Microsoft SCOM Challenges and How to Overcome Them

A Microsoft System Center Operations Manager Compendium by NiCE IT Management Solutions

CONTENT

1. Hybrid & Cloud Integration
2. Security & Compliance
3. Large Environments
4. Performance Monitoring
5. Alert Management
6. Automation & Remediation
7. Customizing & Reporting
8. Closing Knowledge Gaps
9. Third-Party Solutions
10. Handling Resource Constraints
11. Optimizing SCOM
12. Non-Windows Monitoring

November 2023 | www.nice.de

CONTENTS

Introduction 3

1. Easing the Integration with Hybrid and Cloud Environments 6

2. Enhancing Security and Compliance Monitoring 9

3. Enable and Manage Scaling SCOM in Large Environments 14

4. Enhance Application Performance Monitoring 19

5. Enhance Alert Management and Noise Reduction 22

6. Enhancing Automation and Remediation Capabilities 25

7. Enhancing Customization and Reporting 28

8. Enhancing SCOM Knowledge and Closing Skill Gaps 30

9. Enhancing Your Work with Third-Party SCOM Solutions 35

10. Best Practice for Handling Resource Constraints when Working with SCOM 38

11. Optimize the SCOM Performance 43

12. Monitoring Non-Windows Platforms using Microsoft SCOM 46

Resources 49

About NiCE 55

Introduction

As a Microsoft System Center Operations Manager (SCOM) administrator, several challenges might be encountered in managing and maintaining this complex monitoring and management tool. These challenges can vary depending on the organization's size, infrastructure, and specific requirements. Here are some of the common challenges faced by SCOM administrators:

1. Integration with Hybrid and Cloud Environments

As organizations increasingly adopt hybrid and multi-cloud infrastructures, SCOM administrators may face challenges in integrating SCOM with these environments to monitor both on-premises and cloud-based resources effectively. Ensuring seamless monitoring across these diverse environments can be complex.

Click here to read more about easing the integration of hybrid and cloud environments.

2. Scaling for Large Environments

SCOM may be deployed in organizations with large and complex IT infrastructures. Administering SCOM at scale, managing a high volume of agents and data, and maintaining optimal performance can be challenging.

Click here to read more about how to enhance scaling.

3. Security and Compliance Monitoring

With the growing importance of security and compliance, SCOM administrators may need to enhance their monitoring capabilities to address security threats and ensure compliance with industry standards and regulations.

Click here to read more about enhancing security and compliance monitoring.

4. Application Performance Monitoring

Modern applications often consist of distributed and containerized components. SCOM administrators may face challenges in monitoring the performance and health of these complex applications and microservices.

Click here to read more about how to enhance application performance monitoring.

5. Alert Management and Noise Reduction

Dealing with alert fatigue remains a challenge. SCOM administrators need to fine-tune monitoring rules and alerts to reduce noise and focus on critical issues, ensuring that the team doesn't get overwhelmed by non-essential alerts.

Click here to read more on enhancing alert management and noise reduction.

6. Automation and Remediation

Automating routine tasks and implementing automated remediation processes can be challenging yet essential for efficient operations. Integrating SCOM with automation tools and orchestrators is often necessary.

Click here to read more about enhancing automation and remediation.

7. Customization and Reporting

Organizations have unique monitoring needs, and SCOM administrators may need to create custom management packs, dashboards, and reports to address these requirements effectively.

Click here to read more about enhancing customization and reporting.

8. Knowledge and Skill Gaps

Keeping up with the latest features and capabilities of SCOM, as well as staying informed about best practices, can be challenging. Administrators may need to invest in training and skill development to maximize the value of SCOM.

Click here to read more about enhancing SCOM knowledge and closing skill gaps.

9. Third-Party Integrations

Integrating SCOM with other third-party monitoring and management tools, such as ServiceNow, ITSM platforms, and log analytics solutions, can be complex but is often necessary to create a holistic monitoring and management ecosystem.

Click here to read more about best practices when working with third-party solutions.

10. Resource Constraints

Resource constraints, such as limited budgets and hardware limitations, can impact the ability to scale SCOM and implement the desired monitoring solutions effectively.

Click here to read more about best practices when faced with limitations.

11. Monitoring Non-Windows Environments

While SCOM is primarily designed for Windows environments, many organizations also need to monitor non-Windows systems. Integrating SCOM with other monitoring tools or extending its capabilities to cover non-Windows platforms can be challenging.

Click here to read more about monitoring non-windows platforms using Microsoft SCOM.

12. Optimizing the Performance of SCOM

Optimizing the performance of System Center Operations Manager (SCOM) is crucial to ensure that it effectively monitors your IT environment without causing undue strain on resources. Here are several steps a SCOM administrator can take to optimize SCOM performance.

Click here to read more about monitoring non-windows platforms using Microsoft SCOM.

To address these challenges, SCOM administrators may need to stay updated with the latest features and enhancements in newer versions of SCOM, leverage automation and scripting, and collaborate closely with other IT teams to align monitoring efforts with organizational goals. Additionally, seeking support from the Microsoft SCOM community and user groups can provide valuable insights and solutions to common challenges.

1. Easing the Integration with Hybrid and Cloud Environments

Integrating hybrid and multi-cloud infrastructures into System Center Operations Manager (SCOM) can be a complex task, but there are several steps a SCOM admin can take to ensure a smooth integration. Here are some best practices to consider:

1.1 Understand the Environment

Gain a deep understanding of your hybrid and multi-cloud infrastructure, including cloud services, on-premises systems, and their interdependencies.

Click here to read the Operations Manager Planning Guide.

1.2 Update SCOM to the Latest Version

Ensure that SCOM is up to date with the latest patches and updates to support the latest features and compatibility with cloud services.

Click here to read the System Center - Operations Manager build versions.

1.3 Implement Azure Management Pack

Install and configure the Azure Management Pack to monitor Azure resources. This allows SCOM to collect data from Azure services and applications.

Click here to download the Microsoft System Center Operations Manager Management Pack for Microsoft Azure.

1.4 Leverage SCOM Gateways

Use SCOM gateways in on-premises environments to securely monitor resources in different networks, such as branch offices or partner networks.

Click here to read how to install a gateway server.

1.5 Utilize Hybrid Runbook Automation

Integrate Azure Automation Runbooks with SCOM to automate responses to alerts. This can be especially useful in hybrid scenarios where automation is crucial.

Click here to read the Automation Hybrid Runbook Worker overview.

1.6 Implement SCOM Web Application Availability Monitoring

Use SCOM to monitor the availability and performance of web applications hosted in the cloud. This ensures end-to-end visibility for web services.

Click here to learn more about the Web Application Availability Monitoring template.

1.7 Utilize Custom Management Packs

Create custom management packs to monitor specific applications or services that are critical in your hybrid setup but are not covered by default management packs.

NiCE helps you build custom management packs. Click here to learn more about NiCE Custom Management Pack services. For self-authoring management packs, you may want to learn more about the Silect MP Studio.

1.8 Implement Synthetic Transactions

Use synthetic transactions to simulate user interactions with applications. This helps in proactively identifying issues before end-users are affected.

Click here to read more about the Synthetic Transactions Library at System Center Wiki.

Click here to learn how to Create and Configure Users for Synthetic Transactions at Microsoft Tech Community.

Click here to learn How to configure watcher node test users and settings on Microsoft Learn.

1.9 Implement Role-Based Access Control (RBAC)

Define proper RBAC settings to ensure that the right personnel have appropriate access to SCOM data and configuration settings.

Click here to learn more about implementing user roles.

Click here to learn more about Admin RBAC in SCOM 2022 written by Bob Cornelissen.

1.10 Utilize Performance Thresholds and Alert Tuning

Set performance thresholds carefully and fine-tune alerting to avoid unnecessary notifications. This prevents alert fatigue and ensures that admins focus on critical issues.

Click here to learn more about SCOM Alert Basics written by Cookdown.

Click here to watch the recording on SCOM alerting basics explained by Sameer Mhaisekar and Bruce Cullen.

Click here to read about overcoming bottlenecks for monitoring 2.500+ servers.

Click here to learn how to tune SCCM SCOM alerts written by Anoop Nair.

1.11 Implement Log Analytics

Integrate SCOM with Azure Log Analytics to collect, correlate, and act on log and performance data from various sources. This provides a centralized view of your hybrid infrastructure.

Click here to learn how to setup and configure Log Analytics using SCOM.

Click here to learn how to Configure Log Analytics for Azure Monitor SCOM Managed Instance.

Click here to learn how to establish connectivity to Azure Log Analytics.

Click here to learn how to connect the Operations Manager to Azure Monitor.

1.12 Regularly Review and Update Monitoring Strategy

Cloud environments are dynamic. Regularly review and update your monitoring strategy to adapt to changes in your infrastructure.

Click here to read the Operations Manager Planning Guide.

1.13 Monitor Costs and Resources

Implement monitoring for cloud costs and resource utilization. This helps in optimizing resource usage and controlling costs in the cloud environment.

Click here to learn more about Azure Monitor SCOM Managed Instance.

Click here to learn more about the cloud monitoring strategy.

Click here to learn more about monitoring Microsoft Azure and hybrid cloud environments.

1.14 Stay Informed and Engage with the Community

Join forums, user groups, and attend conferences to stay updated with the latest developments and best practices in SCOM and cloud monitoring.

Click here to reach the Microsoft System Center Blog.

Click here to reach the Microsoft System Center Blog SCOM related finds.

Click here to reach the Microsoft System Center Blog OM related finds.

Click here to reach the Microsoft System Center Operations Manager feature suggestion page.

Click here to reach the SCOMathon web page.

Click here to reach the Management Pack Catalog on GitHub.

Click here to reach the System Center discussion page.

Click here to reach the SCOM group on Reddit.

By following these best practices, a SCOM admin can ensure a seamless integration of hybrid and multi-cloud infrastructures into their monitoring setup, enabling effective management and proactive issue resolution.

2. Enhancing Security and Compliance Monitoring

Enhancing security and compliance monitoring in System Center Operations Manager (SCOM) involves implementing best practices, utilizing available tools, and staying proactive in the face of emerging threats and compliance requirements. Here are some strategies for a SCOM admin to enhance security and compliance monitoring:

2.1 Implement Security Monitoring

Utilize SCOM to monitor security events and incidents across your network. Create custom rules and monitors to detect unauthorized access attempts, suspicious activities, and potential security breaches.

Click here to secure your infrastructure monitoring with SCOM.

Click here and here to read more about the Security Monitoring Management Pack.

Click here to watch the recording of SCOM Security – the best tips, tools, and MPs to secure your SCOM environment.

Click here to read the Microsoft SCOM Security Technical Implementation Guide

by UCF.

Click here to watch the recording of Integrating the Security Monitoring MP into Microsoft Sentinel.

Click here to read Nathan Gau's blog post on SCOM Security Monitoring and Sentinel Integration.

2.2 Utilize Security Management Packs

Deploy security management packs specific to the technologies you're using (such as Active Directory, Windows Server, SQL Server, etc.). These packs provide specialized knowledge and monitoring capabilities tailored for security-related events.

Click here to learn more about how to secure your Infrastructure Monitoring with SCOM.

Click here to download the Microsoft System Center Management Pack for Windows Defender.

Click here to download the Microsoft System Center Operations Manager Management Pack for Microsoft 365.

Click here for advanced Microsoft 365 monitoring using the NiCE Active 365 Management pack for SCOM and Azure Monitor SCOM Managed Instance.

Click here to learn more about Operations Manager Management Packs.

Click here to download the Microsoft System Center Management Pack for ADDS.

Click here to learn more about a Management Pack assessment.

Click here to reach the System Center Management Pack Catalog on System Center Wiki.

2.3 Configure Baselines and Anomaly Detection

Establish security baselines for your systems and applications. Implement anomaly detection rules in SCOM to identify deviations from the established baseline, which can indicate security threats.

Click here to learn more about Monitoring strategy for cloud deployment models.

Click here to learn more about Monitoring Active Directory for Signs of Compromise

2.4 Monitor User Activity

Keep an eye on user activities, especially privileged accounts. Detect and alert on suspicious user behavior, such as multiple login failures, unusual login times, or privilege escalation attempts.

Click here to learn more about Service, User, and Security Accounts.

Click here to read more about implementing user roles.

Click here to read the blog post by Nathan Gau on Security Monitoring: Using SCOM to capture Suspicious User Activity.

Click here to read the Microsoft Learn Q&A blog article on SCOM alert when particular user tries to log on to targeted servers.

Click here to read a blog post by Sameer Mhaisekar "Wait, what? An activity log in SCOM? Did I read that right?"

Click here to read about Monitoring Microsoft 365 with SCOM and the NiCE Active 365 Management Pack.

Click here to learn more about Operations Manager key concepts.

Click here to learn more about operations associated with user role profiles.

Click here to learn more about tracking changes in Operations Manager.

2.5 Implement File Integrity Monitoring (FIM)

Use FIM to monitor critical system files and configuration settings for unauthorized changes. This helps in detecting and responding to potential security breaches promptly.

Click here to learn more about File Integrity Monitoring using the Log Analytics agent.

Click here to learn more about File Integrity Monitoring in Microsoft Defender for Cloud

Click here to learn more Enabling File Integrity Monitoring when using the Azure Monitor Agent.

Click here to learn more about Monitoring a file hash using SCOM written by Kevin Holman.

Click here to learn more about advanced Log File monitoring using the free NiCE Log File Management Pack.

2.6 Integrate with Security Information and Event Management (SIEM) Systems

Integrate SCOM with SIEM solutions to centralize security event data. This enables correlation of events and enhances the overall security posture by providing a comprehensive view of security incidents.

Click here to learn how to connect Operations Manager with other management systems.

Click here to learn more about the SQL MCM Addendum pack by Kevin Justin.

Click here to learn more about connecting Microsoft SCOM with ITSM Ticketing Systems

2.7 Automate Security Responses

Integrate SCOM with automation tools to automate responses to security incidents. Implement automated remediation processes to respond to common security threats without manual intervention.

Click here to learn more about Security Orchestration, Automation, and Response (SOAR) in Microsoft Sentinel.

Click here to learn more about creating a Script for collecting data from SCOM.

Click here to learn more about how heartbeats work in Operations Manager.

Click here to learn more about the integration pack for System Center Operations Manager.

Click here to learn how to implement Transport Layer Security 1.2.

Click here to learn more about Run As Accounts and Profiles.

2.8 Regularly Review Security Reports

Schedule and review security reports generated by SCOM. Analyze trends, identify patterns, and proactively address potential security vulnerabilities based on the insights gained from these reports.

Click here to learn more about the Operations Manager reports library.

Click here to learn how to create reports in Operations Manager.

Click here to read more about Scheduling reports by Bob Cornelissen.

2.9 Implement Compliance Monitoring

Use SCOM to monitor compliance with industry standards and regulatory requirements (such as HIPAA, GDPR, PCI DSS). Implement compliance-specific management packs and customize them to meet your organization's specific compliance needs.

Click here to read more about monitoring Auth0 using System Center Operations Manager.

Click here to learn more about implementing TLS 1.2 enforcement with SCOM.

Click here to learn more about the HIPAA Compliance Pack by Silect.

Click here to learn more about the Compliance Manager by Silect.

Click here to learn more about the Sentinel Management Pack by Silect.

Click here to launch the course Monitor and Maintain a Software-Defined Datacenter with SCOM by Steve Buchanan.

Click here to learn more about the TLS Compliance Pack.

2.10 Implement Role-Based Access Control (RBAC)

Enforce strict RBAC policies to ensure that only authorized personnel have access to sensitive security and compliance data within SCOM.

Click here to learn more on implementing user roles.

Click here to learn more about SCOM 2019 role based access and delegation.

Click here to learn more about modifying access in SCOM user roles – without the console.

Click here to read more about Admin RBAC in SCOM 2022.

2.11 Regularly Update Management Packs

Keep the management packs up to date. New versions often include improvements in security monitoring and compliance checks based on the latest security threats and regulatory changes.

Click here to read more on How to Update SCOM Management Packs by Prajwal Desai.

Click here to more about the Management Pack Lifecycle.

Click here to reach the Community Catalog Management Pack.

2.12 Stay Informed and Engage with Security Communities

Stay updated with the latest security threats, vulnerabilities, and best practices by engaging with security communities, attending security conferences, and participating in webinars and workshops.

Click here to learn more about the NCSC.

Click here to reach the Information Security Stack Exchange.

Click here to reach the DefCon web page.

Click here to reach the black hat web page.

Click here to reach the Cybersecurity & Infrastructure Security Agency (CISA) web page.

Click here to reach the Open Worldwide Application Security Project (OWASP).

By implementing these strategies, a SCOM admin can significantly enhance security and compliance monitoring, ensuring a robust and proactive approach to safeguarding the organization's IT environment.

3. Enable and Manage Scaling SCOM in Large Environments

Scaling System Center Operations Manager (SCOM) in large environments is essential to ensure effective monitoring without compromising performance. Here are steps and strategies that SCOM administrators can implement to enable and manage scaling in large environments:

3.1 Design a Scalable Architecture

Begin with a well-thought-out architecture that accounts for the size and complexity of your environment. Consider the number of management servers, databases, and gateway servers required. Distribute the load strategically.

Click here to learn more about the Operations Manager Planning Guide.

Click here to learn more about Planning a Management Group Design.

Click here to learn more about High Availability and Disaster Recovery.

Click here to learn more about Making changes to an Operations Manager Management Group.

Click here to read more about Resource pool design considerations.

Click here to learn more about System requirements for System Center Operations Manager.

Click here to watch the recording "SCOM Management Group and database tuning"

by Stoyan Chalakov.

3.2 Distribute Management Servers

Deploy multiple management servers to distribute the monitoring load. Use load balancing mechanisms to evenly distribute the agents across these servers.

Click here to learn more about the distributed deployment of Operations Manager

3.3 Dedicated Database Servers

Consider using dedicated database servers for the SCOM databases, including the Operations Manager and Data Warehouse databases. This helps optimize database performance.

Click here to learn more about SQL Server Design Considerations

3.4 Agent Placement and Distribution

Carefully plan the placement of agents across servers and devices. Distribute agents evenly across management servers to prevent overloading any one server.

Click here to learn more about Operations Manager Agents.

Click here to read how to upgrade an Operations Manager agent.

3.5 Resource Optimization

Monitor the resource utilization (CPU, memory, and disk space) of your management servers and databases. Add more resources or additional servers as needed to maintain optimal performance.

Click here to learn how to manage resource pools.

3.6 Tune Alerting and Monitoring Rules

Fine-tune alerting and monitoring rules to reduce noise and eliminate redundant or non-critical alerts. Customize management packs to focus on essential metrics.

Click here to learn how an alert is produced.

Click here to learn how to close an alert generated by a monitor.

Click here to understand data driven alert management.

Click here to read Nathan Gau's blog post Monitors vs. Rules and how they Affect Alert Management.

Click here to watch the recording of SCOM alerting basics explained.

Click here to read an article by Neha Garg on Alert Tuning.

Click here to learn more about Easy Tune by Cookdown.

Click here to watch the recording of "SCOM alert tuning tips from the masters".

3.7 Override Management Pack Rules

Use overrides to modify thresholds and settings for specific objects, if necessary, to tailor monitoring to the unique requirements of different components in your environment.

Click here to learn how to override a rule or monitor.

Click here to learn how to create a management pack for overrides.

Click here to learn more about using classes and groups for overrides.

Click here to read more about best practices for configuring overrides in Operations Manager.

3.8 Use Agentless Monitoring Sparingly

Agentless monitoring can be resource intensive. Limit its use to cases where it's essential, and consider using agents for most monitoring tasks.

Click here to learn more about agentless monitoring in Operations Manager.

3.9 High Availability (HA)

Implement high availability for SCOM components, including management servers, databases, and gateways, to ensure continuous monitoring even in case of hardware or software failures.

Click here to learn more about High Availability and Disaster Recovery.

Click here to learn more about Designing for high availability.

Click here to learn more about how to make Reporting console part of high Availability in SCOM, written by Sourav Mahato.

Click here to read the article by Kevin Holman on Understanding SCOM Resource Pools.

3.10 Load Balancing and Network Considerations

Implement load balancing for management servers and gateways to distribute incoming traffic evenly. Optimize network configurations to minimize latency and maximize communication efficiency.

Click here to learn more about load balancing the Service Manager.

Click here to download the System Center Management Pack for Windows Server Network Load Balancing.

Click here to read the article by Kevin Holman "Automating Agent Load Balancing for Management Servers and Gateways".

Click here to read more about the Windows Server Network Load Balancing (NLB) Management Pack.

3.11 Storage Performance

Ensure that the storage subsystems for SCOM databases are optimized for performance. This includes using fast and reliable storage solutions.

Click here to read more about SQL Server Design Considerations.

Click here to learn more about the monitoring configuration in Management Pack for SQL Server.

3.12 Regular Maintenance

Perform routine maintenance tasks, such as database grooming, to keep the database size in check and maintain SCOM's performance.

Click here to learn more about the grooming process in the SCOM Database, written by Kevin Holman.

Click here to learn more about how to configure grooming settings for the Operations Manager database.

Click here to learn more about Data Warehouse Grooming Tool, written by Blake Drumm.

Click here to download the Data Warehouse Grooming Tool

3.13 Automation and Scripting

Use automation and scripting to streamline administrative tasks, such as agent deployments, updates, and maintenance. PowerShell scripts can be particularly useful in this regard.

Click here to learn more about Using Operations Manager Shell.

Click here to read more about useful SCOM PowerShell Scripts.

3.14 Monitoring Dashboards and Reports

Utilize SCOM's reporting and dashboard capabilities to gain insights into the health and performance of your monitoring infrastructure. These tools can help you identify bottlenecks and areas that need optimization.

Click here to learn more about dashboards by SquaredUp.

Click here to learn how to create SCOM reports on Power BI.

3.15 Capacity Planning

Continuously monitor the growth of your environment and plan for future scalability needs. Be prepared to scale up or out as your infrastructure expands.

Click here to read the Operations Manager Planning Guide

3.16 Regularly Update SCOM

Stay current with SCOM updates, patches, and new releases. Microsoft often releases performance improvements and feature enhancements in newer versions.

Click here to learn more about the System Center - Operations Manager build versions.

3.17 Monitoring as Code (MaC)

Consider implementing Monitoring as Code practices to automate the provisioning and configuration of monitoring resources, making it easier to manage at scale.

By following these strategies and best practices, SCOM administrators can effectively scale SCOM in large environments while maintaining optimal performance and ensuring that critical IT resources are continuously monitored.

4. Enhance Application Performance Monitoring

Enhancing application performance monitoring in System Center Operations Manager (SCOM) involves configuring SCOM to provide detailed insights into the performance and health of your applications. Here are steps that a SCOM administrator can take to enhance application performance monitoring:

4.1 Identify Key Applications and Components

Begin by identifying the critical applications and their components that need monitoring. Understand the architecture of these applications to determine what to monitor.

4.2 Install Relevant Management Packs

Install and configure management packs that are specific to the applications and technologies you want to monitor. Microsoft and third-party management packs can provide pre-defined monitoring templates and rules.

4.3 Customize Management Packs

Customize management pack settings to align with your specific monitoring requirements. Modify thresholds, rules, and monitors as needed to match the performance characteristics of your applications.

4.4 Configure Distributed Application Models

Create Distributed Application Models (DAs) in SCOM to represent the structure of your applications. DAs provide a high-level view of application health and relationships between components.

4.5 Monitor End-User Experience

Implement synthetic transactions or real user monitoring (RUM) to measure and report on end-user experience. This can include monitoring response times, transaction success rates, and user interactions.

4.6 Track Application Dependencies

Set up dependency monitoring to track the relationships and dependencies between application components. This helps identify root causes of performance issues more effectively.

4.7 Performance Counters and Metrics

Use SCOM to collect and monitor performance counters and metrics relevant to your applications. Configure thresholds and alerts for critical performance indicators.

4.8 Log Monitoring

Integrate log monitoring into SCOM by utilizing log management solutions like SCOM Log Analytics or third-party log aggregators. Collect and analyze application logs for errors and anomalies.

4.9 Application Component Monitoring

Create custom monitors and rules to monitor specific components of your applications, such as web servers, application servers, databases, and middleware.

4.10 Custom Scripting and Script Monitors

Develop custom scripts and script monitors to collect application-specific data or perform custom checks. PowerShell and other scripting languages can be used for this purpose.

4.11 Transaction Tracing

Implement distributed tracing solutions like Application Insights or Azure Monitor Application Insights to trace transactions across distributed components and services.

4.12 Alerting and Notification

Configure alerting rules to notify IT teams when application performance thresholds are breached. Ensure that alerts are sent to the right personnel through email, SMS, or integration with incident management systems.

4.13 Performance Baselines

Establish performance baselines to understand normal behavior and detect deviations. SCOM can help you create and monitor these baselines over time.

4.14 Capacity Planning

Use SCOM's capacity planning features to forecast resource needs for your applications. This helps prevent performance issues due to resource constraints.

4.15 Dashboard and Reporting

Create custom dashboards and reports in SCOM to visualize application performance data. Share these reports with stakeholders to provide insights into application health.

4.16 Automated Remediation

Implement automated remediation tasks and runbooks in SCOM to address common application performance issues automatically. This can help reduce downtime and manual intervention.

4.17 Regular Maintenance and Updates

Keep SCOM and its management packs up to date to ensure that you have access to the latest features and performance improvements.

4.18 Collaboration and Communication

Foster collaboration between application owners, developers, and operations teams to ensure that monitoring aligns with application performance goals and objectives.

Enhancing application performance monitoring in SCOM requires a combination of proper planning, configuration, customization, and continuous refinement based on evolving application requirements. Regularly review and adjust your monitoring strategy to adapt to changes in your application landscape.

5. Enhance Alert Management and Noise Reduction

Enhancing alert management and noise reduction is crucial for a System Center Operations Manager (SCOM) administrator to ensure that the monitoring environment provides meaningful alerts that lead to actionable insights rather than overwhelming the IT team with noise. Here are steps a SCOM admin can take to achieve this:

5.1 Customize Alert Thresholds

Review and adjust alert thresholds to align with the specific needs of your environment. Fine-tune thresholds to reduce false positives and ensure that alerts are triggered only when actual issues occur.

5.2 Prioritize Alerts

Implement alert prioritization based on the criticality of the monitored components. Assign severity levels to alerts so that the most critical issues receive immediate attention.

5.3 Suppress Noise

Use SCOM's built-in alert suppression mechanisms to prevent redundant or less critical alerts from flooding the console. Configure maintenance mode for planned downtime to suppress alerts during maintenance windows.

5.4 Override Management Pack Rules

Create overrides for management pack rules and monitors to adjust their behavior for specific objects or components. This allows you to tailor monitoring to match the unique characteristics of each system.

5.5 Grouping and Alert Deduplication

Configure SCOM to group related alerts or deduplicate alerts that are essentially reporting the same issue. This reduces the number of alerts generated for a single problem.

5.6 Alert Tuning

Regularly review alerts and analyze their relevance. Disable or adjust rules and monitors that consistently generate false or non-actionable alerts. Implement feedback loops to improve alert accuracy.

5.7 Alert Subscription and Notification Channels

Ensure that alerts are sent to the right personnel or teams. Configure notification channels (e.g., email, SMS, ticketing systems) and subscribe individuals or groups to specific alerts based on their responsibilities.

5.8 Maintenance Mode

Put monitored objects or systems in maintenance mode during planned maintenance activities. This prevents alerts from being generated for expected downtime.

5.9 Script-Based Remediation

Implement script-based automated remediation tasks to resolve known issues automatically. SCOM can execute scripts in response to specific alerts, reducing the need for manual intervention.

5.10 Integration with Incident Management

Integrate SCOM with incident management systems (e.g., ServiceNow, JIRA) to automatically create incidents or tickets for actionable alerts. This streamlines the incident resolution process.

5.11 Alert Aging and Escalation

Implement alert aging policies to escalate unresolved alerts. If an alert remains unacknowledged or unaddressed for a specified period, escalate it to a higher-level team or individual.

5.12 Performance Baselines and Anomaly Detection

Use performance baselines and anomaly detection to identify deviations from normal behavior. Alerts triggered by anomalies are often more indicative of genuine issues.

5.13 Dashboard Views

Create custom dashboards in SCOM to provide a real-time overview of alert status and the health of your monitored environment. Dashboards help administrators quickly identify critical issues.

5.14 Scheduled Maintenance and Blackout Windows

Plan and schedule regular maintenance windows to coincide with low-impact periods. This helps minimize alerts generated during maintenance activities.

5.15 Collaboration and Documentation

Foster collaboration among IT teams, including operations, development, and application owners, to ensure that everyone understands the alert management process. Maintain up-to-date documentation for handling alerts.

5.16 Continuous Monitoring Improvement

Regularly review the effectiveness of your alert management strategy. Analyze historical data to identify patterns and trends in alerts, and adjust as needed.

By implementing these strategies, a SCOM administrator can significantly enhance alert management and noise reduction, ensuring that alerts generated by SCOM are more meaningful, actionable, and contribute to the overall stability and reliability of the IT environment.

6. Enhancing Automation and Remediation Capabilities

Enhancing automation and remediation capabilities in System Center Operations Manager (SCOM) can significantly improve efficiency and responsiveness in managing IT environments. Here are several strategies for a SCOM admin to enhance automation and remediation processes:

6.1 Implement Runbook Automation

Integrate SCOM with automation tools like Azure Automation Runbooks or System Center Orchestrator. Create runbooks to automate common tasks and remediation processes based on SCOM alerts.

6.2 Leverage SCOM Tasks and Diagnostic and Recovery Tasks (DRTs)

Utilize SCOM tasks and DRTs to automate common troubleshooting and remediation procedures directly from SCOM alerts. These can be used to execute scripts, restart services, or initiate other corrective actions.

6.3 Implement Self-Healing Automation

Set up automation rules to enable self-healing capabilities. Create rules that trigger automatic remediation actions for common issues, reducing manual intervention and downtime.

6.4 Use Webhooks for External Integrations

Integrate SCOM with external systems and services using webhooks. Webhooks enable SCOM to communicate with third-party applications and trigger automated responses based on alert notifications.

6.5 Implement Alert Customization

Customize alert notifications to include detailed information and resolution steps. This helps automation scripts understand the context and take appropriate actions without human intervention.

6.6 Implement Change and Configuration Automation

Automate change management processes by integrating SCOM with change management systems. Implement automation for routine configuration changes and updates, ensuring consistency and compliance.

6.7 Implement Alert Correlation

Use automation to correlate related alerts and incidents. Create automation scripts that analyze multiple alerts and initiate remediation actions based on the aggregated information, preventing alert storms.

6.8 Utilize Machine Learning and Predictive Analytics

Implement machine learning algorithms to predict potential issues based on historical data. Proactively automate remediation processes for predicted issues before they escalate.

6.9 Implement Role-Based Access Control (RBAC) for Automation

Define RBAC roles specifically for automation tasks. Limit access to automation scripts and tools to authorized personnel only, ensuring security and compliance.

6.10 Regularly Review and Update Automation Workflows

Continuously review automation workflows to ensure they remain effective and up to date. Update workflows based on changing IT environments, new technologies, and evolving security threats.

6.11 Implement Error Handling and Logging

Include robust error handling mechanisms in automation scripts. Implement logging and reporting to capture errors and exceptions, allowing for effective troubleshooting and script improvement.

6.12 Stay Updated with Automation Tools and Techniques

Stay informed about the latest automation tools, scripting languages, and techniques. Continuously enhance your automation skills to leverage new capabilities and improve existing workflows.

6.13 Collaborate with IT and Development Teams

Collaborate with IT operations, development, and security teams to identify automation opportunities across the organization. Work together to develop comprehensive automation solutions.

By implementing these strategies, a SCOM admin can enhance automation and remediation capabilities, leading to improved efficiency, reduced downtime, and a more responsive IT environment.

7. Enhancing Customization and Reporting

Enhancing customization and reporting within System Center Operations Manager (SCOM) is crucial for tailoring monitoring solutions to specific organizational needs and gaining valuable insights into system performance and health. Here are some strategies for a SCOM admin to enhance customization and reporting capabilities:

7.1 Customization

7.1.1 Custom Management Packs

Create custom management packs to monitor specific applications, services, or components unique to your organization. Tailor monitoring rules, alerts, and performance counters according to your requirements.

7.1.2 Override Management Pack Rules

Customize default management pack rules and thresholds based on your organization's performance and availability requirements. Overrides allow you to adjust monitoring settings without modifying the original management pack.

7.1.3 Custom Alert Notifications

Customize alert notifications to include additional information, relevant links, and resolution steps specific to your organization's processes. Provide detailed context to IT staff for faster issue resolution.

7.1.4 Custom Dashboards

Design custom dashboards using SCOM's built-in tools or third-party solutions. Tailor dashboards to display key performance indicators (KPIs) and metrics relevant to your organization. Include visual representations for quick insights.

7.1.5 Performance Collection Rules

Customize performance collection rules to gather specific performance data from servers and applications. Adjust collection intervals and counters based on your organization's performance analysis requirements.

7.1.6 Web Application Availability Monitoring

Implement custom web application availability tests. Configure tests to monitor critical transactions and user journeys within web applications. Customize thresholds and response times for accurate availability measurements.

7.2 Reporting

7.2.1 Custom Reports

Create custom reports using SQL Server Reporting Services (SSRS) or other reporting tools. Tailor reports to display specific data points, trends, and historical performance data. Custom reports can provide in-depth insights into system performance.

7.2.2 Scheduled Reports

Schedule regular report generation and distribution. Automate report delivery to key stakeholders via email or other communication channels. Ensure reports are delivered in a format (PDF, Excel, etc.) that is easily understandable by recipients.

7.2.3 Data Warehouse

Leverage SCOM's Data Warehouse feature to store historical monitoring data. Utilize the Data Warehouse for in-depth analysis and long-term reporting. Design custom queries and reports to extract valuable insights from the stored data.

7.2.4 Performance Analysis

Implement custom performance analysis reports. Use trend analysis and forecasting to predict potential performance issues. Customize reports to highlight peak usage periods and resource bottlenecks.

7.2.5 Integration with Power BI

Integrate SCOM data with Power BI for advanced data visualization and interactive reporting. Power BI provides a wide range of visualization options and interactive features to create compelling, customized reports.

7.2.6 Custom SQL Queries

Write custom SQL queries to extract specific data from the SCOM database. Use these queries to create highly tailored reports that cater to unique organizational requirements.

7.2.7 User Training and Documentation

Provide training sessions and documentation to end-users and IT staff on how to create custom reports and dashboards. Encourage users to utilize the available customization features effectively.

7.2.8 Regularly Review and Update Customizations

Regularly review customizations and reports to ensure they remain relevant and accurate. Update customizations based on changing organizational needs, technology updates, and user feedback.

By implementing these strategies, a SCOM admin can enhance customization and reporting capabilities, enabling the organization to monitor systems effectively, make informed decisions, and respond promptly to emerging issues.

8. Enhancing SCOM Knowledge and Closing Skill Gaps

Enhancing SCOM (System Center Operations Manager) knowledge and closing skill gaps involves a combination of continuous learning, practical experience, and staying updated with the latest developments in the field of IT infrastructure monitoring. Here are several strategies for a SCOM admin to enhance their knowledge and skills:

8.1 Formal Training and Certification

Enroll in SCOM Training Courses

Participate in formal training programs offered by Microsoft or certified training partners. These courses provide structured learning and cover essential topics.

Click here to read the Getting Started article by Microsoft.

Click here to read more about the SCOM Certification Path Overview by TopQore.

Click here to read more about Learn, Train & Troubleshoot SCOM on SCOMathon.

Click here to learn more about " SCOM: Mastering Microsoft Operations Manager 2022", a 5-days training offered on Glasspaper.

Click here to learn more about smart System Center Operations Manager, a 5-day training offered by ETC Austria.

Click here to learn more about the training "Mastering System Center Operations Manager 2022", by Kåre Rude Andersen.

Pursue SCOM Certifications

Consider certifications like Microsoft Certified: Azure Administrator Associate or Microsoft Certified: Security, Compliance, and Identity Fundamentals. Certifications validate your skills and knowledge.

Click here to browse trainings offered by Microsoft.

8.2 Hands-On Experience

Set Up a Lab Environment

Create a lab environment to experiment with SCOM features and configurations. Hands-on experience is invaluable for understanding how SCOM works in different scenarios.

Click here to read the SCOM 2022 – QuickStart Deployment Guide on Kevin Holman's blog.

Work on Real Projects

If possible, work on real monitoring projects within your organization. Practical experience dealing with actual challenges enhances your problem-solving skills.

8.3 Online Learning Platforms

Use Online Courses

Platforms like Coursera, Udemy, and Pluralsight offer SCOM courses taught by experts. These platforms often include video lectures, quizzes, and practical exercises.

Click here to find SCOM trainings on SCOMathon.

Click here to find SCOM trainings on Udemy.

Click here to find SCOM trainings on Pluralsight.

Click here to find SCOM trainings on YouTube.

Explore Microsoft Learn

Microsoft Learn offers free online resources, tutorials, and hands-on labs specifically tailored to Microsoft technologies, including SCOM.

8.4 Documentation and Official Resources

Read Official Documentation

Familiarize yourself with official SCOM documentation. Microsoft's documentation provides in-depth knowledge about SCOM features, best practices, and troubleshooting tips.

Click here to read the Operations Manager documentation.

Follow Microsoft Tech Community

Engage with the SCOM community on platforms like Microsoft Tech Community. Participate in discussions, ask questions, and learn from the experiences of other SCOM professionals.

Click here to reach SCOMathon.

Click here to reach the Microsoft Tech Community.

Click here to reach the SCOM Feature Suggestions and Rating page.

Click here to read news on LinkedIn from Aakash Basavaraj, Senior Program Manager at Microsoft, SCOM Dev Team.

8.5 Blogs and Online Forums

Read SCOM Blogs

Follow SCOM-focused blogs written by experts and MVPs. These blogs often contain tutorials, tips, and solutions to common problems.

Click here to reach the blog by Kevin Holman.

Click here to reach the blog by Maxim Volkov.

Click here to reach the blog by Ruben Zimmermann.

Click here to reach the Microsoft Management Pack page on Technet / Wiki.

Click here to reach the blog by Tao Yang.

Click here to reach the blog by Warren Kahn.

Click here to reach the blog by the Microsoft Tech Community.

Click here to reach the blog by Bob Cornelissen.

Click here to reach the blog by The Monitoring Guys.

Click here to reach the blog by Mountainss.

Click here to reach the blog by Jonathan Almquist.

Click here to reach the blog by Cookdown.

Click here to reach the blog by Blake Drumm.

Click here to reach the blog by Marnix Wolf.

Click here to reach the blog by Nathan Gau.

Click here to reach the blog by Michael Kamp.

Click here to reach the blog by Kevine Greene.

Click here to reach the blog by Kevin Justin.

Click here to reach the blog by D. Walsham.

Participate in Forums

Engage in forums like TechNet and Stack Overflow. Answering questions and discussing issues with others can deepen your understanding of SCOM concepts.

Click here to reach the SCOM channel on reddit.

Click here to reach the SCOM community on the SCOMathon Slack Channel.

8.6 Webinars and Conferences

Attend Webinars

Participate in webinars hosted by SCOM experts and organizations. Webinars often cover advanced topics and provide insights into industry best practices.

Attend Conferences

If possible, attend IT conferences where SCOM is a topic of discussion. Networking with professionals and attending sessions can broaden your perspective.

Click here to reach the Midwest Management Summit event page.

Click here to reach the SCOMathon event page.

Click here to reach the Twin Cities System Center User Group event page.

Click here to reach the Experts Live event page.

Click here to reach the CollabDays event page.

Click here to reach the Microsoft Ignite event page.

Click here to reach the Microsoft Build event page.

8.7 Practice Problem-Solving

Solve Challenges on Platforms like GitHub

Platforms like GitHub often have SCOM-related projects and challenges. Contributing to open-source projects or solving issues posted by others hones your problem-solving skills.

Click here and here to reach SCOM related results on GitHub.

Participate in Hackathons or Competitions

Engage in SCOM-related hackathons or competitions if available. These events encourage creative problem-solving and innovative thinking.

8.8 Mentorship and Networking

Find a Mentor

If possible, find a mentor who is experienced in SCOM. Learning from someone with practical experience can accelerate your learning process.

Join User Groups

Participate in SCOM user groups or online communities. Networking with peers allows you to share knowledge, ask questions, and learn from the experiences of others.

Click here to reach the Northwest System Center User Group.

Click here to reach the Twin Cities System Center User Group.

Click here to reach the Houston Area Systems Management User Group.

Click here to reach the Modern Enterprise Management User Group.

8.9 Continuous Learning and Experimentation

Stay Updated

IT is a rapidly changing field. Follow updates and new releases related to SCOM. Subscribe to newsletters, blogs, and podcasts to stay informed.

Experiment and Innovate

Don't be afraid to experiment with SCOM configurations and features. Innovation often comes from trying out new approaches and finding creative solutions to challenges.

Closing skill gaps and enhancing SCOM knowledge is a continuous journey. By combining formal education, practical experience, online resources, and networking, you can keep your skills up-to-date and stay competitive in the rapidly evolving IT landscape.

9. Enhancing Your Work with Third-Party SCOM Solutions

Enhancing your work with third-party SCOM (System Center Operations Manager) solutions involves a combination of best practices, communication strategies, and technical skills. Here are some steps a SCOM admin can take to optimize their experience with third-party solutions:

9.1 Understand the Third-Party Solution

Thorough Research

Understand the features, limitations, and integration methods of the third-party solution.

Vendor Support

Establish a communication channel with the third-party vendor for technical support and updates.

9.2 Infrastructure and Configuration

Optimized Infrastructure

Ensure that your SCOM infrastructure (servers, databases, network) is optimized for handling additional workloads from third-party solutions.

Proper Configuration

Configure SCOM and the third-party solution according to best practices and vendor recommendations.

9.3 Monitoring Strategy

Customize Monitoring

Tailor monitoring templates and alerts to suit your organization's specific needs and objectives.

Integration

Integrate third-party alerts seamlessly into SCOM to have a unified alerting system.

9.4 Documentation and Knowledge Sharing

Documentation

Maintain detailed documentation about the third-party solution's configuration, integration methods, and issue resolution procedures.

Knowledge Sharing

Share knowledge within your team about the third-party solution, ensuring everyone is on the same page regarding its capabilities and limitations.

9.5 Regular Updates and Maintenance

Stay Updated

Keep both SCOM and the third-party solution up to date with the latest patches and updates to ensure compatibility and security.

Regular Maintenance

Schedule regular maintenance tasks, including database cleanup, to keep the system running smoothly.

6. Performance Optimization

Performance Monitoring

Monitor the performance of both SCOM and the third-party solution to identify bottlenecks and areas for optimization.

Tuning

Fine-tune performance settings based on the monitoring data to optimize resource usage.

9.7 Security

Access Control

Implement proper access controls to ensure that only authorized personnel can modify configurations and settings related to the third-party solution.

Data Encryption

Enable encryption for data transmitted between SCOM and the third-party solution to maintain security standards.

9.8 Proactive Issue Resolution

Proactive Monitoring

Implement proactive monitoring techniques to identify potential issues before they impact the system.

Troubleshooting Skills

Develop strong troubleshooting skills to diagnose and resolve issues related to both SCOM and the third-party solution promptly.

9.9 Feedback Loop

Provide Feedback

Offer feedback to the third-party vendor about your experiences, including suggestions for improvements and feature requests.

9.10 Training and Certification

Continuous Learning

Stay updated with the latest technologies and best practices through training and certifications related to SCOM and third-party solutions.

Enhancing your experience with third-party SCOM solutions is a continuous process that involves a combination of technical expertise, effective communication, and proactive management strategies. Regularly assess your systems, stay informed about updates and best practices, and adapt your approach as technology evolves.

10. Best Practice for Handling Resource Constraints when Working with SCOM

When a System Center Operations Manager (SCOM) admin is faced with resource constraints, such as limited budgets and hardware limitations, there are several strategies and best practices they can employ to make the most out of the available resources. Here are some suggestions:

10.1 Prioritize Monitoring

Focus on monitoring critical systems and services first. Identify the most important applications and infrastructure components and allocate resources accordingly.

10.2 Optimize SCOM Configuration

Fine-tune SCOM settings to reduce resource usage. This includes adjusting data retention policies, lowering sampling intervals, and optimizing alert thresholds.

10.3 Implement Efficient Hardware Usage

Use hardware wisely. Consider virtualization and cloud options to optimize hardware resources. Utilize existing hardware to its fullest potential before investing in new equipment.

10.4 Use Management Packs Wisely

Be selective about the management packs you use. Disable unnecessary or redundant monitors and rules to reduce overhead. Regularly review and update management packs to ensure they are optimized for performance.

10.5 Implement Synthetic Transactions

Use synthetic transactions to simulate user interactions with critical applications. These transactions can help identify performance issues without putting additional strain on the monitored systems.

10.6 Capacity Planning

Conduct thorough capacity planning to anticipate future resource needs. This proactive approach can help in allocating resources effectively and avoid sudden spikes in resource demands.

10.7 Automation

Automate routine tasks such as maintenance and clean-up. Automation can significantly reduce the workload on the SCOM infrastructure, allowing it to focus on essential monitoring tasks.

10.8 Community and Forums

Engage with the SCOM community and forums. Often, solutions to specific problems or optimizations come from shared experiences within the community.

10.9 Regular Performance Monitoring and Tuning

Continuously monitor the performance of SCOM itself. Identify bottlenecks and tune the configuration as necessary. Regularly review SCOM reports to understand trends and plan resources accordingly.

Monitoring the performance of System Center Operations Manager (SCOM) itself is crucial to ensure that the monitoring system is running optimally and efficiently. Here are several key aspects you should consider when monitoring the performance of SCOM:

10.9.1 Monitoring the performance of SCOM

10.9.1.1 System Resource Usage

CPU Usage

Monitor the CPU usage of the SCOM server(s). High CPU usage could indicate performance bottlenecks.

Memory Usage

Keep an eye on memory consumption. Insufficient RAM can lead to slow performance.

Disk I/O

Monitor disk read/write speeds and ensure that the disk subsystem can handle the I/O operations.

Network Usage

Check network utilization, especially if SCOM management servers and agents are distributed across multiple locations.

10.9.1.2 Database Performance

Database Size

Monitor the size of the SCOM databases. Large databases can impact performance.

Database Latency

Measure the database query execution time. High latency might indicate issues with the database server.

Index Fragmentation

Regularly check for index fragmentation on SCOM databases and rebuild/reorganize indexes as needed.

10.9.1.3 SCOM Services and Components

Health Service Heartbeat

Monitor the heartbeat of SCOM agents to ensure they are communicating properly.

Workflow Health

Keep an eye on workflow statuses. Stuck or failed workflows can impact monitoring.

Management Server Health

Monitor the health of management servers, ensuring they are reachable and responsive.

10.9.1.4 Alerts and Notifications

Alerts Queue

Monitor the queue length of alerts waiting to be processed. A backlog could indicate processing issues.

Notification Delays

Track notification delivery times to ensure timely alert notifications.

10.9.1.5 Performance Counters

Use SCOM management packs or custom scripts to collect and analyze performance counters related to SCOM components. Important counters include those related to the Health Service, SDK Service, and Data Access.

10.9.1.6 Logs and Events

Regularly check SCOM event logs and SCOM operational logs for any errors or warnings. Unusual log entries can provide early indications of problems.

10.9.1.7 Reports and Dashboards

Create custom reports and dashboards in SCOM to visualize performance trends over time. This can help in proactive monitoring and capacity planning.

10.9.1.8 Regular Maintenance

Perform regular maintenance tasks, such as database grooming, purging old data, and optimizing the SCOM databases.

10.9.1.9 Integration with Monitoring Tools

Integrate SCOM with other monitoring tools to cross-verify alerts and performance data. This can provide a more comprehensive view of your infrastructure.

10.9.1.10 Alert Tuning

Fine-tune alert thresholds to reduce noise. Customize alerting based on your specific environment to focus on critical issues.

10.9.1.11 Regular Upgrades and Updates

Keep SCOM up to date with the latest updates and patches. Newer versions often come with performance improvements and bug fixes.

By monitoring these aspects, you can ensure that SCOM is running smoothly, allowing you to effectively monitor your entire infrastructure without any hiccups in the monitoring system itself.

10.10 Consider Cloud-Based Monitoring

Evaluate the possibility of moving some monitoring tasks to cloud-based solutions. Cloud monitoring services often handle scalability and resource management, allowing you to focus on specific, critical tasks.

Click here to reach the Microsoft Azure Monitor web page.

Click here to reach the Microsoft Azure Sentinel web page.

Click here to reach the Microsoft Azure Monitor SCOM Managed Instance web page.

Click here and here to learn more on Azure Monitor SCOM Managed Instance published by NiCE.

10.11 Training and Skill Development

Invest in training for SCOM administrators. A well-trained team can make better use of available resources and find innovative solutions to challenges.

10.12 Regular Review and Adjustments

Regularly review the SCOM setup and adjust based on changing requirements and available resources. A flexible approach is essential when dealing with constraints.

By adopting a combination of these strategies and staying proactive, SCOM administrators can effectively manage resource constraints while ensuring critical systems are monitored efficiently.

11. Optimize the SCOM Performance

Optimizing the performance of System Center Operations Manager (SCOM) is crucial to ensure that it effectively monitors your IT environment without causing undue strain on resources. Here are several steps a SCOM administrator can take to optimize SCOM performance:

11.1 Right-Sizing Hardware Resources

Ensure that the hardware resources (CPU, memory, disk) allocated to the SCOM management servers and databases are adequate for the size and workload of your environment. Monitor resource usage and scale as needed.

11.2 Database Maintenance

Regularly perform maintenance tasks on the SCOM databases, including the Operations Manager and Data Warehouse databases. This includes tasks like index optimization, defragmentation, and database grooming.

11.3 SQL Server Configuration

Optimize the SQL Server instance hosting the SCOM databases. Set appropriate memory, disk, and CPU configurations for SQL Server based on best practices.

11.4 Database Placement

Ensure that the SCOM databases are placed on fast and reliable storage to minimize latency and maximize database performance. Consider using SQL Server AlwaysOn Availability Groups for high availability.

11.5 Distributed Deployment

Distribute the SCOM workload across multiple management servers if your environment is large. Use load balancing to evenly distribute agent traffic.

11.6 Agent Management

Manage the number of agents on each management server to prevent overloading. Distribute agents based on workload and importance.

11.7 Monitoring Overrides

Use overrides to adjust monitoring settings and thresholds for specific objects or groups of objects. This helps tailor monitoring to your environment's specific needs.

11.8 Alert Tuning

Fine-tune alert thresholds and rules to reduce false positives and noise. Disable or adjust rules that consistently generate non-actionable alerts.

11.9 Performance Baselines

Create and monitor performance baselines for your environment to understand normal behavior and detect deviations more accurately.

11.10 Network Optimization

Ensure that network communication between SCOM management servers, agents, and databases is optimized to minimize latency and bottlenecks.

11.11 Maintenance Mode

Place monitored objects or systems in maintenance mode during planned maintenance to prevent alerts and data collection during downtime.

11.12 Log Management

Integrate SCOM with log management solutions to offload long-term storage and analysis of log data. This reduces the load on SCOM databases.

11.13 Reporting Optimization

Configure SCOM reporting services for optimal performance. Ensure that reporting databases are maintained efficiently.

11.14 Security Considerations

Implement proper security measures to prevent unauthorized access to SCOM resources. Ensure that SCOM security roles are well-defined and managed.

11.15 Regular Updates

Keep SCOM and its management packs up to date. Microsoft often releases updates and performance improvements in newer versions.

11.16 Monitoring as Code (MaC)

Consider implementing Monitoring as Code practices to automate the provisioning and configuration of monitoring resources, making it easier to optimize SCOM at scale.

11.17 Test and Staging Environments

Maintain a test or staging environment to evaluate changes, management packs, and configurations before deploying them to the production environment. This helps avoid performance issues caused by untested changes.

11.18 Documentation and Knowledge Sharing

Document your SCOM configurations and best practices. Share knowledge among the SCOM team to ensure that everyone follows performance optimization guidelines.

By implementing these strategies and regularly monitoring the performance of your SCOM environment, you can ensure that SCOM operates efficiently and effectively, providing valuable insights into the health and performance of your IT infrastructure.

12. Monitoring Non-Windows Platforms using Microsoft SCOM

Expanding System Center Operations Manager (SCOM) to monitor non-Windows environments is crucial for organizations with diverse IT infrastructures. SCOM primarily focuses on Windows-based systems, but it can also be extended to monitor non-Windows environments using various methods. Here's what a SCOM admin can do to include monitoring of non-Windows environments:

12.1 Use Management Packs

Leverage third-party or custom-built management packs designed to monitor non-Windows platforms. Many vendors provide management packs for specific applications, databases, networking devices, and other technologies.

Click here to reach the NiCE AIX Management Pack web page.

Click here to reach the NiCE Linux Power Management Pack web page.

Click here to reach the NiCE PowerHA Management Pack web page.

Click here to reach the NiCE zLinux Management Pack web page.

12.2 Custom Scripts and SNMP Monitoring

Write custom scripts or use existing ones to collect performance data from non-Windows systems. SCOM supports scripting languages like PowerShell and VBScript.

Utilize SNMP (Simple Network Management Protocol) to monitor network devices, Unix-based systems, and other SNMP-enabled devices. SCOM has built-in SNMP monitoring capabilities.

12.3 Cross-Platform Extensions

Explore cross-platform extensions compatible with SCOM. These extensions enable SCOM to monitor various non-Windows platforms seamlessly.

12.4 Linux/Unix Monitoring

Utilize management packs specifically designed for Linux/Unix environments. Some management packs enable monitoring of servers, services, processes, and log files on Linux/Unix systems.

Click here to reach the NiCE AIX Management Pack web page.

Click here to reach the DB2 Management Pack web page.

Click here to reach the NiCE Linux Power Management Pack web page.

Click here to reach the MongoDB Management Pack web page.

Click here to reach the Oracle Management Pack web page.

Click here to reach the NiCE PowerHA Management Pack web page.

Click here to reach the Veritas Cluster Management Pack web page.

Click here to reach the NiCE zLinux Management Pack web page.

12.5 JMX (Java Management Extensions) Monitoring

For Java-based applications and servers, use JMX management packs to monitor Java applications and virtual machines.

Click here to learn more about how to configure monitoring for Java applications.

Click here to learn more about the Management Packs for JEE Application Servers on System Center Wiki.

Click here to learn more about the Center Monitoring Pack for Java EE.

12.6 REST APIs and Web Services

Utilize REST APIs and web services provided by applications and devices. SCOM can consume data from APIs to monitor non-Windows environments.

12.7 Log File Monitoring

Use SCOM to monitor log files on non-Windows systems. Configure rules to parse log files for specific events or errors, allowing proactive issue detection.

Click here to learn more about the NiCE Log File Management Pack.

12.8 Database Monitoring

Employ management packs tailored for specific databases like MySQL, Oracle, or PostgreSQL. These management packs enable monitoring of database performance, availability, and health.

Click here to reach the DB2 Management Pack web page.

Click here to reach the MongoDB Management Pack web page.

Click here to reach the Oracle Management Pack web page.

12.9 Custom Data Collection

Develop custom data collection methods using scripts or APIs to gather performance metrics from non-Windows systems. Process this data in SCOM for monitoring and alerting.

12.10 Community and Third-Party Resources

Engage with the SCOM community and explore third-party resources. Often, community-developed management packs and scripts are available for monitoring non-Windows environments.

12.11 Agentless Monitoring

Implement agentless monitoring where applicable. Some non-Windows systems can be monitored without installing agents, reducing resource overhead on the monitored devices.

However, agentless monitoring will not be able to provide the same level of details as agent-based monitoring would.

12.12 Regular Testing and Maintenance

Regularly test and update management packs and custom scripts to ensure compatibility with the latest versions of SCOM and the non-Windows platforms being monitored.

By adopting these strategies, a SCOM admin can effectively extend the monitoring capabilities of SCOM to include non-Windows environments, ensuring a comprehensive view of the entire IT infrastructure.

Resources

Articles & Recordings

https://4sysops.com/archives/monitoring-microsoft-365-with-scom-and-the-nice-active-365-management-pack/

https://auth0.com/docs/deploy-monitor/monitor/monitor-using-scom

https://blakedrumm.com/blog/scom-dw-grooming-tool/

https://blog.topqore.com/new-in-scom-2022-admin-rbac/

https://blog.topqore.com/scom-reporting-series-scheduling-reports/

https://ds.squaredup.com/blog/monitoring-microsoft-azure-and-hybrid-cloud/

https://ds.squaredup.com/blog/scom-activity-log/

https://kevinholman.com/2008/02/12/grooming-process-in-the-scom-database/

https://kevinholman.com/2014/03/12/modifying-access-in-scom-user-roles-without-the-console/

https://kevinholman.com/2016/05/26/monitoring-a-file-hash-using-scom/

https://kevinholman.com/2016/11/21/understanding-scom-resource-pools/

https://kevinholman.com/2018/05/06/implementing-tls-1-2-enforcement-with-scom/

https://kevinholman.com/2021/09/07/automating-agent-load-balancing-for-management-servers-and-gateways/

https://kevinholman.com/2022/05/01/scom-2022-quickstart-deployment-guide/

https://kevinjustin.com/blog/category/sql/

https://nathangau.wordpress.com/2020/04/21/security-monitoring-using-scom-to-capture-suspicious-user-activity/

https://nathangau.wordpress.com/2021/10/20/scom-security-monitoring-and-sentinel-integration/

https://nathangau.wordpress.com/tag/rule/

https://www.cookdown.com/blog/10-useful-scom-powershell-scripts

https://www.cookdown.com/blog/introducing-easy-tune-the-new-way-to-tune-scom

https://www.cookdown.com/blog/scom-alert-basics

https://www.nice.de/2023/04/19/azure-scom-mi-nice-management-packs/

https://www.nice.de/2023/09/11/microsoft-scom-itsm-ticketing-connectors/

https://www.souravmahato.com/how-to-make-reporting-console-part-of-high-availability-in-scom/

https://scomathon.com/blog/coffee-break-integrating-the-security-monitoring-mp-into-microsoft-sentinel/

https://scomathon.com/blog/coffee-break-scom-alerting-basics-explained/

https://scomathon.com/webinars/coffee-break/scom-security/

https://scomathon.com/webinars/workshop-week-2020/scom-management-group-and-database-tuning/

https://www.youtube.com/watch?v=jm7qTFrH-9A

Blogs

http://blog.scomskills.com/

http://thoughtsonopsmgr.blogspot.com/

https://blakedrumm.com/

https://blog.rjz.de/category/scom/

https://blog.topqore.com/

https://blog.tyang.org/categories/

https://kevingreeneitblog.blogspot.com/search/label/SCOM

https://kevinholman.com/

https://kevinjustin.com/blog/tag/scom/

https://maxcoreblog.com/

https://michelkamp.wordpress.com/

https://monitoringguys.com/

https://mountainss.wordpress.com/tag/scom/

https://nathangau.wordpress.com/

https://www.anoopcnair.com/sccm-scom-alerts-fine-tune-alerts/

https://www.cookdown.com/blog

https://www.opsman.co.za/tag/scom/

https://www.walshamsolutions.com/technical-blog

Documentation

https://learn.microsoft.com/en-us/azure/automation/automation-hybrid-runbook-worker

https://learn.microsoft.com/en-us/azure/azure-monitor/agents/om-agents

https://learn.microsoft.com/en-us/azure/azure-monitor/vm/scom-managed-instance-overview

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/manage/monitor/cloud-models-monitor-overview

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/strategy/monitoring-strategy

https://learn.microsoft.com/en-us/azure/defender-for-cloud/file-integrity-monitoring-enable-ama

https://learn.microsoft.com/en-us/azure/defender-for-cloud/file-integrity-monitoring-enable-log-analytics

https://learn.microsoft.com/en-us/azure/defender-for-cloud/file-integrity-monitoring-overview

https://learn.microsoft.com/en-us/azure/sentinel/automation

https://feedback.azure.com/d365community/forum/2a49c9ee-4436-ec11-b6e6-00224824730c

https://learn.microsoft.com/en-us/services-hub/unified/health/establish-connectivity-to-azure

https://learn.microsoft.com/en-us/services-hub/unified/health/setup-config-log-analytics-scom

https://learn.microsoft.com/en-us/skypeforbusiness/management-tools/use-scom-management-pack/test-users-and-settings

https://learn.microsoft.com/en-us/system-center/orchestrator/integration-pack-for-operations-manager?view=sc-orch-2022

https://learn.microsoft.com/en-us/system-center/scom/configure-log-analytics-for-scom-managed-instance?view=sc-om-2022

https://learn.microsoft.com/en-us/system-center/scom/deploy-distributed-deployment?view=sc-om-2022

https://learn.microsoft.com/en-us/system-center/scom/deploy-install-gateway-server?view=sc-om-2022&tabs=InstallGatewayServer

https://learn.microsoft.com/en-us/system-center/scom/deploy-upgrade-agents?view=sc-om-2022

https://learn.microsoft.com/en-us/system-center/scom/get-started?view=sc-om-2022

https://learn.microsoft.com/en-us/system-center/scom/key-concepts?view=sc-om-2022

https://learn.microsoft.com/en-us/system-center/scom/making-changes-to-operations-manager-management-group?view=sc-om-2022

https://learn.microsoft.com/en-us/system-center/scom/manage-agent-heartbeat-overview?view=sc-om-2022

https://learn.microsoft.com/en-us/system-center/scom/manage-agentless-monitoring?view=sc-om-2022

https://learn.microsoft.com/en-us/system-center/scom/manage-alert-created-by-monitor?view=sc-om-2022

https://learn.microsoft.com/en-us/system-center/scom/manage-alert-data-driven-management?view=sc-om-2022

https://learn.microsoft.com/en-us/system-center/scom/manage-alert-generation-overview?view=sc-om-2022

https://learn.microsoft.com/en-us/system-center/scom/manage-configure-monitoring-java-applications?view=sc-om-2022

https://learn.microsoft.com/en-us/system-center/scom/manage-integration-thirdparty-overview?view=sc-om-2022

https://learn.microsoft.com/en-us/system-center/scom/management-pack-change-tracking?view=sc-om-2022

https://learn.microsoft.com/en-us/system-center/scom/manage-mp-create-unsealed-mp?view=sc-om-2022

https://learn.microsoft.com/en-us/system-center/scom/manage-mp-lifecycle?view=sc-om-2022

https://learn.microsoft.com/en-us/system-center/scom/manage-mp-mpassessment?view=sc-om-2022

https://learn.microsoft.com/en-us/system-center/scom/manage-mp-override-rule-monitor?view=sc-om-2022

https://learn.microsoft.com/en-us/system-center/scom/manage-mp-overview-override-targets?view=sc-om-2022

https://learn.microsoft.com/en-us/system-center/scom/manage-omdb-grooming-settings?view=sc-om-2022

https://learn.microsoft.com/en-us/system-center/scom/manage-overview-management-pack?view=sc-om-2022

https://learn.microsoft.com/en-us/system-center/scom/manage-reports-create-reports?view=sc-om-2022

https://learn.microsoft.com/en-us/system-center/scom/manage-reports-installed-during-setup?view=sc-om-2022

https://learn.microsoft.com/en-us/system-center/scom/manage-resource-pools-manage?view=sc-om-2022

https://learn.microsoft.com/en-us/system-center/scom/manage-security-create-runas-account?view=sc-om-2022

https://learn.microsoft.com/en-us/system-center/scom/manage-security-overview?view=sc-om-2022

https://learn.microsoft.com/en-us/system-center/scom/manage-using-omcmdlets?view=sc-om-2022

https://learn.microsoft.com/en-us/system-center/scom/operations-manager-managed-instance-create-reports-on-power-bi?view=sc-om-2022

https://learn.microsoft.com/en-us/system-center/scom/operations-manager-managed-instance-overview?view=sc-om-2022

https://learn.microsoft.com/en-us/system-center/scom/plan-hadr-design?view=sc-om-2022

https://learn.microsoft.com/en-us/system-center/scom/plan-mgmt-group-design?view=sc-om-2022

https://learn.microsoft.com/en-us/system-center/scom/plan-planning-agent-deployment?view=sc-om-2022&tabs=Windows

https://learn.microsoft.com/en-us/system-center/scom/plan-resource-pool-design?view=sc-om-2022

https://learn.microsoft.com/en-us/system-center/scom/plan-security-accounts?view=sc-om-2022

https://learn.microsoft.com/en-us/system-center/scom/plan-security-runas-accounts-profiles?view=sc-om-2022

https://learn.microsoft.com/en-us/system-center/scom/plan-security-tls12-config?view=sc-om-2022

https://learn.microsoft.com/en-us/system-center/scom/plan-sqlserver-design?view=sc-om-2022

https://learn.microsoft.com/en-us/system-center/scom/release-build-versions?view=sc-om-2022

https://learn.microsoft.com/en-us/system-center/scom/sql-server-management-pack-monitoring-configuration?view=sc-om-2022

https://learn.microsoft.com/en-us/system-center/scom/system-requirements?view=sc-om-2022

https://learn.microsoft.com/en-us/system-center/scom/web-application-availability-monitoring-template?view=sc-om-2022

https://learn.microsoft.com/en-us/system-center/scom/welcome?view=sc-om-2022

https://learn.microsoft.com/en-us/troubleshoot/system-center/scom/best-practices-configure-overrides

https://learn.microsoft.com/en-us/system-center/scsm/load-balancing?view=sc-sm-2022

https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/monitoring-active-directory-for-signs-of-compromise

Downloads

https://github.com/blakedrumm/SCOM-DW-Grooming-Tool

https://github.com/MPCatalog/scom-community-catalog

https://github.com/search?q=scom&type=repositories

https://www.microsoft.com/en-us/download/details.aspx?id=103379

https://www.microsoft.com/en-us/download/details.aspx?id=13302

https://www.microsoft.com/en-us/download/details.aspx?id=50013

https://www.microsoft.com/en-us/download/details.aspx?id=54081

https://www.microsoft.com/en-us/download/details.aspx?id=54525

Events

https://build.microsoft.com/en-US/home

https://defcon.org/index.html

https://expertslive.org/

https://ignite.microsoft.com/en-US/home

https://mmsmoa.com/

https://www.collabdays.org/

Microsoft Tech Community, System Center Wiki, Q&As, others

https://azure.microsoft.com/

https://azure.microsoft.com/en-us/products/microsoft-sentinel

https://learn.microsoft.com/en-us/answers/questions/107136/scom-2019-role-based-access-and-delegation

https://learn.microsoft.com/en-us/answers/questions/1349333/scom-bottleneck

https://learn.microsoft.com/en-us/answers/questions/906535/need-a-scom-alert-when-perticular-user-tries-to-lo

https://learn.microsoft.com/en-us/answers/questions/926293/script-for-collecting-data-from-scom

https://techcommunity.microsoft.com/t5/skype-for-business-blog/create-and-configure-users-for-synthetic-transactions/ba-p/619121

https://techcommunity.microsoft.com/t5/system-center/ct-p/SystemCenter

https://techcommunity.microsoft.com/t5/system-center-blog/bg-p/SystemCenterBlog

https://techcommunity.microsoft.com/t5/system-center-blog/finally-alert-tuning-for-scom-solved/ba-p/1192802

https://techcommunity.microsoft.com/t5/system-center-blog/secure-your-infrastructure-monitoring-with-scom/ba-p/2180736

https://social.technet.microsoft.com/wiki/contents/articles/16174.microsoft-management-packs.aspx

https://systemcenter.wiki/

https://systemcenter.wiki/#gsc.tab=0

https://systemcenter.wiki/?GetCategory=Community+Catalog+Management+Pack

https://systemcenter.wiki/?GetCategory=Java+EE+Monitoring

https://systemcenter.wiki/?GetCategory=JEE+Application+Servers

https://systemcenter.wiki/?GetCategory=Windows+Server+Network+Load+Balancing+%28NLB%29

https://systemcenter.wiki/?Get-ManagementPack=Microsoft.SystemCenter.SyntheticTransactions.Library&Version=6.1.7221.0

https://systemcenter.wiki/?Get-ManagementPack=Security.Monitoring&Version=1.0.4.272

https://systemcenter.wiki/?Get-ManagementPack=TLS_Compliance_Pack&Version=1.0.0.21

Third-Party Solutions

https://axanto.com/

https://silect.com/

https://squaredup.com/

https://subscription.packtpub.com/book/cloud-and-networking/9781782176244/1/ch01lvl1sec12/designing-for-high-availability

https://www.nice.de/active-365-mp/

https://www.nice.de/aix-management-pack-for-microsoft-scom/

https://www.nice.de/all-solutions/

https://www.nice.de/ibm-db2-management-pack/

https://www.nice.de/log-file-monitoring-scom-nice-logfile-mp/

https://www.nice.de/microsoft-scom-mp-ibm-system-z-monitoring-nice-zlinux-mp/

https://www.nice.de/nice-linux-power-mp-for-microsoft-scom/

https://www.nice.de/nice-mongodb-management-pack-for-microsoft-scom/

https://www.nice.de/nice-veritas-cluster-mp-for-microsoft-scom/

https://www.nice.de/oracle-database-management-pack/

https://www.nice.de/powerha-management-pack/

Trainings

https://learn.microsoft.com/en-us/training/browse/

https://learn.microsoft.com/

https://scomathon.com/training-tools/

https://topqore.com/topqore-scom-certification-path-overview/

https://www.etc.at/training/scom/

https://www.glasspaper.no/en/courses/scom/

https://www.pluralsight.com/courses/monitor-maintain-software-defined-datacenter-scom

https://www.pluralsight.com/search?q=system%20center%20operations%20manager

https://www.prajwaldesai.com/update-scom-management-packs/

https://www.stigviewer.com/stig/microsoft_scom/

https://www.truesec.com/training/mastering-system-center-operations-manager

https://www.udemy.com/courses/search/?src=ukw&q=system+center+operations+manager

https://www.youtube.com/results?search_query=system+center+operations+manager

User Groups

https://memug.org/

https://nwscug.org/

https://scomathon.com/

https://scomathon.slack.com/

https://tcsmug.org/

https://www.hasmug.com/

https://www.reddit.com/r/scom/

About NiCE

NiCE Services for Microsoft System Center encompass consulting services tailored to System Center Operations Manager, Configurations Manager, and Service Manager. Our offerings include SCOM Health Assessments, advice and provisioning for third-party SCOM tools, as well as SCOM-centric monitoring solutions for business elements such as applications, databases, operating systems, services, and custom applications.

NiCE Management Packs for SCOM are available for AIX, Azure AD Connect, Entra ID, Citrix VAD & ADC, Custom Applications, HCL Domino, IBM Db2, IBM Power HA, Linux on Power Systems, Log Files, Microsoft 365, Microsoft Teams, Microsoft SharePoint, Microsoft Exchange, Microsoft OneDrive, Mongo DB, Oracle, Veritas Clusters, VMware, VMware Horizon, and zLinux.

Our commitment
1. Ongoing development, incl. latest version support
2. Top required metrics come out-of-the-box
3. Integrated source knowledge to solve issues faster
4. Custom development & coaching
5. Highly responsive support team
6. Easy onboarding & renewals
7. Largest set of Microsoft SCOM Management Packs

About Microsoft System Center Operations Manager (SCOM)
Microsoft System Center Operations Manager (SCOM) is a powerful IT management solution designed to help organizations monitor, troubleshoot, and ensure the health of their IT infrastructure. SCOM provides comprehensive infrastructure monitoring, offering insights into the performance, availability, and security of applications and workloads across on-premises, cloud, and hybrid environments. With its robust set of features, SCOM enables IT professionals to proactively identify and address potential issues before they impact the business, improving overall operational efficiency and reducing downtime. By leveraging SCOM, businesses can achieve greater control over their IT environment, ensuring a seamless user experience and enhancing the reliability of their services.

Take advantage of all the benefits of advanced monitoring using NiCE Management Packs for Microsoft System Center Operations Manager. Contact us at solutions@nice.de (EMEA, APAC), or solutions@nice.us.com (US, LATAM) for a quick demo, and a free 30 days trial.

NiCE IT Management Solutions GmbH
Liebigstrasse 9
71229 Leonberg
Germany
www.nice.de
solutions@nice.de

NiCE IT Management Solutions Corporation
3478 Buskirk Avenue, Suite 1000
Pleasant Hill, CA 94523
USA
www.nice.us.com
solutions@nice.us.com