Identity And Access Management Resume

Recognizing the mannerism ways to acquire this books **Identity And Access Management Resume** is additionally useful. You have remained in right site to start getting this info. get the Identity And Access Management Resume colleague that we find the money for here and check out the link.

You could purchase lead Identity And Access Management Resume or get it as soon as feasible. You could speedily download this Identity And Access Management Resume after getting deal. So, later than you require the ebook swiftly, you can straight acquire it. Its appropriately completely easy and correspondingly fats, isnt it? You have to favor to in this song

Identity And Access Management Resume ***2021-02-20***

KYLER LARSON

Digital Identity Management Packt Publishing Ltd

"This book explores important and emerging advancements in digital identity and access management systems, providing innovative answers to an assortment of problems as system managers are faced with major organizational, economic and market changes"--Provided by publisher.
Contemporary Identity and Access Management Architectures: Emerging Research and Opportunities IBM Redbooks
Identity management is the concept of providing a unifying interface to manage all aspects related to individuals and their interactions with the business. It is the process that enables business initiatives by efficiently managing the user life cycle (including identity/resource provisioning for people (users)), and by integrating it into the required business processes. Identity management encompasses all the data and processes related to the representation of an individual involved in electronic transactions. This IBM® Redbooks® publication provides an approach for designing an identity management solution with IBM Tivoli® Identity Manager Version 5.1. Starting from the high-level, organizational viewpoint, we show how to define user registration and maintenance processes using the self-registration and self-care interfaces as well as the delegated administration capabilities. Using the integrated workflow, we automate the submission/approval processes for identity management requests, and with the automated user provisioning, we

take workflow output and automatically implement the administrative requests on the environment with no administrative intervention. This book is a valuable resource for security administrators and architects who wish to understand and implement a centralized identity management and security infrastructure.

Solving Identity Management in Modern Applications Apress

This book is aimed at Security and IT practitioners (especially architects) in end-user organisations who are responsible for implementing an enterprise-wide Identity and Access Management (IAM) system. It is neither a conceptual treatment of Identity (for which we would refer the reader to Kim Cameron's excellent work on the Laws of Identity) nor a detailed technical manual on a particular product. It describes a pragmatic and cost-effective architectural approach to implementing IAM within an organisation, based on the experience of the authors.

Identity & Access Management

Servicemanagers.Org

Develop and Implement an End-to-End IAM Solution Maintain a high-performance, fully integrated security foundation across your enterprise using the detailed information in this Oracle Press guide. Designing an IAM Framework with Oracle Identity and Access Management Suite explains how to reduce risk exposure by effectively managing your full spectrum of users. Learn how to create and provision accounts, employ strong authentication

and authorization, integrate legacy applications, and handle regulatory compliance. The latest performance-testing, self-auditing, and business intelligence reporting techniques are also covered in this comprehensive resource. Establish company requirements and develop implementation plans Build and execute your identity business case Set up accounts, roles, and provisioning workflows using Oracle Identity Manager and Analysis Authenticate and authorize users with Oracle Access Manager Enact strong authorization policies using Oracle Entitlements Server Identify anomalous behavior and create proactive fraud prevention rules with Oracle Adaptive Access Manager Enforce regulatory compliance and generate audit-ready reports Learn about latest additions from the acquired Sun stack

Identity and Access Management - Simple Steps to Win, Insights and Opportunities for Maxing Out Success

Business Science Reference

This certification guide focuses on identity solutions and strategies that will help you prepare for Microsoft Identity and Access Administrator certification, while enabling you to implement what you've learned in real-world scenarios Key FeaturesDesign, implement, and operate identity and access management systems using Azure ADProvide secure authentication and authorization access to enterprise applicationsImplement access and authentication for cloud-only and hybrid infrastructuresBook Description Cloud

technologies have made identity and access the new control plane for securing data. Without proper planning and discipline in deploying, monitoring, and managing identity and access for users, administrators, and guests, you may be compromising your infrastructure and data. This book is a preparation guide that covers all the objectives of the SC-300 exam, while teaching you about the identity and access services that are available from Microsoft and preparing you for real-world challenges. The book starts with an overview of the SC-300 exam and helps you understand identity and access management. As you progress to the implementation of IAM solutions, you'll learn to deploy secure identity and access within Microsoft 365 and Azure Active Directory. The book will take you from legacy on-premises identity solutions to modern and password-less authentication solutions that provide high-level security for identity and access. You'll focus on implementing access and authentication for cloud-only and hybrid infrastructures as well as understand how to protect them using the principles of zero trust. The book also features mock tests toward the end to help you prepare effectively for the exam. By the end of this book, you'll have learned how to plan, deploy, and manage identity and access solutions for Microsoft and hybrid infrastructures. What you will learnUnderstand core exam objectives to pass the SC-300 examImplement an identity management solution with MS Azure

ADManage identity with multi-factor authentication (MFA), conditional access, and identity protectionDesign, implement, and monitor the integration of enterprise apps for Single Sign-On (SSO)Add apps to your identity and access solution with app registrationDesign and implement identity governance for your identity solutionWho this book is for This book is for cloud security engineers, Microsoft 365 administrators, Microsoft 365 users, Microsoft 365 identity administrators, and anyone who wants to learn identity and access management and gain SC-300 certification. You should have a basic understanding of the fundamental services within Microsoft 365 and Azure Active Directory before getting started with this Microsoft book.

Microsoft Identity and Access Administrator Exam Guide Packt Publishing Ltd

Discover how poor identity and privilege management can be leveraged to compromise accounts and credentials within an organization. Learn how role-based identity assignments, entitlements, and auditing strategies can be implemented to mitigate the threats leveraging accounts and identities and how to manage compliance for regulatory initiatives. As a solution, Identity Access Management (IAM) has emerged as the cornerstone of enterprise security. Managing accounts, credentials, roles, certification, and attestation reporting for all resources is now a security and compliance mandate. When identity theft and poor identity

management is leveraged as an attack vector, risk and vulnerabilities increase exponentially. As cyber attacks continue to increase in volume and sophistication, it is not a matter of if, but when, your organization will have an incident. Threat actors target accounts, users, and their associated identities, to conduct their malicious activities through privileged attacks and asset vulnerabilities. Identity Attack Vectors details the risks associated with poor identity management practices, the techniques that threat actors and insiders leverage, and the operational best practices that organizations should adopt to protect against identity theft and account compromises, and to develop an effective identity governance program. What You Will Learn Understand the concepts behind an identity and how their associated credentials and accounts can be leveraged as an attack vector Implement an effective Identity Access Management (IAM) program to manage identities and roles, and provide certification for regulatory compliance See where identity management controls play a part of the cyber kill chain and how privileges should be managed as a potential weak link Build upon industry standards to integrate key identity management technologies into a corporate ecosystem Plan for a successful deployment, implementation scope, measurable risk reduction, auditing and discovery, regulatory reporting, and oversight based on real-world strategies to prevent identity

attack vectors Who This Book Is For Management and implementers in IT operations, security, and auditing looking to understand and implement an identity access management program and manage privileges in these environments

Identity Management with Biometrics Packt Publishing Ltd Understand the IAM toolsets, capabilities, and paradigms of the AWS platform and learn how to apply practical identity use cases to AWS at the administrative and application level Key FeaturesLearn administrative lifecycle management and authorizationExtend workforce identity to AWS for applications deployed to Amazon Web Services (AWS)Understand how to use native AWS IAM capabilities with apps deployed to AWSBook Description AWS identity management offers a powerful yet complex array of native capabilities and connections to existing enterprise identity systems for administrative and application identity use cases. This book breaks down the complexities involved by adopting a use-case-driven approach that helps identity and cloud engineers understand how to use the right mix of native AWS capabilities and external IAM components to achieve the business and security outcomes they want. You will begin by learning about the IAM toolsets and paradigms within AWS. This will allow you to determine how to best leverage them for administrative control, extending workforce identities to the cloud, and using IAM toolsets and paradigms on an app deployed on AWS.

Next, the book demonstrates how to extend your on-premise administrative IAM capabilities to the AWS backplane, as well as how to make your workforce identities available for AWS-deployed applications. In the concluding chapters, you'll learn how to use the native identity services with applications deployed on AWS. By the end of this IAM Amazon Web Services book, you will be able to build enterprise-class solutions for administrative and application identity using AWS IAM tools and external identity systems. What you will learnUnderstand AWS IAM concepts, terminology, and servicesExplore AWS IAM, Amazon Cognito, AWS SSO, and AWS Directory Service to solve customer and workforce identity problemsApply the concepts you learn about to solve business, process, and compliance challenges when expanding into AWSNavigate the AWS CLI to unlock the programmatic administration of AWSExplore how AWS IAM, its policy objects, and notational language can be applied to solve security and access management use casesRelate concepts easily to your own environment through IAM patterns and best practicesWho this book is for Identity engineers and administrators, cloud administrators, security architects, or anyone who wants to explore and manage IAM solutions in AWS will find this book useful. Basic knowledge of AWS cloud infrastructure and services is required to understand the concepts covered in the book more effectively.

Identity Management for Internet of

Things Emereo Publishing
Due to the proliferation of distributed mobile technologies and heavy usage of social media, identity and access management has become a very challenging area. Businesses are facing new demands in implementing solutions, however, there is a lack of information and direction. Contemporary Identity and Access Management Architectures: Emerging Research and Opportunities is a critical scholarly resource that explores management of an organization's identities, credentials, and attributes which assures the identity of a user in an extensible manner set for identity and access administration. Featuring coverage on a broad range of topics, such as biometric application programming interfaces, telecommunication security, and role-based access control, this book is geared towards academicians, practitioners, and researchers seeking current research on identity and access management.

Identity and Access Management
McGraw Hill Professional
Plan, design, and implement identity and access management solutions with Okta Key FeaturesLearn how to use Okta for complete identity and access management in your organizationUse single sign-on, multifactor authentication, and life cycle management for enhanced securitySet up, manage, and audit API access policiesBook Description IAM, short for identity and access management, is a set of policies and technologies for ensuring the security of an organization

through careful role and access assignment for users and devices. With this book, you'll get up and running with Okta, an identity and access management (IAM) service that you can use for both employees and customers. Once you've understood how Okta can be used as an IAM platform, you'll learn about the Universal Directory, which covers how to integrate other directories and applications and set up groups and policies. As you make progress, the book explores Okta's single sign-on (SSO) feature and multifactor authentication (MFA) solutions. Finally, you will delve into API access management and discover how you can leverage Advanced Server Access for your cloud servers and Okta Access Gateway for your on-premises applications. By the end of this Okta book, you'll have learned how to implement Okta to enhance your organization's security and be able to use this book as a reference guide for the Okta certification exam. What you will learnUnderstand different types of users in Okta and how to place them in groupsSet up SSO and MFA rules to secure your IT environmentGet to grips with the basics of end-user functionality and customizationFind out how provisioning and synchronization with applications workExplore API management, Access Gateway, and Advanced Server AccessBecome well-versed in the terminology used by IAM professionalsWho this book is for If you are an IT consultant, business decision-maker, system administrator, system and security engineer, or anyone who

wishes to use Okta to plan, design, and implement identity and access management solutions, this book is for you. A basic understanding of authentication and authorization is necessary.

Access and Identity Management for Libraries Gower Publishing, Ltd.

Identity Management, or IDM, refers to how humans are identified and authorized across computer networks. It encompasses issues such as the way users are given an identity, the protection of that identity, and the technologies supporting that protection, such as network protocols, digital certificates, passwords, and so on. Proper identity management is, of course, an essential component of any security strategy. Identity Management: A Primer provides a complete and comprehensive overview of the elements required for a properly planned identity environment.

Designing an IAM Framework with Oracle Identity and Access Management Suite IGI Global

" Identity and Access Management (IAM) Architect: A Practice Guide" is a comprehensive resource that delves into the world of Identity and Access Management (IAM) architecture. This book outlines the critical role of IAM architects in designing, implementing, and maintaining robust IAM solutions to address modern organizations' evolving needs. The book begins by establishing the significance of IAM in today's digital landscape. It explores the challenges posed by the ever-changing threat

landscape, the importance of regulatory compliance, and the user experience's pivotal role. The target audience includes IAM professionals, security experts, IT managers, and anyone interested in understanding IAM architecture. Key topics covered in the book include: Fundamentals of IAM: The book starts by defining IAM and introducing fundamental concepts and terminology. It provides historical context, showcasing the evolution of IAM and its growing importance in contemporary organizations. The benefits of effective IAM are also discussed. IAM Architect's Role: The book outlines the IAM architect's responsibilities and core competencies, emphasizing the importance of collaboration with stakeholders and highlighting the architect's contribution to security and compliance. IAM Architecture Fundamentals: Design principles, IAM frameworks, and standards, as well as the choice between on-premises and cloud-based IAM, are explored in depth. The book also introduces IAM as a Service (IDaaS) as a modern architectural approach. Planning and Designing IAM Solutions: Readers learn how to assess IAM requirements, create an IAM strategy, and design IAM solutions. The IAM project lifecycle and iterative design and implementation approaches are discussed to help readers plan and execute IAM projects effectively. IAM Technologies and Tools: The book provides insights into various authentication mechanisms, the IAM vendor landscape, integration strategies,

and the role of custom development and APIs in building IAM solutions. Best Practices in IAM Architecture: IAM best practices are detailed, covering identity lifecycle management, access control, security and compliance, monitoring, and user training and awareness. These best practices form a crucial part of successful IAM implementation. IAM Challenges and Future Trends: Common IAM challenges are explored, such as user resistance, scalability issues, and security threats. Emerging trends, including zero-trust architecture and the role of AI in IAM, are also discussed. Real-World IAM Architectures: The book includes case studies and success stories, showcasing real-world implementations of IAM architecture and lessons learned from these experiences. Finally, " Identity and Access Management (IAM) Architect: A Practice Guide " provides a comprehensive roadmap for IAM architects and professionals to navigate the complex world of IAM architecture. It offers practical guidance, best practices, and insights into emerging trends, making it an invaluable resource for those involved in IAM design and implementation. This book empowers readers to build secure, compliant, and user-friendly IAM solutions in an ever-evolving digital landscape. The author, Samuel O Omoniyi is a cybersecurity professional, with vast experience in multiple sectors including oil and gas, telecommunication, banking and financial services, consulting, and more, in the United Kingdom. He has published

more than 12 books including Executing Zero Trust Architecture in the Cloud and Cloud Security Audit of Infrastructure and Applications. He is a member of local and international professional organizations such as the Information Systems Audit and Control Association (ISACA), USA; and the International Information System Security Certification Consortium, or (ISC)2, USA.

An Executive Guide to Identity Access Management Independently Published The Internet of Things is a wide-reaching network of devices, and these devices can intercommunicate and collaborate with each other to produce variety of services at any time, any place, and in any way. Maintaining access control, authentication and managing the identity of devices while they interact with other devices, services and people is an important challenge for identity management. The identity management presents significant challenges in the current Internet communication. These challenges are exacerbated in the internet of things by the unbound number of devices and expected limitations in constrained resources. Current identity management solutions are mainly concerned with identities that are used by end users, and services to identify themselves in the networked world. However, these identity management solutions are designed by considering that significant resources are available and applicability of these identity management solutions to the resource constrained internet of things needs a thorough analysis. Technical

topics discussed in the book include:• Internet of Things;• Identity Management;• Identity models in Internet of Things;• Identity management and trust in the Internet of Things context;• Authentication and access control;Identitymanagement for Internet of Things contributes to the area of identity management for ubiquitous devices in the Internet of Things. It initially presents the motivational factors together with the identity management problems in the context of Internet of Things and proposes an identity management framework. Following this, it refers to the major challenges for Identitymanagement and presents different identity management models. This book also presents relationship between identity and trust, different approaches for trust management, authentication and access control.

Identity and Access Management Platform Standard Requirements Facet Publishing

Who will be responsible for deciding whether Identity and Access Management Platform goes ahead or not after the initial investigations? Who are the people involved in developing and implementing Identity and Access Management Platform? Why is Identity and Access Management Platform important for you now? How do mission and objectives affect the Identity and Access Management Platform processes of your organization? What are your current levels and trends in key measures or indicators of Identity and Access Management Platform product

and process performance that are important to and directly serve your customers? How do these results compare with the performance of your competitors and other organizations with similar offerings? This extraordinary Identity and Access Management Platform self-assessment will make you the dependable Identity and Access Management Platform domain specialist by revealing just what you need to know to be fluent and ready for any Identity and Access Management Platform challenge. How do I reduce the effort in the Identity and Access Management Platform work to be done to get problems solved? How can I ensure that plans of action include every Identity and Access Management Platform task and that every Identity and Access Management Platform outcome is in place? How will I save time investigating strategic and tactical options and ensuring Identity and Access Management Platform costs are low? How can I deliver tailored Identity and Access Management Platform advice instantly with structured going-forward plans? There's no better guide through these mind-expanding questions than acclaimed best-selling author Gerard Blokdyk. Blokdyk ensures all Identity and Access Management Platform essentials are covered, from every angle: the Identity and Access Management Platform self-assessment shows succinctly and clearly that what needs to be clarified to organize the required activities and processes so that Identity and Access Management Platform

outcomes are achieved. Contains extensive criteria grounded in past and current successful projects and activities by experienced Identity and Access Management Platform practitioners. Their mastery, combined with the easy elegance of the self-assessment, provides its superior value to you in knowing how to ensure the outcome of any efforts in Identity and Access Management Platform are maximized with professional results. Your purchase includes access details to the Identity and Access Management Platform self-assessment dashboard download which gives you your dynamically prioritized projects-ready tool and shows you exactly what to do next. Your exclusive instant access details can be found in your book. You will receive the following contents with New and Updated specific criteria: - The latest quick edition of the book in PDF - The latest complete edition of the book in PDF, which criteria correspond to the criteria in... - The Self-Assessment Excel Dashboard - Example pre-filled Self-Assessment Excel Dashboard to get familiar with results generation - In-depth and specific Identity and Access Management Platform Checklists - Project management checklists and templates to assist with implementation INCLUDES LIFETIME SELF ASSESSMENT UPDATES Every self assessment comes with Lifetime Updates and Lifetime Free Updated Books. Lifetime Updates is an industry-first feature which allows you to receive verified self assessment updates, ensuring you always have the

most accurate information at your fingertips.

Identity and Access Management Iam a Complete Guide - 2019 Edition Lulu.com

Identity and Access Management: Business Performance Through Connected Intelligence provides you with a practical, in-depth walkthrough of how to plan, assess, design, and deploy IAM solutions. This book breaks down IAM into manageable components to ease systemwide implementation. The hands-on, end-to-end approach includes a proven step-by-step method for deploying IAM that has been used successfully in over 200 deployments. The book also provides reusable templates and source code examples in Java, XML, and SPML. Focuses on real-word implementations Provides end-to-end coverage of IAM from business drivers, requirements, design, and development to implementation Presents a proven, step-by-step method for deploying IAM that has been successfully used in over 200 cases Includes companion website with source code examples in Java, XML, and SPML as well as reusable templates

Mastering Identity and Access Management with Microsoft Azure

Packt Publishing Ltd

The book is a powerful, novel approach to the analysis and synthesis of IAM systems. It is motivated by the realization that the current practice of Information Systems in general, and Identity and Access Management in particular, is increasingly divorced from its Systems Engineering underpinnings.

Even for the most innovative and resourceful practitioners, the architecture, design, implementation and support of enterprise Information Technology systems has taken a complex inferential approach, driven by algorithmic and rule based protocols and standards. This work creates a solid foundation for IAM by using established concepts from Systems Engineering, using systems representations for major IAM processes like authentication and authorization. Such systems formulations may then be used to analyze IAM systems in complicated organizations using established Systems Engineering methods. For example, the book shows that problems in IAM such as risk propagation and authentication processes that were heretofore analyzed in terms of prescriptive, algorithmic or empirical schemes, are indeed amenable to general theoretical treatment. The book is specifically designed to be accessible to the general IT practitioner. It is with this goal in mind that it teases out the concepts in a way that anyone with some college education will be able to understand.

Access Control and Identity Management

Packt Publishing Ltd

The one-stop-source powering Identity and Access Management success, jam-packed with ready to use insights for success, loaded with all the data you need to decide how to gain and move ahead. An one-of-a-kind book, based on extensive research, this reveals the best practices of the most successful Identity and Access Management knowledge

mavens, those who are adept at continually innovating and seeing opportunity where others do not. This is the first place to go for Identity and Access Management innovation, in today's knowledge-driven business environment, professionals face particular challenges as their purpose is to discover or develop new concepts, products, or processes; the pressure to perform is intense. This title is the entryway to a single source for innovation. BONUS: Included with the book come numerous real-world Identity and Access Management blueprints, presentations and templates ready for you to download and use. This book addresses the crucial issue of Identity and Access Management adoption by presenting the facts to move beyond general observation. The model underpinning this book has been used as a predictive decision tool, tracking thousands of innovations for over more than a decade. And...this all-encompassing analysis focuses on key areas of future Identity and Access Management growth.

Digital Identity and Access Management: Technologies and Frameworks "O'Reilly Media, Inc."

"This book reviews the research and development activities of a number of existing identity management architectures in privately and publicly funded organizations. It provides a holistic view of identity and access management in regard to requirements, technologies, life cycle processes, and overview of present and future

commercial Identity and Access Management systems"--

Okta Administration: Up and Running Packt Publishing Ltd

In this high-level executive guide to Identity and Access Management, we discuss the good the bad and the ugly aspects. We consider why you need IAM, how it helps with security, compliance, governance and importantly how it can save you a fortune in time, effort and money on compliance auditing. However, it's not all good news, so we will discuss the problems you will face, the reasons for the high failure rates in deployment and the best practices you can follow to mitigate the risks of failure. Nonetheless, in this second edition, we contemplate how deploying IAM will reap benefits in the enterprise and discuss strategy and best practices for deployment in the cloud, commerce, IoT, and hybrid enterprise scenarios. We will also contemplate IDaaS and other next-generation approaches to IAM such as Identity Relationship Management (IRM).

Contemporary Identity and Access Management Architectures Complete Publishing

Leverage existing free open source software to build an identity and access management (IAM) platform that can serve your organization for the long term. With the emergence of open standards and open source software, it's now easier than ever to build and operate your own IAM stack. The most common culprit of the largest hacks has been bad personal identification. In terms of bang for your buck, effective

access control is the best investment you can make. Financially, it's more valuable to prevent than to detect a security breach. That's why Identity and Access Management (IAM) is a critical component of an organization's security infrastructure. In the past, IAM software has been available only from large enterprise software vendors. Commercial IAM offerings are bundled as "suites" because IAM is not just one component. It's a number of components working together, including web, authentication, authorization, cryptographic, and persistence services. Securing the Perimeter documents a recipe to take advantage of open standards to build an enterprise-class IAM service using free open source software. This recipe can be adapted to meet the needs of both small and large organizations. While not a comprehensive guide for every application, this book provides the key concepts and patterns to help administrators and developers leverage a central security infrastructure. Cloud IAM service providers would have you believe that managing an IAM is too hard. Anything unfamiliar is hard, but with the right road map, it can be mastered. You may find SaaS identity solutions too rigid or too expensive. Or perhaps you don't like the idea of a third party holding the credentials of your users-the keys to your kingdom. Open source IAM provides an alternative. Take control of your IAM infrastructure if digital services are key to your organization's success. What You'll Learn: Understand why you should

deploy a centralized authentication and policy management infrastructure Use the SAML or Open ID Standards for web or single sign-on, and OAuth for API Access Management Synchronize data from existing identity repositories such as Active Directory Deploy two-factor authentication services.

Digital Identity CreateSpace

Learn to leverage existing free open source software to build an identity and access management (IAM) platform that can serve your organization for the long term. With the emergence of open standards and open source software, it's now easier than ever to build and operate your own IAM stack The most common culprit of the largest hacks has been bad personal identification. In terms of bang for your buck, effective access control is the best investment you can make: financially, it's more valuable to prevent than to detect a security breach. That's why Identity and Access Management (IAM) is a critical component of an organization's security infrastructure. In the past, IAM software has been available only from large enterprise software vendors. Commercial IAM offerings are bundled as "suites" because IAM is not just one component: It's a number of components working together, including web, authentication, authorization, and cryptographic and persistence services. Deploying Identity and Access Management with Free Open Source Software documents a recipe to take advantage of open standards to build an enterprise-class IAM service using free open source software. This

recipe can be adapted to meet the needs of both small and large organizations. While not a comprehensive guide for every application, this book provides the key concepts and patterns to help administrators and developers leverage a central security infrastructure. Cloud IAM service providers would have you believe that managing an IAM is too hard. Anything unfamiliar is hard, but with the right road map, it can be mastered. You may find SaaS identity solutions too rigid or too expensive. Or perhaps you don't like the idea of a third party holding the credentials of your users—the keys to your kingdom. Open source IAM provides an alternative. Take control of your IAM infrastructure if digital services are key to your organization's success. What You'll Learn Why to deploy a centralized authentication and policy management infrastructure Use: SAML for single sign-on, OpenID Connect for web and mobile single sign-on, and OAuth2 for API Access Management Synchronize data from existing identity repositories such as Active Directory Deploy two-factor authentication services Who This Book Is For Security architects (CISO, CSO), system engineers/administrators, and software developers