

Mastering Identity And Access Management With Microsoft Azure

A complete handbook on Microsoft Identity Manager 2016 – from design considerations to operational best practices About This Book Get to grips with the basics of identity management and get acquainted with the MIM components and functionalities Discover the newly-introduced product features and how they can help your organization A step-by-step guide to enhance your foundational skills in using Microsoft Identity Manager from those who have taught and supported large and small enterprise customers Who This Book Is For If you are an architect or a developer who wants to deploy, manage, and operate Microsoft Identity Manager 2016, then this book is for you. This book will also help the technical decision makers who want to improve their knowledge of Microsoft Identity Manager 2016. A basic understanding of Microsoft-based infrastructure using Active Directory is expected. Identity management beginners and experts alike will be able to apply the examples and scenarios to solve real-world customer problems. What You Will Learn Install MIM components Find out about the MIM synchronization, its configuration settings, and advantages Get to grips with the MIM service capabilities and develop custom activities Use the MIM Portal to provision and manage an account Mitigate access escalation and lateral movement risks using privileged access management Configure client certificate management and its detailed permission model Troubleshoot MIM components by enabling logging and reviewing logs Back up and restore the MIM 2015 configuration Discover more about periodic purging and the coding best practices In Detail Microsoft Identity Manager 2016 is Microsoft's solution to identity management. When fully installed, the product utilizes SQL, SharePoint, IIS, web services, the .NET Framework, and SCSM to name a few, allowing it to be customized to meet nearly every business requirement. The book is divided into 15 chapters and begins with an overview of the product, what it does, and what it does not do. To better understand the concepts in MIM, we introduce a fictitious company and their problems and goals, then build an identity solutions to fit those goals. Over the course of this book, we cover topics such as MIM installation and configuration, user and group management options, self-service solutions, role-based access control, reducing security threats, and finally operational troubleshooting and best practices. By the end of this book, you will have gained the necessary skills to deploy, manage and operate Microsoft Identity Manager 2016 to meet your business requirements and solve real-world customer problems. Style and approach The concepts in the book are explained and illustrated with the help of screenshots as much as possible. We strive for readability and provide you with step-by-step instructions on the installation, configuration, and operation of the product. Throughout the book, you will be provided on-the-field knowledge that you won't get from whitepapers and help files. Start empowering users and protecting corporate data, while managing Identities and Access with Microsoft Azure in different environments About This Book Deep dive into the Microsoft Identity and Access Management as a Service (IDaaS) solution Design, implement and manage simple and complex hybrid identity and access management environments Learn to apply solution architectures directly to your business needs and understand how to identify and manage business drivers during transitions Who This Book Is For This book is for business decision makers, IT consultants, and system and security engineers who wish to plan, design, and implement Identity and Access Management solutions with Microsoft Azure. What You Will Learn Apply technical descriptions and solution architectures directly to your business needs and deployments Identify and manage business drivers and architecture changes to transition between different scenarios Understand and configure all relevant Identity and Access Management key features and concepts Implement simple and complex directory integration, authentication, and authorization scenarios Get to know about modern identity management, authentication, and authorization protocols and standards Implement and configure a modern information protection solution Integrate and configure future improvements in authentication and authorization functionality of Windows 10 and Windows Server 2016 In Detail Microsoft Azure and its Identity and Access Management is at the heart of Microsoft's Software as a Service, including Office 365, Dynamics CRM, and Enterprise Mobility Management. It is an essential tool to master in order to effectively work with the Microsoft Cloud. Through practical, project based learning this book will impart that mastery. Beginning with the basics of features and licenses, this book quickly moves on to the user and group lifecycle required to design roles and administrative units for role-based access control (RBAC). Learn to design Azure AD to be an identity provider and provide flexible and secure access to SaaS applications. Get to grips with how to configure and manage users, groups, roles, and administrative units to provide a user- and group-based application and self-service access including the audit functionality. Next find out how to take advantage of managing common identities with the Microsoft Identity Manager 2016 and build cloud identities with the Azure AD Connect utility. Construct blueprints with different authentication scenarios including multi-factor authentication. Discover how to configure and manage the identity synchronization and federation environment along with multi -factor authentication, conditional access, and information protection scenarios to apply the required security functionality. Finally, get recommendations for planning and implementing a future-oriented and sustainable identity and access management strategy. Style and approach A practical, project-based learning experience explained through hands-on examples.

Know how to design and use identity management to protect your application and the data it manages. At a time when security breaches result in increasingly onerous penalties, it is paramount that application developers and owners understand identity management and the value it provides when building applications. This book takes you from account provisioning to authentication to authorization, and covers troubleshooting and common problems to avoid. The authors include predictions about why this will be even more important in the future. Application best practices with coding samples are provided. Solving Identity and Access Management in Modern Applications gives you what you need to design identity and access management for your applications and to describe it to stakeholders with confidence. You will be able to explain account creation, session and access management, account termination, and more. What You'll Learn Understand key identity management concepts Incorporate essential design principles Design authentication and access control for a modern application Know the identity management frameworks and protocols used today (OIDC/ OAuth 2.0, SAML 2.0) Review historical failures and know how to avoid them Who This Book Is For Developers, enterprise or application architects, business application or product owners, and anyone involved in an application's identity management solution

If you have interest in DynamoDB and want to know what DynamoDB is all about and become proficient in using it, this is the book for you. If you are an intermediate user who wishes to enhance your knowledge of DynamoDB, this book is aimed at you. Basic familiarity with programming, NoSQL, and cloud computing concepts would be helpful.

Learn the intricacies of managing Azure AD, Azure AD Connect as well as Active Directory for administration on cloud and Windows Server 2019 Key Features Expert solutions for the federation, certificates, security, and monitoring with Active Directory

Explore Azure AD and AD Connect for effective administration on cloud Automate security tasks using Active Directory and PowerShell Book Description Active Directory is an administration system for Windows administrators to automate network, security and access management tasks in the Windows infrastructure. This book starts off with a detailed focus on forests, domains, trusts, schemas and partitions. Next, you learn how to manage domain controllers, organizational units and the default containers. Going forward, you deep dive into managing Active Directory sites as well as identifying and solving replication problems. The next set of chapters covers the different components of Active Directory and discusses the management of users, groups and computers. You also go through recipes that help you manage your Active Directory domains, manage user and groups objects and computer accounts, expiring group memberships and group Managed Service Accounts with PowerShell. You learn how to work with Group Policy and how to get the most out of it. The last set of chapters covers federation, security and monitoring. You will also learn about Azure Active Directory and how to integrate on-premises Active Directory with Azure AD. You learn how Azure AD Connect synchronization works, which will help you manage Azure AD. By the end of the book, you have learned in detail about Active Directory and Azure AD, too. What you will learn Manage new Active Directory features, such as the Recycle Bin, group Managed Service Accounts, and fine-grained password policies Work with Active Directory from the command line and use Windows PowerShell to automate tasks Create and remove forests, domains, and trusts Create groups, modify group scope and type, and manage memberships Delegate control, view and modify permissions Optimize Active Directory and Azure AD in terms of security Who this book is for This book will cater to administrators of existing Active Directory Domain Services environments and/or Azure AD tenants, looking for guidance to optimize their day-to-day effectiveness. Basic networking and Windows Server Operating System knowledge would come in handy.

Learn how to work with the Automate feature of CloudForms, the powerful Red Hat cloud management platform that lets you administer your virtual infrastructure, including hybrid public and private clouds. This practical hands-on introduction shows you how to increase your operational efficiency by automating day-to-day tasks that now require manual input. Throughout the book, author Peter McGowan provides a combination of theoretical information and practical coding examples to help you learn the Automate object model. With this CloudForms feature, you can create auto-scalable cloud applications, eliminate manual decisions and operations when provisioning virtual machines and cloud instances, and manage your complete virtual machine lifecycle. In six parts, this book helps you: Learn the objects and concepts for developing automation scripts with CloudForms Automate Customize the steps and workflows involved in provisioning virtual machines Create and use service catalogs, items, dialogs, objects, bundles, and hierarchies Use CloudForm's updated workflow to retire and delete virtual machines and services Orchestrate and coordinate with external services as part of a workflow Explore distributed automation processing as well as argument passing and handling

A comprehensive guide to architecting, managing, implementing, and controlling multi-cloud environments Key Features Deliver robust multi-cloud environments and improve your business productivity Stay in control of the cost, governance, development, security, and continuous improvement of your multi-cloud solution Integrate different solutions, principles, and practices into one multi-cloud foundation Book Description Multi-cloud has emerged as one of the top cloud computing trends, with businesses wanting to reduce their reliance on only one vendor. But when organizations shift to multiple cloud services without a clear strategy, they may face certain difficulties, in terms of how to stay in control, how to keep all the different components secure, and how to execute the cross-cloud development of applications. This book combines best practices from different cloud adoption frameworks to help you find solutions to these problems. With step-by-step explanations of essential concepts and practical examples, you'll begin by planning the foundation, creating the architecture, designing the governance model, and implementing tools, processes, and technologies to manage multi-cloud environments. You'll then discover how to design workload environments using different cloud propositions, understand how to optimize the use of these cloud technologies, and automate and monitor the environments. As you advance, you'll delve into multi-cloud governance, defining clear demarcation models and management processes. Finally, you'll learn about managing identities in multi-cloud: who's doing what, why, when, and where By the end of this book, you'll be able to create, implement, and manage multi-cloud architectures with confidence What you will learn Get to grips with the core functions of multiple cloud platforms Deploy, automate, and secure different cloud solutions Design network strategy and get to grips with identity and access management for multi-cloud Design a landing zone spanning multiple cloud platforms Use automation, monitoring, and management tools for multi-cloud Understand multi-cloud management with the principles of BaseOps, FinOps, SecOps, and DevOps Define multi-cloud security policies and use cloud security tools Test, integrate, deploy, and release using multi-cloud CI/CD pipelines Who this book is for This book is for architects and lead engineers involved in architecting multi-cloud environments, with a focus on getting governance right to stay in control of developments in multi-cloud. Basic knowledge of different cloud platforms (Azure, AWS, GCP, VMWare, and OpenStack) and understanding of IT governance is necessary.

Learn how to build a real-world serverless application in the cloud that's reliable, secure, maintainable, and scalable. If you have experience building web applications on traditional infrastructure, this hands-on guide shows you how to get started with Cloud Run, a container-based serverless product on Google Cloud. Through the course of this book, you'll learn how to deploy several example applications that highlight different parts of the serverless stack on Google Cloud. Combining practical examples with fundamentals, this book will appeal to developers who are early in their learning journey as well as experienced practitioners. Build a serverless application with Google Cloud Run Learn approaches for building containers with (and without) Docker Explore Google Cloud's managed relational database: Cloud SQL Use HTTP sessions to make every user's experience unique Explore identity and access management (IAM) on Cloud Run Provision Google Cloud resources using Terraform Learn how to handle background task scheduling on Cloud Run Move your service from Cloud Run to Knative Serving with little effort

Learn to leverage the advanced capabilities of Keycloak, an open-source identity and access management solution, to enable authentication and authorization in applications Key Features Get up to speed with Keycloak, OAuth 2.0, and OpenID Connect using practical examples Configure, manage, and extend Keycloak for optimized security Leverage Keycloak features to secure different application types Book Description Implementing authentication and authorization for applications can be a daunting experience, often leaving them exposed to security vulnerabilities. Keycloak is an open-source solution for identity management and access management for modern applications. Keycloak - Identity and Access Management for Modern Applications is a comprehensive introduction to Keycloak, helping you get started with using it and securing your applications. Complete with hands-on tutorials, best practices, and self-assessment questions, this easy-to-follow guide will show you how to secure a sample application and then move on to securing different application types. As you progress, you

will understand how to configure and manage Keycloak as well as how to leverage some of its more advanced capabilities. Finally, you'll gain insights into securely using Keycloak in production. By the end of this book, you will have learned how to install and manage Keycloak as well as how to secure new and existing applications. What you will learn Understand how to install, configure, and manage Keycloak Secure your new and existing applications with Keycloak Gain a basic understanding of OAuth 2.0 and OpenID Connect Understand how to configure Keycloak to make it ready for production use Discover how to leverage additional features and how to customize Keycloak to fit your needs Get to grips with securing Keycloak servers and protecting applications Who this book is for Developers, sysadmins, security engineers, or anyone who wants to leverage Keycloak and its capabilities for application security will find this book useful. Beginner-level knowledge of app development and authentication and authorization is expected.

Discover high-value Azure security insights, tips, and operational optimizations This book presents comprehensive Azure Security Center techniques for safeguarding cloud and hybrid environments. Leading Microsoft security and cloud experts Yuri Diogenes and Dr. Thomas Shinder show how to apply Azure Security Center's full spectrum of features and capabilities to address protection, detection, and response in key operational scenarios. You'll learn how to secure any Azure workload, and optimize virtually all facets of modern security, from policies and identity to incident response and risk management. Whatever your role in Azure security, you'll learn how to save hours, days, or even weeks by solving problems in most efficient, reliable ways possible. Two of Microsoft's leading cloud security experts show how to:

- Assess the impact of cloud and hybrid environments on security, compliance, operations, data protection, and risk management
- Master a new security paradigm for a world without traditional perimeters
- Gain visibility and control to secure compute, network, storage, and application workloads
- Incorporate Azure Security Center into your security operations center
- Integrate Azure Security Center with Azure AD Identity Protection Center and third-party solutions
- Adapt Azure Security Center's built-in policies and definitions for your organization
- Perform security assessments and implement Azure Security Center recommendations
- Use incident response features to detect, investigate, and address threats
- Create high-fidelity fusion alerts to focus attention on your most urgent security issues
- Implement application whitelisting and just-in-time VM access
- Monitor user behavior and access, and investigate compromised or misused credentials
- Customize and perform operating system security baseline assessments
- Leverage integrated threat intelligence to identify known bad actors

Includes more than 30 percent revised material and five new chapters, covering the new 2.1 features such as EJB Timer Service and JMS as well as the latest open source Java solutions The book was developed as part of TheServerSide.com online EJB community, ensuring a built-in audience Demonstrates how to build an EJB system, program with EJB, adopt best practices, and harness advanced EJB concepts and techniques, including transactions, persistence, clustering, integration, and performance optimization Offers practical guidance on when not to use EJB and how to use simpler, less costly open source technologies in place of or in conjunction with EJB

In the race to compete in today's fast-moving markets, large enterprises are busy adopting new technologies for creating new products, processes, and business models. But one obstacle on the road to digital transformation is placing too much emphasis on technology, and not enough on the types of processes technology enables. What if different lines of business could build their own services and applications—and decision-making was distributed rather than centralized? This report explores the concept of a digital business platform as a way of empowering individual business sectors to act on data in real time. Much innovation in a digital enterprise will increasingly happen at the edge, whether it involves business users (from marketers to data scientists) or IoT devices. To facilitate the process, your core IT team can provide these sectors with the digital tools they need to innovate quickly. This report explores: Key cultural and organizational changes for developing business capabilities through cross-functional product teams A platform for integrating applications, data sources, business partners, clients, mobile apps, social networks, and IoT devices Creating internal API programs for building innovative edge services in low-code or no-code environments Tools including Integration Platform as a Service, Application Platform as a Service, and Integration Software as a Service The challenge of integrating microservices and serverless architectures Event-driven architectures for processing and reacting to events in real time You'll also learn about a complete pervasive integration solution as a core component of a digital business platform to serve every audience in your organization.

Design effective Azure architecture and transform your IT business solutions Key Features Develop a resilient and robust cloud environment Deploy and manage cost-effective and highly available solutions on your public cloud Design and implement enterprise-level cloud solutions Book Description Azure provides cloud-based solutions to support your business demands. Building and running solutions on Azure will help your business maximize the return on investment and minimize the total cost of ownership. Hands-On Cloud Solutions with Azure focuses on addressing the architectural decisions that usually arise when you design or migrate a solution to Microsoft Azure. You will start by designing the building blocks of infrastructure solution on Azure, such as Azure compute, storage, and networking, followed by exploring the database options it offers. You will get to grips with designing scalable web and mobile solutions and understand where to host your Active Directory and Identity Solution. Moving on, you'll learn how to extend DevOps to Azure. You will also benefit from some exciting services that enable extremely smooth operations and streamlined DevOps between on-premises and cloud. The book will help you to design a secure environment for your solution, on both the Cloud and hybrid. Toward the end, you'll see how to manage and monitor cloud and hybrid solutions. By the end of this book, you will be armed with all the tools and knowledge you need to properly plan and design your solutions on Azure, whether it's for a brand new project or migration project. What you will learn Get started with Azure by understanding tenants, subs, and resource groups Decide whether to "lift and shift" or migrate apps Plan and architect solutions in Azure Build ARM templates for Azure resources Develop and deploy solutions in Azure Understand how to monitor and support your application with Azure Make your life easier with Azure best practices and tips Who this book is for If you're an IT consultant, developer, or solutions architect looking to design effective solutions for your organization, this book is for you. Some knowledge of cloud computing will assist with understanding the key concepts covered in this book.

Throughout the book, we will follow a fictional company, the case study will help you in implementing FIM 2010 R2. All the examples in the book will relate to this fictive company and you will be taken from design, to installation, to configuration of FIM 2010 R2. If you are implementing and managing FIM 2010 R2 in your business, then this book is for you. You will need to have a basic understanding of Microsoft based infrastructure using Active Directory. If you are new to Forefront Identity Management, the case-study approach of this book will help you to understand the concepts and implement them.

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 Who This Book Is For Security architects (CISO, CSO), system engineers/administrators, and software developers

Prevent destructive attacks to your Azure public cloud infrastructure, remove vulnerabilities, and instantly report cloud security readiness.

This book provides comprehensive guidance from a security insider's perspective. Cyber Security on Azure explains how this 'security as a service' (SECaaS) business solution can help you better manage security risk and enable data security control using encryption options such as Advanced Encryption Standard (AES) cryptography. Discover best practices to support network security groups, web application firewalls, and database auditing for threat protection. Configure custom security notifications of potential cyberattack vectors to prevent unauthorized access by hackers, hacktivists, and industrial spies. What You'll Learn This book provides step-by-step guidance on how to: Support enterprise security policies Improve cloud security Configure intrusion detection Identify potential vulnerabilities Prevent enterprise security failures Who This Book Is For IT, cloud, and security administrators; CEOs, CIOs, and other business professionals

How smart companies are opening up strategic initiatives to involve front-line employees, experts, suppliers, customers, entrepreneurs, and even competitors. Why are some of the world's most successful companies able to stay ahead of disruption, adopting and implementing innovative strategies, while others struggle? It's not because they hire a new CEO or expensive consultants but rather because these pioneering companies have adopted a new way of strategizing. Instead of keeping strategic deliberations within the C-Suite, they open up strategic initiatives to a diverse group of stakeholders—front-line employees, experts, suppliers, customers, entrepreneurs, and even competitors. Open Strategy presents a new philosophy, key tools, step-by-step advice, and fascinating case studies—from companies that range from Barclays to Adidas—to guide business leaders in this groundbreaking approach to strategy. The authors—business-strategy experts from both academia and management consulting—introduce tools for each of the three stages of strategy-making: idea generation, plan formulation, and implementation. These are digital tools (including strategy contests), which allow the widest participation; hybrid digital/in-person tools (including a “nightmare competitor challenge”); a workshop tool that gamifies the business model development process; and tools that help companies implement and sustain open strategy efforts. Open strategy has an astonishing track record: a survey of 200 business leaders shows that although open-strategy techniques were deployed for only 30 percent of their initiatives, those same initiatives generated 50 percent of their revenues and profits. This book offers a roadmap for this kind of success.

Conquer Microsoft Office 365 Administration—from the inside out! Dive into Microsoft Office 365 Administration—and really put your Office 365 expertise to work. This supremely organized reference packs hundreds of timesaving solutions, tips, and workarounds—all you need to plan, implement, and operate Microsoft Office 365 in any environment. In this completely revamped Second Edition, a new author team thoroughly reviews the administration tools and capabilities available in the latest versions of Microsoft Office 365, and also adds extensive new coverage of Azure cloud services and SharePoint. Discover how experts tackle today's essential tasks—and challenge yourself to new levels of mastery.

- Install, customize, and use Office 365's portal, dashboard, and admin centers
- Make optimal decisions about tenancy, licensing, infrastructure, and hybrid options
- Prepare your environment for the cloud
- Manage Office 365 identity and access via federation services, password and directory synchronization, authentication, and AAD Connect
- Implement alerts and threat management in the Security & Compliance Center
- Establish Office 365 data classifications, loss prevention plans, and governance
- Prepare your on-premises environment to connect with Exchange Online
- Manage resource types, billing and licensing, service health reporting, and support
- Move mailboxes to Exchange Online via cutover, staged, and express migrations
- Establish hybrid environments with the Office 365 Hybrid Configuration Wizard
- Administer Exchange Online, from recipients and transport to malware filtering
- Understand, plan, and deploy Skype for Business Online

Current Book Service In addition, this book is part of the Current Book Service from Microsoft Press. Books in this program receive periodic updates to address significant software changes for 12 to 18 months following the original publication date via a free Web Edition. Learn more at <https://www.microsoftpressstore.com/cbs>.

Become a master at managing enterprise identity infrastructure by leveraging Active Directory About This Book Manage your Active Directory services for Windows Server 2016 effectively Automate administrative tasks in Active Directory using PowerShell Manage your organization's network with ease Who This Book Is For If you are an Active Directory administrator, system administrator, or network professional who has basic knowledge of Active Directory and are looking to gain expertise in this topic, this is the book for you. What You Will Learn Explore the new features in Active Directory Domain Service 2016 Automate AD tasks with PowerShell Get to know the advanced functionalities of the schema Learn about Flexible Single Master Operation (FSMO) roles and their placement Install and migrate Active directory from older versions to Active Directory 2016 Manage Active Directory objects using different tools and techniques Manage users, groups, and devices effectively Design your OU structure in the best way Audit and monitor Active Directory Integrate Azure with Active Directory for a hybrid setup In Detail Active Directory is a centralized and standardized system that automates networked management of user data, security, and distributed resources and enables interoperation with other directories. If you are aware of Active Directory basics and want to gain expertise in it, this book is perfect for you. We will quickly go through the architecture and fundamentals of Active Directory and then dive deep into the core components, such as forests, domains, sites, trust relationships, OU, objects, attributes, DNS, and replication. We will then move on to AD schemas, global catalogs, LDAP, RODC, RMS, certificate authorities, group policies, and security best practices, which will help you gain a better understanding of objects and components and how they can be used effectively. We will also cover AD Domain Services and Federation Services for Windows Server 2016 and all their new features. Last but not least, you will learn how to manage your identity infrastructure for a hybrid-cloud setup. All this will help you design, plan, deploy, manage operations on, and troubleshoot your enterprise identity infrastructure in a secure, effective manner. Furthermore, I will guide you through automating administrative tasks using PowerShell cmdlets. Toward the end of the book, we will cover best practices and troubleshooting techniques that can be used to improve security and performance in an identity infrastructure. Style and approach This step-by-step guide will help you master the core functionalities of Active Directory services using Microsoft Server 2016 and PowerShell, with real-world best practices at the end.

In Self-Sovereign Identity: Decentralized digital identity and verifiable credentials, you'll learn how SSI empowers us to receive digitally-signed credentials, store them in private wallets, and securely prove our online identities. Summary In a world of changing privacy regulations, identity theft, and online anonymity, identity is a precious and complex concept. Self-Sovereign Identity (SSI)

is a set of technologies that move control of digital identity from third party “identity providers” directly to individuals, and it promises to be one of the most important trends for the coming decades. Now in Self-Sovereign Identity, privacy and personal data experts Drummond Reed and Alex Preukschat lay out a roadmap for a future of personal sovereignty powered by the Blockchain and cryptography. Cutting through the technical jargon with dozens of practical use cases from experts across all major industries, it presents a clear and compelling argument for why SSI is a paradigm shift, and shows how you can be ready to be prepared for it. About the technology Trust on the internet is at an all-time low. Large corporations and institutions control our personal data because we’ve never had a simple, safe, strong way to prove who we are online. Self-sovereign identity (SSI) changes all that. About the book In Self-Sovereign Identity: Decentralized digital identity and verifiable credentials, you’ll learn how SSI empowers us to receive digitally-signed credentials, store them in private wallets, and securely prove our online identities. It combines a clear, jargon-free introduction to this blockchain-inspired paradigm shift with interesting essays written by its leading practitioners. Whether for property transfer, ebanking, frictionless travel, or personalized services, the SSI model for digital trust will reshape our collective future. What's inside The architecture of SSI software and services The technical, legal, and governance concepts behind SSI How SSI affects global business industry-by-industry Emerging standards for SSI About the reader For technology and business readers. No prior SSI, cryptography, or blockchain experience required. About the authors Drummond Reed is the Chief Trust Officer at Evernym, a technology leader in SSI. Alex Preukschat is the co-founder of SSIMeetup.org and AlianzaBlockchain.org. Table of Contents PART 1: AN INTRODUCTION TO SSI 1 Why the internet is missing an identity layer—and why SSI can finally provide one 2 The basic building blocks of SSI 3 Example scenarios showing how SSI works 4 SSI Scorecard: Major features and benefits of SSI PART 2: SSI TECHNOLOGY 5 SSI architecture: The big picture 6 Basic cryptography techniques for SSI 7 Verifiable credentials 8 Decentralized identifiers 9 Digital wallets and digital agents 10 Decentralized key management 11 SSI governance frameworks PART 3: DECENTRALIZATION AS A MODEL FOR LIFE 12 How open source software helps you control your self-sovereign identity 13 Cypherpunks: The origin of decentralization 14 Decentralized identity for a peaceful society 15 Belief systems as drivers for technology choices in decentralization 16 The origins of the SSI community 17 Identity is money PART 4: HOW SSI WILL CHANGE YOUR BUSINESS 18 Explaining the value of SSI to business 19 The Internet of Things opportunity 20 Animal care and guardianship just became crystal clear 21 Open democracy, voting, and SSI 22 Healthcare supply chain powered by SSI 23 Canada: Enabling self-sovereign identity 24 From eIDAS to SSI in the European Union

Provides information on the features, functions, and implementation of Active Directory.

Build advanced authentication solutions for any cloud or web environment Active Directory has been transformed to reflect the cloud revolution, modern protocols, and today’s newest SaaS paradigms. This is an authoritative, deep-dive guide to building Active Directory authentication solutions for these new environments. Author Vittorio Bertocci drove these technologies from initial concept to general availability, playing key roles in everything from technical design to documentation. In this book, he delivers comprehensive guidance for building complete solutions. For each app type, Bertocci presents high-level scenarios and quick implementation steps, illuminates key concepts in greater depth, and helps you refine your solution to improve performance and reliability. He helps you make sense of highly abstract architectural diagrams and nitty-gritty protocol and implementation details. This is the book for people motivated to become experts. Active Directory Program Manager Vittorio Bertocci shows you how to: Address authentication challenges in the cloud or on-premises Systematically protect apps with Azure AD and AD Federation Services Power sign-in flows with OpenID Connect, Azure AD, and AD libraries Make the most of OpenID Connect’s middleware and supporting classes Work with the Azure AD representation of apps and their relationships Provide fine-grained app access control via roles, groups, and permissions Consume and expose Web APIs protected by Azure AD Understand new authentication protocols without reading complex spec documents

No society is without crime, prompting Nathaniel Hawthorne’s narrator to make his famous statement in *The Scarlet Letter* that, however high its hopes are, no civilization can fail to allot a portion of its soil as the site of a prison. By establishing the category of crime - by drawing a line between the lawful and criminal, however thin, blurry, or even effectively meaningless the line may in practice become - society offers its own perhaps most consequential self-definition. Film, argues Carl Freedman, is an especially fruitful medium for considering questions like these. With *Versions of Hollywood Crime Cinema*, he offers a series of critical readings spanning several genres, by directors Coppola, Scorsese, Ford, Wilder. From among the mob movies, Freedman focuses on Francis Ford Coppola’s *Godfather* trilogy - arguably the foremost work of crime cinema - using it to reflect on the Marxist notion of primitive accumulation and relationship between “gangsterism and capitalism”. The volume also includes in-depth critique of classics of film noir (including *Double Indemnity* and *Body Heat*) and, surprisingly, Western, which is not often thought of as a kind of crime film even though its setting is an entire society in which crime flourishes yet is fought against, bringing into focus films of John Wayne. For crime fans and scholars alike, the radical readings of known classics in *Versions of Hollywood Crime Cinema* provide an insightful critique of modern culture and high capitalism that produced, and that are reflected in, the range of films discussed.

The growing potential of GIS for supporting policing and crimereduction is now being recognised by a broader community. GIS canbe employed at different levels to support operational policing,tactical crime mapping, detection, and wider-ranging strategicanalyses. With the use of GIS for crime mapping increasing, thisbook provides a definitive reference. *GIS and Crime Mapping* provides essential information andreference material to support readers in developing andimplementing crime mapping. Relevant case studies help demonstratethe key principles, concepts and applications of crime mapping. This book combines the topics of theoretical principles, GIS,analytical techniques, data processing solutions, informationsharing, problem-solving approaches, map design, and organisationalstructures for using crime mapping for policing and crimereduction. Delivered in an accessible style, topics are covered ina manner that underpins crime mapping use in the three broad areasof operations, tactics and strategy. Provides a complete start-to-finish coverage of crime mapping,including theory, scientific methodologies, analysis techniques anddesign principles. Includes a comprehensive presentation of crime mappingapplications for operational, tactical and strategic purposes. Includes global case studies and examples to demonstrate goodpractice. Co-authored by Spencer Chainey, a leading researcher andconsultant on GIS and crime mapping, and Jerry Ratcliffe, arenowned professor and former police officer. This book is essential reading for crime analysts and otherprofessionals working in intelligence roles in law enforcement orcrime reduction, at the local, regional and national governmentlevels. It is also an excellent reference for undergraduateand Masters students taking courses in GIS, Geomatics, CrimeMapping, Crime Science, Criminal Justice and Criminology.

Work with common biometrics such as face, fingerprint, and iris recognition for business and personal use to ensure secure identification and authentication for fintech, homes, and computer systems

Key Features Explore the next iteration of identity protection and overcome real-world challenges Understand different biometric use cases to deploy a large-scale biometric system Curated by renowned security ambassador and experienced author Lisa Bock

Book Description Biometric technologies provide a variety of robust and convenient methods to securely identify and authenticate an individual. Unlike a password or smart card, biometrics can identify an attribute that is not only unique to an individual, but also eliminates any possibility of duplication. Identity Management with Biometrics is a solid introduction for anyone who wants to explore biometric techniques, such as fingerprint, iris, voice, palm print, and facial recognition. Starting with an overview of biometrics, you'll learn the various uses and applications of biometrics in fintech, buildings, border control, and many other fields. You'll understand the characteristics of an optimal biometric system and then review different types of errors and discover the benefits of multi-factor authentication. You'll also get to grips with analyzing a biometric system for usability and accuracy and understand the process of implementation, testing, and deployment, along with addressing privacy concerns. The book outlines the importance of protecting biometric data by using encryption and shows you which factors to consider and how to analyze them before investing in biometric technologies. By the end of this book, you'll be well-versed with a variety of recognition processes and be able to make the right decisions when implementing biometric technologies.

What you will learn Review the advantages and disadvantages of biometric technology Understand the characteristics of an optimal biometric system Discover the uses of biometrics and where they are used Compare different types of errors and see how to tune your system Understand the benefits of multi-factor authentication Work with commonly used biometrics such as face, fingerprint, and iris Analyze a biometric system for usability and accuracy Address privacy concerns and get a glimpse of the future of biometrics

Who this book is for Identity Management with Biometrics is for IT managers, security professionals, students, teachers, and anyone involved in selecting, purchasing, integrating, or securing a biometric system. This book will help you understand how to select the right biometric system for your organization and walk you through the steps for implementing identity management and authentication. A basic understanding of biometric authentication techniques, such as fingerprint and facial recognition, and the importance of providing a secure method of authenticating an individual will help you make the most of the book.

Start empowering users and protecting corporate data, while managing identities and access with Microsoft Azure in different environments

Key Features Understand how to identify and manage business drivers during transitions Explore Microsoft Identity and Access Management as a Service (IDaaS) solution Over 40 playbooks to support your learning process with practical guidelines

Book Description Microsoft Azure and its Identity and access management are at the heart of Microsoft's software as a service products, including Office 365, Dynamics CRM, and Enterprise Mobility Management. It is crucial to master Microsoft Azure in order to be able to work with the Microsoft Cloud effectively. You'll begin by identifying the benefits of Microsoft Azure in the field of identity and access management. Working through the functionality of identity and access management as a service, you will get a full overview of the Microsoft strategy. Understanding identity synchronization will help you to provide a well-managed identity. Project scenarios and examples will enable you to understand, troubleshoot, and develop on essential authentication protocols and publishing scenarios. Finally, you will acquire a thorough understanding of Microsoft Information protection technologies.

What you will learn Apply technical descriptions to your business needs and deployments Manage cloud-only, simple, and complex hybrid environments Apply correct and efficient monitoring and identity protection strategies Design and deploy custom Identity and access management solutions Build a complete identity and access management life cycle Understand authentication and application publishing mechanisms Use and understand the most crucial identity synchronization scenarios Implement a suitable information protection strategy

Who this book is for This book is a perfect companion for developers, cyber security specialists, system and security engineers, IT consultants/architects, and system administrators who are looking for perfectly up-to-date hybrid and cloud-only scenarios. You should have some understanding of security solutions, Active Directory, access privileges/rights, and authentication methods. Programming knowledge is not required but can be helpful for using PowerShell or working with APIs to customize your solutions.

In depth informative guide to implement and use AWS security services effectively.

About This Book Learn to secure your network, infrastructure, data and applications in AWS cloud Log, monitor and audit your AWS resources for continuous security and continuous compliance in AWS cloud Use AWS managed security services to automate security. Focus on increasing your business rather than being diverged onto security risks and issues with AWS security. Delve deep into various aspects such as the security model, compliance, access management and much more to build and maintain a secure environment.

Who This Book Is For This book is for all IT professionals, system administrators and security analysts, solution architects and Chief Information Security Officers who are responsible for securing workloads in AWS for their organizations. It is helpful for all Solutions Architects who want to design and implement secure architecture on AWS by the following security by design principle. This book is helpful for personnel in Auditors and Project Management role to understand how they can audit AWS workloads and how they can manage security in AWS respectively. If you are learning AWS or championing AWS adoption in your organization, you should read this book to build security in all your workloads. You will benefit from knowing about security footprint of all major AWS services for multiple domains, use cases, and scenarios.

What You Will Learn Learn about AWS Identity Management and Access control Gain knowledge to create and secure your private network in AWS Understand and secure your infrastructure in AWS Understand monitoring, logging and auditing in AWS Ensure Data Security in AWS Learn to secure your applications in AWS Explore AWS Security best practices

In Detail Mastering AWS Security starts with a deep dive into the fundamentals of the shared security responsibility model. This book tells you how you can enable continuous security, continuous auditing, and continuous compliance by automating your security in AWS with the tools, services, and features it provides. Moving on, you will learn about access control in AWS for all resources. You will also learn about the security of your network, servers, data and applications in the AWS cloud using native AWS security services. By the end of this book, you will understand the complete AWS Security landscape, covering all aspects of end-to-end software and hardware security along with logging, auditing, and compliance of your entire IT environment in the AWS cloud. Lastly, the book will wrap up with AWS best practices for security.

Style and approach The book will take a practical approach delving into different aspects of AWS security to help you become a master of it. It will focus on using native AWS security features and managed AWS services to help you achieve continuous security and continuous compliance.

Start empowering users and protecting corporate data, while managing identities and access with Microsoft Azure in different

environments Key Features Understand how to identify and manage business drivers during transitions Explore Microsoft Identity and Access Management as a Service (IDaaS) solution Over 40 playbooks to support your learning process with practical guidelines Book Description Microsoft Azure and its Identity and access management are at the heart of Microsoft's software as a service products, including Office 365, Dynamics CRM, and Enterprise Mobility Management. It is crucial to master Microsoft Azure in order to be able to work with the Microsoft Cloud effectively. You'll begin by identifying the benefits of Microsoft Azure in the field of identity and access management. Working through the functionality of identity and access management as a service, you will get a full overview of the Microsoft strategy. Understanding identity synchronization will help you to provide a well-managed identity. Project scenarios and examples will enable you to understand, troubleshoot, and develop on essential authentication protocols and publishing scenarios. Finally, you will acquire a thorough understanding of Microsoft Information protection technologies. What you will learn Apply technical descriptions to your business needs and deployments Manage cloud-only, simple, and complex hybrid environments Apply correct and efficient monitoring and identity protection strategies Design and deploy custom Identity and access management solutions Build a complete identity and access management life cycle Understand authentication and application publishing mechanisms Use and understand the most crucial identity synchronization scenarios Implement a suitable information protection strategy Who this book is for This book is a perfect companion for developers, cyber security specialists, system and security engineers, IT consultants/architects, and system administrators who are looking for perfectly up-to-date hybrid and cloud-only scenarios. You should have some understanding of security solutions, Active Directory, access privileges/rights, and authentication methods. Programming knowledge is not required but can be helpful for using PowerShell or working with APIs to customize your solutions. Downloading the example code for this book You can download the example code files for all Packt books you have purchased from your account at [http://www.Pack ...](http://www.Pack...)

Brand Management: Mastering Research, Theory and Practice is a valuable resource for those looking to understand how a brand can be conceptualized and thus managed in all its complexity. Going beyond the 'quick fixes' of branding, it offers a comprehensive overview of brand management theories from the last 35 years. A highly regarded textbook, this fully updated third edition brings fresh perspectives on the latest research in, and analysis of, the various approaches to brand management. More than 1,000 academic sources have been carefully divided into a taxonomy with eight schools of thought – offering depth, breadth and precision to one of the most elusive management disciplines of our time. Perfectly marrying theory with practice, this comprehensive text is particularly useful for advanced undergraduate and postgraduate students of brand management, strategy and marketing.

PART OF THE JONES & BARTLETT LEARNING INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES Series meets all standards put forth by CNSS 4011 & 4013A! Access control protects resources against unauthorized viewing, tampering, or destruction. They serve as a primary means of ensuring privacy, confidentiality, and prevention of unauthorized disclosure. Revised and updated with the latest data from this fast paced field, Access Control, Authentication, and Public Key Infrastructure defines the components of access control, provides a business framework for implementation, and discusses legal requirements that impact access control programs. It looks at the risks, threats, and vulnerabilities prevalent in information systems and IT infrastructures and how to handle them. It provides a student and professional resource that details how to put access control systems to work as well as testing and managing them. New to the Second Edition: Updated references to Windows 8 and Outlook 2011 A new discussion of recent Chinese hacking incidence Examples depicting the risks associated with a missing unencrypted laptop containing private data. New sections on the Communications Assistance for Law Enforcement Act (CALEA) and granting Windows folder permissions are added. New information on the Identity Theft Enforcement and Restitution Act and the Digital Millennium Copyright Act (DMCA).

Leverage Azure security services to architect robust cloud solutions in Microsoft Azure Key Features Secure your Azure cloud workloads across applications and networks Protect your Azure infrastructure from cyber attacks Discover tips and techniques for implementing, deploying, and maintaining secure cloud services using best practices Book Description Security is always integrated into cloud platforms, causing users to let their guard down as they take cloud security for granted. Cloud computing brings new security challenges, but you can overcome these with Microsoft Azure's shared responsibility model. Mastering Azure Security covers the latest security features provided by Microsoft to identify different threats and protect your Azure cloud using innovative techniques. The book takes you through the built-in security controls and the multi-layered security features offered by Azure to protect cloud workloads across apps and networks. You'll get to grips with using Azure Security Center for unified security management, building secure application gateways on Azure, protecting the cloud from DDoS attacks, safeguarding with Azure Key Vault, and much more. Additionally, the book covers Azure Sentinel, monitoring and auditing, Azure security and governance best practices, and securing PaaS deployments. By the end of this book, you'll have developed a solid understanding of cybersecurity in the cloud and be able to design secure solutions in Microsoft Azure. What you will learn Understand cloud security concepts Get to grips with managing cloud identities Adopt the Azure security cloud infrastructure Grasp Azure network security concepts Discover how to keep cloud resources secure Implement cloud governance with security policies and rules Who this book is for This book is for Azure cloud professionals, Azure architects, and security professionals looking to implement secure cloud services using Azure Security Centre and other Azure security features. A fundamental understanding of security concepts and prior exposure to the Azure cloud will help you understand the key concepts covered in the book more effectively.

Active Directory stores data about objects such as users and groups in structured data stores and then allows network users and administrators to find and use these data when required.

Is your leadership a competitive advantage, or is it costing you? How do you know? Are you developing your leadership effectiveness at the pace of change? For most leaders today, complexity is outpacing their personal and collective development. Most leaders are in over their heads, whether they know it or not. The most successful organizations over time are the best led. While this has always been true, today escalating global complexity puts leadership effectiveness at a premium. Mastering Leadership involves developing the effectiveness of leaders—individually and collectively—and turning that leadership into a competitive advantage. This comprehensive roadmap for optimal leadership features: Breakthrough research that connects increased leadership effectiveness with enhanced business performance The first fully integrated Universal Model of Leadership—one that integrates the best theory and research in the fields of Leadership and Organizational Development over the last half century A free, online self-assessment of your leadership,

using the Leadership Circle Profile, visibly outlining how you are currently leading and how to develop even greater effectiveness The five stages in the evolution of leadership—Egocentric, Reactive, Creative, Integral, and Unitive—along with the organizational structures and cultures that develop at each of these stages Six leadership practices for evolving your leadership capability at a faster pace A map of your optimal path to greater leadership effectiveness Case stories that facilitate pragmatic application of this Leadership Development System to your particular situation This timeless, authoritative text provides a systemic approach for developing your senior leaders and the leadership system of your organization. It does not recommend quick fixes, but argues that real development requires a strategic, long-term, and integrated approach in order to forge more effective leaders and enhanced business performance. Mastering Leadership offers a developmental pathway to bring forth the highest and best use of yourself, your life, and your leadership. By more meaningfully deploying all of who you are every day, individually and collectively, you will achieve a leadership legacy consistent with your highest aspirations.

Become an expert at managing enterprise identity infrastructure by leveraging Active Directory Key Features Explore the new features in Active Directory Domain Service Manage your Active Directory services for Windows Server 2016 effectively Automate administrative tasks in Active Directory using PowerShell Core 6.x Book Description Active Directory (AD) is a centralized and standardized system that automates networked management of user data, security, and distributed resources and enables inter-operation with other directories. This book will first help you brush up on the AD architecture and fundamentals, before guiding you through core components, such as sites, trust relationships, objects, and attributes. You will then explore AD schemas, LDAP, RMS, and security best practices to understand objects and components and how they can be used effectively. Next, the book will provide extensive coverage of AD Domain Services and Federation Services for Windows Server 2016, and help you explore their new features. Furthermore, you will learn to manage your identity infrastructure for a hybrid cloud setup. All this will help you design, plan, deploy, manage operations, and troubleshoot your enterprise identity infrastructure in a secure and effective manner. You'll later discover Azure AD Module, and learn to automate administrative tasks using PowerShell cmdlets. All along, this updated second edition will cover content based on the latest version of Active Directory, PowerShell 5.1 and LDAP. By the end of this book, you'll be well versed with best practices and troubleshooting techniques for improving security and performance in identity infrastructures. What you will learn Design your Hybrid AD environment by evaluating business and technology requirements Protect sensitive data in a hybrid environment using Azure Information Protection Explore advanced functionalities of the schema Learn about Flexible Single Master Operation (FSMO) roles and their placement Install and migrate Active Directory from older versions to Active Directory 2016 Control users, groups, and devices effectively Design your OU structure in the most effective way Integrate Azure AD with Active Directory Domain Services for a hybrid setup Who this book is for If you are an Active Directory administrator, system administrator, or network professional who has basic knowledge of Active Directory and is looking to become an expert in this topic, this book is for you.

Enhance Windows security and protect your systems and servers from various cyber attacks Key Features Protect your device using a zero-trust approach and advanced security techniques Implement efficient security measures using Microsoft Intune, Configuration Manager, and Azure solutions Understand how to create cyber-threat defense solutions effectively Book Description Are you looking for effective ways to protect Windows-based systems from being compromised by unauthorized users? Mastering Windows Security and Hardening is a detailed guide that helps you gain expertise when implementing efficient security measures and creating robust defense solutions. We will begin with an introduction to Windows security fundamentals, baselining, and the importance of building a baseline for an organization. As you advance, you will learn how to effectively secure and harden your Windows-based system, protect identities, and even manage access. In the concluding chapters, the book will take you through testing, monitoring, and security operations. In addition to this, you'll be equipped with the tools you need to ensure compliance and continuous monitoring through security operations. By the end of this book, you'll have developed a full understanding of the processes and tools involved in securing and hardening your Windows environment. What you will learn Understand baselining and learn the best practices for building a baseline Get to grips with identity management and access management on Windows-based systems Delve into the device administration and remote management of Windows-based systems Explore security tips to harden your Windows server and keep clients secure Audit, assess, and test to ensure controls are successfully applied and enforced Monitor and report activities to stay on top of vulnerabilities Who this book is for This book is for system administrators, cybersecurity and technology professionals, solutions architects, or anyone interested in learning how to secure their Windows-based systems. A basic understanding of Windows security concepts, Intune, Configuration Manager, Windows PowerShell, and Microsoft Azure will help you get the best out of this book.

A bestselling Exchange Server guide, updated for the 2016 release Mastering Microsoft Exchange Server 2016 is the gold-standard reference for system administrators and first-time users alike. Fully updated to align with the latest release, this expert-led guide provides comprehensive coverage and easy-to-follow tutorials for all aspects of Exchange Server installation, configuration, and management. Whether you're migrating from an earlier version or installing Exchange Server for the first time, this book gives you quick access to the answers you need. Step-by-step instructions walk you through planning and design, installation, administration and management, maintenance, and more, so you can get up to speed quickly and get back to work. With a focus on the hands-on details, the Microsoft Certified Masters author team provides practical insight and invaluable guidance on every aspect of Exchange Server 2016, from mastering the basics to leveraging new features. Microsoft Exchange allows access to e-mail, voicemail, and calendars at any time, from almost any device. The 2016 release is designed specifically to appeal to enterprises; if you've been tasked with the

