1. Record Nr. UNINA9910816209003321

Titolo	Identity and access management solutions : using WebSphere Portal V5. 1, Tivoli Identity Manager V4.5.1, and Tivoli Access Manager V5.1 / / John Ganci ... [et al.]
Pubbl/distr/stampa	Research Triangle Park, N.C., : IBM, International Technical Support Organization, 2005
Edizione	[1st ed.]
Descrizione fisica	xviii, 608 p. : ill
Collana	Redbooks
Altri autori (Persone)	GanciJohn
Soggetti	Web portals - Security measures Computer networks - Security measures Computers - Access control
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	"August 2005." "This edition applies to IBM Tivoli Identity Manager V4.5.1, IBM Tivoli Access Manager V5.1 for e-business, IBM Tivoli Directory Server V5.2, IBM Tivoli Directory Integrator V6.0, IBM WebSphere Portal V5.1, IBM DB2 Content Manager V8.3, Enterprise Edition, and IBM Rational Application Developer V6.0.0.1 on the Microsoft Windows platform."
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 -- Part 1 Introduction to identity and access management -- Chapter 1. Introduction -- 1.1 Introduction to identity and access management -- 1.1.1 Key concepts -- 1.1.2 High level solution architecture -- 1.2 Solution software -- 1.2.1 Runtime environment solution software -- 1.2.2 Development environment solution software -- 1.3 Target audience -- 1.3.1 Roles and skills -- 1.3.2 Matching redbook topics to roles and skills -- Chapter 2. Architecture and design guidelines -- 2.1 Operational modeling guidelines -- 2.1.1 Operational model overview -- 2.1.2 Topology zones -- 2.1.3 Application architecture components -- 2.1.4 Product mapping -- 2.1.5 Runtime environment topology selection -- 2.1.6 Development environment topology selection -- 2.2 Design principles -- 2.2.1 Centralized authority -- 2.2.2 Access decision evaluated on

demand -- 2.2.3 Capture authentication events and logs -- 2.3 User provisioning guidelines -- 2.3.1 Identity management overview -- 2.3.2 Common LDAP directory -- 2.3.3 Tivoli Identity Manager services, workflows, and policies -- 2.3.4 Tivoli Directory Integrator assembly lines -- 2.3.5 Tivoli Directory Integrator connectors -- 2.4 Single sign-on authentication guidelines -- 2.4.1 WebSphere Portal authentication -- 2.4.2 DB2 Content Manager authentication -- 2.4.3 Single sign-on for WebSphere Portal and Content Manager -- 2.4.4 Single sign-on authentication using Tivoli Access Manager -- 2.5 Authorization guidelines -- 2.5.1 WebSphere Portal authorization -- 2.5.2 DB2 Content Manager authorization -- 2.5.3 Tivoli Access Manager authorization -- 2.5.4 WebSphere Portal vs. Tivoli Access Manager authorization -- 2.6 Product-specific integration guidelines -- 2.6.1 WebSEAL junctions.
2.6.2 Junction considerations for use with TAI -- 2.6.3 Handling of back-end application cookies -- 2.6.4 Junction Mapping Table (JMT) -- 2.6.5 WebSEAL URL-based access control -- 2.6.6 Access control of WebSphere Portal resources -- 2.6.7 Access control of resources within portlet applications -- 2.6.8 WebSEAL and WebSphere Portal session considerations -- 2.7 Sequence diagrams for common access patterns -- 2.7.1 UCT1: Access unprotected portal page -- 2.7.2 UCT2: Access protected portal page, provide valid credentials -- 2.7.3 UCT3: Access protected portal page with existing valid session -- 2.7.4 UCT4: Access protected portal page with invalid credentials -- 2.7.5 UCT5: WebSEAL session times out before portal session -- 2.7.6 UCT6: Portal session times out before WebSEAL session -- 2.7.7 UCT7: Both WebSEAL and WebSphere Portal sessions time out -- 2.7.8 UCT8: WebSphere Portal logout after WebSEAL session timeout -- Part 2 ITSO identity and access management working example -- Chapter 3. Requirements analysis and solution design -- 3.1 Business scenario -- 3.1.1 Initial context -- 3.1.2 Business challenges -- 3.2 Business requirements -- 3.2.1 Functional requirements -- 3.2.2 Non-functional requirements -- 3.3 Use case model -- 3.3.1 Use case overview -- 3.3.2 Use case details -- 3.4 Solution architecture -- 3.4.1 Architecture overview -- 3.4.2 Architectural decisions -- 3.4.3 Solution architecture details -- 3.4.4 Runtime topology and product mapping -- 3.4.5 Development environment topology and product mapping -- Chapter 4. Runtime environment installation -- 4.1 Planning -- 4.1.1 Hardware and software prerequisites -- 4.1.2 Hardware used within the ITSO runtime environment -- 4.1.3 Software used within the ITSO runtime environment -- 4.2 Directory node installation -- 4.2.1 Windows 2000 Server installation.
4.2.2 DB2 Universal Database V8.2 installation -- 4.2.3 IBM GSKit installation -- 4.2.4 WebSphere Application Server V5.0.2 installation -- 4.2.5 Tivoli Directory Server V5.2 installation -- 4.2.6 Tivoli Directory Server configuration -- 4.2.7 Tivoli Web Administration Tool configuration -- 4.2.8 Tivoli Directory Integrator installation -- 4.2.9 DB2 Information Integrator for Content installation -- 4.3 Access Manager node installation -- 4.3.1 Windows 2000 Server installation -- 4.3.2 IBM Java Runtime Environment (JRE) V1.3.1 installation -- 4.3.3 IBM GSKit installation -- 4.3.4 Tivoli Directory Client SDK 5.2 installation -- 4.3.5 WebSphere Application Server V5.0.2 installation -- 4.3.6 Configure Directory Server for Tivoli Access Manager -- 4.3.7 Tivoli Access Manager installation -- 4.3.8 Tivoli Access Manager configuration -- 4.3.9 Tivoli Access Manager Web Portal Manager installation -- 4.3.10 Tivoli Access Manager V5.1 Base Fixpack 9 installation -- 4.3.11 Configure Web Portal Manager -- 4.3.12 Verify the Web Portal Manager -- 4.3.13 Tivoli Identity Manager Agent for

modify URLs to back-end systems -- 5.6.6 Configure additional WebSEAL parameters -- 5.6.7 Import WebSphere Portal users and groups into TAM -- 5.6.8 Define access controls for WebSphere Portal URIs -- 5.6.9 Configure the junction mapping table (JMT) -- 5.6.10 Configure SSO for WebSEAL and WebSphere via TAI -- 5.6.11 Configure Portal login/logout for use with WebSEAL -- 5.7 Configure WebSphere Portal authorization with TAM -- 5.7.1 Configure SSL between WebSphere and TAM -- 5.7.2 Configure WebSphere Portal authorization for TAM -- 5.7.3 Verify entries in TAM for Portal external authorization -- 5.8 Configure reverse password synchronization. 5.8.1 Prerequisites.