



Implementace Label Based Access Control v Informix Dynamic Server 11.10

Jan Musil
IT Specialist SWG IBM



Přehled prezentace

- Popis základního konceptu LBAC
- Popis všech LBAC komponent
- Konfigurace zabezpečení dat pomocí LBAC
- Praktická ukázka
- Otázky a odpovědi

Label-Based Access Control (LBAC)

- Implementace Mandatory Access Control
- Visačky (labels) se používají na ochranu dat
 - ▶ Jednotlivé záznamy v tabulce
 - ▶ Tabulkové položky
- Visačkami se přidělují přístupová práva uživatelům
- LBAC nelze použít pro
 - ▶ Virtual-Table Interface (VTI) tabulky
 - ▶ Virtual-Index Interface (VII)
 - ▶ Dočasné tabulky
 - ▶ Typované tabulky
 - ▶ Hierarchické tabulky

LBAC objekty

- Komponenta - Security Label Component
 - ▶ Array (pole - uspořádaná množina elementů)
 - ▶ Set (neuspořádaná množina elementů)
 - ▶ Tree (stromová hierarchie elementů)
- Bezpečnostní politika - Security Policy
 - ▶ Databázový objekt, který definuje ochrannou tabulku
 - ▶ Skládá se z komponent
- Visačka - Security Label
 - ▶ Vždy vztažena k politice
 - ▶ Je definovaná pomocí jedné nebo více komponent příslušné politiky
 - ▶ Každá komponenta pak obsahuje výběr požadovaných elementů

Komponenta Array

- Uspořádaný seznam elementů
 - ▶ Max. 64 elementů
- První element má nejvyšší prioritu
- Komponenta ve visačce dovoluje použít pouze jeden Array element
- Uživatel může přečíst všechna data, jejichž visačka obsahuje elementy stejné nebo nižší úrovně jako visačka uživatele
- Uživatel může zapsat pouze data, jejichž visačka obsahuje element stejné úrovně jako visačka uživatele

```
CREATE SECURITY LABEL COMPONENT level ARRAY ['Secret',  
      'Confidential', 'Public'];
```

Komponenta Set

- Neuspořádaná množina elementů
 - ▶ Max. 64 elementů
- Komponenta ve visačce dovoluje použít jeden a více Set elementů
- Uživatel může přecíst nebo zapsat pouze taková data, jejichž visačka obsahuje všechny elementy, která má visačka uživatele

```
CREATE SECURITY LABEL COMPONENT department SET{'Marketing',  
        'Product Development', 'Quality Assurance'};
```

Komponenta Tree

- Hierarchická množina elementů
 - ▶ Max. 64 elementů
- Komponenta ve visačce dovoluje použít jeden a více Tree elementů
- Pokud visačka uživatele obsahuje některý element datové visačky nebo obsahuje předka takového elementu, pak může uživatel přečíst nebo zapsat data

```
CREATE SECURITY LABEL COMPONENT region TREE ('Entire Region'  
  ROOT, 'East' UNDER 'Entire Region', 'West' UNDER 'Entire  
  Region');
```

Vytváření politiky

- Politika (security policy) je vytvořena z komponent (security components)
 - ▶ Maximálně lze použít 16 komponent

```
CREATE SECURITY POLICY company COMPONENTS level, department,  
region;
```

- Tato politika obsahuje tři komponenty
- Visačky pro tuto politiku mohou mít buď žádný nebo více elementů z každé komponenty definované v této politice

Vytváření visaček

- Visačka (security label) se definuje hodnotami (elementy) komponent z politiky

```
CREATE SECURITY LABEL company.director  
  COMPONENT level 'Secret',  
  COMPONENT department 'Product Development', 'Quality Assurance',  
  COMPONENT region 'Entire Region';
```

- ▶ Komponenty *level* a *region* obsahují jeden element
- ▶ Komponenta *department* obsahuje více elementů

Přidělování visaček

- Uživatelům se visačky přidělují prostřednictvím SQL příkazu GRANT

```
GRANT SECURITY LABEL company.director  
TO mr_ceo  
FOR ALL ACCESS;
```

- Tabulkám je třeba přiřadit politiku...
- ... a visačkami se opatří položka(y) tabulky nebo/a celý záznam

Zabezpečení tabulek

- Zabezpečení jednotlivých záznamů
 - ▶ Je třeba přiřadit politiku tabulce ...
 - ▶ ... a visačku každému záznamu
 - Visačky se přidělují záznamům prostřednictvím položky typu IDSSECURITYLABEL
- Zabezpečení položek
 - ▶ Je třeba přiřadit politiku tabulce ...
 - ▶ ... a visačku jedné nebo více položkám
- Příklady SQL příkazů pro zabezpečení záznamů a položek

```
CREATE TABLE T1 (C1 IDSSECURITYLABEL, C2 INT,  
                 C3 CHAR(10) COLUMN SECURED WITH manager)  
                 SECURITY POLICY company;  
  
ALTER TABLE T1 ADD (C1 IDSSECURITYLABEL DEFAULT 'director'),  
                   MODIFY (C3 CHAR(10) COLUMN SECURED WITH manager),  
                   ADD SECURITY POLICY company;
```

Přehled přístupových pravidel pro čtení a zápis

- Pokud se data čtou, aplikují se následující přístupová pravidla
 - ▶ IDSLBACREADARRAY
 - ▶ IDSLBACREADSET
 - ▶ IDSLBACREADTREE
- Pokud se data zapisují, aplikují se následující přístupová pravidla
 - ▶ IDSLBACWRITEARRAY
 - ▶ IDSLBACWRITESET
 - ▶ IDSLBACWRITETREE

Výjimky

- Pravidla pro zápis a čtení jsou poměrně přísná
 - ▶ V komponentách Array a Tree není povoleno čtení „směrem vzhůru“ a zápis „směrem dolu“
- Výjimky (exemptions) dovolují obejít pravidla pro čtení a zápis
 - ▶ Tyto výjimky je možné přidělit uživateli, aby mohl obejít jedno nebo více přístupových pravidel pro příslušnou komponentu v politice
- Pouze DBSECADM může přidělovat výjimky
 - ▶ DBSECADM nemůže udělit výjimku nebo visačku sám sobě

Přidělování a odejímání výjimek

- Přidělení výjimky

```
GRANT EXEMPTION ON RULE
```

```
IDSLBACWRITEARRAY WRITEDOWN
```

```
FOR company TO mr_ceo;
```

- ▶ Uživatel **mr_ceo** může nyní porušit *array* pravidlo
- ▶ Může zapsat také záznam s úrovní 'Public' nebo 'Confidential'
- ▶ Stále však musí dodržovat pravidla pro komponenty *department* a *region*

- Výjimky je třeba přidělovat pouze na **nezbytně nutnou dobu**

- ▶ Jinak by přeci nebylo vůbec nutné se obtěžovat s LBAC !!!

- Odejmutí výjimky

```
REVOKE EXEMPTION ON RULE
```

```
IDSLBACWRITEARRAY
```

```
WRITEDOWN
```

```
FOR company FROM mr_ceo;
```

SQL funkce

- **SECLABEL_BY_COMP**

```
INSERT INTO T1 VALUES
```

```
SECLABEL_BY_COMP('company', 'Confidential:Marketing:West'), 1, 'xyz');
```

- **SECLABEL_BY_NAME**

```
UPDATE T1 SET C1 = SECLABEL_BY_NAME('company', 'manager');
```

- **SECLABEL_TO_CHAR**

```
SELECT SECLABEL_TO_CHAR('company', C1), C2, C3 FROM T1;
```

Privilegium SETSESSIONAUTH

- SQL příkaz SET SESSION AUTHORIZATION dovoluje předstírat identitu jiného uživatele, včetně LBAC přístupových práv
- IDS 11.10 a vyšší verze s podporou LBAC pracují odlišně s privilegiem SETSESSIONAUTH
 - ▶ Privilegium SETSESSIONAUTH musí uživateli přidělit DBSECADM
 - ▶ DBSECADM musí být nanejvýš opatrný při přidělení tohoto privilegia jinému uživateli
 - ▶ Při automatické konverzi ze starších verzí, které nepodporovaly LBAC, uživatel s právem DBA má migračním procesem automaticky nastavenou možnost přidělovat privilegium SETSESSIONAUTH pro PUBLIC
 - Po migraci je nutné všem DBA právo SETSESSIONAUTH ihned odejmout !!!

Role DBSECADM

- Database security administrator
- Tuto roli může přidělit pouze DBSA
- Zodpovědnosti
 - ▶ Vytváření, mazání, změny a přejmenovávání komponent
 - ▶ Vytváření, mazání a přejmenovávání politik
 - ▶ Vytváření, mazání a přejmenovávání visaček
 - ▶ Přidělování a odejímání politik tabulkám
 - ▶ GRANT a REVOKE pro visačky
 - ▶ GRANT a REVOKE pro výjimky
 - ▶ GRANT a REVOKE setsessionauth privilegia

Programy dotčené bezpečnostní politikou LBAC

- `dbschema/dbexport/dbimport`
 - ▶ Uživatel musí mít přidělenou roli DBSECADM, pokud má databáze LBAC objekty
 - ▶ Uživatel musí mít potřebné visačky nebo výjimky, pokud je třeba exportovat/importovat všechny záznamy z chráněné tabulky
- `onload/onunload`
 - ▶ Uživatel musí mít všechny potřebné výjimky, aby mohl obejít bezpečnostní politiku
- `HPL (express mode)`
 - ▶ Uživatel musí mít všechny potřebné výjimky, aby mohl obejít bezpečnostní politiku
- `Other load/unload utilities`
 - ▶ Uživatel musí mít potřebné visačky nebo výjimky, pokud je třeba provést load/unload záznamů z chráněné tabulky

Praktická ukáзка