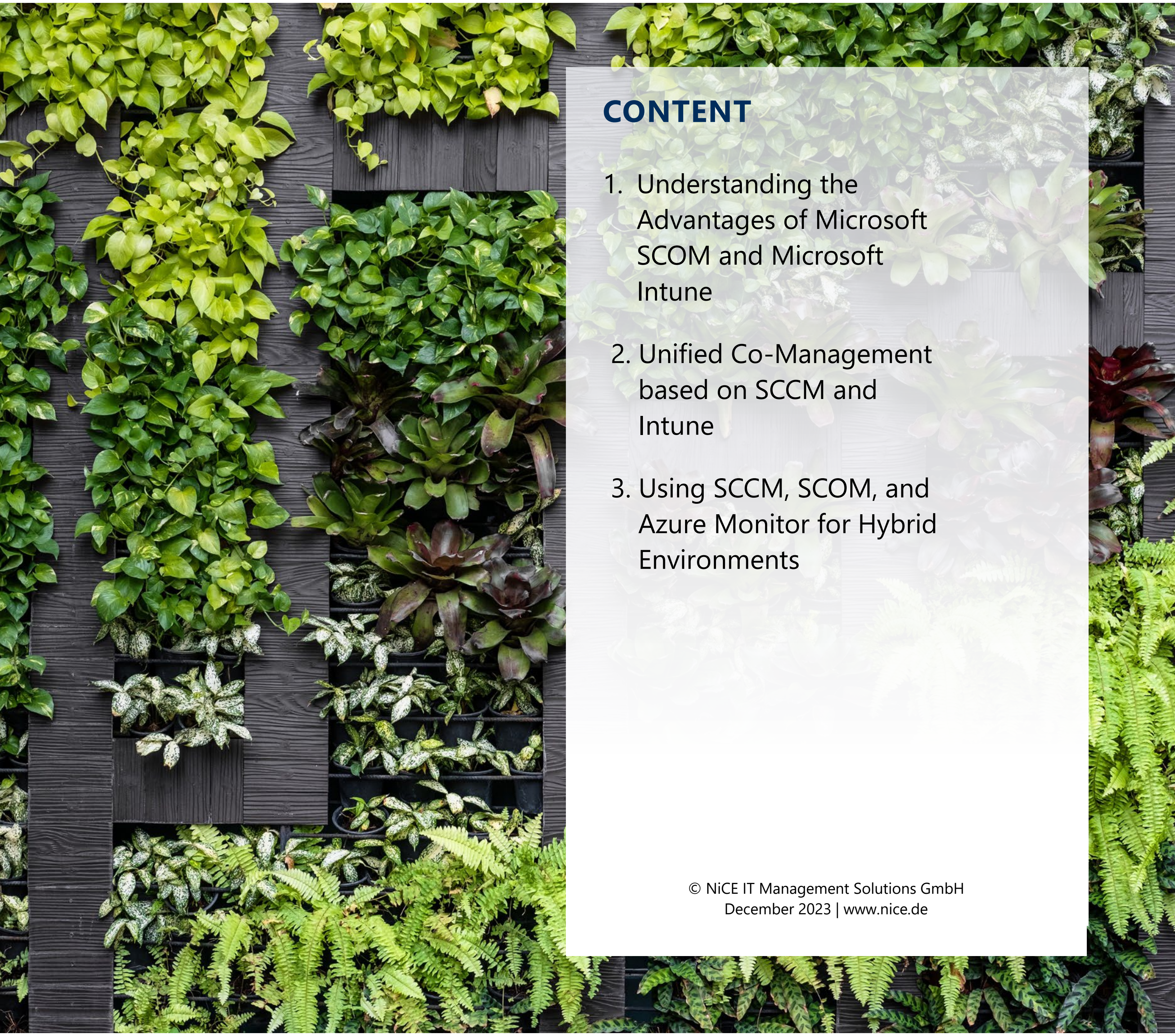
Managing Hybrid Environments Using SCCM, Intune, and SCOM

A White Paper by NiCE IT Management Solutions



CONTENT

December 2023 | www.nice.de

Content

Understanding Microsoft SCOM and Intune

In the dynamic landscape of IT management, organizations face the **challenge of monitoring infrastructure health and managing diverse endpoints efficiently**. Microsoft offers two powerful solutions, System Center Operations Manager (SCOM) and Intune, each tailored to address distinct aspects of IT management. In this blog post, we will delve into the functionalities of SCOM and Intune, explore their detailed differences, and understand why paying attention to Intune alerts is crucial.

System Center Operations Manager (SCOM)

SCOM is a stalwart in the realm of IT infrastructure monitoring. Its primary function is to scrutinize the health, performance, and availability of on-premises datacenter resources and applications. SCOM achieves this through a deployment that involves installing agents on servers and devices, which then report data back to the SCOM management server.

Key Features of SCOM

On-Premises Orientation

SCOM is traditionally deployed on-premises, aligning with the needs of organizations managing in-house datacenters.

Complexity and Customization

SCOM provides a high degree of customization, allowing organizations to create tailored management packs for monitoring specific applications or services.

Alerting and Reporting

It boasts a sophisticated alerting system and detailed reporting capabilities, enabling administrators to proactively address issues.

Microsoft Intune

In contrast, Intune embodies Microsoft's modern management approach, focusing on endpoint management. As a cloud-based service, Intune leverages the Microsoft Azure platform to manage and secure a diverse range of endpoints, including Windows, macOS, iOS, Android, and IoT devices.

Key Features of Intune

Cloud-Based Solution

Intune is a cloud-native service, eliminating the need for on-premises servers and ensuring scalability and flexibility.

Modern Device Management

It excels in managing modern devices, supporting features like Mobile Device Management (MDM) and catering to a broad spectrum of devices.

Security and Compliance

Intune emphasizes security with features like conditional access policies and security baselines, ensuring a robust security posture for managed devices.

Differences and Use Cases of SCOM and Intune

	SCOM	**Intune**
Deployment Model	On-premises deployment for organizations managing in-house datacenters.	Cloud-based deployment suitable for modern, diverse device ecosystems.
Focus Area	Infrastructure monitoring with a focus on datacentre resources.	Endpoint management covering a variety of devices, applications, and security aspects.
Customization	Highly customizable with the ability to create specific management packs.	Customization is more streamlined, emphasizing a user-friendly, cloud-native approach.
Integration	Part of the System Center Suite, allowing integration with other on-premises System Center components.	Tightly integrated with Microsoft 365 services, offering seamless collaboration with Azure Active Directory and Endpoint Security.

Why Pay Attention to Intune Alerts

Intune alerts play a pivotal role in maintaining a secure and efficient endpoint management environment. Here are key reasons to pay close attention to Intune alerts.

Security Threat Mitigation

Intune alerts provide real-time insights into potential security threats, allowing administrators to take immediate action to mitigate risks and protect sensitive data.

Compliance Enforcement

By monitoring Intune alerts, organizations can ensure that device configurations adhere to compliance standards, preventing security vulnerabilities and maintaining regulatory compliance.

Proactive Issue Resolution

Intune alerts proactively notify administrators of issues related to device management, application deployment, and security policies, enabling swift resolution before they impact business operations.

Insight into Endpoint Health

Monitoring Intune alerts offers visibility into the health and performance of managed endpoints, facilitating proactive maintenance and ensuring a smooth end-user experience.

In conclusion, the choice between SCOM and Intune hinges on the specific requirements and priorities of an organization. While SCOM excels in traditional infrastructure monitoring, Intune is tailored for the complexities of managing modern endpoints in a cloud-centric world. Many organizations find value in utilizing both solutions, leveraging the strengths of each to comprehensively address their IT management needs.

As the IT landscape evolves, understanding the nuances of SCOM and Intune becomes crucial for making informed decisions that align with organizational objectives, and the vigilance in monitoring Intune alerts is paramount for maintaining a secure and well-managed endpoint environment.

Unified Co-Management based on System Center Configuration Manager and Intune

Co-management in the context of Microsoft System Center Configuration Manager (SCCM) refers to the ability to manage devices using both SCCM and Microsoft Intune simultaneously. This approach enables organizations to leverage the strengths of both platforms while providing a unified management experience.

How co-management works with SCCM and Intune

Device Management

Co-management allows devices to be managed by both SCCM and Intune. This setup provides flexibility in managing various device types, such as traditional on-premises devices (managed by SCCM) and modern cloud-based devices (managed by Intune).

Configuration and Policies

With co-management, administrators can create policies and configurations in SCCM and Intune and apply them to devices based on specific requirements. This capability ensures consistent management across both platforms.

Conditional Access and Compliance

Co-management enables the enforcement of security policies and conditional access based on compliance rules set in both SCCM and Intune. This ensures that devices adhere to organizational security standards regardless of their management source.

Migration and Transition

Organizations can gradually transition workloads and functionalities from SCCM to Intune at their own pace. This phased approach allows for a smooth migration without disrupting ongoing operations.

Reporting and Monitoring

Co-management provides a unified view of device inventory, compliance, and performance across both SCCM and Intune. It simplifies reporting and monitoring by offering a consolidated dashboard for administrators.

Feature Parity and Integration

Microsoft continuously works on aligning features between SCCM and Intune, ensuring that both platforms offer similar capabilities. This integration allows administrators to seamlessly manage devices without compromising on functionalities.

By utilizing co-management, organizations can take advantage of the hybrid approach to device management, leveraging the strengths of both SCCM and Intune. It also paves the way for a more streamlined and efficient management strategy, especially in environments where a mix of on-premises and cloud-based resources coexist.

System Center Configuration Manager, Operations Manager, and Azure Monitor for Hybrid Environments

System Center Configuration Manager (SCCM) remains a robust solution, especially for datacenters that are tightly integrated with Azure. Here's how SCCM excels in the datacenter space and its relevance in Azure-connected environments.

On-Premises Management

SCCM has been a cornerstone for on-premises device management for years, offering comprehensive control over endpoints, servers, and devices within datacenters. It provides features for software deployment, patch management, inventory tracking, and compliance enforcement, crucial for datacenter operations.

Hybrid Capabilities with Azure

SCCM's integration with Azure services facilitates hybrid management scenarios. This means SCCM can effectively manage devices both on-premises and in the cloud. It enables organizations to extend their datacenter management capabilities to the Azure environment seamlessly.

Azure Services Integration

SCCM leverages Azure services for various functionalities, such as Azure Active Directory for identity management, Azure Monitor for enhanced monitoring capabilities, and Azure Security Center for security management. This integration allows SCCM to extend its capabilities into the Azure ecosystem.

Migration Paths and Coexistence

SCCM provides pathways for coexistence and migration strategies, allowing organizations to gradually transition their management workload from on-premises SCCM to cloud-based solutions like Intune without disrupting existing operations in the datacenter.

System Center Operations Manager and its relevance in this context

SCOM plays a vital role in monitoring and maintaining the health of datacenter infrastructure. It provides deep insights into the performance, availability, and health of servers, applications, and workloads within the datacenter environment. SCOM's Management Packs, especially those designed for Azure, extend its capabilities to monitor Azure resources effectively.

When integrated with SCCM, SCOM enhances the monitoring capabilities of the datacenter environment. It offers insights into not just the performance and health of the infrastructure but also the status of deployed applications and their impact on the overall system.

In conclusion, **SCCM remains a powerful solution for datacenter management**, especially for environments that have a strong connection to Azure. Its ability to manage on-premises and hybrid environments, coupled with its integration with Azure services, makes it a compelling choice for organizations looking to maintain a robust, centralized management system for their datacenters. When **paired with SCOM for comprehensive monitoring**, SCCM proves its continued relevance in modern datacenter operations.

Resources

Co-Management

https://learn.microsoft.com/en-us/mem/configmgr/comanage/overview

Endpoint Manager

https://learn.microsoft.com/en-us/mem/endpoint-manager-overview

Microsoft Intune

https://learn.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune

Configuration Manager

https://learn.microsoft.com/en-us/mem/configmgr/core/understand/introduction

Microsoft SCOM

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

Azure Monitor

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

Azure Monitor SCOM Managed Instance

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

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 and Azure Monitor SCOM Managed Instance (SCOM MI) 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