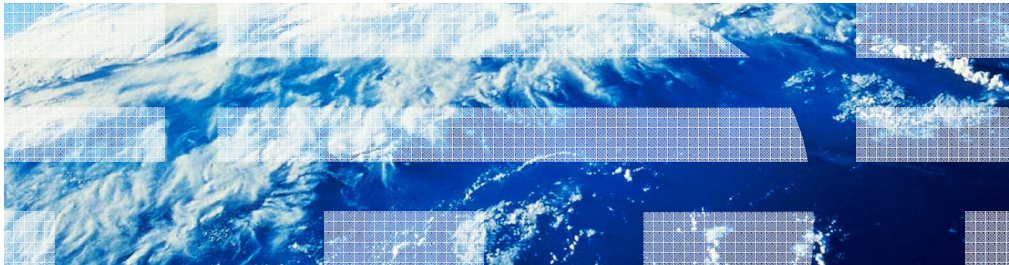


z/OS V1R13

RACF: New KERB segment field



Session objectives

- Describe function and value of new support
- Overview how function is implemented and how to exploit it
- List considerations when implementing support

Overview

- **Address checking in tickets**
- Problem Statement / Need Addressed
 - RFC4120 requires that addresses in tickets be validated prior to ticket use
 - For ease of migration must be implemented at the system level when installation is ready
- Solution
 - The Kerberos server will validate addresses in tickets prior to use if function is activated via RACF profile definition
 - A system wide switch is defined in RACF to control when function is active
- Benefit / Value
 - Higher level of security and compliance with RFC4120 set across the entire realm

Usage and invocation

- RDEFINE and RALTER commands updated to allow the installation to define whether or not address checking should be done in tickets via a keyword on the command:
 - **KERB([CHECKADDRS (YES | NO) | NOCHECKADDRS])**
 - The CHECKADDRS setting only has meaning on the REALM Class KRBDFLT profile
 - NOCHECKADDRS only allowed on RALTER
- R_Admin updated to support new field
- ISPF panels updated to support new field
- Database Unload updated to report on new field

Field Name	Flag Byte Values	RDEFINE/RALTER keyword reference	Allowed on ADD requests	Allowed on ALTER requests	Returned on Extract requests
CHKADDRS	'Y'	KERB(CHKADDRS(Y))	YES	YES	YES
	'N'	KERB(CHKADDRS(N))	YES	YES	
Field Name	Type	Length	Start	End	Description
GRKERB_CHKADDRS	YES/NO	3	620	623	Should the Kerberos server check addresses in tickets?

Interactions and dependencies

- Software Dependencies
 - None
- Hardware Dependencies
 - None
- Exploiters
 - Any installation activating address checking and running applications that request tickets with addresses

Installation, migration and coexistence considerations

- None

Session summary

- Description of function and value of new support
- Overview of how function is implemented and how to exploit it
- List of considerations when implementing support

Appendix

- Security Server RACF Callable Services (SA22-7691)
- Security Server RACF Command Language Reference (SA22-7687)
- Security Server RACF Macros and Interfaces (SA22-7682)
- Network Authentication Service Administration (SC24-5926)
- RFC4120 – The Kerberos Network Authentication Service (V5)



Trademarks, disclaimer, and copyright information

IBM, the IBM logo, ibm.com, RACF, and z/OS are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of other IBM trademarks is available on the web at "[Copyright and trademark information](http://www.ibm.com/legal/copytrade.shtml)" at <http://www.ibm.com/legal/copytrade.shtml>

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS OR SOFTWARE.

© Copyright International Business Machines Corporation 2012. All rights reserved.