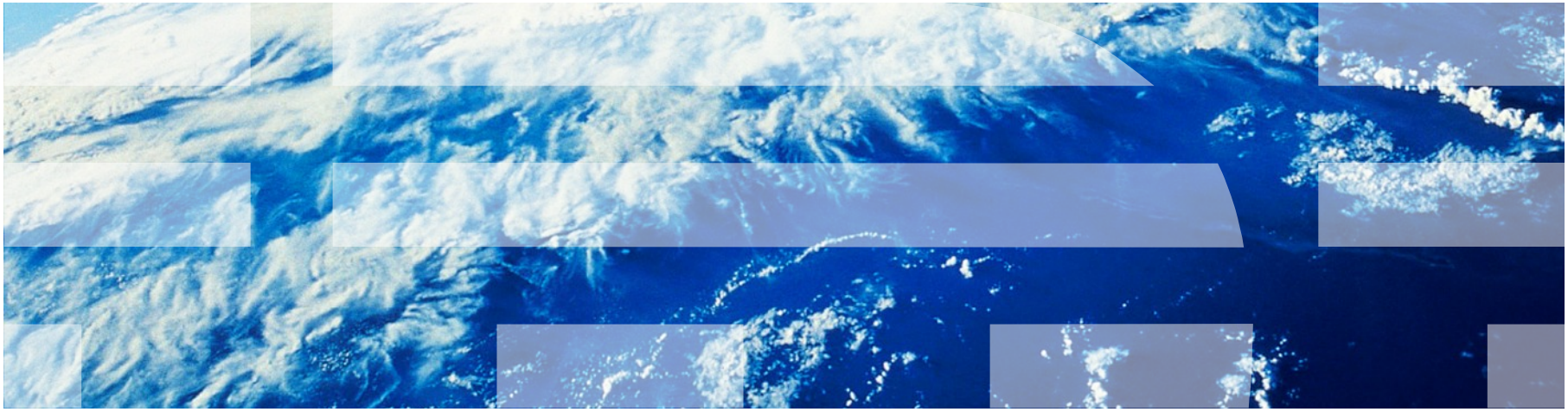
Tomáš Zahradník – IBM Informix Advanced Support

21.9.2011

Použití Single Sign On (SSO) v IBM Informix Serveru



Agenda

- Single Sign-On – novinka v IBM Informix Server 11.50
- Kerberos – trocha teorie
- Jak 'to' nastavit – ještě víc teorie
- Jak 'to' nastavit – ukázka na závěr (IDS na Linuxu versus Windows Active Directory)

Autentikace uživatelů – tradiční metody

- Použití mechanismů OS
  - userid/heslo uživatele je předáno OS
- PAM/LDAP
  - userid/heslo uživatele je předáno konfigurovaným PAM modulům
- Nutnost zadávání userid/hesla při každém připojení k databázové instanci

Autentikace uživatelů – nová alternativa

- Single Sign On (SSO)
  - od verze IBM Informix Server 11.50
  - umožňuje uživatelům vložit userid/heslo pouze jednou, při přihlášení k pracovní stanici
  - umožňuje využívat služby/aplikace poskytované různými servery v síti bez nutnosti re-autentikace
  - zjednodušuje aplikace, protože uživatel nemusí opakovaně vkládat přihlašovací udaje
- Zavedení podpory SSO umožňuje integraci Informix řešení do stávající SSO infrastruktury

SSO - Kerberos

- Informix využívá protokol Kerberos v. 5
  - bezpečný protokol pro autentizaci po síti
  - hesla nejsou nikdy posílána přes síť
  - využívají se tzv. 'shared secret' kryptovací klíče
  - správu/distribuci klíčů zajištuje Key Distribution Centre (KDC)
  - umožnuje 'vzájemnou authentikaci' (Informix zatím nepodporuje)

Kerberos – Jak to funguje (AS Exchange)

- KDC poskytuje 2 služby
  - Authentication Service (AS)
  - Ticket Granting Service (TGS)

- KRB_AS_REQ: uživatel se přihlásí na klientské stanici s použitím userid/hesla a autentikuje se vůči AS; součástí přihlášení je časové razítko a žádost o vystavení tzv. ticket-granting ticketu (TGT); autentikační žádost je kryptována a jako klíč je použita hash hodnota odvozená z hesla

- KRB_AS_REP: AS po přijetí žádosti načte uživatelovo heslo (z databaze účtů), vygeneruje z něj hash hodnotu a použije ji jako klíč pro dekryptování žádosti uživatele; pokud se to podaří, extrahuje se z žádosti časové razítko a ověří se aktuálnost žádosti; pokud je žádost aktuální, AS vystaví pro klienta TGT a odešle tzv. AS-reply
- AS-reply obsahuje 2 části
  - TGT kryptovaný klíčem, který je znám pouze TGS
  - logon session key kryptovaný hash hodnotou hesla

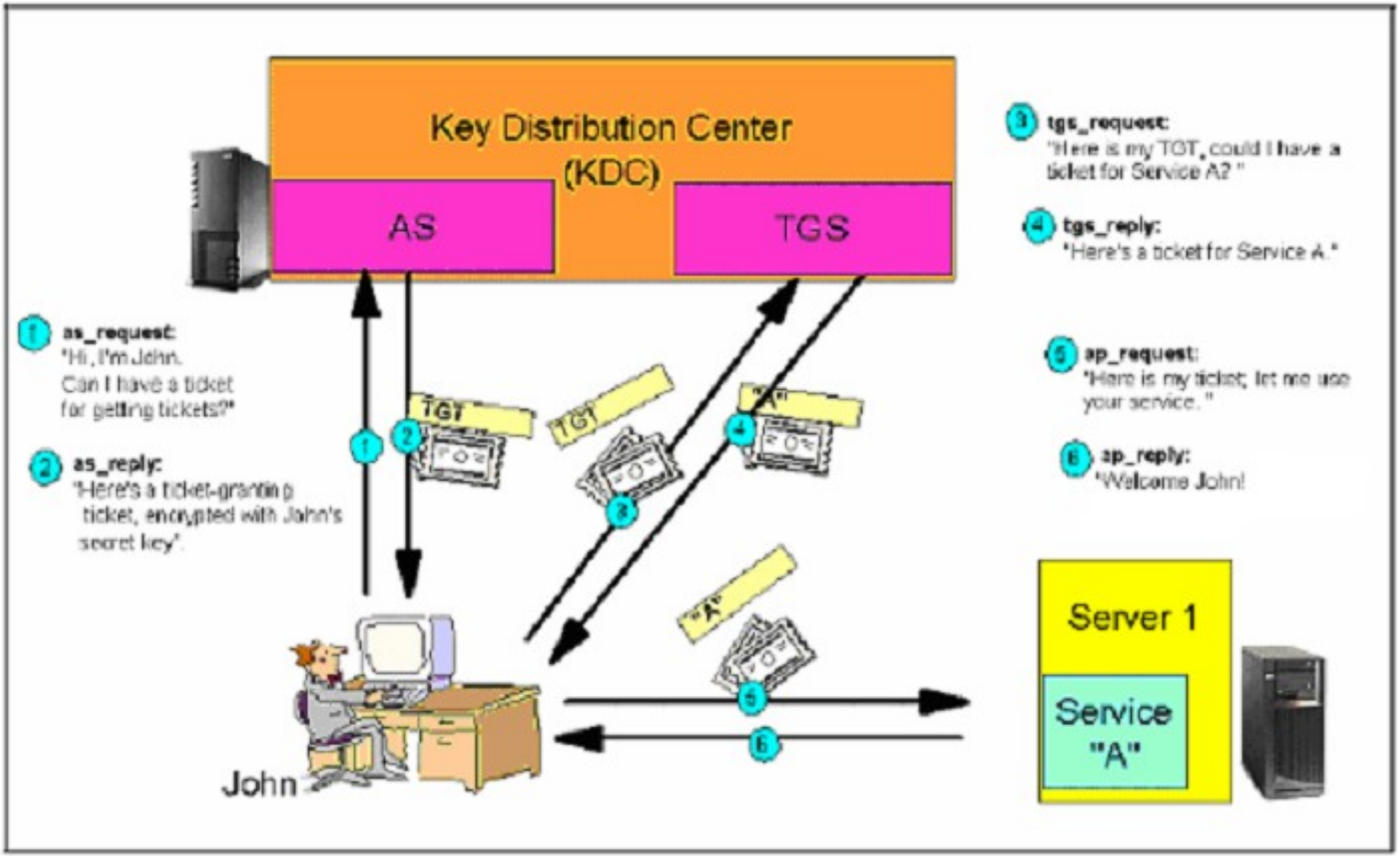
Kerberos – Jak to funguje (TGS Exchange)

- KRB_TGS_REQ: klient odešle svůj TGT společně se jménem služby kterou chce využít (service principal name – SPN) a tzv. autentikátorem (kryptovaným pomocí logon session key) do TGS a požádá o vystavení 'service ticketu' pro danou službu
- KRB_TGS_REP: TGS ověří klientův TGT a autentikátor; pokud je vše v pořádku, vystaví se service ticket pro danou službu, zakryptuje se pomocí klíče sdíleného mezi KDC a službou a odešle se klientovi v rámci TGS_reply
- TGS_reply obsahuje :
  - session key pro komunikaci mezi klientem a službou kryptovaný pomocí logon session key
  - service ticket, jehož součástí je znovu session key pro 'klient-služba' komunikaci
- Service ticket i session key jsou uloženy ve vyrovnávací paměti klienta

Kerberos – Jak to funguje (Client/Server Exchange)

- KRB_AP_REQ: klient odešle service ticket a autentikátor (kryptovaný pomocí session key) službě
- Služba dekryptuje ticket pomocí klíče sdíleného s KDC, extrahuje z něj informace o uživateli a session key pro vzájemnou komunikaci; ten se pak použije k dekryptování autentikátoru a pokud je tento v pořádku (a klientem není vyžadována vzájemná autentizace), je autentizační proces úspěšně ukončen
- KRB_AP_REP (volitelně): v případě požadavku na vzájemnou autorizaci služba znovu zakryptuje časové razítko z klientova autentikatoru (pomocí session key) a odešle ho klientovi; ten jej dekryptuje a porovná s původně odeslanou hodnotou. Pokud souhlasí, klient ví, že komunikuje se správnou službou

SSO – Kerberos v obraze



SSO - Konfigurace Kerberos

- Požadavky
  - KDC, IBM Informix Server i klienti musí patřit do stejného KRB realmu (nebo do 'trusted')
  - na IBM Informix Serveru musí existovat keytab soubor (s náležitými příst. právy)
  - čas na všech stanicích musí být synchronizován (max. 5 minut rozdíl)

- Detaily viz Kerberos dokumentace

SSO – Konfigurace IBM Informix Serveru

- Přidat alias do $INFORMIXDIR/etc/$ONCONFIG
  - DBSERVERNAME on_tcp
  - DBSERVERALIAS on_sso

- $INFORMIXDIR/etc/sqlhosts (resp. $INFORMIXSQLHOSTS)
  - v poli option (sloupec 5) nastavit “s=7” společně s GSSCSM jako CSM modulem

```
on_tcp  onsoctcp   aixmachine   tcp_serv
on_sso  onsoctcp   aixmachine   sso_serv   s=7,csm=(GSSCSM)
```

- $INFORMIXDIR/etc/concsm.cfg
  - GSSCSM(“/usr/informix/lib/csm/igss11a.so”,””,””)

SSO – Konfigurace IBM Informix Serveru

- Knihovny – Unix
  - server
    - `$INFORMIXDIR/lib/csm/igsss11a.so`
    - `$INFORMIXDIR/lib/csm/libixgss.so`
  - klient
    - `$INFORMIXDIR/lib/csm/client/igsss11a.so`
    - `$INFORMIXDIR/lib/csm/libixgss.so`

- Knihovny – Windows
  - server
    - `%INFORMIXDIR%\bin\igsss11a.dll`
    - `%INFORMIXDIR%\bin\libixgss.dll`
  - klient
    - `%INFORMIXDIR%\lib\client\csm\igsss11a.dll`
    - `%INFORMIXDIR%\lib\client\csm\libixgss.dll`

SSO – Konfigurace klientů (ESQL/C, ODBC, JDBC)

SQLHOSTS entry

- `on_sso  onsoctcp  aixmachine  sso_serv  s=7,csm=(GSSCSM)`

- ESQL/C
  - Nastavit SQLHOSTS aby obsahoval novou SSO option “s=7” a definici CSM modulu
  - Na Windows pomocí setnet32 upravit pole 'option' v definici Ifmx serveru

- ODBC
  - Upravit odbc.ini aby obsahoval option “s=7” a definici CSM

```
Driver=/usr/informix/lib/cli/iclit01b.so
Description=IBM INFORMIX ODBC DRIVER LogonID=informix
Database=stores ServerName=on_sso
Options=s=7,csm=(GSSCSM)
```

- Úprava $INFORMIXDIR/etc/concsm.cfg

SSO – Konfigurace klientů (JDBC)

- JDBC používá JAAS (login moduly) pro 'netradiční' metody autentikace
- specifikují se v konfiguračním souboru použitém při startu aplikace

```
$ cat /path/to/myapplogin.conf
com.sun.security.jgss.initiate {
    com.sun.security.auth.module.Krb5LoginModule required
    useTicketCache=true
    doNotPrompt=true;
}
```

- SSO v Ifmx vyžaduje 'useTicketCache' a 'doNotPrompt' nastaveno na 'true'

SSO – Konfigurace klientů (JDBC) pokr.

- Dále je potřeba upravit connection URL – volby 'user' a 'password' nahradí volba 'CSM'

```
String connect =
"jdbc:informix-sqli://aixmachine:11701/stores7:"
+ "informixserver=on_tcp;user=krbtest;password=abcdef";

String connectSSO =
"jdbc:informix-sqli://aixmachine:11702/stores7:"
+ "informixserver=on_sso;“
+ "CSM=(SSO=on_sso/aixmachine.ibm.com@LOCAL.TC,ENC=true)";
```

- Nastavení 'ENC=true' zapíná kryptování a kontrolu integrity

- Spuštění Java aplikace

```
java -Djava.security.auth.login.config=/path/to/myapplogin.conf MyJavaApp
```

SSO – Konfigurace klientů (JDBC na Windows)

- Pokud se po spuštení aplikace objeví chyba GSSException 14:

```
c:\tmp\java>java.exe -cp
".;c:\ProgramFiles\ibm\Informix_JDBC_Driver\lib\ifxjdbc.jar"
-Djava.security.auth.login.config=IfxLogin.cfg Stmt

ERROR: failed to connect!
java.sql.SQLException: com.informix.csm.IfxCsmException: Unknown error
GSSException: No valid credentials provided (Mechanism level: KDC has no
support for encryption type (14))
Exception in thread "main" java.lang.NullPointerException
        at Stmt.main(Stmt.java:31)
```

- Zkontrolovat registry klíč:

```
My Computer\HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\
Kerberos\Parameters\allowtgtsessionkey=1
```

- Více viz MS článek:
  - Registry Key to Allow Session Keys to Be Sent in Kerberos Ticket-Granting-Ticket (http://support.microsoft.com/kb/308339)

SSO – Příklad konfigurace SSO autentikace proti Windows AD

- Windows 2003 Server (SP2)
  - doménové jméno: icc.local.tc
  - Kerberos realm & doména: LOCAL.TC (local.tc)
  - funkce: Active directory domain controler, DNS Server, DHCP Server
  - SW: Informix CSDK 3.70.TC1,
    JRE/JDK 1.6.0_24

- RHEL 5.3
  - doménové jméno: rhel5b.local.tc
  - funkce: IBM Informix Server (aliasy tcp_1170uc1 & tcpsso_1170uc1), Kerberos client
  - SW: IBM Informix Server 11.70.UC1
    krb5-auth-dialog-0.7-1
    pam_krb5-2.2.14-15
    krb5-libs-1.6.1-36.el5_5.6
    krb5-workstation-1.6.1-36.el5_5.6

SSO – Příklad konfigurace SSO autentikace proti Windows AD

- Příprava na straně Windows AD:
  - vytvořit počítač (computer) pro stroj, kde běží IBM Informix Server
  - vytvořit uživatele informix (a další, kteří budou využívat SSO)
  - vytvořit uživatele tcpsso_1170uc1 (nesmí mít nastaveno “change password at next logon”)
  - zaregistrovat tzv. 'Service Principal Name' (SPN)
    - unikátní identifikátor pro službu využívající Kerberos autentikaci
    - setspn -A ServiceClass/Host[:Port] hostname
    - Tedy: `setspn -A tcpsso_1170uc1/rhel5b.local.tc@LOCAL.TC rhel5b.local.tc`
  - pomocí 'ktpass' namapovat SPN na uživatele, nastavit heslo, exportovat klíč a přenést ho na Ifmx stroj

```
ktpass /out c:\temp\tcpsso_1170uc1.keytab
/princ tcpsso_1170uc1/rhel5b.local.tc@LOCAL.TC
/mapUser tcpsso_1170uc1
/mapOp set
/pass <enter password here or '*' for interactive prompt>
/crypto DES-CBC-CRC
/pType KRB5_NT_PRINCIPAL
```

SSO – Příklad konfigurace SSO autentikace proti Windows AD

- Konfigurace na straně Informix Serveru
  - vytvořit příslušné uživatele
  - pomocí ktutil importovat klíč SPN do Kerberos keytab souboru:

```
# /usr/kerberos/sbin/ktutil
ktutil: rkt /tmp/ol_ids_1150_1.keytab
ktutil: wkt /etc/krb5.keytab
ktutil: quit
```

  - do $INFORMIXSQLHOSTS doplnit dbserveralias pro SSO authentikaci
    - `tcp_1170uc1    onsoctcp        rhel5b          11701`
    - `tcpsso_1170uc1 onsoctcp        rhel5b          11702 s=7,csm=(GSSCSM)`
  - upravit $INFORMIXDIR/etc/concsm.cfg
    - `GSSCSM("/home/informix/1170uc1/lib/csm/igsss11a.so","","c=1,i=1");`
  - jako 'informix' spustit server (pokud 'informix' nedostal TGT při logonu, je nutno spustit nejdříve 'kinit' a autentikovat se vůči Windows AD)

SSO – Příklad konfigurace SSO autentikace proti Windows AD

- Konfigurace klientů
- Ověření funkčnosti
  - na Informix stroji se přihlásit jako libovolný uživatel (který má účet i ve Win AD)
  - nastavit $INFORMIXSERVER na SSO alias a spustit dbaccess <dbname>
  - pokud je součastí login processu i autentikace vůči Win AD, uživatel již má TGT a přístup bude úspešný
  - pokud ne, je vrácena chyba 5000 (CSM error)
  - v tom případě provést autentikaci pomoci 'kinit' a opakovat dbaccess

Reference

- [1] Sun Microsystems Documentation on GSSAPI: http://docs.sun.com/app/docs/doc/816-1331
- [2] RFC proposal for GSSAPI: http://www.faqs.org/faqs/kerberos-faq/general/section-84.html
- [3] SSO using Kerberos V: http://www.tkk.fi/cc/docs/kerberos/sso.html
- [4] Using Kerberos V on Linux: http://www.linuxjournal.com/article/7336
- [5] DCE Reference: http://www.opengroup.org/dce/info/papers/tog-dce-ds-1296.htm#Heading21
- [6] DCE Reference: http://www.opengroup.org/onlinepubs/9668899/toc.htm
- [7] Heimdal Reference: http://www.pdc.kth.se/heimdal/
- [8] MIT Standard for Kerberos V: http://web.mit.edu/Kerberos/
- [9] GSSAPI RFC: http://www.ietf.org/rfc/rfc2743.txt
- [10] Kerberos Definitions: http://www.zeroshell.net/eng/kerberos/Kerberos-definitions/
- [11] How the Kerberos Version 5 Authentication Protocol Works:
  - http://technet.microsoft.com/en-us/library/cc772815(WS.10).aspx
- [12] KRB5LoginModule reference:
  - http://java.sun.com/j2se/1.4.2/docs/guide/security/jaas/spec/com/sun/security/auth/module/Krb5LoginModule.html

SSO - Otázky