

Custom Crafted Management Pack Use Cases

F5 Monitoring on Microsoft SCOM

Content

1. F5 Monitoring
2. Key Aspects for Microsoft SCOM Admins
3. About NiCE



Content

- F5 Monitoring3**
 - What is F5? 3
 - Why Monitor F5? 4
- Top Areas to Monitor in F54**
 - Availability 4
 - Performance 5
 - Security & Access 5
- F5 Cloud vs On-Prem Monitoring: Key Differences6**
 - Overview 6
 - F5 On-Prem Monitoring..... 6
 - F5 Cloud Monitoring (e.g., AWS, Azure, GCP)..... 7
 - Summary Table 8
 - Recommendations for SCOM Monitoring 8
- Essential Features of an F5 Management Pack for SCOM9**
 - Key Areas SCOM Admins Should Focus on When Monitoring F5 11
- F5 Monitoring Use Cases.....12**
 - Detecting Performance Degradation Before Users Complain..... 12
 - Detecting Unauthorized Access Attempts and Potential Security Breaches..... 13
 - Ensuring High Availability of Application Delivery..... 13
 - Scaling Capacity in Line with Growing Traffic 14
- NiCE Services and Training for Microsoft SCOM.....15**
- About NiCE16**

F5 Monitoring

As part of a recent customer project, we developed a custom F5 Management Pack for Microsoft System Center Operations Manager (SCOM). This bespoke solution enables IT operations teams to monitor the performance, availability, and health of F5 infrastructure directly within the SCOM environment. It provides deep visibility into key metrics, helping ensure application delivery remains stable, secure, and efficient.

With this Use Case paper, we're sharing our experience with the SCOM community to showcase what's possible with tailored monitoring integrations. Our goal is to help IT teams extend the value of SCOM and enhance their operational capabilities through advanced monitoring of F5 systems.

What is F5?

F5 refers to a suite of **application delivery and security solutions**, best known for its **BIG-IP platform**. Organizations use F5 primarily to ensure their applications are **fast, secure, and always available**, whether those applications are hosted on-premises, in the cloud, or in hybrid environments.

Key Use Cases for F5

Load Balancing: Distributes traffic across multiple servers to ensure high availability, performance, and scalability of applications.

Application Delivery Control (ADC): Optimizes the flow of traffic between users and applications, improving responsiveness and reliability.

SSL Offloading: Handles encryption/decryption tasks to reduce the burden on backend servers and speed up secure connections.

Web Application Firewall (WAF): Protects web applications from threats such as SQL injection, cross-site scripting (XSS), and other OWASP Top 10 vulnerabilities.

Traffic Management and Routing: Provides intelligent traffic steering based on policies, geolocation, device type, and other factors.

DDoS Protection: Defends against distributed denial-of-service attacks to keep services available even under attack.

Authentication & Access Control: Offers secure user access through identity-aware access policies, SSO (Single Sign-On), and MFA (Multi-Factor Authentication).

In short, **F5 acts as the front door** to critical applications, helping ensure they are secure, performant, and resilient—no matter where they're hosted or accessed from.

Why Monitor F5?

F5 devices are critical for maintaining the availability and responsiveness of enterprise applications by distributing traffic, protecting against attacks, and ensuring seamless failover. Any misconfiguration, performance degradation, or security incident on F5 can lead to application outages, slow user experiences, or security breaches impacting business continuity.

Proactive monitoring ensures optimal F5 health and configuration, supports compliance, and reduces downtime risks.

Top Areas to Monitor in F5

Availability

Device and module uptime: Confirms F5 devices and modules (e.g., LTM, GTM, ASM) are operational to prevent service interruptions.

Failover and HA status: Ensures active/passive or clustered devices are synchronized and failover mechanisms work as expected.

Interface/link health: Monitors network interface statuses and link flaps to avoid connectivity loss.

Pool member and node availability: Tracks backend server statuses managed by F5 pools to maintain reliable application delivery.

Performance

Traffic throughput and connection counts: Measures network traffic volume and concurrent sessions to assess load and capacity.

CPU, memory, and resource utilization: Monitors device resource consumption to detect saturation or impending performance issues.

SSL/TLS handshake times and offload status: Tracks cryptographic processing efficiency critical for secure application delivery.

Pool and node response times: Measures backend server response times as seen by the load balancer to detect slow services.

Health check response latency: Ensures backend health probes run timely to keep pool status accurate.

Security & Access

WAF event monitoring: Captures blocked attacks, suspicious requests, and policy violations to protect applications.

Firewall and access control logs: Tracks denied or anomalous traffic to detect potential intrusions or policy breaches.

Configuration changes audit: Monitors administrative changes for compliance and security governance.

SSL certificate expiration and status: Avoids security risks from expired or invalid certificates.

F5 Cloud vs On-Prem Monitoring: Key Differences

Overview

While F5 devices, whether deployed on-premises or in the cloud, serve similar functions (load balancing, security, application delivery), monitoring strategies differ due to deployment architecture, visibility, and integration points.

F5 On-Prem Monitoring

Typical Setup

- F5 BIG-IP hardware or virtual appliances deployed in a data center
- Managed directly via SNMP, iControl REST API, or CLI
- Full network visibility and control

Monitoring Considerations

- Use of SNMP, WMI, or API for deep metrics
- Network-level monitoring (interfaces, VLANs, hardware health)
- Direct access for configuration tracking and log collection
- SCOM can poll frequently and store performance history
- High-availability monitoring (active/standby failover pairs)
- Better customization of thresholds and alerting

Challenges

- Complexity of managing at scale
- Patch/version drift if devices aren't centrally managed

F5 Cloud Monitoring (e.g., AWS, Azure, GCP)

Typical Setup

- F5 BIG-IP Virtual Editions (VE) or F5 Distributed Cloud Services (formerly Volterra)
- Often deployed as part of a cloud-native stack with autoscaling
- May rely on cloud-native monitoring tools (e.g., CloudWatch, Azure Monitor)

- **Monitoring Considerations**
- API-based access only; SNMP might be limited or blocked
- Must account for cloud orchestration: autoscaling, ephemeral IPs, redeployments
- Licensing and throughput limits might be dynamic—monitor license and resource usage
- Requires integration with cloud-specific logging and metrics (e.g., log forwarding to SCOM)
- Focus on app-level and user-experience metrics over hardware status

Challenges

- Limited visibility into underlying infrastructure
- Multi-cloud and hybrid environments may increase complexity
- Network topology may change dynamically, complicating discovery and health checks

Summary Table

Feature / Concern	On-Prem F5	F5 in the Cloud
Discovery Method	SNMP, CLI, API	API, cloud service integration
Performance Metrics	CPU, memory, traffic, sessions	App performance, cloud metrics
Hardware Health	Yes	Not applicable
High Availability	Active/Standby monitored directly	HA is often managed by cloud orchestration
Configuration Monitoring	Full access	Limited / API-only
Log Collection	Direct (syslog/SNMP traps)	Requires cloud-native log shipping
Monitoring Tooling	SCOM, native SNMP tools	SCOM via connectors, cloud APIs
Challenges	Scale, manual config drift	Ephemeral architecture, limited control

Recommendations for SCOM Monitoring

On-Prem: Use a custom or full-featured F5 SCOM Management Pack leveraging SNMP and REST APIs.

Cloud: Use lightweight, API-based monitoring or cloud-native connectors; track autoscaling and API limits.

Hybrid: Combine both strategies and unify alerts in SCOM for a single pane of glass.

Essential Features of an F5 Management Pack for SCOM

To ensure seamless integration of F5 infrastructure into Microsoft SCOM, a robust Management Pack should offer comprehensive monitoring across availability, performance, and configuration states. The following are the core features and capabilities an effective F5 Management Pack should provide to deliver actionable insights and maintain operational stability.

Device Discovery

- Automatically discover F5 BIG-IP devices
- Support for multiple device types and virtual editions
- Hierarchical representation (device > modules > virtual servers, pools, nodes)

Health Monitoring

Monitor health states of:

- Virtual servers
- Pools and pool members
- Nodes
- Interfaces and VLANs
- Alert on degraded, unavailable, or down states

Performance Metrics Collection

Key performance counters for:

- CPU and memory usage
- Throughput (bps)
- Concurrent connections
- HTTP/HTTPS requests
- iRules execution metrics
- Historical data for trend analysis

Traffic and Load Insights

- Monitor connection statistics, load balancing metrics, and traffic throughput
- Visibility into spikes or drops in traffic across virtual servers or pools

Configuration Monitoring

- Detect changes to key configurations
- Alert on unauthorized or risky changes (config drift)

Failover and HA Monitoring

- Track high availability (HA) status
- Alert on failover events or HA degradation

SSL Offloading / Certificate Monitoring

- Monitor SSL profile usage and expiration dates of installed certificates
- Alert before certs expire or become invalid

Event and Alert Integration

- Native SCOM alerts with severity mapping
- Customizable thresholds and alert tuning
- Integration with SCOM dashboards and reporting

Security Monitoring

- Basic WAF (if provisioned) alerting such as blocked requests or signature matches
- Monitor denied requests or unusual traffic patterns

Custom Views and Dashboards

SCOM views for:

- Device overviews
- Health summaries
- Alert trends
- Optionally, integrate with SCOM widgets or third-party dashboards

Key Areas SCOM Admins Should Focus on When Monitoring F5

For SCOM administrators, monitoring F5 devices involves more than just uptime checks—it requires visibility into the health, performance, and reliability of application delivery components. The key areas below highlight what admins should focus on to proactively manage F5 environments and quickly respond to issues that could impact user experience or system availability.

Availability

Are F5 devices reachable and operational?

Are virtual servers, pools, and nodes online?

Performance

Is traffic flowing as expected?

Are there unusual spikes in CPU/memory usage or dropped packets?

Load Balancing Health

Are traffic distribution policies working?

Are any pools over/underutilized?

Redundancy & HA

Is failover working?

Is the active/standby state maintained correctly?

Configuration Drift

Have any changes been made to the system that could affect stability?

Security Events

Are there any anomalies that may indicate attacks or misconfigurations?

Certificate Lifecycle

Are any SSL certificates approaching expiration?

F5 Monitoring Use Cases

Detecting Performance Degradation Before Users Complain

Use Case

An enterprise notices periodic slowdowns in application responsiveness but no immediate complaints from users. The root cause is traced back to resource contention on the F5 load balancer during peak traffic hours.

How Monitoring Helps

- Tracks CPU, memory, and throughput metrics in real time
- Alerts on approaching resource saturation before impact occurs
- Correlates backend server health with traffic patterns for deeper insight

Benefits

- Prevents user experience degradation proactively
- Reduces firefighting by identifying bottlenecks early
- Supports capacity planning for scaling decisions

Detecting Unauthorized Access Attempts and Potential Security Breaches

Use Case

Security teams want to detect suspicious traffic patterns and blocked attacks targeting web applications protected by F5's WAF.

How Monitoring Helps

- Monitors WAF logs for blocked attack signatures and anomalies
- Alerts on repeated policy violations or unusual traffic spikes
- Audits configuration changes to catch unauthorized modifications

Benefits

- Strengthens security posture with early threat detection
- Helps meet compliance with audit trails and real-time alerts
- Protects sensitive data and application availability

Ensuring High Availability of Application Delivery

Use Case

An organization's critical applications rely on a high-availability pair of F5 devices. Unexpected failover events cause service interruptions and user frustration.

How Monitoring Helps

- Continuously monitors device and failover status
- Detects synchronization issues or failover failures immediately
- Tracks network interfaces and pool member health to ensure overall service uptime

Benefits

- Maintains seamless failover, minimizing downtime
- Enables rapid incident response to hardware or software failures
- Increases confidence in business continuity capabilities

Scaling Capacity in Line with Growing Traffic

Use Case

Rapid business growth leads to increased traffic loads through F5 devices, risking overload and slower response times.

How Monitoring Helps

- Measures traffic throughput, connection counts, and resource utilization trends
- Provides historical data to predict capacity needs
- Identifies inefficient SSL processing or misconfigured pools affecting performance

Benefits

- Supports proactive infrastructure scaling
- Avoids outages or performance bottlenecks due to overload
- Ensures consistent application delivery quality

We hope this F5 Monitoring Use Case paper inspires you to extend your monitoring on Microsoft SCOM. Feel free to reach out for help building your next custom Management Pack.

NiCE Services and Training for Microsoft SCOM

NiCE Services & Training for Microsoft System Center Operations Manager (SCOM) offers specialized expertise in enhancing IT monitoring through the development of custom Management Packs tailored to an organization's unique infrastructure and business needs.

By leveraging NiCE's deep knowledge of SCOM, their services empower IT teams to extend native monitoring capabilities, enabling precise, scalable, and efficient oversight of complex environments. The custom management packs crafted by NiCE address specific applications, devices, and services not covered by default SCOM templates, ensuring comprehensive visibility and proactive issue detection.

In addition to bespoke management pack creation, NiCE provides targeted training to equip IT professionals with the skills to maintain, customize, and optimize SCOM environments independently. This combination of tailored solutions and knowledge transfer significantly improves operational reliability, reduces downtime, and maximizes the return on investment in Microsoft SCOM deployments.

For more information please visit <https://www.nice.de/nice-services-for-microsoft-system-center/>.

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 HMC & VIOS, IBM Power HA, Linux on Power Systems, Log Files, MariaDB, Microsoft 365, Microsoft Teams, Microsoft SharePoint, Microsoft Exchange, Microsoft OneDrive, Mongo DB, NetApp ONTAP, 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 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