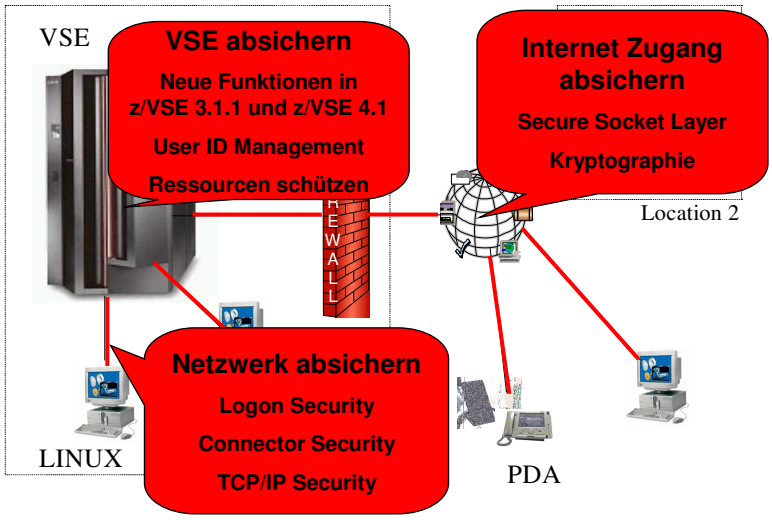
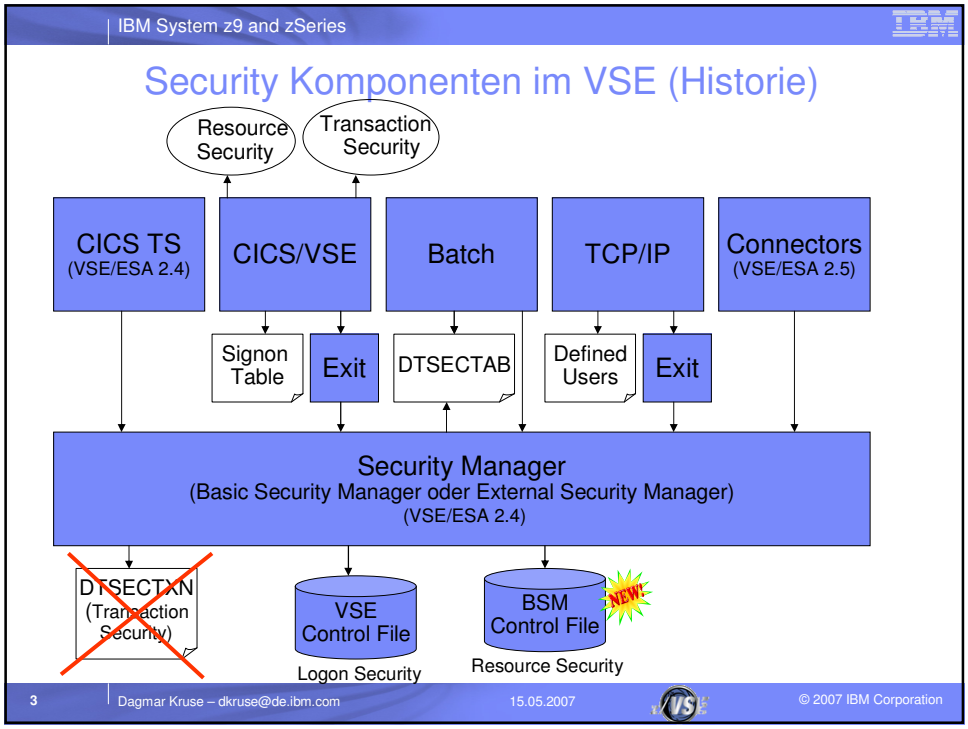
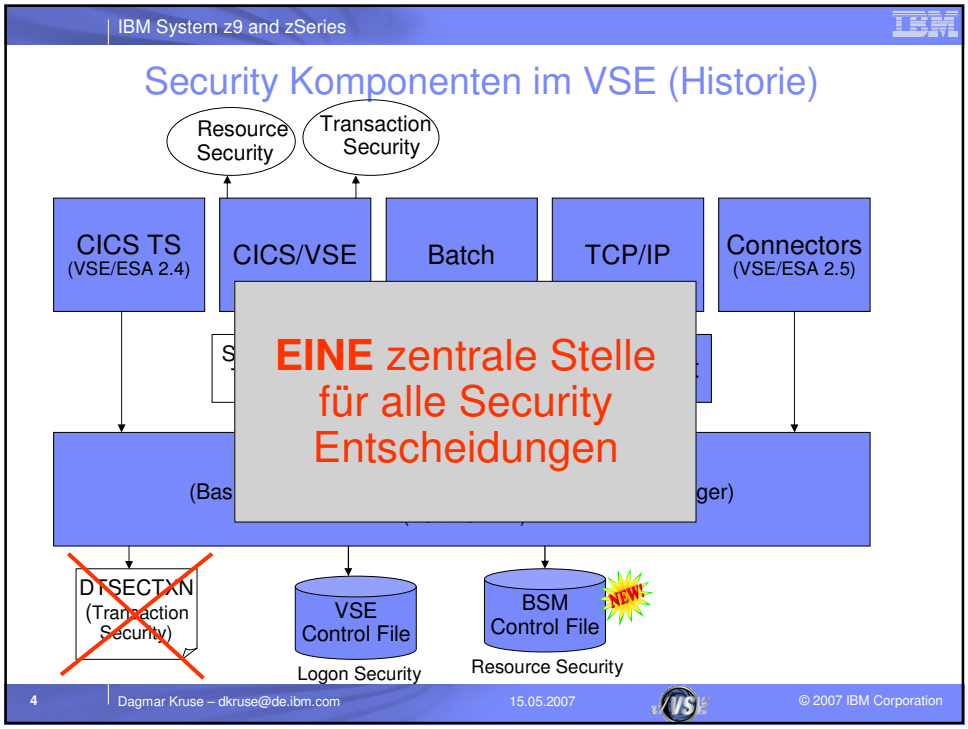
Das neue Security-Konzept (des BSM) im z/VSE

Dagmar Kruse
Technical Sales z/VSE

IT Sicherheit in einem heterogenen Umfeld




IBM System z9 and zSeries
Security Komponenten im VSE (Historie)
Resource Security
Transaction Security
CICS TS (VSE/ESA 2.4)
CICS/VSE
Batch
TCP/IP
Connectors (VSE/ESA 2.5)
Signon Table
Exit
DTSECTAB
Defined Users
Exit
Security Manager
(Basic Security Manager oder External Security Manager)
(VSE/ESA 2.4)
DTSECTXN (Transaction Security)
VSE Control File
Logon Security
BSM Control File
NEW!
Resource Security
3
Dagmar Kruse – dkruse@de.ibm.com
15.05.2007
© 2007 IBM Corporation


IBM System z9 and zSeries
Security Komponenten im VSE (Historie)
Resource Security
Transaction Security
CICS TS (VSE/ESA 2.4)
CICS/VSE
Batch
TCP/IP
Connectors (VSE/ESA 2.5)
EINE zentrale Stelle für alle Security Entscheidungen
DTSECTXN (Transaction Security)
VSE Control File
Logon Security
BSM Control File
NEW!
Resource Security
4
Dagmar Kruse – dkruse@de.ibm.com
15.05.2007
© 2007 IBM Corporation

Basic Security Manager – Neu mit z/VSE 3.1.1

- **Erweiterung des RACROUT-Interfaces analog zum RACF im z/OS**
- **Neue RESSOURCE Klassen**
  - TCICSTRN - Transaktionen (bisher DTSECTXN)
  - MCICSPPT - Anwendungs-Programme
  - FCICSFCT - Dateien
  - JCICSJCT - Journale
  - SCICSTST - Temporary Storage Queues
  - DCICISDCT - Transient Data Queues
  - ACICSPCT - Transaktionen (CICS START)
  - APPL - VTAM-Anwendungen (CICS1,CICS2,..)
  - FACILITY - weitere Ressourcen (Spooling Files, RCF,…)

- **Benutzer können in Gruppen eingeteilt werden**
  - Berechtigungen können basierend auf der Gruppenzugehörigkeit vergeben werden
  - Vereinfacht das User-ID Management

Neues BSM-Security-Konzept ab z/VSE 3.1.1

- Der Benutzer bekommt Zugriffsrecht:
  - **Adminstratoren dürfen alles !**

    Sie müssen nicht explizit berechtigt werden !

  - **Über die „Access List“ der Resource (II-Dialog 281)**
    - **User wird direkt dort eingetragen**

    oder

    - **gehört zu einer “User Group”, die dort eingetragen ist**
      - **User in “User Group” eintragen (II-Dialog 282)**

    Priorität in Zugriffsliste: “User” vor “User Group”

Neues BSM-Security-Konzept ab z/VSE 3.1.1

- Zu schützende Ressource erhält ein Resource Profile (II-Dialog 281)
  - **in einer 'Resource Class' definiert sein**
  - **Eine 'Universal Access Authority' haben:**
    NONE (default), READ, UPDATE, ALTER
  - **besitzt eine 'Access List'**
- CICS TS-Ressourcen:
  - **CICS-Security für die gewünschten Ressource-Klassen aktivieren**
    - **z.B. XFCT=YES für Dateien (DFHSIT)**
  - **Transaktion mit RESSEC=YES definieren**

Administration im neuen BSM-Security-Konzept

- **Daten, wie Resource Profiles, User Groups,… werden im VSE.BSTCNTL.FILE gespeichert.**
- **Änderungen müssen dem Basic Securtiy Manager (BSM) übergeben und dort aktiviert werden:**

  // EXEC BSTADMIN

  Befehle, s. z/VSE Adminstration Guide, Kapitel 8

  oder II-Dialog 2.8.3

Ressource Klasse: TCICSTRN (Transaktionen)

- Altes BSM-Konzept:
  - **Transaktionen werden über Transaction Security Key 01 bis 64 geschützt. Benutzer müssen für diesen Key berechtigt sein.**
  - **Kontrolliert wird über die DTSECTXN.**
- Neues BSM-Konzept:
  - **Transaktionen müssen in der Ressource-Klasse TCICSTRN definiert sein:**
    - **Universal Access Authority (Default: NONE)**
    - **Benutzer-Zuordnung über Zugriffsliste:**
      - **Direkt oder über User Groups**
      - **Nicht Adminstratoren ("Sie dürfen alles")**
  - **Kontrolliert wird über die VSE.BSTCNTL.FILE.**
- **Migrationsschritte und -hilfen sind im z/VSE Administration Guide beschrieben**

Ressource Klasse: Facility

- **Wichtig, wenn Sie den Report Controll Facility (RCF) oder sonstige Programme verwenden mit**

  EXEC CICS ...

  SPOOLOPEN / SPOOLREAD SPOOLWRITE / SPOOLCLOSE

- **Dann müssen im z/VSE 3.1.1**

  die PTFs UK14161 (in z/VSE 3.1.2 enthalten) und UK19662* installiert sein.

- **Danach muss in der ICCF Library 59 das Skeleton SKRCFSEC ausgeführt werden, um die Security für RCF und EXEC CICS SPOOLOPEN zu definieren.**

*** PreReqs: UK14212 (in z/VSE3.1.2 enthalten), UK18593**

Basic Security Manager – Neu mit z/VSE 4.1

- **Audit-Logging und Reporting**
  - Alle Zugriffe auf geschützte Ressourcen können protokolliert werden
    - Sowohl erlaubte als auch unerlaubte Zugriffe
  - Versuchte Angriffe können erkannt werden
    - z.B. mehrfache Logon-Versuche mit falschem Passwort
  - Man kann nachvollziehen wer wann welche Ressource im Zugriff hatte
  - Auswertung mit Hilfe eines Report-Tools
    - Zusammenfassung
    - Detaillierte Auflistung aller Zugriffe
  - Benutzt das CICS DMF Tool
    - Erstellt SMF Records für Protokoll-Informationen

Literatur zum neuen BSM-Security-Konzept

- **z/VSE Planning 3.1.1, 4.1.0**
- **z/VSE Administration 3.1.1, 4.1.0 (ist ausführlicher)**
- **CICS TS Security Guide (SC33-1942-03)**
- **RACROUTE documentation as part of the VSE Collection on**
  - DVD, SK3T-8348
  - CDROM, SK2T-0060
- **VSE Security documentation from Internet**
  - http://www-1.ibm.com/servers/eserver/zseries/zvse/documentation/security.html
- **GSE-Vortrag**
  ftp://ftp.software.ibm.com/eserver/zseries/zos/vse/pdf3/gse2007/berlin/S12.pdf

Haben Sie noch Fragen?

Danke
für
Ihre Aufmerksamkeit !