IBM Software Group

zSecure Suite 1.12

Glinda Cummings
WW Sr. Product Manager

Mark S. Hahn
Technical Support Professional

Tivoli software

Short Review of zSecure v1.11Functions and Features (in case you forgot)

- Currency for z/OS v1.11
  - Format and analyze live Communication Server (TCP/IP) stack configuration information for auditing and alerting
  - Support for new RACF and SMF fields for identity propa ation
  - Support Load Module Signature Verification as required y regulations and government requirements such as PCI DSS

- RACF Database Cleanup
  - Access Monitor ---- Address the problem of:
    - obsolete authorizations with RACF database clean-up function
    - including unused user, group authorizations, unused connects

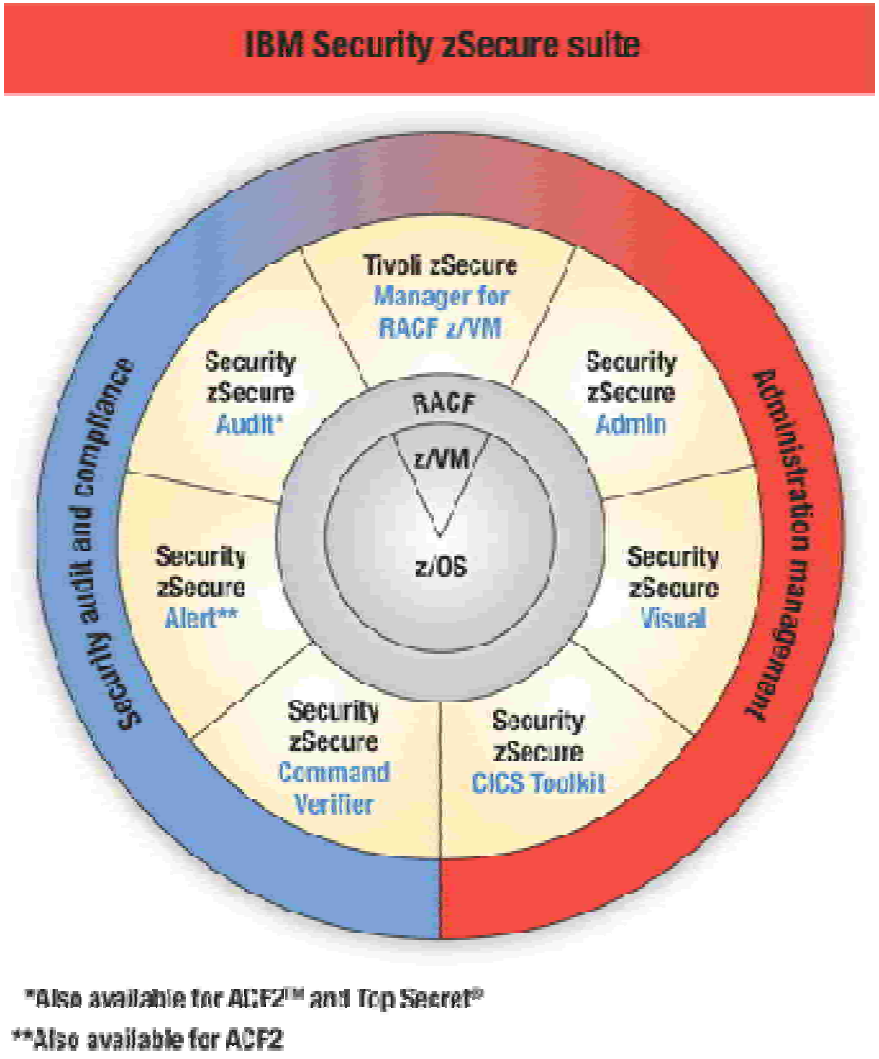
Short Review of zSecure v1.11Functions and Features (in case you forgot

- **Extended monitoring of status changes in z/OS and RACF**
- **Integration with CICS to deal with multiple events contained in a single CICS SMF 110 Record, plus**
- **New CICS event information provided to Tivoli Security Information and Event Manager via the Tivoli zSecure TCIM Enabler or z/OS**
- **Report on IBM Data Facility Storage Management Subsystem (DFSMS) Re-movable Media Manager (RMM) new dynamic variants**
- **Using MVS System Management Facilities (SMF) format administrative commands from OMEGAMON for regulatory compliance**
- **Support Partitioned Data Set Extended (PDSE) and PDS m mber level auditing**
- **Audit and Alert on Internet Protocol Security (IPSEC) configuration information**

Short Review of zSecure v1.11Functions and Features (in case you forgot

- **Report on IBM Tivoli Key Lifecycle Manager for security events**
- **Report on IBM WebSphere Application Server V7 security events**
- **Audit and report for security events from Object Access Method (OAM) by using SMF**
- **Administration enhancements to the user interface (UI) multiple permits and connects**
- **Ability to deliver globalization enhancements for Double Byte Character Set (DBCS)**

  Reports with audit concerns in Japanese



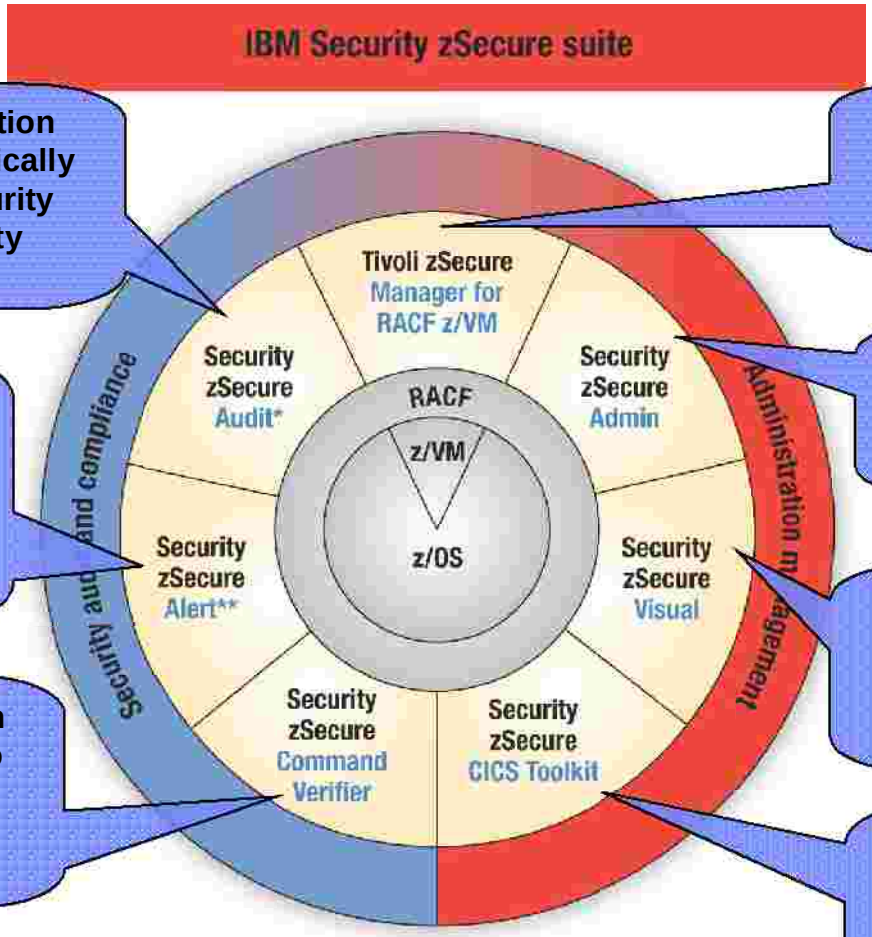
Security zSecure Suite 1.12.0

Security zSecure Suite 1.12.0

- New releases for z/OS products
  - 5655-T01 IBM Security zSecure Admin 1.12.0
  - 5655-T02 IBM Security zSecure Audit 1.12.0
  - 5655-T09 IBM Security zSecure Visual 1.12.0
  - 5655-T11 IBM Security zSecure Alert 1.12.0
  - 5655-T05 IBM Security zSecure CICS Toolkit 1.12.0
  - 5655-T07 IBM Security zSecure Command Verifier 1.12.0
  - 5655-T15 IBM Tivoli Compliance Insight Manager Enabler for z/OS 1.12.0

- z/VM offering released earlier this year (GA July 9, 2010)
  - 5655-T13 IBM Tivoli zSecure Manager for RACF z/VM 1.11.0

IBM Security zSecure Suite



Compliance and audit solution that enables you to automatically analyze and report on security events and detect security exposures

Combined audit and administration for RACF in the VM environment

Real-time mainframe threat monitoring allowing you to monitor intruders and identify configuration mistakes that could hamper your compliance efforts

Enables more efficient and effective RACF administration, using significantly less resources

Policy enforcement solution that enforces compliance to company and regulatory policies by preventing erroneous commands

Reduces the need for scarce, RACF-trained expertise through a Microsoft Windows–based GUI for RACF administration

Allows you to perform mainframe administrative tasks from a CICS environment, freeing up native-RACF resources

*Also available for ACF2™ and Top Secret®

**Also available for ACF2

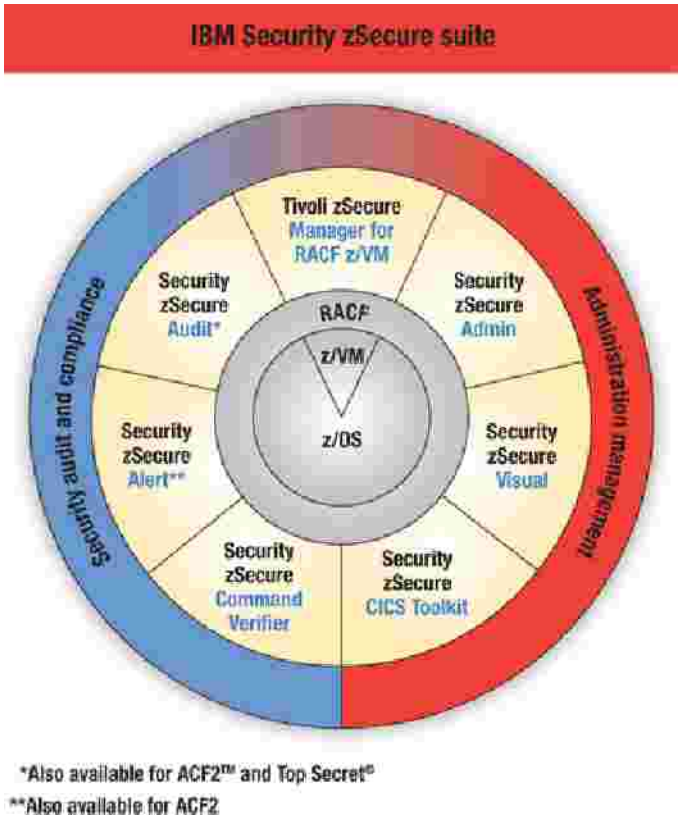
zSecure Suite…

What's new in 1.12

What's new in zSecure Suite 1.12.0 - topics

- Multi-system support
- RRSF support
- Apply command to multiple profiles
- z/OS UNIX administration
- New support and reporting of SMF records
- Send alerts to UNIX syslog
- TCP/IP alerts and audit concerns
- z/OS currency
- Globalization
- and more…

Multi-system support



zSecure Admin
zSecure Audit
zSecure Visual

Data from multiple live systems in a single session Updates to multiple RACF databases with/out RRSF

- Multi-system support requirements
  - Administer multiple systems from a single application instance
    - Live data access
    - Fast data access
  - Allow sending the same commands to multiple systems
    - Use RACF Remote Sharing Facility (RRSF) network ***if present***
      - Support for AT and for ONLYAT keywords
    - ***Without*** RRSF network
  - Use data encryption

Multi-system support – specifying data sources

§ The data set detail panel of the SETUP FILES menu allows specifying remote destinations

ü zSecure Node – by Plex
ü zSecure System – system

Multi-system support – compare databases at a glance

§ SETUP VIEW has a new option for tweaking the RA.U/G/D/R menus:

```
/  Add summary to RA displays for multiple RACF sources (normally on)
```

This is a new kind of summary designed to highlight differences

Flags and such: shows percentage of complexes for which it is true

Text and such: shows value if all the same, or the *common prefix* followed by >

Numbers and such: shows value if all the same, or <more>

Ø Let's look at two similar databases:

```
   User      # Name                 DfltGrp  Owner    Rev Ina Res Ptc Spc Opr
__ CERT004   2 TESTUSER DIG.CERT    C##B     SYSAUTH  100  50   0 100   0   0
s_ CERT005   2                      SYS>     <more>    50   0   0 100   0   0
```

ü These userids occur in both databases (the 2 under #)

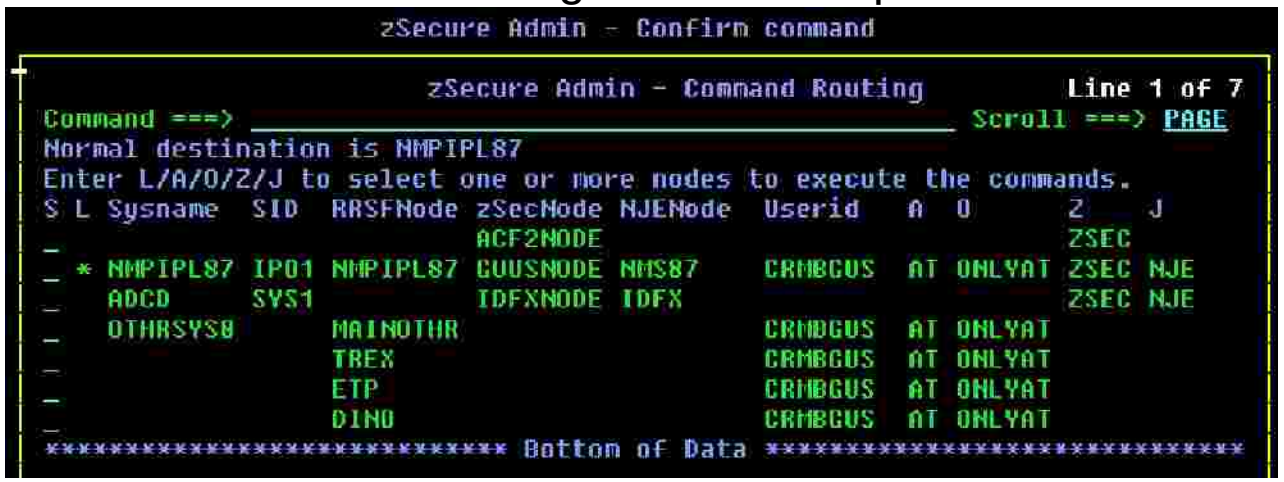
ü CERT004 has all the same values, except for the `revoke_inactive` flag (50%)

ü CERT005 has two different owners, with no common prefix (hence <more>)

```
   User     Complex  Name                DfltGrp  Owner    RIRP SOA gC LCX Grp
__ CERT005  DD981216                    SYSPROG  C##BMR1                X   1
__ CERT005  DINO                        SYSAUTH  SYSAUTH  R             X   1
```

Multi-system support – command routing

- In ‘Ask’ mode the following confirmation panel is shown:

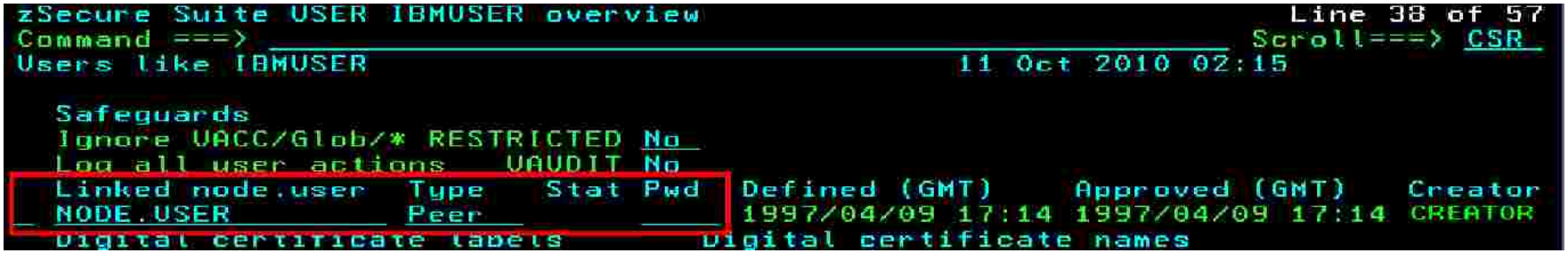


- Ø Routing options are: Local, to an RRSF node using At or Onlyat, to a zSecure Node, or to an NJE (JES) node

- First the server is located, then the command is issued under the “user” authority, and feedback is passed back to the user.

- Routing can work on a single command or on a data set, in which case the zSecure Command Execution Utility (CKX) is used

RRSF support – RACLINK overtype



- Admin: Line commands and overtype for RACLINK field
  - A – approve pending user ID association
  - C – copy existing association to define a new one
  - D – undefine a user ID association
  - I – define a new association

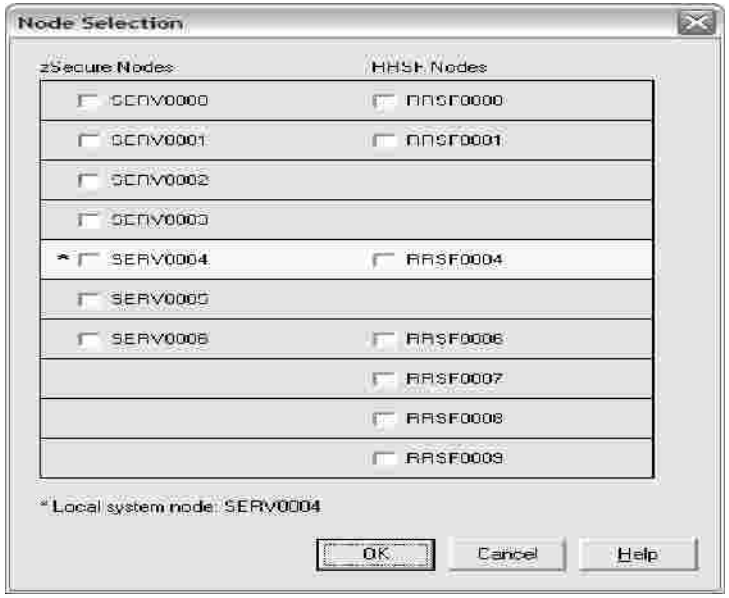
RRSF support – VERIFY and MERGE

- VERIFY PERMIT, EMPTY, and ALLNOTEMPTY are now aware of RRSF
  - Userids and data sets will not be deleted when still in use on a connected RRSF node
    - Provided that information is available
    - Unless OPTION ONLYAT requests to do so
  - CKGRACF USER RACLINK UNDEF [(*node.id*)]
    - Can remove one-sided associations

Multi-system and RRSF support – zSecure Visual

- Visual client can run with or without multi-system services
  - Indicate the desired mode in the option form before logon
    - Ø Checkbox 'Use zSecure Server for multi-system services'
    - ! Must logoff and re-logon to change mode

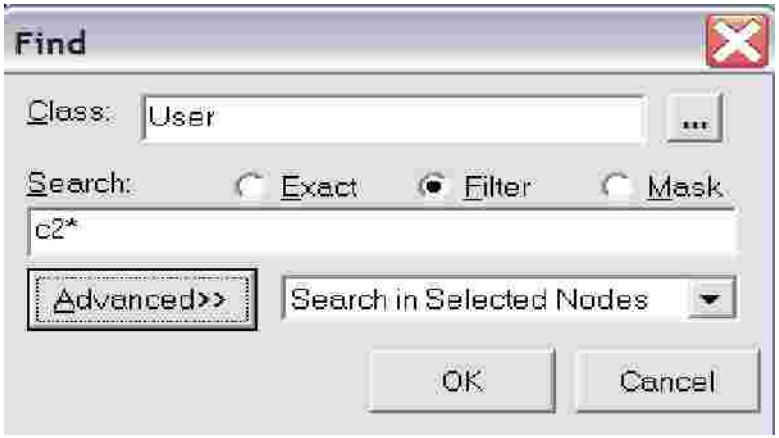
- After logon, choose the zSecure and RRSF nodes to work with



- Ø During the session the 'Available nodes' menu option can be used to change the set of nodes being worked with

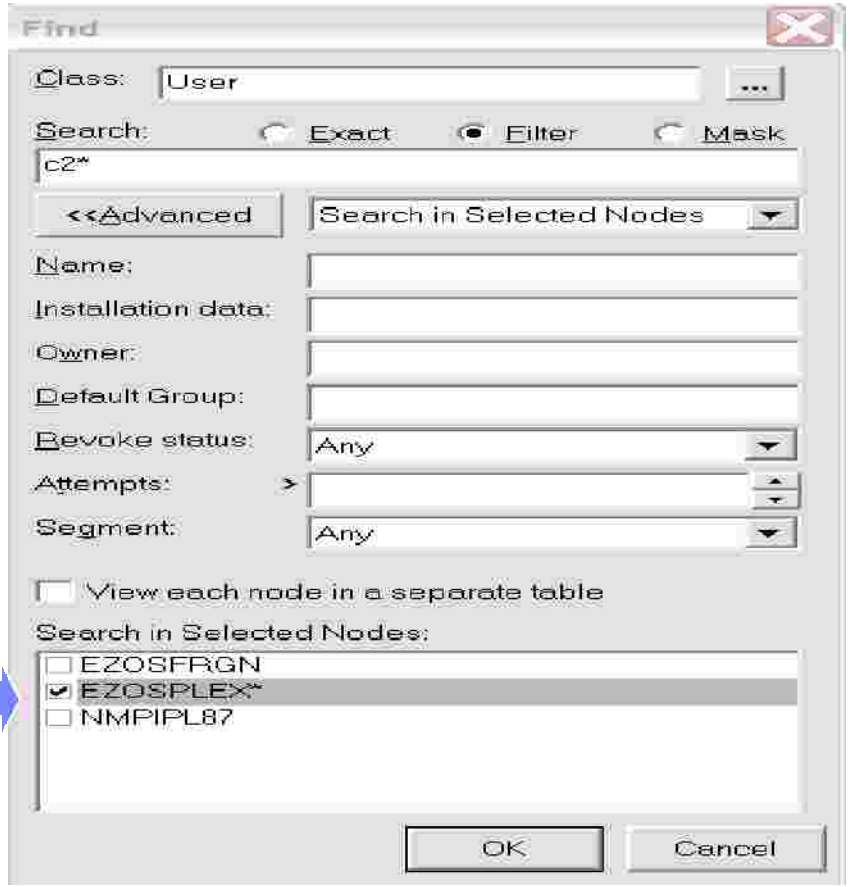
Multi-system and RRSF support – zSecure Visual

§ Find dialog allows fine-tuning for searches



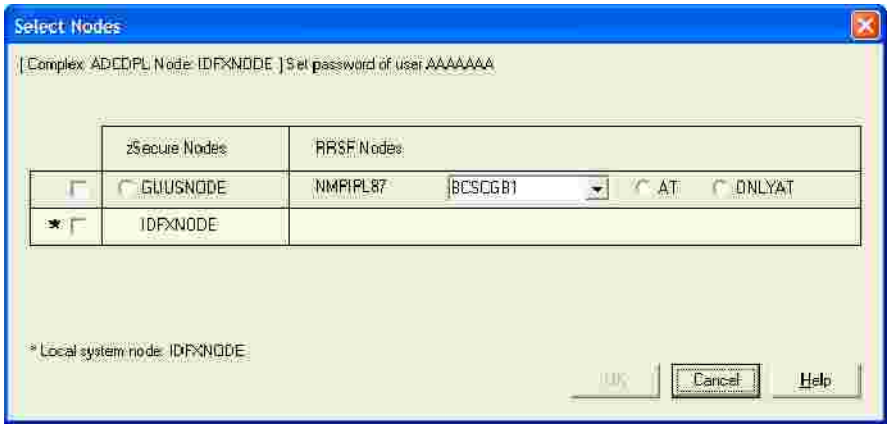
Ø The basic Find dialog uses all nodes being worked with

Ø The Advanced Find dialog allows more specific search



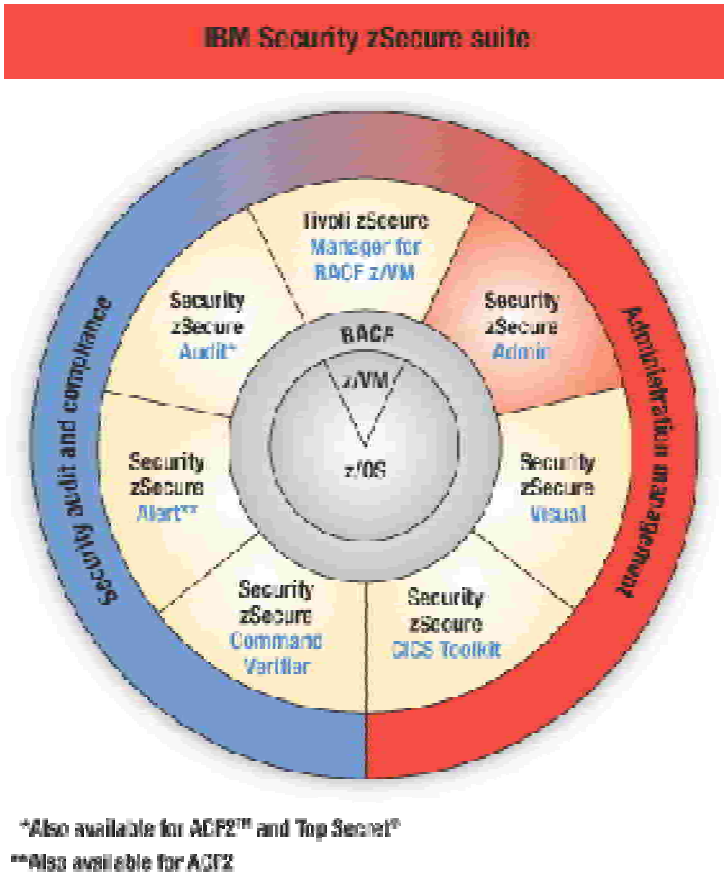
Multi-system and RRSF support – zSecure Visual

- Additional interface changes to work with multiple systems:
  - Data displays show a column Complex to indicate the source nodes
  - Captions of property dialogs show Complex and source node
  - Changes can be directed to one or more nodes. When clicking OK, select nodes and methods (zSecure, RRSF AT, RRSF ONLYAT)



    - ! Copying users or groups requires zSecure nodes
  - Menu options (e.g. Grouptree) require specifying a particular node
    - Ø Selection box in dialog is similar to the one in Advan nd

z/OS UNIX administration



zSecure Admin

z/OS UNIX administration

- z/OS UNIX reports are now available in zSecure Admin
  Before, they were only available in zSecure Audit

- U line command brings up ISPF's z/OS UNIX Directory List Utility, which can be used to display directories and edit, browse, delete, rename, or copy files, as well as modify file mode fields and extended attributes, and execute commands.

```
IBM Tivoli zSecure UNIX summary                          1 s elapsed, 2.8 s CPU
Command ===> ____________________________________________ Scroll===> CSR
Files for complex like :'tomo'c                28 Nov 2008 00:07
   Complex  System   Count
   EEND     EEND         6
   Count FS mount point
       2 /u
   T FileMode  + apsl AuF Owner    Group    Relative pathname (within FS)
u_ d r-xr-xr-x        fff C##BHJ1  OMVSGRP  automount
__ d r-xr-xr-x        fff C##BHJ1  OMVSGRP  automount2
****************************** Bottom of Data *******  **********************
```

z/OS UNIX administration

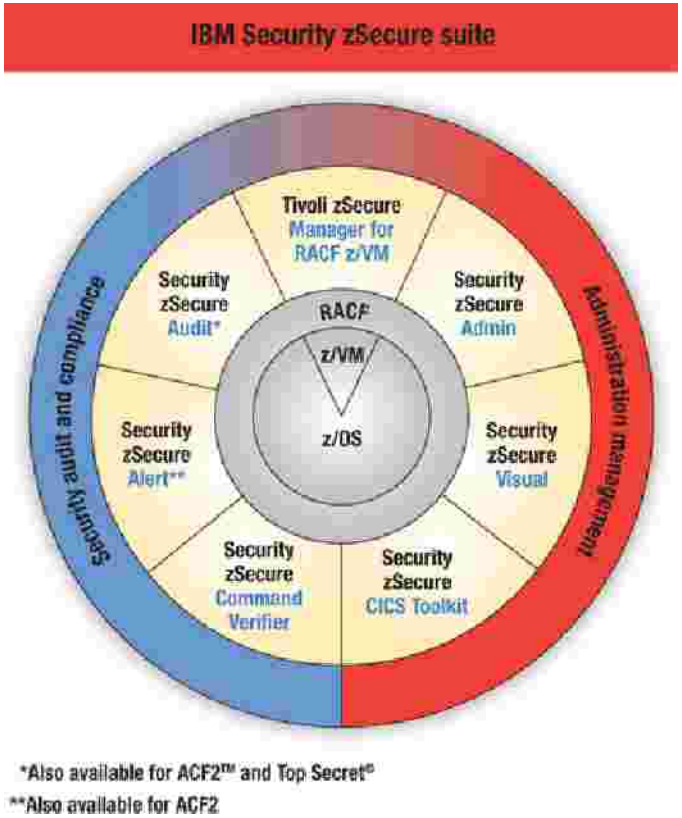
§ On z/OS V1R12 this immediately brings up this panel:

```
                          z/OS UNIX Directory List            Row 1 to 3 of 3
Command ===>                                                  Scroll ===> PAGE

Pathname . : /u/automount

Command  Filename        Message          Type Permission Audit  Ext   Fmat
-------------------------------------------------------------------------------
________ .                                 Dir  r-xr-xr-x  ------
________ ..                                Dir  rwxr-xr-x  fff---
/_______ c##bjti                           Dir  rwx------  fff---
```

! The DIRLIST service invoked acts on directories. For a file the directory it is contained in will be shown; the end user must locate the file themselves.
! This service works on the local live z/OS UNIX
  Ø Requires read permission (file permission, or RACF auditor, UID(0), access to FACILITY BPX.SUPERUSER or UNIXPRIV BPX.FILESYS.**, …)

Ø Once here, / brings up the available commands
Ø Free form commands can also be entered

Apply Commands to Multiple Records on Display - Block commands

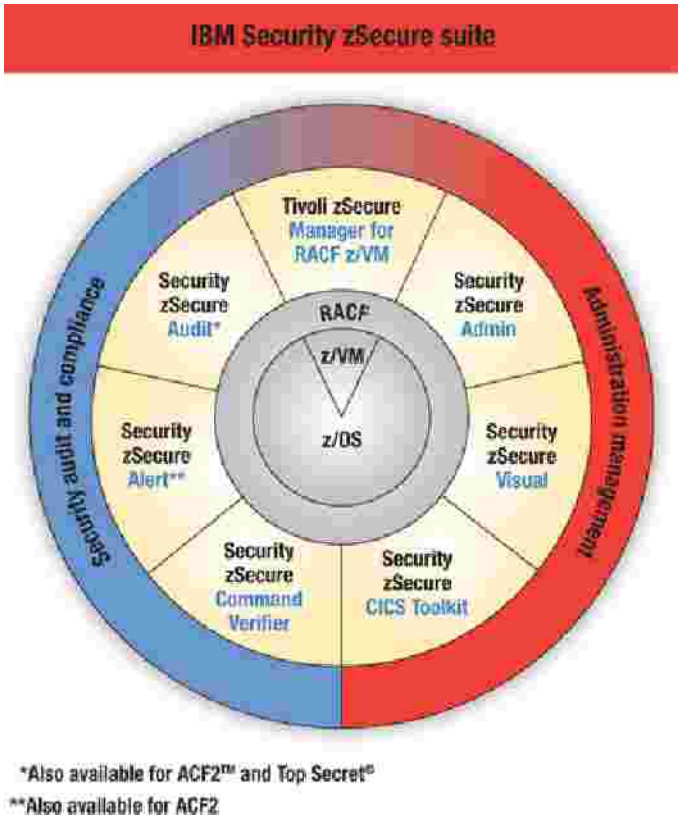


zSecure Admin
zSecure Audit

Apply command to multiple records on a display

- zSecure 1.12 introduces block commands on ISPF displays:
  - Admin: RR..RR to Recreate multiple profiles
  - Admin: DD..DD to Delete multiple profiles
- Commands for all selected records are executed at once
- In addition a primary command FORALL is provided
  - With no selection, it applies a command to all records on the display

SMF record support extensions



zSecure Audit
zSecure Alert
TCIM Enabler (for TSIEM)

New SMF record types and fields – DB2

- DB2 V10R1 events (SMF record type 102)
  - New trace records of interest for:
    - Row and column access control
    - Audit administrative authorities
    - Begin audit trace with AUDITPOLICY
  - Basic support for IFCids 357, 358, 359, 363, 364, 401, 402
  - New privileges added to IFCid 140
  - DB2 privilege translated to access intent (ALTER, CONTROL, …) by IFCids 140/361
  - New object type ‘session variable’
  - IFCids 142 enhanced to show row/column ACCESSCTRL information
  - IFCids 145 enhanced to show row/column enforcement

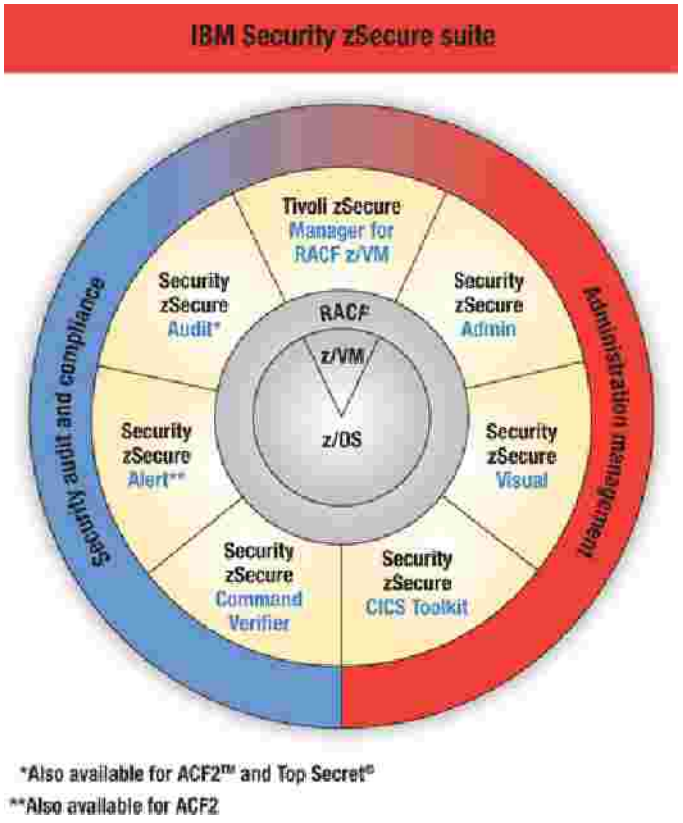
New SMF record types and fields - SMTP

- Communications Server NJE mail client (CSSMTP) events
  - This new client is a mail "forwarder" that takes mail messages in data sets from the JES spool and forwards them to an SMTP server
  - SMF record type 119 subtypes 48-52
    - configuration records
    - connection records
    - mail records
    - spool records
    - statistics records
  - Many new CARLa fields CSSMTP_* with extracted information

New SMF record types and fields – Linux for System Z

- Linux for System Z events (SMF record type 83 subtype 4)
  - SMF record type 83 subtypes have shared and individual data sections
  - SMF record type 83-4 records remote audit events
  - One application that can write them is a Linux plug-in (daemon) audispd
- New R_LOGDATA field - application-specific data from relocate section 114
  - RACF_LINK_EVENT and RACF_LINK_AUDIT associate multiple records for the same event

Other Admin+Audit enhancements



zSecure Audit
zSecure Admin

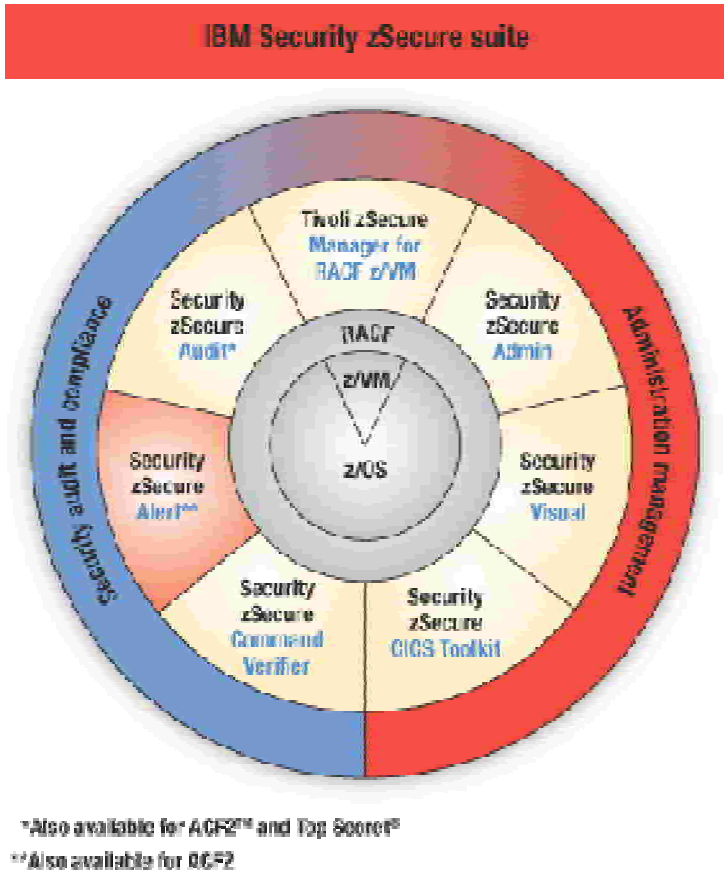
Other Admin and Audit enhancements

- Audit: TYPE=RACF_ACCESS is now entitled for zSecure Audit
  - Enables reporting on the RACLIST merged access list fo a resource

- zSecure Audit for ACF2: Capability provided to report on all authorized users and associated access levels for an particular $KEY or NEXTKEY

- Revoked connects shown in RvC column on ACL

Send alerts to UNIX syslog

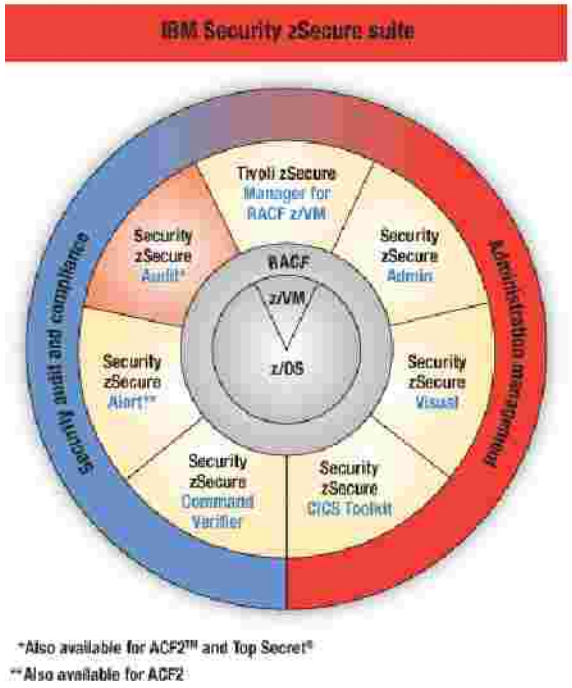


zSecure Alert

Writing alerts to a UNIX syslog socket

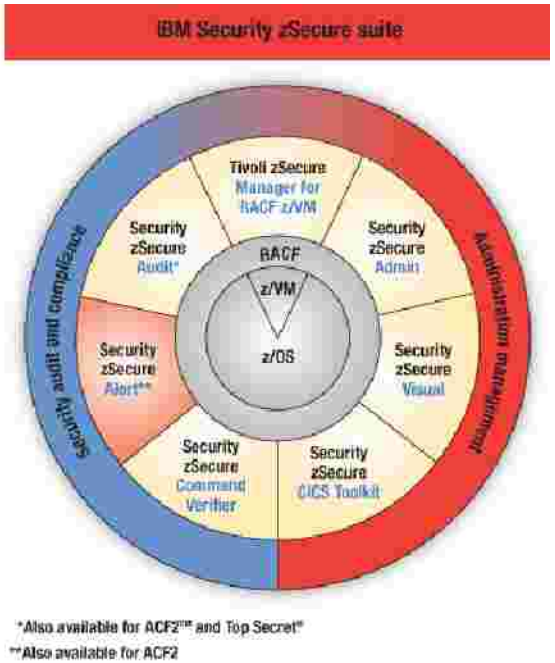
- UNIX syslog added as an alert destination
  - Syslog receivers are commonly used to collect messages from m ltiple systems, store them for log collection purposes and analyze them for alerting purposes. z/OS UNIX has a Syslog receiver that has been enhanced in z/OS V1R11, it can be used as a central point of log collection, e.g., for Linux for System Z systems. There are many cross-platform log collection solutions that zSecure Alert can now easily feed into.
- Was also added into zSecure 1.11.0 last summer

TCP/IP alerts and concerns



*Also available for ACF2™ and Top Secret®
**Also available for ACF2

zSecure Audit
zSecure Alert



*Also available for ACF2™ and Top Secret®
**Also available for ACF2

TCP/IP Audit concerns – IP_STACK and IP_PORT

- Audit concerns pertaining to IP stacks — review required:
  - 32 By default, anyone can modify TCP/IP security param ters
  - 30 IPv[4|6] IP filtering support and IPSec tunnel supp t not active
  - 30 Denial-of-service possible without authentication
  - 28 No access control to/from foreign and local networks
  - 26 No access control required to/from foreign networks
  - 24 No access control in local network
  - 23 Ports below 1024 are not reserved - any user or program can bind to low [TCP|UDP] ports to masquerade as a legitimate s vice
  - 21 SMF119 *subtype* is not written - audit trail incomplete
  - 20 No audit trail of attacks stopped by filter rules

TCP/IP concerns – IP_STACK and IP_PORT

- Audit concerns pertaining to IP stacks - worthy of attention:
  - 18 No audit trail of attacks stopped by default filter rules
  - 15 or 11 By default, anyone can read netstat [*netstatoption*] output that might help attackers
- Audit concerns pertaining to IP ports - review required:
  - 22 Because there is no SAF parameter, any user or program can bind to a privileged [TCP|UDP] port [*begin_port-end_port*|*port*] under jobname *jobname* (filter) by default, thus masquerading as a legitimate service and receive passwords
  - 20 Because there is no SAF parameter, any user or program can bind to a privileged [TCP|UDP] port [*begin_port-end_port*|*port*] under jobname *jobname* (filter) by default, thus masquerading as a legitimate service

TCP/IP concerns – TRUSTED

- Audit concerns for access to Trusted Computing Base:
  - 6 User can modify TCP/IP security parameters
  - 3 Can run attack program on a privileged *protocol* port between *begin_port* and *end_port* under jobname *jobname* (filter), thus masquerading as a legitimate service and receive passw rds
  - 2 Can run attack program on a privileged *protocol* port between *begin_port* and *end_port* under jobname *jobname* (filter), thus masquerading as a legitimate service

TCP/IP alerts – deactivating TCP/IP security features

- Alerts added for TCP/IP security reduction

Warnings:

Attacks blocked by filter rules are no longer logged

Attacks blocked by default filter rules are no longer logged

The security class of an interface has changed

IP filter rules changed

Minor:

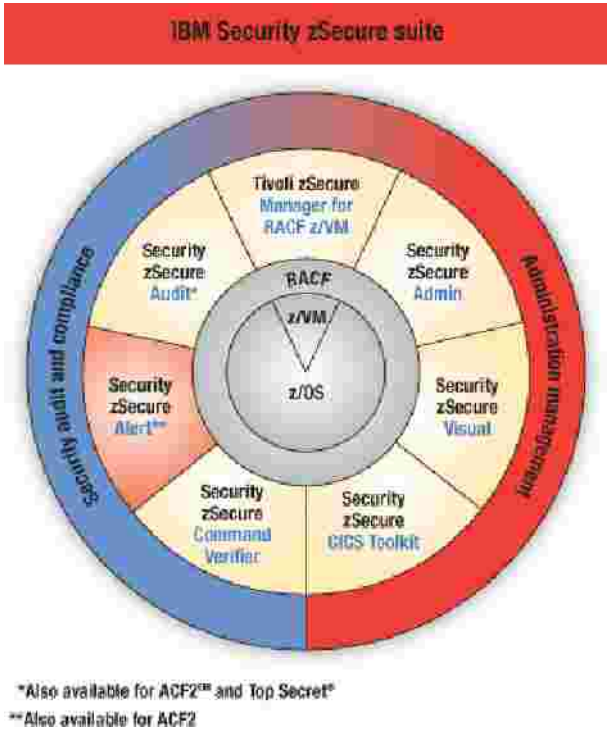
Certain SMF 119 records are no longer written; audit trail incomplete

Critical:

IPv4 or IPv6 filtering support and IPsec tunnel support deactivated

TCP or UDP ports below 1024 are not reserved anymore

Other Alert enhancements

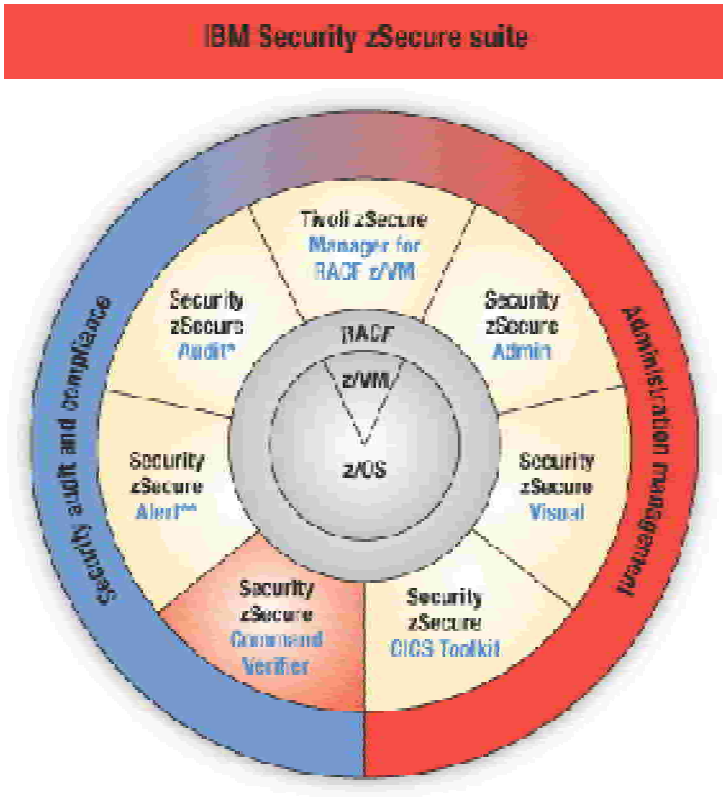


zSecure Alert

Other alert enhancements - new alerts

- IBM Health Checker - Alerts 1604, 1605, and 1606 added to pass on low, medium and high severity alerts from IBM Health Checker
- SMF Record Flood detection - Alerts 1607 and 1608 are issued for z/OS V1R12 SMF record flood detection
  - 1607 - SMF record flood detected
  - 1608 - SMF record flood starts dropping records

zSecure Command Verifier



*Also available for ACF2™ and Top Secret®
**Also available for ACF2

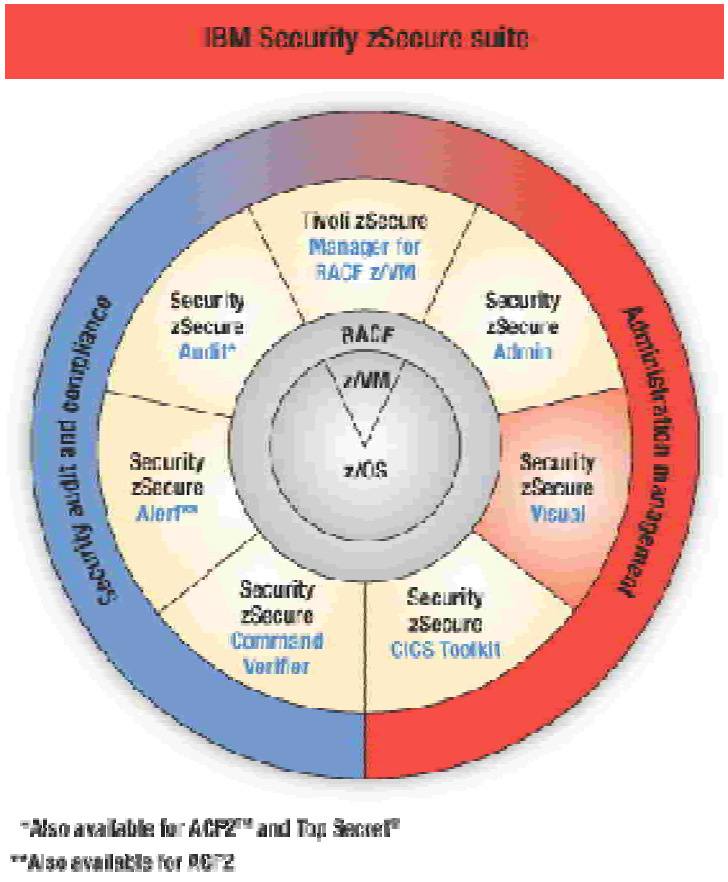
Command Verifier enhancements

- Notification controls for when commands are changed
  - DEFAULTS – due to default policy
  - MANDATORY – due to mandatory policy
  - SUPPRESS – due to violated policy
- C4R.=MSG.CMD specifies that command must be displayed
  - C4R.DEBUG deprecated
- New RACF Keywords –

  Recognize SYMCPACFWRAP keyword for ICSF segment

  Recognize NOGENERIC keyword

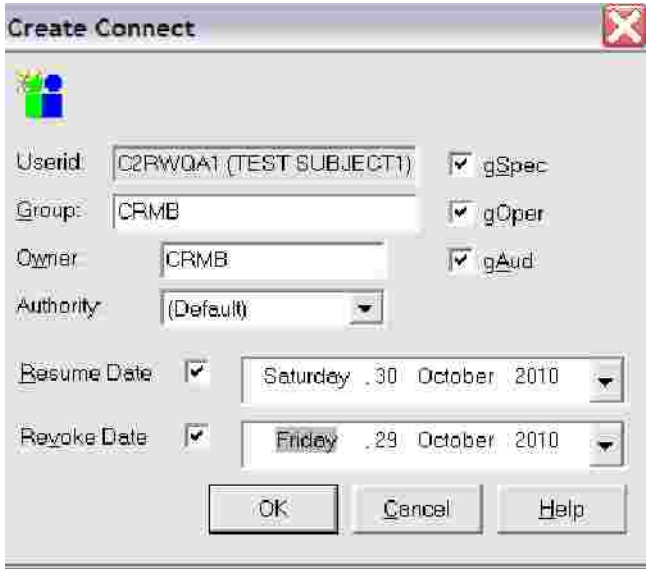
Other Visual enhancements



zSecure Visual

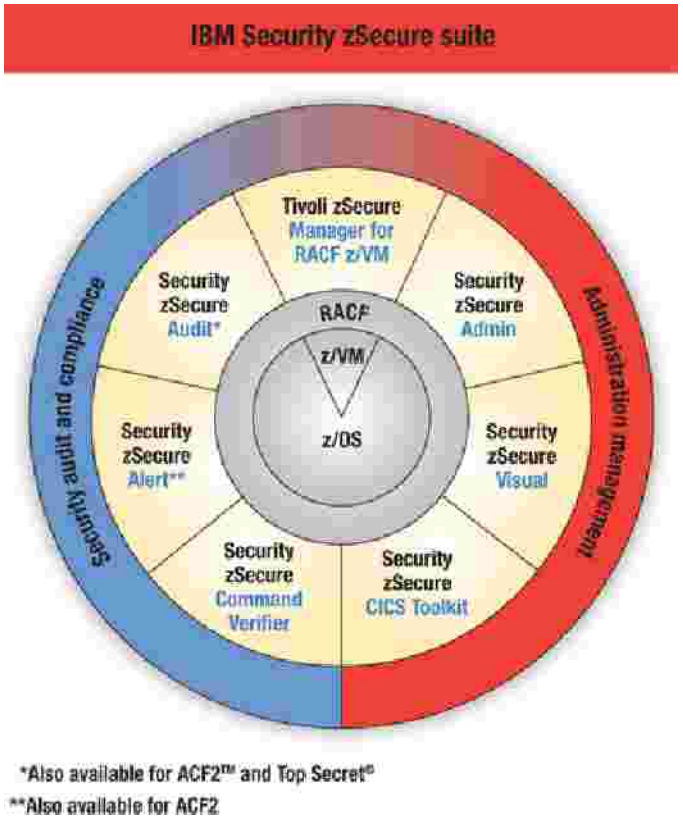
Other Visual enhancements (1/2)

- Support added for revoke and resume dates on connects



- Support for ICSF symmetric key CPACF wrap property

z/OS currency



zSecure Admin
zSecure Audit
zSecure Alert
zSecure Visual
TCIM Enabler – (for TSIEM)

z/OS currency – RACF

- RACF enhancements for digital certificates
  - Certificate start and end dates beyond 2041
  - Issuer's distinguished name up to 1024 characters
  - Support for new encryption types (NISTECC and BPECC)
  - New keyword KEYAGREE for KEYUSAGE
- New attribute SYMCPACFWRAP for ICSF keys classes
- RACF performance control SET GENERICANCHOR
  - Specifies the number of HLQ caches used for generic pr iles
  - Can be specified on the system or job name level
  - Security relevant because it can influence access decisions

z/OS currency – SMF flood detection

- SMF flood detection and filtering

  System Management Facilities log – protect from filling up

  ISSUE: loss of critical auditing information

- Alert: Trap messages issued when these conditions occur

zSecure Suite 1.12.0

Availability information

Availability

Supported releases are z/OS V1R8 through z/OS V1R12

- There is a standard support extension for z/OS V1R8 and V1R9

Visual client 1.12 is supported on Windows 7, Vista and XP SP3

Support for CICS Transaction Server V3R1 through V4R1

Support for DB2 V8R1 through DB2 V10R1 (GA'd on October 22)

Support for CA ACF2 and CA Top Secret up to r12

TCIM Enabler 1.12.0 works with TSIEM 2.0, TCIM 8.0, and 8.5

SUMMARY: What's new in zSecure Suite 1.12.0 - topics

- Multi-system administration
- RACF Remote Sharing Facility (RRSF) support
- Apply commands to multiple RACF profiles
- z/OS UNIX administration
- New support and reporting of SMF records
- Ability to send alerts to UNIX syslog
- TCP/IP alerts and audit support
- Currency with z/OS V1.12 and new RACF capabilities:
  - Support for new RACF fields and new values for certificates
  - Support for new dynamic exits to increase ensured security
  - Support for years beyond 2041 in certificate start and end dates
  - Support for the extension of Distinguished Names of 1024 bytes
- Globalization supporting DBCS for compliance efforts

zSecure 1.12 Benefits

- Increase productivity for administrators and users
- Reduce errors for administration to multiple RACF databases which could decrease security integrity
- Simplify security for customers with multiply RACF databases
- Support for customers who want to utilize RACF Remote Sharing Facility (RRSF)
- Enhanced alerting for possible loss of auditing inform tion and alerts for IBM Health Checker
- Extend security auditing, monitoring and compliance ou ide of JUST the security access control –
  - i.e. SMPT, TCP/IP, Digital certificates, and more

Resources for you to use

- **New White Paper: "Consolidating security across platforms with IBM System z"**
  IBM Tivoli and IBM Information Management solutions for security work with the IBM System z platform to allow the mainframe to serve as an enterprise security hub, providing comprehensive, centralized security capabilities for organizations with distributed, multi platform IT environments.

  http://www.servicemanagementcenter.com/main/pages/IBMRBMS/SMRC/ShowCollateral.aspx?oid=80003

- **White Paper: "Realizing business value with mainframe security management"**
  This white paper shows how organizations can reduce co and improve ROI by implementing IBM Tivoli Security Management for z/OS on IBM System z mainframes. It also provides specific examples of how IBM customers have realized tangible business value from this solution.

  http://www.servicemanagementcenter.com/main/pages/IBMRBMS/SMRC/ShowCollateral.aspx?oid=70071

- **Customer Video: Allied Irish Banks customer video**

  On YouTube: http://www.youtube.com/watch?v=rW3-P8ndEts

  On SMRC: http://www.servicemanagementcenter.com/main/pages/IBMRBMS/SMRC/ShowCollateral.aspx?oid=75286

- **New IBM Redpaper: Empowering Security and Compliance Management for the z/OS RACF Environment using IBM Tivoli Security Management for z/OS**

  http://www.redbooks.ibm.com/abstracts/redp4549.html?Open

Resources for you to use

- **“Zowee” zSecure demo video:**
  http://www.servicemanagementcenter.com/main/pages/IBMRBMS/SMRC/ShowCollateral.aspx?oid=77702

- **Tivoli Beat: IBM Tivoli zSecure: Leverage IBM System z as a Security Hub**

  http://www-01.ibm.com/software/tivoli/beat/12012009.html?cm_sp=MTE10097

- **Demo: IBM Tivoli Security Management for z/OS**

  http://www.servicemanagementcenter.com/main/pages/IBMRBMS/SMRC/ShowCollateral.aspx?oid=67410&S_CMP=rnav

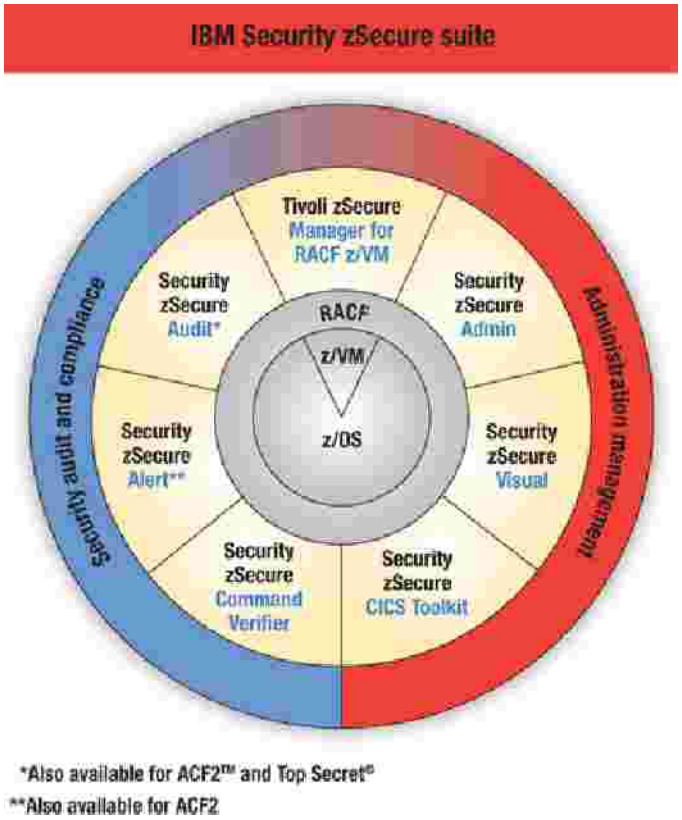
- **Redbooks: z/OS Mainframe Security and Audit Management using IBM Tivoli zSecure**

  http://www.redbooks.ibm.com/Redbooks.nsf/WebComment?OpenForm&ParentUNID=6A07891F5A43E3DC8525741000507EAA

zSecure suite Benefits

- Simplify administration and reduce the complexity of securing mainframes, making administrators more effective
- Enforce security policy to implement best security practices such as separation of duties
- Automate security event auditing and analysis to help anage risk and reduce threats and outages
- Enhance reporting capabilities to help auditors demonstrate compliance and pass audits
- Increase overall operational effectiveness and service management
- Reduce costs and improve return on investment

Questions



Contacts:

WW Product Manager – Glinda Cummings
glinda@us.ibm.com

External web page: located at http://www-01.ibm.com/software/tivoli/products/zsecure