1. Record Nr. UNINA9910824357103321

Titolo	Linux on IBM e-server zSeries and S/390 : best security practices / / [Gregory Geiselhart ... et al.]
Pubbl/distr/stampa	Poughkeepsie, NY, : IBM, International Technical Support Organization, c2004
Edizione	[1st ed.]
Descrizione fisica	xii, 164 p. : ill
Collana	IBM redbooks
Altri autori (Persone)	GeiselhartGregory
Disciplina	005.8
Soggetti	Operating systems (Computers) Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	"May 2004." "SG24-7023-00."
Nota di bibliografia	Includes bibliographical references 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. Introduction -- 1.1 Security goals -- 1.1.1 Security policy -- 1.2 Elements of security -- 1.2.1 Physical security -- 1.2.2 System security -- 1.2.3 Network security -- 1.3 System installation and backup -- 1.3.1 Verifying the RPM package -- Chapter 2. z/VM integrity and security -- 2.1 zSeries and z/VM system integrity -- 2.1.1 LPAR integrity -- 2.1.2 Integrity provided by the z/VM Control Program -- 2.2 zSeries network security -- 2.3 Securing your z/VM system -- 2.3.1 System integrity statement for z/VM -- 2.4 CP privilege classes -- 2.5 The z/VM SYSTEM CONFIG file -- 2.5.1 Enabling journaling -- 2.5.2 System features -- 2.5.3 Defining privilege classes -- 2.5.4 z/VM virtual networking -- 2.5.5 Configuring virtual networks -- 2.5.6 Redefining a command privilege class -- 2.6 The z/VM user directory -- 2.6.1 The USER directory entry statement -- 2.6.2 The INCLUDE statement -- 2.6.3 The IPL statement -- 2.6.4 The LOGONBY statement -- 2.6.5 The MDISK statement -- 2.6.6 The LINK statement -- 2.6.7 The DEDICATE statement -- 2.6.8 The OPTION statement -- 2.6.9 The SPECIAL statement -- 2.7 Directory Maintenance Facility -- 2.7.1 DirMaint security features -- 2.8 RACF for z/VM -- Chapter 3. Hardening a Linux installation -- 3.1 Linux system

logging -- 3.1.1 Configuring syslogd -- 3.1.2 Using a central log server -- 3.2 Pluggable Authentication Modules -- 3.2.1 PAM configuration files -- 3.2.2 Limiting superuser login to secure terminals -- 3.2.3 Restricting user login -- 3.2.4 Mandatory access control -- 3.2.5 Linux Security Module (LSM) -- 3.3 Delegating superuser authority with sudo -- 3.3.1 Configuring sudo -- 3.3.2 Using the sudo command -- 3.3.3 Command logging with sudo.
3.3.4 Security considerations with sudo -- 3.4 Securing Internet services with TCP_wrappers -- 3.4.1 TCP_wrappers access control specification -- 3.4.2 Configuring TCP_wrappers -- 3.5 Securing Linux using Bastille -- 3.5.1 Configuring security settings with Bastille -- 3.5.2 Reverting changes -- 3.5.3 Copying the Bastille setup to other hosts -- Chapter 4. Secure Sockets Layer and the Secure Shell -- 4.1 Introduction to Secure Sockets Layer -- 4.2 Enabling OpenSSL in Apache -- 4.2.1 Creating SSL keys -- 4.2.2 Generating an SSL certificate -- 4.2.3 Activating mod_ssl -- 4.2.4 Configuring mod_ssl -- 4.3 Using hardware acceleration with OpenSSL -- 4.3.1 Installing the crypto engine -- 4.3.2 Creating a crypto device node -- 4.3.3 Configuring mod_ssl to use the crypto engine -- 4.4 Secure Shell overview -- 4.5 Secure network access using SSH -- 4.5.1 Known hosts -- 4.5.2 SSH access control -- 4.6 File transfer and remote command execution -- 4.6.1 The scp command -- 4.6.2 The sftp command -- 4.6.3 Remote command execution using SSH -- 4.7 Authentication without passwords -- 4.8 Secure tunneling using port forwarding -- 4.8.1 Local port forwarding -- 4.8.2 Remote port forwarding -- 4.8.3 When to use local or remote forwarding -- 4.8.4 Implications of and options for port forwarding -- 4.9 X forwarding -- 4.9.1 Security considerations with X forwarding -- 4.10 Securing VNC using port forwarding -- 4.10.1 Installing the VNC server -- 4.10.2 Installing the VNC client on Windows -- 4.10.3 Installing an SSH server on Windows -- 4.10.4 Configuring the Windows SSH server -- 4.10.5 Creating a local forwarded tunnel from Windows to Linux -- 4.10.6 Connecting to the VNC server over the SSH tunnel -- Chapter 5. Implementing virtual private networks using FreeS/WAN -- 5.1 An overview of FreeS/WAN -- 5.1.1 Opportunistic encryption -- 5.2 Starting FreeS/WAN.
5.3 Configuring FreeS/WAN -- 5.3.1 Displaying public/private keys -- 5.3.2 Testing the IPSEC tunnel -- Chapter 6. StoneGate firewall -- 6.1 The role of firewalls -- 6.2 Firewall technologies -- 6.2.1 Packet filtering firewalls -- 6.2.2 Proxy firewalls -- 6.2.3 Stateful inspection firewalls -- 6.2.4 StoneGate and multi-layer inspection -- 6.2.5 Firewall functions -- 6.2.6 Requirements for modern firewalls -- 6.2.7 Firewall weaknesses -- 6.3 StoneGate firewall components -- 6.3.1 StoneGate GUI -- 6.3.2 Management system -- 6.3.3 Communications between the components -- 6.3.4 Network address translation between components -- 6.3.5 Secured communication -- 6.3.6 Certificate backups -- 6.3.7 Distributed management -- 6.3.8 Implementation strategies -- 6.4 StoneGate on Linux for zSeries -- 6.4.1 High availability technologies -- 6.4.2 Benefits of multilink technology -- 6.4.3 Applying multilink technology -- 6.5 StoneGate installation -- 6.5.1 The z/VM guest definition -- 6.5.2 Ensuring file integrity -- 6.5.3 Downloading the installation files to z/VM -- 6.5.4 Installing the firewall engine -- 6.5.5 Configuring the StoneGate firewall engine -- Chapter 7. Using z/OS features in a Linux environment -- 7.1 z/OS HiperSockets Accelerator -- 7.2 IBM Tivoli Access Manager for e-business -- 7.3 Authentication using IBM Tivoli Access Manager -- 7.3.1 Configuring LDAP on z/OS -- 7.3.2 Modifying the z/OS LDAP schema -- 7.3.3 Enabling z/OS LDAP native authentication -- 7.3.4 Installing Tivoli Access Manager Policy Director on Linux -- 7.3.5