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

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