1. Record Nr. UNINA9910819554203321

Autore	Narayanan Sudheesh
Titolo	Securing Hadoop / / Sudheesh Narayanan
Pubbl/distr/stampa	Birmingham : , : Packt Publishing, , 2013
ISBN	1-78328-526-5
Edizione	[1st edition]
Descrizione fisica	1 online resource (116 p.)
Collana	Community experience distilled
Disciplina	004.36
Soggetti	Electronic data processing - Distributed processing File organization (Computer science)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Cover -- Copyright -- Credits -- About the Author -- About the Reviewers -- www.PacktPub.com -- Table of Contents -- Preface -- Chapter 1: Hadoop Security Overview -- Why do we need to secure Hadoop? -- Challenges for securing the Hadoop ecosystem -- Key security considerations -- Reference architecture for Big Data security -- Summary -- Chapter 2: Hadoop Security Design -- What is Kerberos? -- Key Kerberos terminologies -- How Kerberos works? -- Kerberos advantages -- The Hadoop default security model with Kerberos -- Hadoop Kerberos security implementation -- User-level access controls -- Service-level access controls -- User and service authentication -- Delegation Token -- Job Token -- Block Access Token -- Summary -- Chapter 3: Setting up a Secured Hadoop Cluster -- Prerequisites -- Setting up Kerberos -- Installing the Key Distribution Center -- Configuring the Key Distribution Center -- Establishing the KDC database -- Setting up the administrator principal for KDC -- Starting the Kerberos daemons -- Setting up the first Kerberos administrator -- Adding the user or service principals -- Configuring LDAP as the Kerberos database -- Supporting AES-256 encryption for a Kerberos ticket -- Configuring Hadoop with Kerberos authentication -- Setting up the Kerberos client on all the Hadoop nodes -- Setting up the Hadoop service principals -- Creating a keytab file for the Hadoop services -- Distributing the keytab file for all slaves -- Setting up the Hadoop configuration files -- HDFS-related configurations -- MRV1-related configurations -- MRV2-related

configurations -- Setting up secured DataNode -- Setting up the TaskController class -- Configuring users for Hadoop -- Automation of secured Hadoop deployment -- Summary -- Chapter 4: Securing the Hadoop Ecosystem -- Configuring Kerberos for Hadoop ecosystem components -- Securing Hive.
Securing Hive using Sentry -- Securing Oozie -- Securing Flume -- Securing Flume sources -- Securing Hadoop sink -- Securing a Flume channel -- Securing HBase -- Securing Sqoop -- Securing Pig -- Best practices for securing the Hadoop ecosystem components -- Summary -- Chapter 5: Integrating Hadoop with Enterprise Security Systems -- Integrating Enterprise Identity Management systems -- Configuring EIM integration with Hadoop -- Integrating Active Directory-based EIM with the Hadoop ecosystem -- Accessing a secured Hadoop cluster from an enterprise network -- HttpFS -- HUE -- Knox Gateway Server -- Summary -- Chapter 6: Securing Sensitive Data in Hadoop -- Securing sensitive data in Hadoop -- Approach for securing insights in Hadoop -- Securing data in motion -- Securing data at rest -- Implementing data encryption in Hadoop -- Summary -- Chapter 7: Security Event and Audit Logging in Hadoop -- Security Incident and Event Monitoring in a Hadoop Cluster -- The Security Incident and Event Monitoring (SIEM) system -- Setting up audit logging in a secured Hadoop cluster -- Configuring Hadoop audit logs -- Summary -- Appendix: Solutions Available for Securing Hadoop -- Hadoop distribution with enhanced security support -- Automation of secured Hadoop cluster deployment -- Cloudera Manager -- Zettaset -- Different Hadoop data encryption options -- Dataguise for Hadoop -- Gazzang zNcrypt -- eCryptfs for Hadoop -- Securing the Hadoop ecosystem with Project Rhino -- Mapping of the security technologies with the reference architecture -- Infrastructure security -- OS and filesystem security -- Application security -- Network perimeter security -- Data masking and encryption -- Authentication and authorization -- Audit logging, security policies, and procedures -- Security Incident and Event Monitoring -- Index.

Sommario/riassunto

Implement robust end-to-end security for your Hadoop ecosystem Master the key concepts behind Hadoop security as well as how to secure a Hadoop-based Big Data ecosystem Understand and deploy authentication, authorization, and data encryption in a Hadoop-based Big Data platform Administer the auditing and security event monitoring system In Detail Security of Big Data is one of the biggest concerns for enterprises today. How do we protect the sensitive information in a Hadoop ecosystem? How can we integrate Hadoop security with existing enterprise security systems? What are the challenges in securing Hadoop and its ecosystem? These are the questions which need to be answered in order to ensure effective management of Big Data. Hadoop, along with Kerberos, provides security features which enable Big Data management and which keep data secure. This book is a practitioner’s guide for securing a Hadoop-based Big Data platform. This book provides you with a step-by-step approach to implementing end-to-end security along with a solid foundation of knowledge of the Hadoop and Kerberos security models. This practical, hands-on guide looks at the security challenges involved in securing sensitive data in a Hadoop-based Big Data platform and also covers the Security Reference Architecture for securing Big Data. It will take you through the internals of the Hadoop and Kerberos security models and will provide detailed implementation steps for securing Hadoop. You will also learn how the internals of the Hadoop security model are implemented, how to integrate Enterprise Security Systems with Hadoop security, and how you can manage and control user access to a Hadoop ecosystem seamlessly. You will also get acquainted with

implementing audit logging and security incident monitoring within a Big Data platform.