log analytics workspace workbooks

log analytics workspace workbooks are essential tools for organizations looking to harness the power of data analytics within their cloud environments. These workbooks enable users to create customized reports and visualizations, helping them gain insights from the vast amounts of data generated by their applications and infrastructure. This article delves into the various aspects of log analytics workspace workbooks, including their benefits, features, and best practices for utilization. We will also explore how they integrate with other services and the role they play in enhancing operational efficiency and decision-making processes. By the end of this article, readers will have a comprehensive understanding of how to leverage log analytics workspace workbooks effectively.

What are Log Analytics Workspace Workbooks?

Log analytics workspace workbooks are interactive documents that allow users to visualize and analyze log data collected from various sources within a cloud environment. These workbooks are part of the Azure Monitor suite and are specifically designed to assist users in creating tailored views of their data, which can include charts, tables, and metrics. The core functionality revolves around querying log data using Azure's Kusto Query Language (KQL), which enables users to extract meaningful insights from their logs.

Workbooks serve as a bridge between raw log data and actionable intelligence, allowing teams to monitor system performance, detect anomalies, and troubleshoot issues more effectively. By utilizing these workbooks, organizations can empower their teams with the tools necessary for data-driven decision-making.

Benefits of Using Workbooks

The implementation of log analytics workspace workbooks comes with numerous benefits that can significantly enhance an organization's analytical capabilities. These benefits include:

- **Enhanced Data Visualization:** Workbooks provide a variety of visualization options such as graphs, pie charts, and histograms, which help users understand complex data at a glance.
- **Customizability:** Users can tailor workbooks to meet specific needs, adjusting layouts, queries, and visualizations according to their requirements.
- **Collaboration:** Workbooks can be shared among team members, fostering collaboration and collective problem-solving within an organization.
- **Real-Time Monitoring:** Users can set up dashboards that reflect real-time data, enabling proactive monitoring of systems and applications.
- **Streamlined Reporting:** The ability to generate reports from workbooks simplifies the process of sharing insights with stakeholders.

Key Features of Workbooks

Log analytics workspace workbooks come equipped with various features that enhance their effectiveness. Some of the key features include:

Interactive Querying

Workbooks allow users to run queries using KQL, enabling them to extract specific data points from their logs. This interactive querying capability is crucial for detailed analysis and troubleshooting.

Custom Visualizations

Users can create custom visualizations to represent their data in the most effective way possible. The flexibility in choosing different visualization types enhances the understanding of log data.

Template Gallery

Workbooks come with a template gallery that provides pre-built templates for common scenarios. This feature enables users to quickly get started without having to create a workbook from scratch.

Parameterization

Workbooks support parameters, allowing users to create dynamic queries that can be adjusted based on user input. This feature is particularly useful for generating reusable reports.

Creating and Customizing Workbooks

Creating a workbook in a log analytics workspace is a straightforward process. Users can start with a blank workbook or use a template from the gallery. The following steps outline the process:

1. **Access Your Workspace:** Log in to the Azure portal and navigate to your log analytics workspace.

2. **Create a New Workbook:** Click on the "Workbooks" option in the left menu and select "Add new." Choose whether to start from a template or a blank workbook.

3. **Use KQL Queries:** Add queries using KQL to extract the necessary data. Users can write custom queries or modify existing ones.

4. **Add Visualizations:** After running a query, users can choose from various visualization options to present the data effectively.

5. **Save and Share:** Once the workbook is customized to satisfaction, it can be saved and shared with team members for collaborative analysis.

Integrations with Other Services

Log analytics workspace workbooks are designed to integrate seamlessly with other Azure services, enhancing their functionality. Some of the key integrations include:

- **Azure Monitor:** Workbooks are part of Azure Monitor, allowing users to monitor performance metrics and log data in one unified platform.

- **Azure Sentinel:** Integration with Azure Sentinel provides security analytics capabilities, allowing users to visualize security logs and respond to threats.

- **Application Insights:** Workbooks can pull data from Application Insights, aiding developers in monitoring application performance and user interactions.

- **Power BI:** Exporting data to Power BI for advanced reporting and visualization is also possible, facilitating deeper analytical insights.

Best Practices for Using Workbooks

To maximize the effectiveness of log analytics workspace workbooks, organizations should adhere to several best practices:

- **Define Clear Objectives:** Before creating a workbook, establish what insights are needed and how they will be used. This clarity will guide the design process.

- **Limit Complexity:** While it can be tempting to add numerous visualizations, keeping workbooks simple and focused enhances usability and comprehension.
- **Regular Updates:** Periodically review and update workbooks to ensure they remain relevant and aligned with changing business needs.
- **Engage Stakeholders:** Involve team members and stakeholders in the workbook creation process to gather diverse perspectives and requirements.
- **Utilize Templates:** Make use of the template gallery to save time and leverage best practices established in other workbooks.

Conclusion

Log analytics workspace workbooks are pivotal in transforming raw log data into actionable insights. By leveraging their interactive querying capabilities, customizable visualizations, and integration with other Azure services, organizations can enhance their monitoring and reporting processes. Following best practices when creating and utilizing workbooks will further optimize their effectiveness, leading to improved operational efficiency and informed decision-making. As businesses continue to generate vast amounts of data, mastering log analytics workspace workbooks will be crucial for maintaining a competitive edge in the digital landscape.

Q: What is the primary function of log analytics workspace workbooks?

A: The primary function of log analytics workspace workbooks is to provide a customizable platform for visualizing and analyzing log data collected from various sources, enabling users to extract insights and monitor system performance effectively.

Q: Can workbooks be shared with team members?

A: Yes, workbooks can be easily shared with team members, facilitating collaboration and collective analysis of data insights.

Q: What programming language is used for querying data in workbooks?

A: Kusto Query Language (KQL) is used for querying data in log analytics workspace workbooks, allowing users to extract and analyze log information efficiently.

Q: Are there any templates available for creating workbooks?

A: Yes, log analytics workspace workbooks include a template gallery that offers pre-built templates

for common scenarios, making it easier for users to get started.

Q: How do workbooks integrate with Azure Monitor?

A: Workbooks are part of Azure Monitor, which means they can directly utilize performance metrics and log data collected by Azure Monitor for comprehensive monitoring and reporting.

Q: What are some best practices for using log analytics workspace workbooks?

A: Some best practices include defining clear objectives, limiting complexity, regularly updating workbooks, engaging stakeholders in the creation process, and utilizing available templates.

Q: Can workbooks pull data from other Azure services?

A: Yes, workbooks can integrate with various Azure services such as Azure Sentinel and Application Insights, allowing users to visualize and analyze data across different platforms.

Q: How can I customize the visualizations in a workbook?

A: Users can customize visualizations in a workbook by selecting different chart types, adjusting data ranges, and modifying settings according to their analytical needs.

Q: What types of visualizations can I create in workbooks?

A: Users can create various types of visualizations in workbooks, including line graphs, bar charts, pie charts, and tables, among others.

Q: Is it possible to create dynamic queries in workbooks?

A: Yes, workbooks support parameterization, allowing users to create dynamic queries that can be adjusted based on user input, enhancing the interactivity of the reports.

Log Analytics Workspace Workbooks

log analytics workspace workbooks: *Azure Data Engineering Cookbook* Nagaraj Venkatesan,

Ahmad Osama, 2022-09-26 Nearly 80 recipes to help you collect and transform data from multiple sources into a single data source, making it way easier to perform analytics on the data Key FeaturesBuild data pipelines from scratch and find solutions to common data engineering problemsLearn how to work with Azure Data Factory, Data Lake, Databricks, and Synapse AnalyticsMonitor and maintain your data engineering pipelines using Log Analytics, Azure Monitor, and Azure PurviewBook Description The famous quote 'Data is the new oil' seems more true every day as the key to most organizations' long-term success lies in extracting insights from raw data. One of the major challenges organizations face in leveraging value out of data is building performant data engineering pipelines for data visualization, ingestion, storage, and processing. This second edition of the immensely successful book by Ahmad Osama brings to you several recent enhancements in Azure data engineering and shares approximately 80 useful recipes covering common scenarios in building data engineering pipelines in Microsoft Azure. You'll explore recipes from Azure Synapse Analytics workspaces Gen 2 and get to grips with Synapse Spark pools, SQL Serverless pools, Synapse integration pipelines, and Synapse data flows. You'll also understand Synapse SQL Pool optimization techniques in this second edition. Besides Synapse enhancements, you'll discover helpful tips on managing Azure SQL Database and learn about security, high availability, and performance monitoring. Finally, the book takes you through overall data engineering pipeline management, focusing on monitoring using Log Analytics and tracking data lineage using Azure Purview. By the end of this book, you'll be able to build superior data engineering pipelines along with having an invaluable go-to guide. What you will learnProcess data using Azure Databricks and Azure Synapse AnalyticsPerform data transformation using Azure Synapse data flowsPerform common administrative tasks in Azure SQL DatabaseBuild effective Synapse SQL pools which can be consumed by Power BIMonitor Synapse SQL and Spark pools using Log AnalyticsTrack data lineage using Microsoft Purview integration with pipelinesWho this book is for This book is for data engineers, data architects, database administrators, and data professionals who want to get well versed with the Azure data services for building data pipelines. Basic understanding of cloud and data engineering concepts will help in getting the most out of this book.

log analytics workspace workbooks: *Mastering Azure Virtual Desktop* Ryan Mangan, Neil McLoughlin, Marcel Meurer, 2024-07-26 Explore the advanced capabilities of Azure Virtual Desktop and enhance your skills in cloud-based virtualization and remote application delivery Key Features Learn how to design a strong architecture for your Azure Virtual Desktop Implement, monitor, and maintain a virtual desktop environment Gain insights into Azure Virtual Desktop and prepare successfully for the AZ-140 exam Purchase of the print or Kindle book includes a free PDF eBook Book Description Acquire in-depth knowledge for designing, building, and supporting Azure Virtual Desktop environments with the updated second edition of Mastering Azure Virtual Desktop. With content aligned with exam objectives, this book will help you ace the Microsoft AZ-140 exam. This book starts with an introduction to Azure Virtual Desktop before delving into the intricacies of planning and architecting its infrastructure. As you progress, you'll learn about the implementation process, with an emphasis on best practices and effective strategies. You'll explore key areas such as managing and controlling access, advanced monitoring with the new Azure Monitoring Agent, and advanced application deployment. You'll also gain hands-on experience with essential features like the MSIX app attach, enhancing user experience and operational efficiency. Beyond advancing your skills, this book is a crucial resource for those preparing for the Microsoft Certified: Azure Virtual Desktop Specialty certification. By the end of this book, you'll have a thorough understanding of the Azure Virtual Desktop environment, from design to implementation. What you will learn Architect a robust Azure Virtual Desktop setup Master the essentials of networking and storage configurations Create and configure session host images and host pools Gain insights into controlling access and enhancing security Implement FSLogix profile containers and Cloud Cache for improved performance Discover MSIX app attach for efficient application delivery Understand strategies for business continuity and disaster recovery Monitor and manage the performance and health of your Azure Virtual Desktop environment Who this book is for Mastering Azure Virtual Desktop is for IT

professionals, modern workspace administrators, architects, and consultants who want to learn how to design, implement, and manage Azure Virtual Desktop environments. Whether you're aiming to enhance your expertise in cloud virtualization or preparing for the Microsoft AZ-140 exam, this guide is an invaluable resource for advancing your skills.

log analytics workspace workbooks: Microsoft Defender for Cloud Yuri Diogenes, Tom Janetscheck, 2022-10-18 The definitive practical guide to Microsoft Defender for Cloud covering new components and multi-cloud enhancements! Microsoft Defender for Cloud offers comprehensive tools for hardening resources, tracking security posture, protecting against attacks, and streamlining security management – all in one natively integrated toolset. Now, leading Microsoft security experts Yuri Diogenes and Tom Janetscheck help you apply its robust protection, detection, and response capabilities throughout your operations, protecting workloads running on all your cloud, hybrid, and on-premises platforms. This guide shows how to make the most of new components, enhancements, and deployment scenarios, as you address today's latest threat vectors. Sharing best practices, expert tips, and optimizations only available from Microsoft's Defender for Cloud team, the authors walk through improving everything from policies and governance to incident response and risk management. Whatever your role or experience, they'll help you address new security challenges far more effectively—and save hours, days, or even weeks. Two of Microsoft's leading cloud security experts show how to: Assess new threat landscapes, the MITRE ATT&CK framework, and the implications of ''assume-breach'' Explore Defender for Cloud architecture, use cases, and adoption considerations including multicloud with AWS and GCP Plan for effective governance, successful onboarding, and maximum value Fully visualize complex cloud estates and systematically reduce their attack surfaces Prioritize risks with Secure Score, and leverage at-scale tools to build secure cloud-native apps Establish consistent policy enforcement to avoid drift Use advanced analytics and machine learning to identify attacks based on signals from all cloud workloads Enhance security posture by integrating with the Microsoft Sentinel SIEM/SOAR, Microsoft Purview, and Microsoft Defender for Endpoint Leverage just-in-time VM access and other enhanced security capabilities About This Book For architects, designers, implementers, SecOps professionals, developers, and security specialists working in Microsoft Azure environments For all IT professionals and decision-makers concerned with securing modern hybrid/multicloud environments, cloud-native apps, and PaaS services

log analytics workspace workbooks: *Exam Ref SC-300 Microsoft Identity and Access Administrator* Razi Rais, Ilya Lushnikov, Jeevan Bisht, Padma Chilakapati, Vinayak Shenoy, 2022-12-30 Prepare for Microsoft Exam SC-300 and demonstrate your real-world ability to design, implement, and operate identity and access management systems with Microsoft Azure Active Directory (AD). Designed for professionals involved in secure authentication, access, or identity management, this Exam Ref focuses on the critical thinking and decision-making acumen needed for success at the Microsoft Certified: Identity and Access Administrator Associate level. Focus on the expertise measured by these objectives: Implement identities in Azure AD Implement authentication and access management Implement access management for applications Plan and implement identity governance in Azure AD This Microsoft Exam Ref: Organizes its coverage by exam objectives Features strategic, what-if scenarios to challenge you Assumes that you are an administrator, security engineer, or other IT professional who provides, or plans to provide, secure identity and access services for an enterprise About the Exam Exam SC-300 focuses on the knowledge needed to configure and manage Azure AD tenants; create, configure, and manage Azure AD identities; implement and manage external identities and hybrid identity; plan, implement, and manage Azure Multifactor Authentication (MFA), self-service password reset, Azure AD user authentication, and Azure AD conditional access; manage Azure AD Identity Protection; implement access management for Azure resources; manage and monitor app access with Microsoft Defender for Cloud Apps; plan, implement, and monitor enterprise app integration; enable app registration; plan and implement entitlement management and privileged access; plan, implement, and manage access reviews; and monitor Azure AD. About Microsoft Certification Passing this exam fulfills your

requirements for the Microsoft Certified: Identity and Access Administrator Associate certification, demonstrating your abilities to design, implement, and operate identity and access management systems with Azure AD; configure and manage identity authentication and authorization for users, devices, resources, and applications; provide seamless experiences and self-service; verify identities for Zero Trust; automate Azure AD management; troubleshoot and monitor identity and access environments; and collaborate to drive strategic identity projects, modernize identity solutions, and implement hybrid identity and/or identity governance. See full details at: microsoft.com/learn

log analytics workspace workbooks: Microsoft Defender for Cloud Cookbook Sasha Kranjac, 2022-07-22 Effectively secure their cloud and hybrid infrastructure, how to centrally manage security, and improve organizational security posture Key Features • Implement and optimize security posture in Azure, hybrid, and multi-cloud environments • Understand Microsoft Defender for Cloud and its features • Protect workloads using Microsoft Defender for Cloud's threat detection and prevention capabilities Book Description Microsoft Defender for Cloud is a multi-cloud and hybrid cloud security posture management solution that enables security administrators to build cyber defense for their Azure and non-Azure resources by providing both recommendations and security protection capabilities. This book will start with a foundational overview of Microsoft Defender for Cloud and its core capabilities. Then, the reader is taken on a journey from enabling the service, selecting the correct tier, and configuring the data collection, to working on remediation. Next, we will continue with hands-on guidance on how to implement several security features of Microsoft Defender for Cloud, finishing with monitoring and maintenance-related topics, gaining visibility in advanced threat protection in distributed infrastructure and preventing security failures through automation. By the end of this book, you will know how to get a view of your security posture and where to optimize security protection in your environment as well as the ins and outs of Microsoft Defender for Cloud. What you will learn • Understand Microsoft Defender for Cloud features and capabilities • Understand the fundamentals of building a cloud security posture and defending your cloud and on-premises resources • Implement and optimize security in Azure, multi-cloud and hybrid environments through the single pane of glass - Microsoft Defender for Cloud • Harden your security posture, identify, track and remediate vulnerabilities • Improve and harden your security and services security posture with Microsoft Defender for Cloud benchmarks and best practices • Detect and fix threats to services and resources Who this book is for This book is for Security engineers, systems administrators, security professionals, IT professionals, system architects, and developers. Anyone whose responsibilities include maintaining security posture, identifying, and remediating vulnerabilities, and securing cloud and hybrid infrastructure. Anyone who is willing to learn about security in Azure and to build secure Azure and hybrid infrastructure, to improve their security posture in Azure, hybrid and multi-cloud environments by leveraging all the features within Microsoft Defender for Cloud.

log analytics workspace workbooks: Microsoft Sentinel in Action Richard Diver, Gary Bushey, John Perkins, 2022-02-10 Learn how to set up, configure, and use Microsoft Sentinel to provide security incident and event management services for your multi-cloud environment Key FeaturesCollect, normalize, and analyze security information from multiple data sourcesIntegrate AI, machine learning, built-in and custom threat analyses, and automation to build optimal security solutionsDetect and investigate possible security breaches to tackle complex and advanced cyber threatsBook Description Microsoft Sentinel is a security information and event management (SIEM) tool developed by Microsoft that helps you integrate cloud security and artificial intelligence (AI). This book will teach you how to implement Microsoft Sentinel and understand how it can help detect security incidents in your environment with integrated AI, threat analysis, and built-in and community-driven logic. The first part of this book will introduce you to Microsoft Sentinel and Log Analytics, then move on to understanding data collection and management, as well as how to create effective Microsoft Sentinel queries to detect anomalous behaviors and activity patterns. The next part will focus on useful features, such as entity behavior analytics and Microsoft Sentinel playbooks, along with exploring the new bi-directional connector for ServiceNow. In the next part,

you'll be learning how to develop solutions that automate responses needed to handle security incidents and find out more about the latest developments in security, techniques to enhance your cloud security architecture, and explore how you can contribute to the security community. By the end of this book, you'll have learned how to implement Microsoft Sentinel to fit your needs and protect your environment from cyber threats and other security issues. What you will learnImplement Log Analytics and enable Microsoft Sentinel and data ingestion from multiple sourcesTackle Kusto Query Language (KQL) codingDiscover how to carry out threat hunting activities in Microsoft SentinelConnect Microsoft Sentinel to ServiceNow for automated ticketingFind out how to detect threats and create automated responses for immediate resolutionUse triggers and actions with Microsoft Sentinel playbooks to perform automationsWho this book is for You'll get the most out of this book if you have a good grasp on other Microsoft security products and Azure, and are now looking to expand your knowledge to incorporate Microsoft Sentinel. Security experts who use an alternative SIEM tool and want to adopt Microsoft Sentinel as an additional or a replacement service will also find this book useful.

log analytics workspace workbooks: Learn Azure Sentinel Richard Diver, Gary Bushey, 2020-04-07 Understand how to set up, configure, and use Azure Sentinel to provide security incident and event management services for your environment Key FeaturesSecure your network, infrastructure, data, and applications on Microsoft Azure effectivelyIntegrate artificial intelligence, threat analysis, and automation for optimal security solutionsInvestigate possible security breaches and gather forensic evidence to prevent modern cyber threatsBook Description Azure Sentinel is a Security Information and Event Management (SIEM) tool developed by Microsoft to integrate cloud security and artificial intelligence (AI). Azure Sentinel not only helps clients identify security issues in their environment, but also uses automation to help resolve these issues. With this book, you'll implement Azure Sentinel and understand how it can help find security incidents in your environment with integrated artificial intelligence, threat analysis, and built-in and community-driven logic. This book starts with an introduction to Azure Sentinel and Log Analytics. You'll get to grips with data collection and management, before learning how to create effective Azure Sentinel queries to detect anomalous behaviors and patterns of activity. As you make progress, you'll understand how to develop solutions that automate the responses required to handle security incidents. Finally, you'll grasp the latest developments in security, discover techniques to enhance your cloud security architecture, and explore how you can contribute to the security community. By the end of this book, you'll have learned how to implement Azure Sentinel to fit your needs and be able to protect your environment from cyber threats and other security issues. What you will learnUnderstand how to design and build a security operations centerDiscover the key components of a cloud security architectureManage and investigate Azure Sentinel incidentsUse playbooks to automate incident responsesUnderstand how to set up Azure Monitor Log Analytics and Azure SentinelIngest data into Azure Sentinel from the cloud and on-premises devicesPerform threat hunting in Azure SentinelWho this book is for This book is for solution architects and system administrators who are responsible for implementing new solutions in their infrastructure. Security analysts who need to monitor and provide immediate security solutions or threat hunters looking to learn how to use Azure Sentinel to investigate possible security breaches and gather forensic evidence will also benefit from this book. Prior experience with cloud security, particularly Azure, is necessary.

log analytics workspace workbooks: Azure FinOps Essentials Parag Bhardwaj, Arun Kumar Samayam, 2024-09-30 DESCRIPTION Azure FinOps, the intersection of finance, operations, and technology, has become paramount in optimizing cloud spending. "Azure FinOps Essentials "is a guide to help you navigate easily with cost management and optimization within Microsoft Cloud. This book is a practical guide to cutting cloud costs in Microsoft Azure. It covers everything from understanding Azure services and cost management to advanced strategies like Infrastructure as Code and serverless computing. You will learn to set up Azure Cost Management, optimize resources with tools like Reserved Instances, and enforce governance using Azure Policy. The book also

highlights case studies and best practices to help you build a FinOps culture, streamline costs, and enhance cost-efficiency in your cloud environment. If you are new to cloud financial management or need a refresher on some of the best practices, Azure FinOps Essentials is designed for anyone running an operational workload in both public and private clouds who wants to improve their expense management within the environment. KEY FEATURES ● An in-depth guide to the fundamentals of Azure cost management. ● Detailed instructions for creating cost alerts and establishing budgets. ● Practical strategies to enhance cloud resource efficiency. WHAT YOU WILL LEARN ● Establish and enforce standards for Azure cloud cost management through auditing. ● Learn cost-saving tactics like rightsizing and using Reserved Instances. ● Master Azure tools for monitoring spending, budgeting, and setting up alerts. ● Build custom dashboards to accurately display key financial metrics. ● Implement governance and compliance for effective cloud financial management. WHO THIS BOOK IS FOR This book is for cloud architects, DevOps engineers and IT professionals managing costs in Azure environments. It provides the necessary knowledge and skills to optimize cloud spending, improve efficiency, and drive business value. TABLE OF CONTENTS 1. Introduction to Azure FinOps 2. Azure Fundamentals for FinOps 3. Azure Cost Management and Billing 4. Cost Optimization Strategies 5. Azure Monitoring 6. Cost Allocation and Chargebacks 7. Governance and Compliance 8. Advanced Azure FinOps Techniques 9. Azure FinOps Best Practices 10. Azure Case Studies and Real-world Examples 11. Future Trends and Innovations in Azure FinOps 12. Final Thoughts and Next Steps

log analytics workspace workbooks: The Art of Site Reliability Engineering (SRE) with Azure Unai Huete Beloki, 2025-08-30 Gain a foundational understanding of SRE and learn its basic concepts and architectural best practices for deploying Azure IaaS, PaaS, and microservices-based resilient architectures. The new edition of the book has been updated with the latest Azure features for high-availability in storage, networking, and virtual machine computing. It also includes new updates in Azure SQL, Cosmos DB, and Azure Load Testing. Additionally, the integration of agents with Microsoft services has been covered in this revised edition. After reading this book, you will understand the underlying concepts of SRE and its implementation using Azure public cloud. What You Will Learn: Learn SRE definitions and metrics like SLI/SLO/SLA, Error Budget, toil, MTTR, MTTF, and MTBF Understand Azure Well-Architected Framework (WAF) and Disaster Recovery scenarios on Azure Understand resiliency and how to design resilient solutions in Azure for different architecture types and services Master core DevOps concepts and the difference between SRE and tools like Azure DevOps and GitHub Utilize Azure observability tools like Azure Monitor, Application Insights, KQL or Grafana Who Is This Book For: IT operations administrators, engineers, security team members, as well as developers or DevOps engineers.

log analytics workspace workbooks: *Cloud Observability with Azure Monitor* José Ángel Fernández, Manuel Lázaro Ramírez, 2024-11-22 Implement real-time monitoring, visualization, analytics, and troubleshooting strategies on Azure to ensure optimal performance and reliability in your cloud environment Key Features Monitor Azure-native, hybrid, and multi-cloud infrastructure effectively Design proactive incident responses and visualization dashboards for configuring, optimizing, and monitoring data Implement strategies for monitoring Azure applications using real-world case studies Purchase of the print or Kindle book includes a free PDF eBook Book Description Cloud observability is complex and costly due to the use of hybrid and multi-cloud infrastructure as well as various Azure tools, hampering IT teams' ability to monitor and analyze issues. The authors distill their years of experience with Microsoft to share the strategic insights and practical skills needed to optimize performance, ensure reliability, and navigate the dynamic landscape of observability on Azure. You'll get an in-depth understanding of cloud observability and Azure Monitor basics, before getting to grips with the configuration and optimization of data sources and pipelines for effective monitoring. You'll learn about advanced data analysis techniques using metrics and the Kusto Query Language (KQL) for your logs, design proactive incident response strategies with automated alerts, and visualize reports via dashboards. Using hands-on examples and best practices, you'll explore the integration of Azure Monitor with Azure Arc and third-party

tools, such as Datadog, Elastic Stack, or Dynatrace. You'll also implement artificial intelligence for IT Operations (AIOps) and secure monitoring for hybrid and multi-cloud environments, aligned with emerging trends. By the end of this book, you'll be able to develop robust and cost-optimized observability solutions for monitoring your Azure infrastructure and apps using Azure Monitor. What you will learn Get a holistic overview of cloud observability with Azure Monitor Configure and optimize data sources to monitor Azure solutions Analyze logs and metrics using advanced data analysis techniques with KQL Design proactive incident response strategies with automated alerts Visualize monitoring data through impactful dashboards and reports Extend observability to hybrid and multi-cloud environments with Azure Arc Build and implement monitoring solutions on Azure, aligned with industry standards Who this book is for If you're a seasoned cloud engineer, cloud architect, DevOps engineer, SRE, or an aspiring cloud practitioner eager to elevate your observability skills on Azure and implement monitoring strategies using Azure Monitor, then this book is for you. A basic understanding of Azure cloud services, cloud infrastructure management, and network virtualization will be helpful.

log analytics workspace workbooks: The Definitive Guide to KQL Mark Morowczynski, Rod Trent, Matthew Zorich, 2024-05-16 Turn the avalanche of raw data from Azure Data Explorer, Azure Monitor, Microsoft Sentinel, and other Microsoft data platforms into actionable intelligence with KQL (Kusto Query Language). Experts in information security and analysis guide you through what it takes to automate your approach to risk assessment and remediation, speeding up detection time while reducing manual work using KQL. This accessible and practical guide—designed for a broad range of people with varying experience in KQL—will quickly make KQL second nature for information security. Solve real problems with Kusto Query Language— and build your competitive advantage: Learn the fundamentals of KQL—what it is and where it is used Examine the anatomy of a KQL query Understand why data summation and aggregation is important See examples of data summation, including count, countif, and dcount Learn the benefits of moving from raw data ingestion to a more automated approach for security operations Unlock how to write efficient and effective queries Work with advanced KQL operators, advanced data strings, and multivalued strings Explore KQL for day-to-day admin tasks, performance, and troubleshooting Use KQL across Azure, including app services and function apps Delve into defending and threat hunting using KQL Recognize indicators of compromise and anomaly detection Learn to access and contribute to hunting queries via GitHub and workbooks via Microsoft Entra ID

log analytics workspace workbooks: Microsoft Intune Administration Manish Bangia, 2024-07-31 DESCRIPTION This book is outlined in a way that will help the readers learn the concepts of Microsoft Intune from scratch, covering the basic terminologies used. It aims to start your Intune journey in the most efficient way to build your career and help you upscale existing skills. It not only covers the best practices of Microsoft Intune but also co-management and migration strategy for Configuration Manager. Readers will understand the workload feature of SCCM and learn how to create a strategy to move the workload steadily. The book includes all practical examples of deploying applications, updates, and policies, and a comparison of the same with on-premises solutions including SCCM/WSUS/Group Policy, etc. Troubleshooting aspects of Intune-related issues are also covered. The readers will be able to implement effective solutions to their organization the right way after reading the book. They will become confident with device management and further expand their career into multiple streams based upon the solid foundation. KEY FEATURES ● Understanding the basics and setting up environment for Microsoft Intune. ● Optimizing device performance with Endpoint analytics. ● Deploying applications, updates, policies, etc., using Intune. WHAT YOU WILL LEARN ● Microsoft Intune basics and terminologies. ● Setting up Microsoft Intune and integration with on-premises infrastructure. ● Device migration strategy to move away from on-premises to cloud solution. ● Device configuration policies and settings. ● Windows Autopilot configuration, provisioning, and deployment. ● Reporting and troubleshooting for Intune-related tasks. WHO THIS BOOK IS FOR This book targets IT professionals, particularly those managing devices, including system administrators, cloud architects, and security specialists,

looking to leverage Microsoft Intune for cloud-based or hybrid device management. TABLE OF CONTENTS 1. Introduction to the Course 2. Fundamentals of Microsoft Intune 3. Setting Up and Configuring Intune 4. Device Enrollment Method 5. Preparing Infrastructure for On-premises Infra with SCCM 6. Co-management: Migration from SCCM to Intune 7. Explore Device Management Features 8. Configure Windows Update for Business 9. Application Management 10. Configuration Policies and Settings 11. Windows Autopilot 12. Device Management and Protection 13. Securing Device 14. Reporting and Monitoring 15. Endpoint Analytics 16. Microsoft Intune Suite and Advance Settings 17. Troubleshooting

log analytics workspace workbooks: Migrating Linux to Microsoft Azure Rithin Skaria, Toni Willberg, 2021-07-28 Discover expert guidance for moving on-premises virtual machines running on Linux servers to Azure by implementing best practices and optimizing costs Key FeaturesWork with real-life migrations to understand the dos and don'ts of the processDeploy a new Linux virtual machine and perform automation and configuration managementGet to grips with debugging your system and collecting error logs with the help of hands-on examplesBook Description With cloud adoption at the core of digital transformation for organizations, there has been a significant demand for deploying and hosting enterprise business workloads in the cloud. Migrating Linux to Microsoft Azure offers a wealth of actionable insights into deploying Linux workload to Azure. You'll begin by learning about the history of IT, operating systems, Unix, Linux, and Windows before moving on to look at the cloud and what things were like before virtualization. This will help anyone new to Linux become familiar with the terms used throughout the book. You'll then explore popular Linux distributions, including RHEL 7, RHEL 8, SLES, Ubuntu Pro, CentOS 7, and more. As you progress, you'll cover the technical details of Linux workloads such as LAMP, Java, and SAP, and understand how to assess your current environment and prepare for your migration to Azure through cloud governance and operations planning. Finally, you'll go through the execution of a real-world migration project and learn how to analyze and debug some common problems that Linux on Azure users may encounter. By the end of this Linux book, you'll be proficient at performing an effective migration of Linux workloads to Azure for your organization. What you will learnGrasp the terminology and technology of various Linux distributionsUnderstand the technical support co-operation between Microsoft and commercial Linux vendorsAssess current workloads by using Azure MigratePlan cloud governance and operationsExecute a real-world migration projectManage project, staffing, and customer engagementWho this book is for This book is for cloud architects, cloud solution providers, and any stakeholders dealing with migration of Linux workload to Azure. Basic familiarity with Microsoft Azure would be a plus.

log analytics workspace workbooks: Azure Databricks Cookbook Phani Raj, Vinod Jaiswal, 2021-09-17 Get to grips with building and productionizing end-to-end big data solutions in Azure and learn best practices for working with large datasets Key FeaturesIntegrate with Azure Synapse Analytics, Cosmos DB, and Azure HDInsight Kafka Cluster to scale and analyze your projects and build pipelinesUse Databricks SQL to run ad hoc queries on your data lake and create dashboardsProductionize a solution using CI/CD for deploying notebooks and Azure Databricks Service to various environmentsBook Description Azure Databricks is a unified collaborative platform for performing scalable analytics in an interactive environment. The Azure Databricks Cookbook provides recipes to get hands-on with the analytics process, including ingesting data from various batch and streaming sources and building a modern data warehouse. The book starts by teaching you how to create an Azure Databricks instance within the Azure portal, Azure CLI, and ARM templates. You'll work through clusters in Databricks and explore recipes for ingesting data from sources, including files, databases, and streaming sources such as Apache Kafka and EventHub. The book will help you explore all the features supported by Azure Databricks for building powerful end-to-end data pipelines. You'll also find out how to build a modern data warehouse by using Delta tables and Azure Synapse Analytics. Later, you'll learn how to write ad hoc queries and extract meaningful insights from the data lake by creating visualizations and dashboards with Databricks SQL. Finally, you'll deploy and productionize a data pipeline as well as

deploy notebooks and Azure Databricks service using continuous integration and continuous delivery (CI/CD). By the end of this Azure book, you'll be able to use Azure Databricks to streamline different processes involved in building data-driven apps. What you will learnRead and write data from and to various Azure resources and file formatsBuild a modern data warehouse with Delta Tables and Azure Synapse AnalyticsExplore jobs, stages, and tasks and see how Spark lazy evaluation worksHandle concurrent transactions and learn performance optimization in Delta tablesLearn Databricks SQL and create real-time dashboards in Databricks SQLIntegrate Azure DevOps for version control, deploying, and productionizing solutions with CI/CD pipelinesDiscover how to use RBAC and ACLs to restrict data accessBuild end-to-end data processing pipeline for near real-time data analyticsWho this book is for This recipe-based book is for data scientists, data engineers, big data professionals, and machine learning engineers who want to perform data analytics on their applications. Prior experience of working with Apache Spark and Azure is necessary to get the most out of this book.

log analytics workspace workbooks: Microsoft Azure Security Technologies (AZ-500) - A Certification Guide Jayant Sharma, 2021-10-14 With Azure security, you can build a prosperous career in IT security. KEY FEATURES ● In-detail practical steps to fully grasp Azure Security concepts. ● Wide coverage of Azure Architecture, Azure Security services, and Azure Security implementation techniques. ● Covers multiple topics from other Azure certifications (AZ-303, AZ-304, and SC series). DESCRIPTION 'Microsoft Azure Security Technologies (AZ-500) - A Certification Guide' is a certification guide that helps IT professionals to start their careers as Azure Security Specialists by clearing the AZ-500 certification and proving their knowledge of Azure security services. Authored by an Azure security professional, this book takes readers through a series of steps to gain a deeper insight into Azure security services. This book will help readers to understand key concepts of the Azure AD architecture and various methods of hybrid authentication. It will help readers to use Azure AD security solutions like Azure MFA, Conditional Access, and PIM. It will help readers to maintain various industry standards for an Azure environment through Azure Policies and Azure Blueprints. This book will also help to build a secure Azure network using Azure VPN, Azure Firewall, Azure Front Door, Azure WAF, and other services. It will provide readers with a clear understanding of various security services, including Azure Key vault, Update management, Microsoft Endpoint Protection, Azure Security Center, and Azure Sentinel in detail. This book will facilitate the improvement of readers' abilities with Azure Security services to sprint to a rewarding career. WHAT YOU WILL LEARN ● Configuring secure authentication and authorization for Azure AD identities. ● Advanced security configuration for Azure compute and network services. ● Hosting and authorizing secure applications in Azure. ● Best practices to secure Azure SQL and storage services. ● Monitoring Azure services through Azure monitor, security center, and Sentinel. ● Designing and maintaining a secure Azure IT infrastructure. WHO THIS BOOK IS FOR This book is for security engineers who want to enhance their career growth in implementing security controls, maintaining the security posture, managing identity and access, and protecting data, applications, and networks of Microsoft Azure. Intermediate-level knowledge of Azure terminology, concepts, networking, storage, and virtualization is required. TABLE OF CONTENTS 1. Managing Azure AD Identities and Application Access 2. Configuring Secure Access by Using Azure Active Directory 3. Managing Azure Access Control 4. Implementing Advance Network Security 5. Configuring Advance Security for Compute 6. Configuring Container Security 7. Monitoring Security by Using Azure Monitor 8. Monitoring Security by Using Azure Security Center 9. Monitoring Security by Using Azure Sentinel 10. Configuring Security for Azure Storage 11. Configuring Security for Azure SQL Databases

log analytics workspace workbooks: *Microsoft 365 Security, Compliance, and Identity Administration* Peter Rising, 2023-08-18 Explore expert tips and techniques to effectively manage the security, compliance, and identity features within your Microsoft 365 applications Purchase of the print or Kindle book includes a free PDF eBook Key Features Discover techniques to reap the full potential of Microsoft security and compliance suite Explore a range of strategies for effective security and compliance Gain practical knowledge to resolve real-world challenges Book Description

The Microsoft 365 Security, Compliance, and Identity Administration is designed to help you manage, implement, and monitor security and compliance solutions for Microsoft 365 environments. With this book, you'll first configure, administer identity and access within Microsoft 365. You'll learn about hybrid identity, authentication methods, and conditional access policies with Microsoft Intune. Next, you'll discover how RBAC and Azure AD Identity Protection can be used to detect risks and secure information in your organization. You'll also explore concepts such as Microsoft Defender for endpoint and identity, along with threat intelligence. As you progress, you'll uncover additional tools and techniques to configure and manage Microsoft 365, including Azure Information Protection, Data Loss Prevention (DLP), and Microsoft Defender for Cloud Apps. By the end of this book, you'll be well-equipped to manage and implement security measures within your Microsoft 365 suite successfully. What you will learn Get up to speed with implementing and managing identity and access Understand how to employ and manage threat protection Manage Microsoft 365's governance and compliance features Implement and manage information protection techniques Explore best practices for effective configuration and deployment Ensure security and compliance at all levels of Microsoft 365 Who this book is for This book is for IT professionals, administrators, or anyone looking to pursue a career in security administration and wants to enhance their skills in utilizing Microsoft 365 Security Administration. A basic understanding of administration principles of Microsoft 365 and Azure Active Directory is a must. A good grip of on-premises Active Directory will be beneficial.

log analytics workspace workbooks: Exam Ref AZ-303 Microsoft Azure Architect Technologies Timothy L. Warner, Mike Pfeiffer, Derek Schauland, Nicole Stevens, Gurvinder Singh, 2020-12-09 Prepare for Microsoft Exam AZ-303—and help demonstrate your real-world mastery of architecting high-value Microsoft Azure solutions for your organization or customers. Designed for modern IT professionals, this Exam Ref focuses on the critical thinking and decision-making acumen needed for success at the Microsoft Certified Expert level. Focus on the expertise measured by these objectives: • Implement and monitor an Azure infrastructure • Implement management and security solutions • Implement solutions for apps • Implement and manage data platforms This Microsoft Exam Ref: • Organizes its coverage by exam objectives • Features strategic, what-if scenarios to challenge you • Assumes you are an IT professional who wants to demonstrate your ability to design modern Microsoft Azure solutions involving compute, network, storage, and security About the Exam Exam AZ-303 focuses on knowledge needed to implement cloud infrastructure monitoring, storage accounts, and VMs (Windows and Linux); automate resource deployment and configuration; implement virtual networking and Azure Active Directory; implement and manage hybrid identities; manage Azure workloads; implement Azure Site Recovery; implement application infrastructure; manage application security; implement load balancing and network security; integrate Azure virtual networks with on-premises networks; implement and manage Azure governance solutions; manage Role-Based Access Control; implement application infrastructure and container-based apps; implement NoSQL and Azure SQL databases; and implement Azure SQL database managed instances. About Microsoft Certification Passing this exam and Exam AZ-304: Microsoft Azure Architect Design fulfills your requirements for the Microsoft Certified: Azure Solutions Architect Expert credential, demonstrating your expertise in compute, network, storage, and security for designing and implementing modern cloudbased solutions that run on Microsoft Azure. See full details at: microsoft.com/learn

log analytics workspace workbooks: Microsoft Teams Administration Cookbook Fabrizio Volpe, 2023-08-22 Microsoft Teams is used in hundreds of thousands of organizations to help keep remote and hybrid workplaces with dispersed workforces running smoothly. But while Microsoft Teams can seem easy for the user, Teams administrators must stay on top of a wide range of topics, including device administration techniques, quality benchmarks, and security and compliance measures. With this handy cookbook, author Fabrizio Volpe provides a clear, concise overview of administrative tasks in Teams-along with step-by-step recipes to help you solve many of the common problems that system administrators, project managers, solution architects, and IT consultants may

face when configuring, implementing, and managing Microsoft Teams. Think of this book as a detailed, immensely practical cheat sheet for Microsoft Teams administrators. Recipes in the book will show you how to: Apply Teams best practices, compliance, and security Automate administrative tasks Successfully deploy Teams Implement Teams collaboration Deploy and manage Microsoft Teams Rooms Leverage the monitoring, productivity, and accessibility features Foresee roadblocks in migrations to Teams and Teams Voice Optimize Teams on virtual machines

log analytics workspace workbooks: *Microsoft Security Operations Analyst Associate (SC-200) Certification Guide* Aditya Katira, 2025-06-12 TAGLINE Detect, Investigate, and Respond to Threats with Microsoft tools KEY FEATURES ● In-depth coverage of Microsoft SC 200 Certification to secure identities, endpoints, and cloud workloads across hybrid environments. ● Hands-on guidance with KQL, threat hunting, and automation to simulate real-world security operations. ● Exclusive insights on AI-powered security using Microsoft Copilot and emerging trends shaping the future of SOC operations. DESCRIPTION The Microsoft Security Operations Analyst certification (SC-200) is a vital credential for anyone aiming to excel in modern cybersecurity roles. The Microsoft Security Operations Analyst Associate (SC-200) Certification Guide is your companion for mastering the skills and tools needed to pass the exam and thrive as a Security Operations Analyst in Microsoft environments. Through in-depth coverage of Microsoft Sentinel, Microsoft Defender for Cloud, and Microsoft 365 Defender, you'll learn to detect, investigate, and respond to threats across hybrid and cloud infrastructures. With a focus on real-world use cases, this book walks you through key concepts such as threat mitigation, incident response, and security monitoring—all aligned with the latest SC-200 objectives. You'll gain hands-on experience configuring Microsoft's security tools, writing queries using Kusto Query Language (KQL), creating custom detection rules, and automating responses for streamlined SOC operations. Each chapter builds your expertise through practical examples and exercises, helping bridge the gap between certification prep and operational readiness. Whether you're looking to boost your cybersecurity career or strengthen your organization's defenses, this guide provides the knowledge and exam confidence you need. Take the next step to become a Microsoft Security Operations Analyst expert. WHAT WILL YOU LEARN ● Configure and operationalize Microsoft Defender for Identity, Endpoint, and Cloud to protect users and resources. ● Leverage Microsoft Copilot for Security to enhance investigation and response using generative AI capabilities. ● Implement Data Loss Prevention (DLP), Insider Risk Management, and eDiscovery for robust information protection. ● Use Kusto Query Language (KQL) to analyze logs, hunt threats, and develop custom queries. ● Enhance security visibility through effective use of data connectors and threat intelligence feeds in Microsoft Sentinel. ● Automate detection and response workflows using Sentinel's playbooks, analytics rules, and notebooks for advanced threat management. WHO IS THIS BOOK FOR? This book is ideal for security analysts, system administrators, and IT professionals preparing for the SC-200: Microsoft Security Operations Analyst certification. It is also valuable for those looking to deepen their expertise in Microsoft security solutions. A working knowledge of Microsoft Azure, Microsoft 365, and core cybersecurity concepts is recommended to get the most from this guide. TABLE OF CONTENTS 1. Microsoft Defender Identity Endpoint Cloud and More 2. Microsoft Copilot for Security with AI Assistance 3. Mastering Data Protection with Data Loss Prevention, Insider Risk, and Content Search 4. Securing Endpoint Deployment Management and Investigation 5. Managing Security Posture Across Platforms 6. KQL Mastery for Querying Analyzing and Working with Security Data 7. Optimizing Security Operations with Log Management Watchlists and Threat Intelligence 8. Expanding Security Visibility with Data Connectors in Microsoft Sentinel 9. Tactical Threat Management with Detection Automation and Response 10. Decoding Threat Hunting by Leveraging Search Jobs and Notebooks 11. Future Trends in Security Operations Index

log analytics workspace workbooks: *Mastering Microsoft 365 Security Technologies* Pramiti Bhatnagar, 2025-05-28 DESCRIPTION Microsoft security technologies provide a robust, integrated defense against evolving cyber threats, spanning identity, endpoints, applications, and data across hybrid environments. It offers a unified and intelligent defense across an organization's digital

landscape. This book will introduce readers to Microsoft security solutions. It covers Microsoft Defender, Microsoft Entra ID, and Microsoft Purview. Readers will learn how they can protect their organization across different attack vectors such as email, identity, data, endpoints, and applications. It discusses how to protect the user identities using Microsoft Entra ID, protect devices and applications using Microsoft Defender and Microsoft Sentinel, and protect organization data using Microsoft Purview. With a focus on real-world scenarios, hands-on labs, and expert guidance, cybersecurity professionals will gain a deep understanding of Microsoft security solutions and how to use them to protect their organizations from bad actors. By the end of this book, you will possess the practical knowledge and skills to design, implement, and manage a strong security posture across your organization's Microsoft infrastructure, confidently protecting identities, data, and applications from modern cyberattacks. WHAT YOU WILL LEARN ● Data security and governance using Microsoft Purview information protection and DLP. ● Protecting devices, identities, M365, and non-M365 applications using Microsoft Defender. ● Microsoft’s Zero Trust Network Access solution – secure services edge. ● Manage Entra ID users, groups, RBAC, Admin Units, Protected Actions effectively. ● Managing regulatory compliance and privacy. WHO THIS BOOK IS FOR This book is ideal for IT professionals and administrators seeking careers in security administration using Microsoft security technologies. Readers need foundational cloud computing knowledge (IaaS, PaaS, SaaS), basic M365 cloud and Azure familiarity, plus awareness of Zero Trust, identity and access, and platform protection. TABLE OF CONTENTS 1. Introduction to Microsoft Entra 2. Implementing Identity 3. Identity Management 4. Identity Protection 5. Identity Governance 6. Microsoft Defender XDR 7. Protecting Identities 8. Protecting Endpoints 9. Protecting M365 Apps 10. Protecting Non-Microsoft Cloud Apps 11. Security Management Using Microsoft Sentinel 12. Protect and Govern Sensitive Data 13. Managing Insider Risks 14. Managing eDiscovery Cases 15. Managing Regulatory Compliance 16. Managing Privacy 17. Best Practices

Related to log analytics workspace workbooks

在数学中，**log (x)**表示什么含义呢？ **-** 知乎 在数学中，log (x)表示什么含义呢？在某些地方看到，单单写一个log，没有底数，请问这是什么含义呢？显示全部 关注者 19

为什么一些资料将以**10**为底或以**e**为底的对数写作**log**，而不是**lg**或 美国数学学会 AMS 的习惯是 log x 不带底数时默认表示自然对数。但是 ISO 80000-2 规定了必须用 ln x ， log x 仅用于底数不重要的情况（比如算法复杂度）。

计算机是如何计算 **log** 函数的？ **-** 知乎 计算机是如何计算 log 函数的？就是比如已知一个实数（或者复数）k，求其 log (base n)。想知道具体算法以用于简化一些修正算法。显示全部 关注者 486 被浏览

对数坐标轴的绘制规则？ **-** 知乎 刚好最近遇到了这个问题，百度无果，顺便回答一下吧。对数坐标很常用，刻度不均匀，一直理所当然的使用却没考虑过如何定义的刻度间距。直到最近要求在对数坐标下不同位置画出同样长

数学中**log**和**lg**读音一样吗？ **-** 知乎 lg连起来读的话，可能会和log混淆。为了避免歧义，说成“以10为底的对数”的时候应该会比把ln说得更复杂的时候更多。

三星**Galaxy S25**系列评测：**2025**年旗舰机皇，值不值得买？一文 作为数码博主，根据三星Galaxy S25系列参数体现，今天从 产品定位、核心亮点、选购建议 三个维度，帮你分析这款手机到底值不值入手。一、产品类型与定位 Galaxy S25系

C盘清理，**log**数据文件可以删吗**? -** 知乎 C盘清理，log数据文件可以删吗？c盘senseshield文件中的log数据占了50多g这个是有什么用的，可以删除吗？希望有大神回答一下谢谢啦 [图片] 显示全部 关注者 7

有没有好用的看**log**工具呢**? -** 知乎 用了notepad++和UltraEdit，都觉得不太好用。请用大牛有没有看log效率高的工具可推荐呢？

Apple ProRes和**Apple log**有什么区别？ **-** 知乎 prores和log是两种不同的东西。 prores是苹果魔改版的hevc，是一种图像压缩模式，对比hevc特点是帧内压缩（但hevc同样支持帧内压缩），相比于帧间压缩虽然压缩率较低，但能提供更好

log，**lg**和**ln**的读法分别如何**? -** 知乎 log是logarithm，ln是natural logarithm，那lg呢?

在数学中，**log (x)**表示什么含义呢？ **-** 知乎 在数学中，log (x)表示什么含义呢？在某些地方看到，单单写一个log，没有底数，请问这是什么含义呢？显示全部 关注者 19

为什么一些资料将以**10**为底或以**e**为底的对数写作**log**，而不是**lg**或 美国数学学会 AMS 的习惯是 log x 不带底数时默认表示自然对数。但是 ISO 80000-2 规定了必须用 ln x ， log x 仅用于底数不重要的情况（比如算法复杂度）。

计算机是如何计算 **log** 函数的？ **-** 知乎 计算机是如何计算 log 函数的？就是比如已知一个实数（或者复数）k，求其 log (base n)。想知道具体算法以用于简化一些修正算法。显示全部 关注者 486 被浏览

对数坐标轴的绘制规则？ **-** 知乎 刚好最近遇到了这个问题，百度无果，顺便回答一下吧。对数坐标很常用，刻度不均匀，一直理所当然的使用却没考虑过如何定义的刻度间距。直到最近要求在对数坐标下不同位置画出同样长

数学中**log**和**lg**读音一样吗？ **-** 知乎 lg连起来读的话，可能会和log混淆。为了避免歧义，说成“以10为底的对数”的时候应该会比把ln说得更复杂的时候更多。

三星**Galaxy S25**系列评测：**2025**年旗舰机皇，值不值得买？一文说 作为数码博主，根据三星Galaxy S25系列参数体现，今天从 产品定位、核心亮点、选购建议 三

个维度，帮你分析这款手机到底值不值入手。一、产品类型与定位 Galaxy S25系

C盘清理，**log**数据文件可以删吗**? -** 知乎 C盘清理，log数据文件可以删吗? c盘senseshield文件中的log数据占了50多g这个是有什么用的，可以删除吗? 希望有大神回答一下谢谢啦 [图片] 显示全部 关注者 7

有没有好用的看**log**工具呢**? -** 知乎 用了notepad++和UltraEdit，都觉得不太好用。请用大牛有没有看log效率高的工具可推荐呢?

Apple ProRes和**Apple log**有什么区别? **-** 知乎 prores和log是两种不同的东西。 prores是苹果魔改版的hevc，是一种图像压缩模式，对比hevc特点是帧内压缩（但hevc同样支持帧内压缩），相比于帧间压缩虽然压缩率较低，但能提供更好

log，**lg**和**ln**的读法分别如何**? -** 知乎 log是logarithm，ln是natural logarithm，那lg呢?

在数学中，**log (x)**表示什么含义呢? **-** 知乎 在数学中，log (x)表示什么含义呢? 在某些地方看到，单单写一个log，没有底数，请问这是什么含义呢? 显示全部 关注者 19

为什么一些资料将以**10**为底或以**e**为底的对数写作**log**，而不是**lg**或 美国数学学会 AMS 的习惯是 log x 不带底数时默认表示自然对数。但是 ISO 80000-2 规定了必须用 ln x ， log x 仅用于底数不重要的情况（比如算法复杂度）。

计算机是如何计算 **log** 函数的? **-** 知乎 计算机是如何计算 log 函数的? 就是比如已知一个实数（或者复数）k，求其 log (base n)。想知道具体算法以用于简化一些修正算法。显示全部 关注者 486 被浏览

对数坐标轴的绘制规则? **-** 知乎 刚好最近遇到了这个问题，百度无果，顺便回答一下吧。对数坐标很常用，刻度不均匀，一直理所当然的使用却没考虑过如何定义的刻度间距。直到最近要求在对数坐标下不同位置画出同样长

数学中**log**和**lg**读音一样吗? **-** 知乎 lg连起来读的话，可能会和log混淆。为了避免歧义，说成“以10为底的对数”的时候应该会比把ln说得更复杂的时候更多。

三星**Galaxy S25**系列评测：**2025**年旗舰机皇，值不值得买? 一文说 作为数码博主，根据三星Galaxy S25系列参数体现，今天从 产品定位、核心亮点、选购建议 三个维度，帮你分析这款手机到底值不值入手。一、产品类型与定位 Galaxy S25系

C盘清理，**log**数据文件可以删吗**? -** 知乎 C盘清理，log数据文件可以删吗? c盘senseshield文件中的log数据占了50多g这个是有什么用的，可以删除吗? 希望有大神回答一下谢谢啦 [图片] 显示全部 关注者 7

有没有好用的看**log**工具呢**? -** 知乎 用了notepad++和UltraEdit，都觉得不太好用。请用大牛有没有看log效率高的工具可推荐呢?

Apple ProRes和**Apple log**有什么区别? **-** 知乎 prores和log是两种不同的东西。 prores是苹果魔改版的hevc，是一种图像压缩模式，对比hevc特点是帧内压缩（但hevc同样支持帧内压缩），相比于帧间压缩虽然压缩率较低，但能提供更好

log，**lg**和**ln**的读法分别如何**? -** 知乎 log是logarithm，ln是natural logarithm，那lg呢?

在数学中，**log (x)**表示什么含义呢? **-** 知乎 在数学中，log (x)表示什么含义呢? 在某些地方看到，单单写一个log，没有底数，请问这是什么含义呢? 显示全部 关注者 19

为什么一些资料将以**10**为底或以**e**为底的对数写作**log**，而不是**lg**或 美国数学学会 AMS 的习惯是 log x 不带底数时默认表示自然对数。但是 ISO 80000-2 规定了必须用 ln x ， log x 仅用于底数不重要的情况（比如算法复杂度）。

计算机是如何计算 **log** 函数的? **-** 知乎 计算机是如何计算 log 函数的? 就是比如已知一个实数（或者复数）k，求其 log (base n)。想知道具体算法以用于简化一些修正算法。显示全部 关注者 486 被浏览

对数坐标轴的绘制规则? **-** 知乎 刚好最近遇到了这个问题，百度无果，顺便回答一下吧。对数坐标很常用，刻度不均匀，一直理所当然的使用却没考虑过如何定义的刻度间距。直到最近要求在对数坐标下不同位置画出同样长

数学中**log**和**lg**读音一样吗? **-** 知乎 lg连起来读的话，可能会和log混淆。为了避免歧义，说成“以10为底的对数”的时候应该会比把ln说得更复杂的时候更多。

三星**Galaxy S25**系列评测：**2025**年旗舰机皇，值不值得买? 一文说 作为数码博主，根据三星Galaxy S25系列参数体现，今天从 产品定位、核心亮点、选购建议 三个维度，帮你分析这款手机到底值不值入手。一、产品类型与定位 Galaxy S25系

C盘清理，**log**数据文件可以删吗**? -** 知乎 C盘清理，log数据文件可以删吗? c盘senseshield文件中的log数据占了50多g这个是有什么用的，可以删除吗? 希望有大神回答一下谢谢啦 [图片] 显示全部 关注者 7

有没有好用的看**log**工具呢**? -** 知乎 用了notepad++和UltraEdit，都觉得不太好用。请用大牛有没有看log效率高的工具可推荐呢?

Apple ProRes和**Apple log**有什么区别? **-** 知乎 prores和log是两种不同的东西。 prores是苹果魔改版的hevc，是一种图像压缩模式，对比hevc特点是帧内压缩（但hevc同样支持帧内压缩），相比于帧间压缩虽然压缩率较低，但能提供更好

log，**lg**和**ln**的读法分别如何**? -** 知乎 log是logarithm，ln是natural logarithm，那lg呢?

在数学中，**log (x)**表示什么含义呢? **-** 知乎 在数学中，log (x)表示什么含义呢? 在某些地方看到，单单写一个log，没有底数，请问这是什么含义呢? 显示全部 关注者 19

为什么一些资料将以**10**为底或以**e**为底的对数写作**log**，而不是**lg**或 美国数学学会 AMS 的习惯是 log x 不带底数时默认表示自然对数。但是 ISO 80000-2 规定了必须用 ln x ， log x 仅用于底数不重要的情况（比如算法复杂度）。

计算机是如何计算 **log** 函数的? **-** 知乎 计算机是如何计算 log 函数的? 就是比如已知一个实数（或者复数）k，求其 log (base n)。想知道具体算法以用于简化一些修正算法。显示全部 关注者 486 被浏览

对数坐标轴的绘制规则? **-** 知乎 刚好最近遇到了这个问题，百度无果，顺便回答一下吧。对数坐标很常用，刻度不均匀，一直理所当然的使用却没考虑过如何定义的刻度间距。直到最近要求在对数坐标下不同位置画出同样长

数学中**log**和**lg**读音一样吗? **-** 知乎 lg连起来读的话，可能会和log混淆。为了避免歧义，说成“以10为底的对数”的时候应该会比把ln说得更复杂的时候更多。

三星**Galaxy S25**系列评测：**2025**年旗舰机皇，值不值得买? 一文说 作为数码博主，根据三星Galaxy S25系列参数体现，今天从 产品定位、核心亮点、选购建议 三个维度，帮你分析这款手机到底值不值入手。一、产品类型与定位 Galaxy S25系

C盘清理，**log**数据文件可以删吗**? -** 知乎 C盘清理，log数据文件可以删吗? c盘senseshield文件中的log数据占了50多g这个是有什么用的，可以删除吗? 希望有大神回答一下谢谢啦 [图片] 显示全部 关注者 7

有没有好用的看**log**工具呢**? -** 知乎 用了notepad++和UltraEdit，都觉得不太好用。请用大牛有没有看log效率高的工具可推荐呢?

Apple ProRes和**Apple log**有什么区别? **-** 知乎 prores和log是两种不同的东西。 prores是苹果魔改版的hevc，是一种图像压缩模式，对比hevc特点是帧内压缩（但hevc同样支持帧内压缩），相比于帧间压缩虽然压缩率较低，但能提供更好

log，**lg**和**ln**的读法分别如何**? -** 知乎 log是logarithm，ln是natural logarithm，那lg呢?

在数学中，**log (x)**表示什么含义呢? **-** 知乎 在数学中，log (x)表示什么含义呢? 在某些地方看到，单单写一个log，没有底数，请问这是什么含义呢? 显示全部 关注者 19

为什么一些资料将以**10**为底或以**e**为底的对数写作**log**，而不是**lg**或 美国数学学会 AMS 的习惯是 log x 不带底数时默认表示自然对数。但是 ISO 80000-2 规定了必须用 ln x ， log x 仅用于底数不重要的情况（比如算法复杂度）。

计算机是如何计算 **log** 函数的? **-** 知乎 计算机是如何计算 log 函数的? 就是比如已知一个实数（或者复数）k，求其 log (base n)。想知道具体算法以用于简化一些修正算法。显示全部 关注者 486 被浏览

对数坐标轴的绘制规则? **-** 知乎 刚好最近遇到了这个问题，百度无果，顺便回答一下吧。对数坐标很常用，刻度不均匀，一直理所当然的使用却没考虑过如何定义的刻度间距。直到最近要求在对数坐标下不同位置画出同样长

数学中**log**和**lg**读音一样吗? **-** 知乎 lg连起来读的话，可能会和log混淆。为了避免歧义，说成“以10为底的对数”的时候应该会比把ln说得更复杂的时候更多。

三星**Galaxy S25**系列评测: **2025**年旗舰机皇，值不值得买? 一文 作为数码博主，根据三星Galaxy S25系列参数体现，今天从 产品定位、核心亮点、选购建议 三个维度，帮你分析这款手机到底值不值入手。一、产品类型与定位 Galaxy S25系

C盘清理，**log**数据文件可以删吗**? -** 知乎 C盘清理，log数据文件可以删吗? c盘senseshield文件中的log数据占了50多g这个是有什么用的，可以删除吗? 希望有大神回答一下谢谢啦 [图片] 显示全部 关注者 7

有没有好用的看**log**工具呢**? -** 知乎 用了notepad++和UltraEdit，都觉得不太好用。请用大牛有没有看log效率高的工具可推荐呢?

Apple ProRes和**Apple log**有什么区别? **-** 知乎 prores和log是两种不同的东西。 prores是苹果魔改版的hevc，是一种图像压缩模式，对比hevc特点是帧内压缩（但hevc同样支持帧内压缩），相比于帧间压缩虽然压缩率较低，但能提供更好

log，**lg**和**ln**的读法分别如何**? -** 知乎 log是logarithm，ln是natural logarithm，那lg呢?

Back to Home: https://ns2.kelisto.es