1. Record Nr. UNINA9910815991903321

Titolo	Putting the latest z/OS security features to work / / [Chris Rayns ... et al.]
Pubbl/distr/stampa	[San Jose, Calif.?], : IBM International Technical Support Organization, 2002
Edizione	[1st ed.]
Descrizione fisica	xii, 278 p. : ill
Collana	Redbooks
Altri autori (Persone)	RaynsChris
Disciplina	005.8
Soggetti	Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	"June 2002." "SG24-6540-00."
Nota di bibliografia	Includes bibliographical references (p. 271-272) and index.
Nota di contenuto	Intro -- Chapter 1. z/OS 1.2 LDAP Directory enhancements -- 1.1 LDAP client enhancements -- 1.2 LDAP server enhancements -- 1.2.1 Server front-end performance/scalability -- 1.2.2 SDBM enhancements -- 1.2.3 TDBM Native authentication -- 1.2.4 Kerberos authentication -- 1.3 Miscellaneous changes -- Part 2 OS/390 2.10 enhancements -- Chapter 2. RACF enhancements -- 2.1 Program control enhancements -- 2.1.1 Overview -- 2.1.2 Introduction -- 2.1.3 Description -- 2.1.4 RACF services -- 2.1.5 Program Control enhancements example errors -- 2.2 Application Identity Mapping (AIM) -- 2.2.1 Overview -- 2.2.2 RACF utilities -- 2.2.3 AIM's purpose -- 2.2.4 Benefits of AIM -- 2.2.5 Migrating and installation of AIM -- 2.2.6 Stage enablement -- 2.2.7 Installation -- 2.2.8 Space requirements -- 2.2.9 When there are more than 130 user IDs with the same UID -- 2.2.10 New Serialization -- 2.3 Digital certificate enhancements -- 2.3.1 Digital certificate enhancements in Release 10 -- 2.3.2 Generating a digital certificate with RACF -- 2.3.3 Installing a RACF digital certificate into your browser -- 2.4 PKIServ - Web interface to certificate generation -- 2.4.1 Overview -- 2.4.2 Directory structure provided -- 2.4.3 The configuration file -- 2.4.4 User interface -- 2.4.5 Installation and configuration -- 2.5 OS/390 UNIX Superuser granularity support -- 2.6 Service Updates -- 2.6.1 APAR OW39128 -- 2.6.2 APAR OW38799 -- 2.6.3 APAR OW42092 -- 2.7 RVARY command enhancement -- 2.7.1

Introduction -- 2.7.2 Logical console security -- 2.7.3 RVARY console samples -- Chapter 3. Network Authentication and Privacy Service -- 3.1 Introduction to Kerberos -- 3.1.1 Kerberos protocol overview -- 3.1.2 Inter-realm operation -- 3.1.3 Some assumptions -- 3.2 Implementing NAPS -- 3.2.1 SKRBKDC daemon setup -- 3.2.2 Setting up the Kerberos environment variable files.
3.2.3 Setting up HFS for Kerberos cache files -- 3.3 Kerberos integrated with RACF -- 3.3.1 Defining RRSF in local mode -- 3.3.2 RACF setup for Kerberos realms -- 3.4 Kerberos principals -- 3.4.1 Local principals -- 3.4.2 Foreign principals -- 3.5 Kerberos commands -- 3.5.1 Description of the Kerberos commands -- 3.5.2 Kerberos command examples -- 3.6 Auditing -- 3.7 Windows 2000 use of Kerberos -- 3.8 Windows 2000 interoperation with OS/390 NAPS -- 3.8.1 Install Windows 2000 DNS server -- 3.8.2 Set up peer trust between the Kerberos realms -- 3.8.3 Define the 390 KDC to each Windows 2000 workstation -- 3.9 DB2 Version 7 usage of Kerberos -- 3.9.1 DB2 Connect Version 7.1 setup -- Part 3 LDAP and its use with other products -- Chapter 4. Policy Director usage of the LDAP server on z/OS -- 4.1 Test environment -- 4.1.1 z/OS LDAP server setup -- 4.1.2 Policy Director Setup -- Chapter 5. IBM Host On-Demand Version 6 -- 5.1 LDAP native authentication -- 5.1.1 Native authentication requirements -- 5.1.2 Installation of native authentication -- 5.1.3 Starting and stopping native authentication services -- 5.1.4 Working with native authentication -- 5.1.5 Problem determination -- 5.2 Telnet-negotiated security -- 5.2.1 Session negotiation -- 5.3 Express logon feature -- 5.3.1 Overview -- 5.3.2 The RACF-secured sign-on PassTicket -- 5.3.3 Configuring the TN3270 server -- 5.3.4 Configuring the client -- 5.3.5 Installing the client certificate into the browser -- Chapter 6. z/OS 1.2 LDAP/WebSphere Application Server -- 6.1 LDAP and WebSphere 4.0.1 -- 6.2 WebSphere Application Server 4.0.1 overview -- 6.2.1 Installing WebSphere Application Server 4.0.1 -- 6.2.2 WebSphere Application Server 4.0.1 and LDAP -- 6.2.3 Installation dialog -- 6.2.4 Problems encountered and lessons learned -- 6.3 Migrating WebSphere Application Server 4.0.1 from RDBM to TDBM.
6.3.1 Migrating existing RDBM data to a TDBM database -- 6.3.2 Setting up the schema for TDBM -- 6.3.3 Restarting WebSphere Application Server after TDBM migration -- 6.3.4 Tips and recommendations for debugging/tracing -- Chapter 7. LDAP server on z/OS -- 7.1 Input file description -- 7.1.1 Customizing ldap.profile -- 7.1.2 Customizing ldap.db2.profile -- 7.1.3 Customizing ldap.racf. profile -- 7.1.4 Customizing ldap.slapd.profile -- 7.2 Starting the ldapcnf utility -- 7.3 Executing system and RACF jobs -- 7.3.1 Update proclib -- 7.3.2 Update PARMLIB -- 7.3.3 Execute RACF jobs -- 7.4 Executing DB2 jobs -- 7.5 Start the LDAP server -- 7.6 Finalize setup of LDAP server -- 7.6.1 Load schemas -- 7.6.2 Load the suffix entry for the TDBM backend -- 7.6.3 Verify configuration -- 7.7 Implementing password encryption with z/OS LDAP -- Chapter 8. LDAP with RACF digital certificates -- 8.1 Preparing to use RACDCERT commands -- 8.2 Server authentication -- 8.3 Client Authentication -- Chapter 9. Overview of security on Linux -- 9.1 Disable unneeded services -- 9.2 Use Secure Shell for remote access -- 9.3 Use shadow password utilities -- 9.4 Use the Pluggable Authentication Module (PAM) -- 9.5 Monitor security news and alerts -- 9.6 Use hardening tools -- 9.7 Integrate VM and z/VM security -- Appendix A. Notes about using SDBM with the LDAP Server -- Related publications -- IBM Redbooks -- Other resources -- Referenced Web sites -- How to get IBM Redbooks -- IBM Redbooks collections -- Index -- Back cover.