

Securing and Encrypting Network Traffic with z/OS Communications Server and Policy Agent

Security Workshop

Agenda

Instructors: Linda Harrison (lharriso@us.ibm.com)



IBM Washington System Center
IBM Technical Sales Support

Trademarks

- **The following are Registered Trademarks of the International Business Machines Corporation in the United States and/or other countries.**
 - IBM
 - z/OS
 - **The following are trademarks or registered trademarks of other companies.**
 - Microsoft is a registered trademark of Microsoft Corporation in the United States and other countries.
 - All other products may be trademarks or registered trademarks of their respective companies.
 - Refer to www.ibm.com/legal for further legal information.
-
- OSA-Express Features
 - There are many different types of OSA-Express features. In this document where OSA is mentioned it refers to an OSA port on any of the OSA-Express/Network Express features unless a specific OSA-Express feature is mentioned.

Course Description

- This workshop is designed to give the student:
- An introduction to z/OS Communications Security Solutions;
- Experience in designing and building x.509 digital certificates to provide security for TLS and IPsec;
- Experience in creating AT-TLS, IPsec, and IDS Policies with z/OS Configuration Assistant and installing the policies to protect network traffic to and from z/OS;
- Experience in implementing Syslog Daemon, Policy Agent, and Traffic Regulation Management Daemon on z/OS managing security policies on z/OS;
- Insight into the differences among various security technologies, including OpenSSH, IPsec, SSL/TLS, and IDS.
- NOTE: The focus of the class is on z/OS Communications Server security technologies, and not on Kerberos or OpenSSH. There are no exercises with Kerberos or SSH.
- Audience:
- Technical Customers, IBMers, and Business Partners who need hands-on experience in building and implementing security policies on z/OS Communications Server.
- Prerequisites:
- Experience in managing and editing file structures on z/OS
- Intermediate to Advanced Experience in the implementation of TCP/IP - in z/OS Communications Server or other platforms
- Course Duration:
4 days:
8:00 AM - 5:00 PM (Day 1)
8:00 AM - 5:00 PM (Day 2)
8:00 AM - 5:00 PM (Day 3)
8:00 AM - 4:00 PM (Day 4)

Agenda

- 001_Security Architectures in IT
- 002_Overview of Security in z/OS Communications Server
- 003_Positioning SSH, TLS, and IPSec for Securing Traffic
 - Comparing File Transfer Methods: OpenSSH, TLS, IPSec, Managed File Transfer
 - LAB: L00_Lab Diagrams
 - LAB: L01_Intro to the Lab Environment
- 004_Implementation of Syslog Daemon
 - LAB: L02_Implementing SYSLOG Daemon on z/OS
- 005_Implementation of Policy Agent
 - LAB: L03_Implementing a Basic Policy Agent with QoS Policies on z/OS
- 006_The Role of x.509 Security Certificates in z/OS Communications Server
 - LAB: L04_Reviewing Certificate Repositories (z/OS, Workstation) and Cleaning Up Old Entries
 - LAB: L05_Analyzing x.509 Digital Security Certificates & Creating Certificates and Keyrings
 - OPTIONAL LAB: L06_Researching Common AT-TLS and x.509 Certificate Errors
- 007_Overview of SSL/TLS/AT-TLS: Concepts and Command Flows
 - LAB L07_Configuring an AT-TLS Policy for FTP Client and Server on z/OS with z/OSMF Network Configuration Assistant
 - Implementing FTP with preconfigured x.509 digital certificates
 - OPTIONAL LAB L08_Exporting Certificates, Configuring AT-TLS for TN3270, Testing TN3270 AT-TLS
 - Implementing labs with student-configured x.509 digital certificates
- 008_Protecting Traffic with IP Filtering
 - LAB: L09_Configuring Default Profile IP Filters and Policy Filters
- 009_Implementation of Traffic Regulation Management Daemon (TRMD)
 - LAB: L10_Implementing TRMD
 - LAB: L11_Implementing and Testing IP Filters in z/OS
- 010_Protecting Traffic with IPSec VPNs
 - LAB: L12_Configuring IPSec to Secure Traffic between Two z/OS Nodes Using RSA Signature Mode
 - Implementing labs using presconfigured x.509 Certificates
 - OPTIONAL LAB: L13_Researching Common IPSec and x.509 Certificate Errors
- 011_Overview of Intrusion Detection Services
 - LAB: L14_Configuring an IDS Policy to Protect z/OS Against Attacks, Scans, and Other Intrusions (Traffic Regulation)
 - LAB: L15_IPSec VPN Using Preshared Key
 - LAB: L16_Network Security Services Daemon (NSSD)
 - LAB: L17_Defense Manager Daemon (DMD)

References



Acknowledgments

- Gwen Dente for original course development, (retired) IBM Washington Systems Center
- Marilyn Allmond, (retired) IBM Cryptography support
- Wai Choi, IBM (zOS RACF Development)
- Alfred Christensen, (retired) IBM z/OS Communications Server Development
- Alyson Comer, IBM (z/OS System SSL Development)
- Erin Farr, IBM z/OS Development
- Christopher Meyer, IBM z/OS Communications Server Development
- Lin Overby, IBM Enterprise Networking Solutions
- Vicente Ranieri, IBM (Advanced Technical Support, System z Security)
- Mary Sweat, (retired) IBM Washington Systems Center
- Richard Theis, IBM Cloud Development

Web Pages

- URLs for Publications
 - <http://www.ibm.com/systems/z/os/zos/bkserv/index.html>
 - <http://www.redbooks.ibm.com>
- Main Security Web Pages:
 - https://www.ibm.com/think/topics/cybersecurity?mhsrc=ibmsearch_a&mhq=security
 - https://ec.europa.eu/info/law/law-topic/data-protection_en
 - <https://www.pcisecuritystandards.org/>
- IBM Mainframe Servers
 - <https://www.ibm.com/it-infrastructure/servers/mainframes>
- IBM Z Servers
 - <https://www.ibm.com/it-infrastructure/z>
- z/OS Communications Server and Performance Benchmarks
 - <http://www.ibm.com/support/docview.wss?uid=swg27005524>

Web Pages (cont.)

- PKI Services web site:
 - <https://www.ibm.com/docs/en/zos/3.1.0?topic=planning-introducing-pki-services>
- PKI Services Red Book:
 - <http://www.redbooks.ibm.com/abstracts/sg246968.html>
- IBM Washington Systems Center Technical Sales Support
 - <http://www.ibm.com/support/techdocs/>
- Request for Comment (RFC)
 - <http://www.rfc-editor.org/rfcsearch.html>
 - <http://www.rfc-editor.org/>

IBM Manuals

- IBM z/OS and z/OS Communications Server Manuals
 - z/OS Communications Server IP Configuration Guide (SC27-3650)
 - z/OS Communications Server IP Configuration Reference (SC27-3651)
 - z/OS IP Diagnosis Guide (GC27-3652)
 - z/OS IP System Administrator Commands (SC27-3661)
 - z/OS Four Volumes of IP Messages (SC27-3654, SC27-3655, SC27-3656, SC27-3657)
 - z/OS Migration Manual (GA32-0889)
 - z/OS System SSL Programming Guide (SC14-7495)
 - z/OS Integrated Cryptographic Services (ICSF) System Programmer Guide (SC14-7507)
 - z/OS Cryptographic Services PKI Services Guide and Reference (SA23-2286)
 - z/OS Security Server RACF Security Administrator's Guide (SA23-2289)
 - z/OS Security Server RACF Command Language Reference (SA23-2292)
 - z/OS UNIX System Services Planning (GA32-0884)
 - z/OS UNIX System Services User's Guide (SA23-2279)
 - z/OS UNIX System Services Command Reference (SA23-2280)
 - z/OS Management Facility (z/OSMF) Configuration Guide (SC27-8419)
 - z/OS Management Facility (z/OSMF) Programming (SC27-8420)
- z/OS Unix System Services OpenSSH
 - z/OS OpenSSH User's Guide (SC27-6806)
- RACF Command Samples for TCP/IP on z/OS
 - SYS1.TCPIP.SEZAINST(EZARACF)
- IBM RedBooks
 - Communications Server for z/OS TCP/IP Implementation
 - Volume I: Base Functions, Connectivity, and Routing (SG24-8360)
 - Volume II: Standard Applications (SG24-8361)
 - Volume III: High Availability, Scalability, and Performance (SG24-8362)
 - Volume IV: Security and Policy-based Networking (SG24-8363)

End of Topic

