

Oracle Database Security In The Cloud

The Definitive Guide to Oracle Database 11g Get full details on the powerful features of Oracle Database 11g from this thoroughly updated Oracle Press guide. Oracle Database 11g: The Complete Reference explains how to use all the new features and tools, execute powerful SQL queries, construct PL/SQL and SQL*Plus statements, and work with large objects and object-relational databases. Learn how to implement the latest security measures, tune database performance, and deploy grid computing techniques. An invaluable cross-reference appendix containing Oracle commands, keywords, features, and functions is also included. Install Oracle Database 11g or upgrade from an earlier version Create database tables, sequences, indexes, views, and user accounts Construct SQL statements, procedures, queries, and subqueries Optimize security using virtual private databases and transparent data encryption Import and export data using SQL*Loader and Oracle Data Pump

Use SQL replay, change management, and result caching Avoid human errors using flashback and automatic undo management Build and tune PL/SQL triggers, functions, and packages Develop database applications using Java, JDBC, and XML Optimize availability and scalability with Oracle Real Application Clusters

Threats to security are increasing in sophistication and frequency. Organizations have both an ethical and oftentimes a legal responsibility to understand the countermeasures available, to compare these against the threats to which they are exposed, and to properly apply such countermeasures. This Oracle 11g training course module considers how encryption technology should, and should not, be employed within an Oracle database environment in response to known threats and risks. It will also discuss other best security practices which pertain to application security, host system configuration and the database installation. Within this training course guidebook we will discuss these topics:- Consider examples of common security threats and sensitive data which might exist within an organization; Review the essentials of a sound and secure database installation;- Consider known database security weaknesses and how these may be addressed;- Consider examples of specific attacks which could be launched against individual components within a data center or within the public networks;- Review the theory and concepts which underlie symmetric and asymmetric encryption;- Consider the primary elements involved in asymmetric encryption, including private and public keys, the Public Key Infrastructure, certificates, Certificate Authorities and wallets;- Discuss how symmetric or asymmetric encryption is applied to network traffic, database storage and external files; Consider the limits of encryption strategies and when encryption could be misapplied and counterproductive;- Discuss the challenges and options available for encryption key storage;- Apply Transparent Data Encryption (TDE) to tablespaces, column, export file, RMAN backup set file and SecureFile LOB encryption;- Use the Oracle Data Pump access driver to encrypt external tables;- Configure Oracle Net Services to repel database attacks and implement advanced security using encrypted network communication;- Implement an application-based encryption solution using the DBMS_CRYPTO() package;- Review the types of attacks which can be launched using SQL injection, and which countermeasures should be applied to repel these;- Implement enhanced application security using the Virtual Private Database (VPD) facility.

This Oracle Press eBook is filled with cutting-edge security techniques for Oracle Database 12c. It covers authentication, access control, encryption, auditing, controlling SQL input, data masking, validating configuration compliance, and more. Each chapter covers a single threat area, and each security mechanism reinforces the others.

Protecting Oracle Database 12c helps you solve the problem of maximizing the safety, resilience, and security of an Oracle database whilst preserving performance, availability, and integration despite ongoing and new security issues in the software. The book demonstrates, through coded examples, how you can enable the consolidation features of Oracle Database 12c without increasing risk of either internal corruption or external vulnerability. In addition, new protections not publicly available are included, so that you can see how demonstrable risk improvements can be achieved, measured, and reported through Enterprise Manager 12c. Most importantly, the challenge of privileged access control within a consolidation environment will be addressed, thus enabling a safe move to greater efficiency.

Implementing Database Security and Auditing

Security, Audit and Control Features

Oracle Incident Response and Forensics

Oracle Database Security, Audit and Control Features

Oracle Database 11g R2

This practical book for PHP/Oracle developers is built around well explained, easy-to-follow example code to build robust, efficient, secure solutions covering popular current topics on using PHP with Oracle. Assuming no special skill level, experienced author Yuli Vasilev shows how to install and configure PHP and Oracle; connect PHP to Oracle; move application business logic to Oracle; build transactional applications; use security features; improve performance with caching; employ XML features; implement SOAP web services; build Ajax-driven PHP/Oracle solutions. Building and deploying PHP applications on Oracle Database combines the power and robustness of Oracle with the easy, rapid development of open-source PHP to achieve high-performance, scalable, reliable data-driven web applications with minimal effort. Unlike some other databases, Oracle allows building the key business logic of PHP applications inside the database, moving data processing from web server to database server.

Secure your Oracle Database 12c with this valuable Oracle support resource, featuring more than 100 solutions to the challenges of protecting your data>About This Book Explore and learn the new security features introduced in Oracle Database 12c, to successfully secure your sensitive data Learn how to identify which security strategy is right for your needs - and how to apply it! Each recipe provides you with a single step-by-step solution, making this book a vital resource, delivering Oracle support in one accessible placeWho This Book Is ForThis book is for DBAs, developers, and architects who are keen to know more about security in Oracle Database 12c. This book is best suited for beginners and intermediate-level database security practitioners. Basic knowledge of Oracle Database is expected, but no prior experience of securing a database is required.What You Will Learn Analyze application privileges and reduce the attack surface Reduce the risk of data exposure by using Oracle Data Redaction and Virtual Private Database Control data access and integrity in your organization using the appropriate database feature or option! Learn how to protect your databases against application bypasses! Audit user activity using the new auditing architecture Restrict highly privileged users from accessing data Encrypt data in Oracle Database Work in a real-world environment where a multi-layer security strategy is applied!DetailedBusinesses around the world are paying much greater attention toward database security than they ever have before. Not only does the current regulatory environment require tight security, particularly when dealing with sensitive and personal data, data is also arguably a company's most valuable asset - why wouldn't you want to protect it in a secure and reliable database? Oracle Database lets you do exactly that. It's why it is one of the world's leading databases - with a rich portfolio of features to protect data from contemporary vulnerabilities, it's the go-to database for many organizations.Oracle Database 12c: Security Cookbook helps DBAs, developers, and architects to better understand database security challenges. Let it guide you through the process of implementing appropriate security mechanisms, helping you to ensure you are taking proactive steps to keep your data safe. Featuring solutions for common security problems in the new Oracle Database 12c, with this book you can be confident about securing your database from a range of different threats and problems.

Expert Oracle and Java Security: Programming Secure Oracle Database Applications with Java provides resources that every Java and Oracle database application programmer needs to ensure that they have guarded the security of the data and identities entrusted to them. You'll learn to consider potential vulnerabilities, and to apply best practices in secure Java and PL/SQL coding. Author David Coffin shows how to develop code to encrypt data in transit and at rest, to accomplish single sign-on with Oracle proxy connections, to generate and distribute two-factor authentication tokens from the Oracle server using pagers, cell phones (SMS), and e-mail, and to securely store and distribute Oracle application passwords. Early chapters lay the foundation for effective security in an Oracle/Java environment. Each of the later chapters brings example code to a point where it may be applied as-is to address application security issues. Templates for applications are also provided to help you bring colleagues up to the same secure application standards. If you are less familiar with either Java or Oracle PL/SQL, you will not be left behind; all the concepts in this book are introduced as to a novice and addressed as to an expert. Helps you protect against data theft, identity theft, SQL injection, and address spoofing Provides techniques for encryption on network and disk, code obfuscation and wrap, database hardening, single sign-on and two-factor Provides what database administrators need to know about secure password distribution, Java security programming, Java stored procedures, secure application roles in Oracle, login triggers, database design, various connection pooling schemes, and much more

Oracle Database 12c Security Cookbook is a multi-tiered web application environments, the criticality of protecting the database has grown at a tremendous rate. The confidentiality, integrity and availability requirements of the database tier are at an all time high because employees, customers and business partners demand access to data in an immediate and consistent manner. Further, the reality and awareness of security risks are growing, resulting in higher security expectations. As a result, more focus is directed toward auditing databases to ensure that there are appropriate safeguards in place to protect against reasonably foreseeable threats. This book provides guidance on Oracle Database including: Understanding the IT environment, and developing a strategy to properly plan the Oracle audit Security and Access control related to the Oracle environment A suggested security and control framework A detailed general controls approach, along with specifics on application level security An internal control questionnaire and audit program linked to COBIT A list of frequently asked questions/answers, and recommendations for the professional A list of automated assessment tools available. Call +1.847.253.1545 ext. 401, visit www.isaca.org/bookstore or e-mail bookstore@isaca.org for more information.

Expert Oracle Practices

Your Unauthorized Guide to Relational Database Security

Data Processing, Security, Caching, XML, Web Services, and Ajax

Oracle Database Administration from the Oak Table

Securing Oracle Database 12c: A Technical Primer eBook

Oracle Quick Guides Part 4 - Oracle Administration: Security and Privilege

Everything a DBA needs to know in one volume--this is the must-have reference for anyone working with the Oracle database, and it's been fully revised and updated for Oracle Database 10g. Co-author Kevin Loney is the all-time, best-selling Oracle Press author.

PL/SQL, Oracle's powerful procedural language, has been the cornerstone of Oracle application development for nearly 15 years. Although primarily a tool for developers, PL/SQL has also become an essential tool for database administration, as DBAs take increasing responsibility for site performance and as the lines between developers and DBAs blur. Until now, there has not been a book focused squarely on the language topics of special concern to DBAs Oracle PL/SQL for DBAs fills the gap. Covering the latest Oracle version, Oracle Database 10g Release 2 and packed with code and usage examples, it contains: A quick tour of the PL/SQL language, providing enough basic information about language fundamentals to get DBAs up and running Extensive coverage of security topics for DBAs: Encryption (including both traditional methods and Oracle's new Transparent Data Encryption, TDE); Row-Level Security(RLS), Fine-Grained Auditing (FGA); and random value generation Methods for DBAs to improve query and database performance with cursors and table functions Coverage of Oracle scheduling, which allows jobs such as database monitoring and statistics gathering to be scheduled for regular execution Using Oracle's built-in packages (DBMS_CRYPTO, DBMS_RLS, DBMS_FGA, DBMS_RANDOM,DBMS_SCHEDULING) as a base, the book describes ways of building on top of these packages to suit particular organizational needs. Authors are Arup Nanda, Oracle Magazine 2003 DBA of the Year, and Steven Feuerstein, the world's foremost PL/SQL expert and coauthor of the classic reference, Oracle PL/SQL Programming. DBAs who have not yet discovered how helpful PL/SQL can be will find this book a superb introduction to the language and its special database administration features. Even if you have used PL/SQL for years, you'll find the detailed coverage in this book to be an invaluable resource.

Cutting-edge techniques from leading Oracle security experts This Oracle Press guide demonstrates practical applications of the most compelling methods for developing secure Oracle database and middleware environments. You will find full coverage of the latest and most popular Oracle products, including Oracle Database and Audit Vaults, Oracle Application Express, and Secure Business Intelligence applications. Applied Oracle Security demonstrates how to build and assemble the various Oracle technologies required to create the sophisticated applications demanded in today's IT world. Most technical references only discuss a single product or product suite. As such, there is no roadmap to explain how to get one product, product-family, or suite to work with another. This book fills that void with respect to Oracle Middleware and Database products and the area of security.

This is Part 4 of a series of quick learning guides for Oracle administrators, designers, developers and managers. Part 4 introduces early entrants with basic Oracle skills to the main concepts of Oracle data security and user privilege management and administration. The guide includes details of how to create and how to manage users and their database object and system access and rights. The guide also provides a basis for understanding different database security strategies such as role-based security, virtual private databases and procedure-based security. Part 4 contains a glossary of Oracle terminology related to database security and user privilege administration with clear explanations of the terms used. These guides are designed to rapidly deliver key information about Oracle to the following audience groups: - Project Managers, Database Administrators, Team Leaders, and Testers who are new to Oracle and need rapid access to strategic information about the Oracle security environment in both development and production databases. - Business Analysts, Software Designers and Developers who are new to Oracle and need to gain a detailed understanding of the data security and administration issues involved in an Oracle database. Part 4 of these guides assumes that the reader has read Parts 1, 2 and 3 of the Oracle Quick guides or their equivalent content. The contents of Part 4 include the following subject headings: 1. Oracle Database Security Architecture 2. Managing Oracle User Security 3. Managing Privileges and Roles 4. Managing Profiles 5. Managing Passwords with Profiles 6. Special Users and Privileges - SYS, SYSTEM, SYSDBA, SYSOPER 7. Managing Developer Security 8. Virtual Private Databases (VPD) 9. Procedure Execution Security 10. Data Security using Views 11. Tool Security - PRODUCT_USER_PROFILE Table 12. Obtaining Security Information from the Data Dictionary 13. Glossary of Terms Appendix 1 - Common System Privileges Appendix 2 - SYSDBA and SYSOPER Privileges Appendix 3 - SQL commands which can be disabled

Protecting Data Accessibility and Availability

Preparing for and Responding to Data Breaches

Programming Secure Oracle Database Applications With Java

Oracle Privacy Security Auditing

Oracle Security Interview Questions, Answers, and Explanations

Oracle PL/SQL for DBAs

Oracle security expert David Knox explains how to design and develop an integrated, secure Oracle environment. "In my experience in the security world, including 32 years at the Central Intelligence Agency, I've not found anyone with more experience in the theory and practice of protecting your data than David Knox." -Dave Carey, former Executive Director of the CIA

This book is an anthology of effective database management techniques representing the collective wisdom of the OakTable Network. With an emphasis upon performance—but also branching into security, national language, and other issues—the book helps you deliver the most value for your company's investment in Oracle Database technologies. You'll learn to effectively plan for and monitor performance, to troubleshoot systematically when things go wrong, and to manage your database rather than letting it manage you.

Oracle is the number one database engine in use today. The HOWTO that it is the choice of military organizations and agencies around the world is part of the company's legacy and is evident in the product. Oracle has more security-related functions, products, and tools than almost any other database engine. Unfortunately, the fact that these capabilities exists does not mean that they are used correctly or even used at all. In fact, most users are familiar with less than twenty percent of the security mechanisms within Oracle. Written by Ron Ben Natan, one of the most respected and knowledgeable database security experts in the world, HOWTO Secure and Audit Oracle 10g and 11g shows readers how to navigate the options, select the right tools and avoid common pitfalls. The text is structured as HOWTOs addressing each security function in the context of Oracle 11g and Oracle 10g. Among a long list of HOWTOs, readers will learn to: Choose configuration settings that make it harder to gain unauthorized access Understand when and how to encrypt data-at-rest and data-in-transit and how to implement strong authentication Use and manage audit trails and advanced techniques for auditing Assess risks that may exist and address them Make use of advanced tools and options such as Advanced Security Options, Virtual Private Database, Audit Vault, and Database Vault The text also provides an overview of cryptography, covering encryption and digital signatures and shows readers how Oracle Wallet Manager and orapki can be used to generate and manage certificates and other secrets. While the book's seventeen chapters follow a logical order of implementation, each HOWTO can be referenced independently to meet a user's immediate needs. Providing authoritative and succinct instructions highlighted by examples, this ultimate guide to security best practices for Oracle bridges the gap between those who install and configure security features and those who secure and audit them.

Take the right steps when a breach of your Oracle Database environment becomes known or suspected. You will learn techniques for discerning how an attacker got in, what data they saw, and what else they might have done. This book helps you understand forensics in relation to Oracle Database, and the tools and techniques that should be used to investigate a database breach. You will learn the measures to put in place now to make it harder for an attack to be successful, and to aid in the detection and investigation of future attacks. You will know how to bring together tools and methods to create a holistic approach and investigation when an event occurs, helping you to be confident of your ability to react correctly and responsibly to threats against your organization's data. What You'll Learn Detect when breaches have or may have occurred React with confidence using an organized plan Determine whether a suspected breach is real Determine the scope of data that has been compromised Preserve evidence for possible criminal prosecutions Put in place measures to aid future investigations Who This Book is For Database administrators, system administrators, and other technology professionals who may be called upon to investigate breaches of security involving Oracle Database

Expert Oracle and Java Security

Developing Secure Database and Middleware Environments

Applied Oracle Security: Developing Secure Database and Middleware Environments

Protecting Oracle Database 12c

Oracle Database 12c Security

Oracle Database Programming using Java and Web Services

*This book is about database security and auditing. You will learn many methods and techniques that will be helpful in securing, monitoring and auditing database environments. It covers diverse topics that include all aspects of database security and auditing - including network security for databases, authentication and authorization issues, links and replication, database Trojans, etc. You will also learn of vulnerabilities and attacks that exist within various database environments or that have been used to attack databases (and that have since been fixed). These will often be explained to an "internals level. There are many sections which outline the "anatomy of an attack" - both in detail and in broad terms. Equally important, you will learn about the database auditing landscape - both from a business and regulatory requirements perspective as well as from a technical implementation perspective. * Useful to the database administrator and/or security administrator - regardless of the precise database vendor (or vendors) that you are using within your organization. * Has a large number of examples - examples that pertain to Oracle, SQL Server, DB2, Sybase and even MySQL. * Many of the techniques you will see in this book will never be described in a manual or a book that is devoted to a certain database product. * Addressing complex issues must take into account more than just the database and focusing on capabilities that are provided only by the database vendor is not always enough. This book offers a broader view of the database environment - which is not dependent on the database platform - a view that is important to ensure good database security.*

The Ultimate Reference & Learning Guide for IT Security and Oracle Database Professionals! Over 150 Oracle Security Interview Questions, Answers, and Explanations It's clear that Oracle is the future for enterprise information systems data storage and retrieval - but finding the right reference materials can be difficult. For the first time, over 150 Oracle Database Security Interview Questions are here to guide your learning. From helping you to assess your Oracle Security skills to evaluating candidates for a job, Oracle Database Security Interview Questions will help you understand very quickly what you really need to know, and what you can safely ignore. The book is organized around Oracle database security vulnerabilities, database security design, and database control and audit functionality. Each question includes everything you need to know to master the security interview or properly evaluate a candidate. More than just a refresh of Oracle documentation and sales presentations, each question is based on project knowledge and experience gained on successful high-profile Oracle implementations. Key certification and interview topics include: Assessing Oracle Database Vulnerabilities - Preserving User Identity, JDBC Connection Pools. Using secure access roles to lock down databases. Using database views to provide row-level access controls. Ensuring user accountability with Auditing

Secure your Oracle Database 12c with this valuable Oracle support resource, featuring more than 100 solutions to the challenges of protecting your data>About This Book Explore and learn the new security features introduced in Oracle Database 12c, to successfully secure your sensitive data Learn how to identify which security strategy is right for your needs - and how to apply it! Each recipe provides you with a single step-by-step solution, making this book a vital resource, delivering Oracle support in one accessible place Who This Book Is ForThis book is for DBAs, developers, and architects who are keen to know more about security in Oracle Database 12c. This book is best suited for beginners and intermediate-level database security practitioners. Basic knowledge of Oracle Database is expected, but no prior experience of securing a database is required.What You Will Learn Analyze application privileges and reduce the risk of data exposure by using Oracle Data Redaction and Virtual Private Database Control data access and integrity in your organization using the appropriate database feature or option! Learn how to protect your databases against application bypasses! Audit user activity using the new auditing architecture Restrict highly privileged users from accessing data Encrypt data in Oracle Database Work in a real-world environment where a multi-layer security strategy is applied! In Detail Businesses around the world are paying much greater attention toward database security than they ever have before. Not only does the current regulatory environment require tight security, particularly when dealing with sensitive and personal data, data is also arguably a company's most valuable asset - why wouldn't you want to protect it in a secure and reliable database? Oracle Database lets you do exactly that. It's why it is one of the world's leading databases - with a rich portfolio of features to protect data from contemporary vulnerabilities, it's the go-to database for many organizations.Oracle Database 12c: Security Cookbook helps DBAs, developers, and architects to better understand database security challenges. Let it guide you through the process of implementing appropriate security mechanisms, helping you to ensure you are taking proactive steps to keep your data safe. Featuring solutions for common security problems in the new Oracle Database 12c, with this book you can be confident about securing your database from a range of different threats and problems. Style and approach Each chapter explains the different aspects of security through a series of recipes. Each recipe presents instructions in a step-by-step manner, supported by explanations of the topic.

From the official Oracle Press comes a comprehensive guide to implementing a sound security plan in your Oracle environment. This expert resource explains how to secure the operating system, the database, and the network and how to use Oracle's built-in security features. The book also explains how to hacker-proof, audit, and troubleshoot your entire system.

Oracle Security

Encryption & Advanced Data Security

Oracle Database 10g DBA Handbook

Oracle DBA's Guide to Database Security

From Novice to Professional

Beginning Oracle Database 11g Administration

*One-stop reference for administration and management of Oracle 10g Database *9i predecessor was a best seller; this edition covers all new features, with fully field-tested examples—not just "showcase" examples *Contains essential primers on Unix, Linux and Windows NT management and on SQL and PL/SQL programming: ideal for new/aspiring DBAs

Security in a relational database management system is complex, and too few DBAs, system administrators, managers, and developers understand how Oracle implements system and database security. This book gives you the guidance you need to protect your databases. Oracle security has many facets. Establishing an organization's security policy and plan Protecting system files and passwords

Controlling access to database objects (tables, views, rows, columns, etc.) Building appropriate user profiles, roles, and privileges Monitoring system access via audit trails Oracle Securitydescribes how these basic database security features are implemented and provides many practical strategies for securing Oracle systems and databases. It explains how to use the Oracle Enterprise Manager and Oracle Security Server to enhance your site's security, and it touches on such advanced security features as encryption, Trusted Oracle, and various Internet and World Wide Web protection strategies. A table of contents follows. Preface Part I: Security in an Oracle System Oracle and Security Oracle System Files Oracle Database Objects The Oracle Data Dictionary Default Roles and User Accounts Profiles, Passwords, and Synonyms Part II: Implementing Security Developing a Database Security Plan Installing and Starting Oracle Developing a Simple Security Application Developing an Audit Plan Developing a Sample Audit Application Backing Up and Recovering a Database Using the Oracle Enterprise Manager Maintaining User Accounts Part III: Enhanced Oracle Security Using the Oracle Security Server Using the Internet and the Web Using Extra-Cost Options Appendix A: References

Make your Oracle database virtually impregnable to hackers using the knowledge in this book. With over 50 recipes, you'll quickly learn protection methodologies that use industry certified techniques to secure the Oracle database server. Learn to protect your sensitive data by using industry certified techniques Implement and use ultimate techniques in Oracle Security and new security features introduced in Oracle 11g R2 Implement strong network communication security using different encryption solutions provided by Oracle Advanced Security In Detail For almost all organizations, data security is a matter of prestige and credibility. The Oracle Database is one of the most rich in features and probably the most used Database in a variety of industries where security is essential. To ensure security of data both in transit and on the disk, Oracle has implemented the security technologies to achieve a reliable and solid system. In Oracle 11g Anti-Hacker's Cookbook, you will learn about the most important solutions that can be used for better database security "Oracle 11g Anti-hacker's Cookbook" covers all the important security measures and includes various tips and tricks to protect your Oracle Database. "Oracle 11g Anti-hacker's Cookbook" uses real-world scenarios to show you how to secure the Oracle Database server from different perspectives and against different attack scenarios. Almost every chapter has a possible threads section, which describes the major dangers that can be confronted. The initial chapters cover how to defend the operating system, the network, the data and the users. The defense scenarios are linked and designed to prevent these attacks. The later chapters cover Oracle Vault, Oracle VPD, Oracle Labels, and Oracle Audit. Finally, in the Appendices, the book demonstrates how to perform a security assessment against the operating system and the database, and how to use a DAM tool for monitoring. What you will learn from this book Get to grips with configuring a secure server at operating system level for Oracle Database Master how to secure data by using Oracle Cryptographic API and Transparent Data Encryption Get step-by-step instructions to implement a solid audit strategy by using the built in solutions and fine grained auditing Understand how to segregate and protect data access by using Oracle Vault Learn about different types of attacks and how to implement a solid defence against them Empathize the attacks and interceptions by using different techniques and tools such as sniffing, man-in-the-middle, brute force and password crackers. Approach This cookbook has recipes written in simple, easy to understand format with lots of screenshots and insightful tips and hints. Who this book is written for If you are an Oracle Database Administrator, Security Manager or Security Auditor looking to secure the Oracle Database or prevent it from being hacked, then this book is for you. This book assumes you have a basic understanding of security concepts.

David Litchfield has devoted years to relentlessly searching out the flaws in the Oracle database system and creating defenses against them. Now he offers you his complete arsenal to assess and defend your own Oracle systems. This in-depth guide explores every technique and tool used by black hat hackers to invade and compromise Oracle and then it shows you how to find the weak spots and

defend them. Without that knowledge, you have little chance of keeping your databases truly secure.

Security, Scheduling, Performance & More

Effective Oracle Database 10g Security by Design

Oracle Database

Oracle Security Handbook

Oracle Database Application Security

Oracle Database 12c Security Cookbook

This book covers database security from all aspects of protecting data accessibility and availability. Coverage ranges from basic database security topics to advanced database security issues at the database and storage layers. In addition, a full presentation of data protection discusses data risks, protection mechanisms logical and physically, and data security. Furthermore, this book is a unique presentation of database security with Oracle 12c implementation covering all security features of Oracle 12c.

The traditional division of labor between the database (which only stores and manages SQL and XML data for fast, easy data search and retrieval) and the application server (which runs application or business logic, and presentation logic) is obsolete. Although the books primary focus is on programming the Oracle Database, the concepts and techniques provided apply to most RDBMS that support Java including Oracle, DB2, Sybase, MySQL, and PostgreSQL. This is the first book to cover new Java, JDBC, SQL, JPublisher and Web Services features in Oracle Database 10g Release 2 (the coverage starts with Oracle 9i Release 2). This book is a must-read for database developers audience (DBAs, database applications developers, data architects), Java developers (JDBC, SQL, J2EE, and OR Mapping frameworks), and to the emerging Web Services assemblers. Describes pragmatic solutions, advanced database applications, as well as provision of a wealth of code samples. Addresses programming models which run within the database as well as programming models which run in middle-tier or client-tier against the database. Discusses languages for stored procedures: when to use proprietary languages such as PL/SQL and when to use standard languages such as Java; also running non-Java scripting languages in the database. Describes the Java runtime in the Oracle database 10g (i.e., OracleJVM), its architecture, memory management, security management, threading, Java execution, the Native Compiler (i.e., NCOMP), how to make Java known to SQL and PL/SQL, data types mapping, how to call-out to external Web components, EJB components, ERP frameworks, and external databases. Describes JDBC programming and the new Oracle JDBC 10g features, its advanced connection services (pooling, failover, load-balancing, and the fast database event notification mechanism) for clustered databases (RAC) in Grid environments. Describes SQL programming and the latest Oracle SQLJ 10g features -, contrasting it with JDBC. Describes the latest Database Web services features, Web services concepts and Services Oriented Architecture (SOA) for DBA, the database as Web services provider and the database as Web services consumer. Abridged coverage of JPublisher 10g, a versatile complement to JDBC, SQL and Database Web Services.

Best Practices for Comprehensive Oracle Database Security Written by renowned experts from Oracle's National Security Group, Oracle Database 12c Security provides proven techniques for designing, implementing, and certifying secure Oracle Database systems in a multitenant architecture. The strategies are also applicable to standalone databases. This Oracle Press guide addresses everything from infrastructure to audit lifecycle and describes how to apply security measures in a holistic manner. The latest security features of Oracle Database 12c are explored in detail with practical and easy-to-understand examples. Connect users to databases in a secure manner Manage identity, authentication, and access control Implement database application security Provide security policies across enterprise applications using Real Application Security Control data access with Oracle Virtual Private Database Control sensitive data using data redaction and transparent sensitive data protection Control data access with Oracle Label Security Use Oracle Database Vault and Transparent Data Encryption for compliance, cybersecurity, and insider threats Implement auditing technologies, including Unified Audit Trail Manage security policies and monitor a secure database environment with Oracle Enterprise Manager Cloud Control

*A typical Oracle database has multiple users working simultaneously. Data is shared amongst the users, and this of course leads to security concerns. This book comes in from the angle of developing and maintaining a secure Oracle database with multiple users. The book shows how data can be shared in an orderly fashion and what a good secure database is. In this book, we assume that you are acquainted with basic Oracle SQL and fundamentals of relational database**

Php Oracle Web Development

Database Security with Oracle 12c

An Enhancement of Data Security for Oracle Database

Oracle SQL for Secure Relational Databases

With Oracle Internet Directory, Oracle Access Manager, and Oracle Identity Manager

Expert Oracle Database 10g Administration

This is Part 4 of a series of quick learning guides for Oracle designers, developers and managers including database administrators. Part 4 introduces early entrants with basic Oracle skills to the main concepts of Oracle data security and user privilege management and administration. The guide includes details of how to create and how to manage users and their database object and system access and rights. The guide also provides a basis for understanding different database security strategies such as role-based security, virtual private databases and procedure-based security. Part 4 contains a glossary of Oracle terminology related to database security and user privilege management with clear explanations of the terms used. These guides are designed to rapidly deliver key information about Oracle to the following audience groups: Oracle Project and System Managers, Analysts, Oracle Software Designers and Developers and Database Administrators.

A high-level handbook on how to develop auditing mechanisms for HIPAA compliant Oracle systems focuses on the security access and auditing requirements of the Health/Insurance Portability and Accountability Act of 1996 and discusses Oracle auditing features such as redo logs, system-level triggers, Oracle9i and the retrieval of sensitive data, and other key topics. Original. (Advanced)

Focus on the security aspects of designing, building, and maintaining a secure Oracle Database application. Starting with data encryption, you will learn to work with transparent data, back-up, and networks. You will then go through the key principles of audits, where you will get to know more about identity preservation, policies and fine-grained audits. Moving on to virtual private databases, you'll set up and configure a VPD to work in concert with other security features in Oracle, followed by tips on managing configuration drift, profiles, and default users. Shifting focus to coding, you will take a look at secure coding standards, multi-schema database models, code-based access control, and SQL injection. Finally, you'll cover single sign-on (SSO), and will be introduced to Oracle Internet Directory (OID), Oracle Access Manager (OAM), and Oracle Identity Management (OIM) by installing and configuring them to meet your needs. Oracle databases hold the majority of the world's relational data, and are attractive targets for attackers seeking high-value targets for data theft. Compromise of a single Oracle DBMS can result in tens of millions of breached records costing millions in breach-mitigation activity. This book gets you ready to avoid that nightmare scenario that You Will LearnWork with Oracle Internet Directory using the command-line and the console Integrate Oracle Access Manager with different applications Work with the Oracle Identity Manager console and connectors, while creating your own custom one Troubleshooting Works with OID, OAM, and OIHDive deep into file system and network security concepts Who This Book Is For Oracle DBAs and developers. Readers will find a basic understanding of Oracle RDBMS and Oracle Application Server to take complete advantage of this book.

Hacking and Defending Oracle

Oracle 11g Anti-Hacker's Cookbook

Big Data Security

Practical Oracle Security

HOWTO Secure and Audit Oracle 10g and 11g
Includes Federal Law Compliance with HIPAA, Sarbanes Oxley and the Gramm Leach Bliley Act GLB

THE SERIES: FRONTIERS IN COMPUTATIONAL INTELLIGENCE The series Frontiers In Computational Intelligence is envisioned to provide comprehensive coverage and understanding of cutting edge research in computational intelligence. It intends to augment the scholarly discourse on all topics relating to the advances in artificial life and machine learning in the form of metaheuristics, approximate reasoning, and robotics. Latest research findings are coupled with applications to varied domains of engineering and computer sciences. This field is steadily growing especially with the advent of novel machine learning algorithms being applied to different domains of engineering and technology. The series brings together leading researchers that intend to continue to advance the field and create a broad knowledge about the most recent research. Series Editor Dr. Siddhartha Bhattacharyya, CHRIST (Deemed to be University), Bangalore, India Editorial Advisory Board Dr. Elizabeth Behrman, Wichita State University, Kansas, USA Dr. Goran Klepac Dr. Leo Mrcic, Algebra University College, Croatia Dr. About Ella Hassanien, Cairo University, Egypt Dr. Jan Platos, VSB-Technical University of Ostrava, Czech Republic Dr. Xiao-Zhi Gao, University of Eastern Finland, Finland Dr. Wellington Pinheiro dos Santos, Federal University of Pernambuco, Brazil

This is the only practical, hands-on guide available to database administrators to secure their Oracle databases. This book will help the DBA to assess their current level of risk as well as their existing security posture. It will then provide practical, applicable knowledge to appropriately secure the Oracle database. The only practical, hands-on guide for securing your Oracle database published by independent experts. Your Oracle database does not exist in a vacuum, so this book shows you how to securely integrate your database into your enterprise.

This book, written by veteran Oracle database administrator Iggy Fernandez, a regular on the Oracle conference circuit and the editor of NoCOUG Journal, is a manageable introduction to key Oracle database administration topics including planning, installation, monitoring, troubleshooting, maintenance, and backups, to name just a few. As is clear from the table of contents, this book is not simply a recitation of Oracle Database features such as what you find in the reference guides available for free download on the Oracle web site. For example, the chapter on database monitoring explains how to monitor database availability, database changes, database security, database backups, database growth, database workload, database performance, and database capacity. The chapters of this book are logically organized into four parts that closely track the way your database administration career will naturally evolve. Part 1 gives you necessary background in relational database theory and Oracle Database concepts, Part 2 teaches you how to implement an Oracle database correctly, Part 3 exposes you to the daily routine of a database administrator, and Part 4 introduces you to the fine art of performance tuning.

Each chapter has exercises designed to help you apply the lessons of the chapter. Each chapter also includes a list of reference works that contain more information on the topic of the chapter. In this book, you'll find information that you won't find in other books on Oracle Database. Here you'll discover not only technical information, but also guidance on work practices that are as vital to your success as technical skills. The author's favorite chapter is "The Big Picture and the Ten Deliverables." If you take the lessons in that chapter to heart, you can quickly become a much better Oracle database administrator than you ever thought possible.

Security and Privilege
The Oracle Hacker's Handbook
Oracle Quick Guides Part 4 - Administration
Oracle Database Security Certification Review
Oracle Database 11g The Complete Reference