

1. Record Nr.	UNINA9910816215203321
Autore	Tuttle Steven
Titolo	AIX 5L version 5.2 security supplement // Steven Tuttle, Gabriel Pizano, Chris Smith
Pubbl/distr/stampa	Austin, TX, : IBM Corp., International Technical Support Organization, c2003
Descrizione fisica	1 online resource (198 p.)
Collana	Redbooks
Altri autori (Persone)	PizanoGabriel SmithChris
Soggetti	Operating systems (Computers)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	"November 2003."
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. AIX security flashes -- 1.1 Recommended reading -- 1.2 Security flash information by e-mail -- 1.3 Obtaining fixes -- Chapter 2. Virtual private networks -- 2.1 Architecture -- 2.2 Security -- 2.2.1 Transport mode -- 2.2.2 Tunnel mode -- 2.2.3 Security parameter index -- 2.2.4 Security associations -- 2.2.5 Filter rules -- 2.2.6 Encapsulating Security Payloads -- 2.2.7 Authentication Header -- 2.2.8 Key management -- 2.2.9 Security features -- 2.3 Installing IPsec -- 2.3.1 Installing the IP Security feature -- 2.3.2 Enabling IPsec offload -- 2.3.3 Starting IP Security -- 2.3.4 Installation Verification Procedure -- 2.4 Using administration interfaces -- 2.4.1 Starting IPsec -- 2.4.2 Stopping IPsec -- 2.4.3 IKE tunnels using SMIT -- 2.4.4 IKE tunnels using Web-based System Manager -- 2.4.5 Using certificates -- 2.4.6 Manual tunnels using the System Management Interface Tool -- 2.4.7 Filtering through the System Management Interface Tool -- 2.5 Functionality -- 2.5.1 Scenario I -- 2.5.2 Scenario II -- 2.5.3 Scenario III -- 2.5.4 Scenario IV -- 2.5.5 Scenario V -- 2.5.6 Scenario VI -- 2.6 Differences and limitations -- 2.7 Event and alert management -- 2.8 Common problems and solutions -- 2.8.1 Activation failure of the tunnel -- 2.8.2 Pinging from a non-secure machine to a secured machine hangs

-- 2.8.3 Cannot ping from a secured machine to a non-secure machine
-- 2.8.4 Network address translation doesn't work in IPSec environments -- 2.8.5 Firewall doesn't work in IPSec environments --
2.8.6 Cannot connect two machines where tunnels used to be active --
2.8.7 Both tunnels activated but there is no active/negotiating in the IKE tunnel monitor.
2.8.8 Can no longer connect from a non-secure machine to a secure machine with the tunnel active -- 2.8.9 IP security started but IKE command does not work -- 2.8.10 isakmpd is not running -- 2.8.11 The IKE subsystem group is inoperative -- 2.8.12 Tunnels are in a dormant state after running ike cmd=activate -- 2.8.13 Editing tunnel information with Web-based System Manager panels differs from ike cmd=list db verbose -- 2.8.14 Cannot activate a tunnel because the remote ID is invalid -- 2.8.15 General procedure to obtain the cause of problems -- Chapter 3. Exploiting Network Authentication Service --
3.1 Architecture -- 3.1.1 Recommended reading -- 3.1.2 Ease-of-use example -- 3.2 Security -- 3.3 Installation example -- 3.3.1 Planning -- 3.3.2 Installation -- 3.3.3 Configuring the server -- 3.3.4 Configuring the client -- 3.3.5 Creating the keytab file -- 3.3.6 Kerberos administration -- 3.3.7 Changing authentication methods to allow Kerberos -- 3.3.8 Obtaining Kerberos authentication for administration -- 3.3.9 Creating a test user -- 3.3.10 Testing the user and services -- 3.3.11 Configuring another client system -- 3.3.12 Testing the user and services on the new host -- 3.4 Administration --
3.4.1 AIX -- 3.4.2 Network Authentication Service -- 3.5 Functions --
3.5.1 Integrated login -- 3.5.2 Secure remote commands -- 3.5.3 User management commands -- 3.6 Differences and limitations -- 3.7 Event and alert management -- 3.8 Common problems and solutions --
3.8.1 Checklist -- 3.8.2 Logs -- 3.8.3 Typical problems -- Chapter 4. Pluggable Authentication Module -- 4.1 Architecture -- 4.1.1 PAM library -- 4.1.2 PAM modules -- 4.1.3 PAM configuration file -- 4.1.4 Recommended reading -- 4.2 Security -- 4.2.1 Security issues -- 4.3 Installing and configuring PAM -- 4.3.1 Installing PAM for AIX (pam_aix) -- 4.3.2 Installing PAM for LDAP (pam_ldap).
4.4 Common problems and solutions -- 4.4.1 Enabling PAM debug -- Chapter 5. Restricting users -- 5.1 Restricted shells -- 5.1.1 Recommended reading -- 5.1.2 Configuring the system and creating a restricted shell user -- 5.2 User limits for a system resource -- 5.2.1 Architecture -- 5.2.2 Security -- 5.2.3 Resources -- 5.2.4 Administration -- 5.3 User login controls -- 5.3.1 Setting up login controls -- 5.3.2 Changing the welcome message on the login display -- 5.3.3 Changing the login display for the CDE -- 5.3.4 Securing unattended terminals -- 5.3.5 Enforcing automatic logoff -- 5.4 Preventing denial-of-service attacks -- Appendix A. AIX Security Planning and Implementation Worksheet -- Abbreviations and acronyms -- Related publications -- IBM Redbooks -- Other publications -- Online resources -- How to get IBM Redbooks -- Help from IBM -- Index -- Back cover.

Sommario/riassunto

This IBM Redbooks publication serves as a supplement to the IBM AIX 5L Version 5.2 product documentation, particularly "AIX 5L Version 5.2 Security Guide", SC23-4860. This book provides additional detailed information about virtual private networks (VPN), Kerberos security and the use of secure remote commands (RCMDS), Pluggable Authentication Modules (PAM), and examples on how to restrict users. You can use these features individually or integrate them together to improve AIX system security. Use this book as an additional source for security information. Together with existing sources, you may use this book to enhance your knowledge of security and the features included with AIX

5L Version 5.2. You learn about the practical use of these security features, why they are necessary, and how you can use them in your environment to improve security. Plus you gain practical guidance through the examples that are provided and the recommendations for best practice.
