1.	Record Nr.	UNINA9910816476403321
	Titolo	Security configuration in a TCP/IP Sysplex environment / / [Chris Rayns ... et al.]
	Pubbl/distr/stampa	Poughkeepsie, NY, : IBM, International Technical Support Organization, 2003
	Edizione	[1st ed.]
	Descrizione fisica	x, 248 p. : ill
	Collana	IBM redbooks
	Altri autori (Persone)	RaynsChris
	Disciplina	005.8
	Soggetti	Computer networks - Security measures TCP/IP (Computer network protocol)
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	"May 2003." "SG24-6527-00."
	Nota di bibliografia	Includes bibliographical references (p. 243-244) and index.
	Nota di contenuto	Front cover -- Contents -- Notices -- Trademarks -- Preface -- The team that wrote this redbook -- Become a published author -- Comments welcome -- Chapter 1. Review of z/OS operating system security -- 1.1 The threats -- 1.1.1 What is security? -- 1.1.2 Implementing the security mechanisms -- 1.2 Implementing security at the platform level -- 1.2.1 The MVS security approach -- 1.3 z/OS Security Server (RACF) -- 1.3.1 Identification and authentication -- 1.3.2 Alternatives to passwords -- 1.3.3 Checking authorization -- 1.3.4 RACF logging and reporting -- 1.3.5 RACF and z/OS UNIX System Services -- 1.4 Security in UNIX systems -- 1.4.1 Traditional UNIX security mechanisms -- 1.5 OS/390 and z/OS UNIX System Services security -- 1.5.1 UNIX-level security -- 1.5.2 z/OS UNIX System Services-level security -- 1.5.3 Brief review of the z/OS UNIX user's dual identity -- 1.5.4 Why z/OS UNIX System Services is a more secure UNIX -- 1.5.5 Access permission to HFS files and directories -- 1.5.6 Displaying files and directories -- 1.5.7 UID/GID assignment to a process -- 1.5.8 Defining UNIX System Services users -- 1.5.9 Default user -- 1.5.10 Superuser -- 1.5.11 Started task user IDs -- 1.5.12 FACILITY class profile BPX.SUPERUSER -- 1.5.13 FACILITY class profile BPX.DAEMON -- 1.5.14 Additional BPX.* FACILITY class profiles -- 1.5.15 Programs in the Hierarchical File System -- 1.5.16 z/OS UNIX

kernel address space -- 1.5.17 z/OS UNIX security considerations for TCP/IP -- 1.5.18 IBM-supplied daemons -- 1.5.19 MVS sockets server applications -- 1.5.20 Summary -- 1.6 Access control list (ACL) support for z/OS 1.3 -- 1.6.1 File access authorization checking -- 1.6.2 New UNIXPRIV profiles with z/OS V1R3 -- 1.6.3 ACL overview -- 1.6.4 Security product and ACLs -- 1.7 Enhancements for UID/GID support in z/OS 1.4 -- 1.7.1 RACF database and AIM.

1.7.2 Search enhancements to map UIDs and GIDs -- 1.7.3 Shared UID prevention -- 1.7.4 Automatic UID/GID assignment -- 1.7.5 Group ownership option -- Chapter 2. Overview of Parallel Sysplex technologies -- 2.1 Parallel Sysplex definition -- 2.1.1 Hardware -- 2.1.2 Software -- 2.1.3 SYS1.PARMLIB members used for sysplex setup -- 2.1.4 Couple data sets -- 2.1.5 Signaling -- 2.1.6 Structures within the coupling facility -- 2.1.7 Coupling Facility Resource Management (CFRM) -- 2.1.8 Sysplex Failure Management (SFM) -- 2.1.9 Automatic Restart Manager (ARM) -- 2.1.10 Workload Manager (WLM) -- 2.1.11 MVS System Logger -- 2.1.12 Global Resource Serialization (GRS) -- 2.1.13 Shared HFS -- 2.2 Advantages of a Parallel Sysplex -- 2.2.1 Determining the appropriate number of Parallel Sysplexes -- Chapter 3. Running ICSF in a Parallel Sysplex environment -- 3.1 zSeries integrated cryptography review -- 3.1.1 zSeries integrated cryptography implementation -- 3.1.2 The Master Key concept -- 3.1.3 LPAR domains and TKE -- 3.2 Sharing of CKDS and PKDS -- 3.3 Sharing CKDS and PKDS in a sysplex -- 3.3.1 Miscellaneous sysplex ICSF issues -- Chapter 4. Exploitation and protection of the coupling mechanisms -- 4.1 Coupling facility structure -- 4.1.1 Resource sharing -- 4.1.2 RACF data sharing -- 4.1.3 Data sharing -- 4.2 Couple data sets -- 4.2.1 Sysplex files -- 4.2.2 Authorizing use of IXCMIAPU utility -- 4.2.3 Authorizations for system logger applications -- 4.3 Sysplex Timer® -- 4.4 Sysplex operator commands protection -- 4.4.1 Console security -- 4.4.2 Command resource names -- Chapter 5. TCP/IP security in a sysplex configuration -- 5.1 TCP/IP in Parallel Sysplex -- 5.1.1 Supported connectivity protocols and devices -- 5.2 VIPA and Dynamic VIPA -- 5.3 Sysplex Distributor -- 5.3.1 Sysplex Distributor functionality -- 5.3.2 Backup capability -- 5.3.3 Recovery.

5.4 How dynamic routing works with the Sysplex Distributor -- 5.5 Sysplex Distributor and policy -- 5.6 Sysplex Distributor implementation -- 5.6.1 Requirements -- 5.6.2 Incompatibilities -- 5.6.3 Limitations -- 5.6.4 Implementation -- 5.7 Monitoring Sysplex Distributor -- Chapter 6. Securing the connection to the Internet -- 6.1 Our configuration -- 6.2 Implementing security at the network level -- 6.3 General discussion on Internet threats -- 6.4 What z/OS can do for you -- 6.4.1 Platform-level security - RACF -- 6.4.2 z/OS TCP/IP stack security -- 6.5 Exploiting the z/OS firewall technologies in a sysplex -- 6.6 IP filtering -- 6.6.1 z/OS IP Filtering and sysplex -- 6.6.2 IPSec Virtual Private Network -- 6.6.3 IPSec VPNs and Parallel Sysplex -- 6.7 Network security configurations -- 6.7.1 The demilitarized zone (DMZ) -- 6.7.2 Applicability of the DMZ principle to Parallel Sysplex -- 6.7.3 The shared HFS case -- 6.7.4 The sysplex and Denial of Services attack -- 6.7.5 TCP/IP classification -- 6.7.6 TCP/IP server classification -- Chapter 7. Intrusion detection services -- 7.1 Intrusion detection overview -- 7.1.1 Network-based intrusion detection -- 7.1.2 Host-based intrusion detection -- 7.2 The z/OS Intrusion Detection Services -- 7.2.1 Policy-based networking -- 7.2.2 The z/OS IDS policy -- 7.3 Preparing to run IDS -- 7.3.1 The z/OS Policy Agent (Pagent) -- 7.3.2 TRMD -- 7.3.3 SyslogD configuration -- 7.4 IDS policy definition and installation -- 7.4.1 The z/OS Communications Server policies schema -- 7.4.2 |The IDS policy definition -- 7.4.3 Policy object model -- 7.4.4

Policies for scan detection -- 7.4.5 Policies for attack detection and prevention -- 7.4.6 Policies for Traffic Regulation -- 7.4.7 Policy Rules samples -- 7.5 Putting the IDS policy to work -- 7.5.1 Starting TRMD and SyslogD -- 7.5.2 Loading the policies with Pagent.

7.5.3 pasearch utility -- 7.5.4 Netstat command and options -- 7.5.5 TRMDSTAT utility -- Chapter 8. IDS configuration using zIDS Manager -- 8.1 What a zIDS is -- 8.2 Requirements and support -- 8.2.1 Requirements -- 8.2.2 Support - Legal notice -- 8.3 Download and installation -- 8.3.1 Windows 2000 steps -- 8.3.2 Linux steps -- 8.4 Using the GUI -- 8.4.1 zIDS Manager configuration -- 8.4.2 PAGENT configuration -- 8.4.3 Work with IDS objects/rules -- 8.5 Policy priorities -- 8.5.1 Conjunctive Normal Form (CNF) policies -- 8.6 Additional information -- 8.6.1 Limitations -- 8.6.2 Common mistakes -- Related publications -- IBM Redbooks -- Other resources -- Referenced Web sites -- How to get IBM Redbooks -- IBM Redbooks collections -- Index -- Back cover.