného procesu:  
**`$SYSTEM.Security.Check(Resource,Privilege)`**

## Cvičení 4: Přidělení rolí



- Otevřete **Systems Management Portal** a vyberte položku **Security Management**, zde vyberte **Roles**.
- Zvolte **Edit** pro roli **Inventory** a vyberte záložku **Users**.
- Přidejte uživatele "**Bob**" do seznamu vybraných a klikněte na **Assign**.
- Bob bude přidán do seznamu uživatelů **vlastnících tuto roli**.

# Přidané role and přiřazené role



- Každý proces Caché má sadu rolí určujících aktuální **oprávnění** procesu.
- Tato sada rolí obsahuje jak **uživatelské role**, pocházející z definice uživatele, tak **přidané roles**, přidané z definice spuštěné aplikace.
- Pro každou definici aplikace existuje mapování **aktuálních rolí** k **rolím přiřazeným**.
- Po inicializaci aplikace proces pro každou drženou roli přidá příslušné přiřazené **role aplikace**, pokud jsou definovány.

## Cvičení 5: Přiřazené role



- Otevřete **Systems Management Portal** a vyberte položku **Security Management**, potom vyberte **Roles**.
- Zvolte **Edit** role **Supervisor** a vyberte záložku **Users**.
- Přidejte uživatele "**Bob**" do seznamu vybraných a klikněte na **Assign**.
- Zalogujte se do CSP aplikace jako "**Bob**" s heslem password "**test**".
- Bob má nyní autorizaci k použití všech položek, protože drží roli **Supervisor**.

---

# INTERSYSTEMS

# SYMPOSIUM 2005

**Auditování a  
Bezpečnostní poradce**



# Bezpečnostní poradce



- Navržen, aby pomohl systémovým správcům při zabezpečení systému Caché.
- Je to webová stránka portálu, znázorňující současné informace zaměřené na nastavení bezpečnosti systému.
- Doporučené změny nebo oblasti k prozkoumání.
- Odkazy na ostatní stránky k provedení doporučených změn.

# Cvičení 6: Použití Bezpečnostního poradce



- Otevřete **Systems Management Portal** a zvolte **Security management**, poté vyberte **Security Advisor** z menu bezpečnostních úloh
- Všimněte si **doporučení**, která pro vás Bezpečnostní poradce připravil made.
- Klikněte na odkaz **detaily** pro kategorii **Auditing** a to vás přenesse do menu potřebného ke změně nastavení.
- Zvolte **Enable Auditing** na stránce **System-wide Security Parameters** a klikněte na tlačítko **Save**.

# Auditování



- Záznam klíčových událostí do bezpečného auditovacího logu je třetím hlavním prvkem of Vyspělé bezpečnosti Caché.
- Caché má zabudovanou podporu auditování pro:
  - **události na úrovni systému** (*jako je start Caché a uživatelské přihlášení*).
  - **události na úrovni bezpečnosti** (*jako jsou změny v bezpečnosti nebo nastavení auditu*).
  - **uživatelsky definované události**.
- Aplikace může generovat své vlastní vstupy do auditovacího logu.

# Co Caché neaudituje



- Caché automaticky negeneruje záznamy pro:
  - normální aktivitu v databázi.
  - aplikace to může dělat snadno pomocí metod objektů nebo pomocí SQL (triggers).
- Databázová aktivita, jako jsou všechny přístupy, nové záznamy, změny nebo mazání dat by generovalo tak mnoho vstupů do auditu, že by bylo neúčelné až kontraproduktivní
- Mnohem účinnější je nechat aplikaci vytvořit jednotlivý záznam do auditu než generovat tisíce záznamů nastavením databáze!
- Více v přednášce „Vyspělá bezpečnost Caché“

# Přístup k datům auditu



- Auditovací log je uložen ve speciálně chráněné databázi Caché nazvané **CACHEAUDIT**.
- Přístup je řízen standardními bezpečnostními omezeními na úrovni databáze nebo názvového prostoru.
- Caché nabízí několik standardních **auditovacích výpisů**.
- Obsah Auditovacího logu je přístupný standardně pomocí **SQL**, také pomocí **Audit rozhraní (API)** (nástroji Caché a programově).

# Správa auditovacího logu



- Správa auditovací databáze je přístupná přes System Management Portal.
- Tato databáze je žurnálována a zálohována jako kterákoli jiná.
- Speciální nástroje jsou dostupné pro smazání všech záznamů nebo vybraných dní.
- Pro usnadnění kontroly bezpečnosti Caché uchovává čítač pro každý typ události a umožňuje přístup k těmto čítačům pomocí standardního monitorovacího rozhraní Caché.
- Např. správce může monitorovat čítač špatného přihlášení, aby mohl detekovat pokus o průnik do systému.

## Cvičení 7: Prohlížení auditu



- Otevřete **Systems Management Portal** a vyberte **Security Management**, zvolte **Auditing** z menu Security Tasks.
- Klikněte na tlačítko **Search**.
- Všimněte si události **AuditReport**.
- Vyberte **Search** z menu a klikněte znovu na tlačítko **Search**.
- Ověřte, že událost **AuditReport** byla přidána do logu.
- Událost **AuditReport** je do logu přidána při každém přístupu do databáze auditu!!!

# Záznamy do auditu z aplikace



- Aplikace může přidat vlastní záznamy do logu pomocí funkce Audit() :

`$SYSTEM.Security.Audit(EventSource, EventType, Event, EventData, Description)`

- Tím je umožněno vývojářům a aplikaci upravit vlastní události
- Žádné speciální oprávnění není potřeba k přidání záznamu do auditovacího logu.

---

INTERSYSTEMS

SYMPOSIUM 2005

Šifrování databází



# Ochrana dat v Caché 5.1



- Data lze nalézt a chránit ve třech základních stavech:
  - **Data používaná:** Caché používá autentizační mechanismus protokolu Kerberos k řízení přístupu k datům v paměti (*jako doplněk k ochraně používané operačním systémem*).
  - **Data v pohybu:** Caché používá Kerberos k zabezpečení integrity dat a utajení služeb při přenosu na síti.
  - **Data v klidu:** Caché umožňuje šifrování databáze na úrovni bloků k ochraně dat uložených na citlivých médiích jako jsou disky nebo pásky.

## Cíle návrhu – ochrana dat v klidu



- Dva rozhodující požadavky pro **efektivní** a **užitečné** řešení šifrování dat:
  - Zabezpečit **silnou** bezpečnost podle **standardů** moderní kryptografie
  - Řešení **nesmí** mít podstatný **vliv** na **výkon databáze** (propustnost dat a zpoždění při čtení a zápisu).
  - Dostupné pro všechny platformy Caché.
- **Výsledkem** je pružné, na platformě nezávislé šifrování databází, které je **transparentní** pro kód aplikace!

# Šifrování databází Caché: ochrana dat v klidu



- **Navrženo** k zamezení neautorizovaným uživatelům, aby viděli nebo používali data z databáze Caché.
- **Šifrování** je nastaveno na úrovni jednotlivé databáze v okamžiku jejího vytvoření
- Caché zavádí šifrování a dešifrování s využitím algoritmu **AES (Advanced Encryption Standard)**.
- **Šifrování** a **dešifrování** probíhá v okamžiku čtení či zápisu do databáze... „**za pochodu**”.
- Soubor **WIJ** je rovněž **šifrován**.
- **Minimální** vliv na výkonnost!

# Šifrovací klíče



- Každá instance Caché může vytvořit **unikátní** klíč k šifrování databáze.
- Je to **trvalý** klíč, takže jej nemusíte měnit po jeho vytvoření a aktivaci
- Caché umožňuje použití **128, 192, or 256-bitových** klíčů.
- Klíč je spolu s účtem administrátora klíče uložen v **souboru šifrovacího klíče**.

# Soubor šifrovacího klíče



- Obsahuje několik **šifrovaných** kopií šifrovacího klíče.
- Každá kopie je k přiřazena jednomu **účtu správce klíče** (uživatelské jméno a heslo).
- Tento účet je **vyžadován k aktivaci** šifrovacího klíče a ke správě šifrované databáze.
- Jakmile si klíč uložíte, můžete jej **přesunou** na libovolné místo dle výběru.
- Ztráta nebo zničení klíče může učinit všechny šifrované databáze trvale nečitelné .
- Je nezbytné, abyste si **kopii** souboru s klíčem uložili na bezpečné místo, které nemůže být zničeno... doporučen je vyjímatelný USB Flash disk.

## Cvičení 8: Vytvoření šifrovacího klíče



- Otevřete **Systems Management Portal** a vyberte položku **Database Encryption**, potom zvolte **Create Encryption Key File** z menu.
- Zadejte “**c:\symposium.key**” jako název souboru šifrovacího klíče.
- Zadejte “**Bob**” jako jméno správce a “**test**” jako **heslo**.
- Klikněte na tlačítko **Save** pro uložení klíče na disk.
- Takto se vytvoří soubor, kde každá kopie šifrovacího klíče databáze je dále šifrována pomocí správce „klíče šifrovacího klíče (Key Encryption Key - KEK).
- Poznámka: Uložení klíče jej současně aktivujete.

# Správa účtů administrátorů klíčů



- Správci souboru šifrovacího klíče mohou být přidávání či vyjímání z menu **System Management Portal – Database Encryption**.
- Informace o každém novém správci je **přidána** do souboru klíče.
- Každý správce může dostat **kopii** klíče.
- Záloha aktuálního klíče uchovávána na **bezpečném** místě.

## Cvičení 9: Správa účtů administrátorů klíčů



- Otevřete **Systems Management Portal** a zvolte **Database Encryption**, pak vyberte **Add or Remove Users from Encryption Key File** z menu.
- Zadejte "**c:\symposium.key**" jako název klíče nebo použijte tlačítko **Browse**.
- Klikněte na položku **Delete** za jménem správce "**Bob**" (*všimněte si, že nemůžete smazat posledního správce klíče*).
- Klikněte na tlačítko **Add** a přidejte dalšího správce klíče
- **Uložte** a potom **smažte** tohoto **nového** správce klíče (*žádný problém, pokud alespoň jeden zůstává*).

# Vytvoření šifrované databáze



- Databáze je šifrována v okamžiku jejího vytvoření (pokud je zvoleno).
- *Poznámka: nelze šifrovat již existující databázi! Řešením je import dat a rutin do nové, šifrované databáze.*
- Caché musí obsahovat **aktivovaný** šifrovací klíč před tím než **vytvoříte** nebo **namontujete** šifrovanou databázi.
- Jakmile je databáze šifrována (s aktuálně “aktivovaným” šifrovacím klíčem), nemůže být navrácena do nešifrované podoby a je trvale spojena s daným šifrovacím klíčem.
- K trvalému “odšifrování” dat je nutné vytvořit nešifrovanou databázi a data do ní zkopírovat.

# Cvičení 10: Vytvoření šifrované databáze



- Otevřete **System Management Portal** a zvolte **System Configuration**, poté **Namespaces** a konečně **Create New Namespace** z menu.
- Zadejte **“ENCRYPTED”** jako název nového názvového prostoru a zvolte **Define a new Database for this Namespace** – definici nové databáze.
- Zadejte **“ENCRYPTED”** jako název nové databáze, zaškrtněte políčko **Encrypt Database?** a zvolte **Next**.
- Zadejte místo uložení nově vytvořené databáze - **“c:\cachesys\mgr\ENCRYPTED”** a zvolte **Next**.
- Zadejte **Next** pro defaultní hodnoty nastavení.
- Zadejte **Finish** a **Save** k dokončení procesu.

# Cvičení 11: Používání šifrované databáze



- Spustíte **Terminál** a přepnete se do názvového prostoru **“ENCRYPTED”** (USER>zn “ENCRYPTED”).
- Vytvořte nový datový globál (set ^SYMP=“Moje šifrovaná data.”  
Zavřete **Terminál**.
- Otevřete **System Management Portal**, zvolte si **System Configuration**, poté **Databases**, a dále volbu **Dismount** na řádku databáze ENCRYPTED.
- Klikněte na tlačítko **Perform Action Now** a databáze bude odmontována.
- Otevřete soubor databáze **ENCRYPTED** - CACHE.DAT umístěný v adresáři **“c:\cachesys\mgr\ENCRYPTED”** - použijte např. Windows **Notepad**.

# Cvičení 11: Používání šifrované databáze



- Všimněte si, že data jsou kompletně **šifrována**.
- Zavřete **editor**.
- Otevřte **System Management Portal**, zvolte **Database Encryption**, poté **Deactivate Encryption Key**, a dále klikněte na tlačítko **Perform Action Now**.
- Vyberte si z hlavního menu **System Management** a **Databases**.
- Zkuste **namontovat** databázi „**ENCRYPTED**“.

## Cvičení 11: Používání šifrované databáze



- Databázi není možno přimontovat („**Not Mountable**”) protože šifrovací klíč není aktivní.
- Aktivací **šifrovacího klíče** s použitím souboru šifrovacího klíče vytvořeného dříve lze databázi opět **namontovat**.

# Přesun šifrovaných databází mezi instalacemi.



- Pokud vaše organizace udržuje více instalací/lokalit Caché, můžete potřebovat použít šifrovanou databázi, která byla vytvořena v jiné instalaci, s jiným šifrovacím klíčem.
- Postup při přesunu databáze mezi instalacemi:
  - Na zdrojové instalaci namontujte šifrovanou databázi.
  - Vytvořte novou, nešifrovanou databázi.
  - Zkopírujte data do nešifrované databáze.
  - Přesuňte nešifrovanou databázi do cílového místa/instalace.
  - Na cílové instalaci vytvořte novou, šifrovanou databázi.
  - Zkopírujte data do této šifrované databáze.

---

# INTERSYSTEMS

# SYMPOSIUM 2005

Závěrem...





## Vyspělá bezpečnost Caché:

- Autentizace
- Autorizace, zdroje, role, oprávnění
- System Management Portal
- Audit a Bezpečnostní poradce
- Šifrování databází

---

# INTERSYSTEMS

# SYMPOSIUM 2005

Děkuji za pozornost!

