Real-Time Monitoring with Data Protector Management Pack

Learn how Data Protector Management pack supports SCOM and offers a cross-platform data center management system.
Data Protector Management Pack: Analytical Insight and Adaptive Intelligence

Today’s organizations are creating and managing information that is often characterized as unique, complex, and growing at speeds that challenge even the best IT professionals. Additionally, this information is often being stored on an IT infrastructure that is also unique, complex, and growing. Backup and recovery represent a core process in maintaining this IT setting.

In this volatile landscape, IT organizations can face serious challenges such as trying to:

- Balance the pressures of maintaining predictable service levels across a heterogeneous and siloed infrastructure stack
- Continue to address the growth of information
- Maintain an active approach to how resources and information are protected amid tightening CAPEX and OPEX budgets
- Maintain stringent service level requirements to support successful operations

Relying on traditional backup and recovery solutions alone no longer meets the needs of these organizations. Instead, your backup and recovery solution must enable them to make more intelligent decisions by integrating predictive analysis and an adaptive approach. When your backup and recovery software is based on operational analytics, you can create a more adaptive core IT function that is just as elastic as your data center. A solution that can create a shared and collaborative view of backup and recovery operations, in real-time enables an approach that supports informed decisions and the appropriate mobilization of resources. This new option is causing IT administrators to reexamine alternate processes and tools that can enable them to meet these needs for all functions of IT.

Micro Focus® Data Protector Management Pack for Microsoft System Center Operations Manager (SCOM) delivers real-time intelligent monitoring, analysis, isolation, remediation, and reporting for Data Protector environments. As seen in Figure 1, Data Protector Management Pack continually monitors the health and state of each component in the backup and recovery infrastructure to provide you with actionable insight that can increase the effectiveness of your data protection services.

While many IT organizations use Microsoft® SCOM to monitor and troubleshoot applications and servers, the solution often lacks backup and recovery health visibility, and the means to identify where and to what degree issues and changes impact your backup infrastructure, especially in a distributed environment. Although IT may not be directly responsible for monitoring the physical components of the infrastructure, the additional hardware and software information provided by the Data Protector Management Pack solution can dramatically enhance troubleshooting capabilities in the following ways:

- Continually monitor backup infrastructure component
- Isolate and report on problems impacting your ability to meet service level agreements
- Offer remediation recommendations and orchestrating solutions to identified issues

With Data Protector Management Pack, your IT staff benefits from detailed backup and recovery health information delivered to Microsoft SCOM about the physical, virtual, and logical components of the Data Protector environment. The result is unprecedented visibility into the health of your backup and recovery infrastructure from within SCOM. IT administrators can use Data Protector’s SCOM interface for integrated end-to-end monitoring, automated diagnosis, and intuitive reporting across their complete backup and recovery infrastructure (physical and/or virtual).

Data Protector Management Pack Delivers

- Real-time discovery, visualization, and utilization analysis—Proactively monitor, cross-correlate, and auto-detect issues that impact backup and recovery operations in heterogeneous
virtualized and physical infrastructures. Additionally, you gain deep visibility into backup and recovery infrastructure usage to dramatically accelerate backup and recovery performance monitoring and reduce the time and complexities involved in mastering multiple management tools or having to negotiate proprietary monitoring tools related to the components of backup and recovery—without leaving Microsoft SCOM.

- **Instant diagnostics and actionable Insight**—Separate cause from effect and dramatically accelerate diagnosis in simple or complex backup infrastructures to give IT administrators actionable information by pinpointing the real root cause of data protection problems more quickly and accurately.

- **Context-sensitive issue isolation with assistive remediation**—Gain configurable alerting for correlated events, sustained conditions, and escalations, enabling the IT staff to remain abreast of critical issues in the backup and recovery infrastructure with assistive troubleshooting to resolve issues before they affect those who rely on the data protection service.

- **Flexible visualization and reporting**—Get intelligent insights into the current backup and recovery infrastructure presented graphically to meet the needs of the IT administrator, enabling them to discover ways to improve utilization. IT can identify unused components to better load balance workloads, identify whether or not Recovery Point Objectives and service-level agreements remain achievable, visualize the precise information needed to enable proactive decision making, and take the most appropriate action associated with the report content.

- **Manage and control backup and recovery operations**—Context-sensitive orchestration of the Data Protector technology stack (backup target(s) to cells, to cell managers, to backup agents) and gain control over the actions that can be taken on each to achieve a well-defined and highly functioning data protection posture.

**Real-Time Discovery, Visualization, and Utilization Analysis**

Data Protector Management Pack actively collects, correlates, and analyzes the state of the components (physical and/or virtual) used in the backup and recovery process, providing topological displays with context-sensitive, state-based cues. This level of visualization allows IT administrators to operate in a backup and recovery operations mode, allowing you to make informed decisions and take decisive actions based on real-time information. The interactive map correlates backup and recovery information and state from edge-based or remote offices to the core data center. With Data Protector Management Pack, IT administrators have a single pane of glass view of the performance and health of the backup and recovery infrastructures to use in making proactive decisions on current and future data protection operations.

In addition to monitoring, Data Protector Management Pack provides utilization analytics of the backup and recovery infrastructure. With this level of insight into the technology stack, the IT staff gains deep visibility into how efficiently the data protection infrastructure is being utilized. When combined with real-time monitoring, you can dramatically improve the over/under utilization of the infrastructure while reducing operational complexities associated with distributed IT organizations. Correlating this information in a single pane of glass further improves the efficiencies of IT staff, allowing them to perform these tasks without the need to specialize in and negotiate through proprietary monitoring tools.
Statistics allow you to determine where the backup and recovery infrastructure is oversubscribed and underutilized. Oversubscription results in extended backup windows and an unbalanced workload that affects the backup operation. The impacts to the backup and recovery process can be just as detrimental when infrastructure is underutilized. Striking an efficient balance between workloads and infrastructure capability/availability enables IT administrators to make sure that SLAs are achieved and to better plan for new workloads when they are brought online. With Data Protector Management Pack’s real-time monitoring of the backup and recovery environment, you can easily identify the bottlenecks associated with oversubscription and underutilization.

**Instant Diagnostics and Actionable Insight**

Monitoring the health and performance of the backup and recovery infrastructure is the first step in identifying what has happened. The next logical step is to identify how one issue may relate to the next. The diagnostic and actionable insight provided Data Protector Management Pack allows for the separation of cause and effect while uncovering often-unrelated dependencies that have an effect on the infrastructure.

Using graphical cues and visualization interfaces, Data Protector Management Pack delivers actionable insight by providing the tasks that can be used to address the issues uncovered in the diagnostic analysis. In real time, IT staff can quickly isolate issues and execute solutions that make use of Data Protector best practices. This degree of self-service greatly improves the IT organization’s ability to resolve issues before the end user experiences an issue related to the backup and recovery of their critical and operational data.

**Context-Sensitive Issue Isolation with Assistive Remediation**

Data Protector Management Pack is designed to isolate problems within the backup and recovery infrastructure to include the identification of relationships and dependencies.

Architected in this manner, IT administrators can rely on Data Protector Management Pack when performing root cause analysis during problem discovery efforts. It also provides context-sensitive assistive remediation in the form of linked tasks that can be executed from within Microsoft SCOM to resolve issues. Assistive remediation is available for each component of the data protection infrastructure, local or remote.

**Figure 4.** Active monitoring of critical and warning-level events to proactively identify potential problems

**Figure 5.** Drill-down reporting uncovers additional event details and recommendations

**Figure 6.** Correlation is not causation unless the tool provides granular-level issue isolation
Flexible Views with Qualitative Statistics
Because the backup and recovery infrastructure encompasses clients, backup servers, and devices, Data Protector Management Pack is capable of monitoring, analyzing, and reporting at every level of the data protection topology. This interactive monitoring tool allows IT administrators to drill as deeply into the dependencies and relationship as required to isolate and resolve issues. Data Protector Management Pack is delivered with ready-made views that can monitor backup device requests and operational states, client-level backup states, Data Protector server status (including internal components), and can also display the current infrastructure’s ability to meet Recovery Point Objectives based on ongoing backup and recovery operations.

Dynamic reporting of the backup and recovery infrastructure delivers levels of visualization to support decision making. When this capability is bound to intelligent trending, based on an operational analytics engine, IT administrators are able to understand the true capabilities of the infrastructure. Business leaders identify with and develop expectations based on assurances that their information is being protected and can be recovered when it is needed. Addressing the need for this level of detail is often manual, requiring the correlation of data from different management interfaces. With the Data Protector Management Pack, IT administrators can interrogate the backup and recovery infrastructure to determine and quantify the true Recovery Point Objectives that the backup and recovery infrastructure can deliver. This information is provided through the results of the analytics and qualitative statistics engine embedded within the management pack.

Beyond tailoring the user experience, IT administrators can create customized reports allowing them to choose how they want to visualize the information from the backup and recovery process. Custom reports can be built through the preset content definitions listed in the table below. Users simply select the type of report they need, based on a component of the backup infrastructure (logical or physical), and then define how it is to be presented.

Data Protector Management Pack Features

<table>
<thead>
<tr>
<th>Monitoring and reporting source</th>
<th>What’s monitored</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup server monitoring and reporting</td>
<td>Data Protector services and service states Data Protector license compliance monitoring Data Protector internal database consistency</td>
</tr>
</tbody>
</table>

Figure 7. Correlation is not causation unless the tool provides granular-level issue isolation

Figure 8. Reports specific to the Data Protector backup and recovery infrastructure

Figure 9. Uncover the infrastructures ability to meet Recovery Point Objectives
Manage and Control Backup and Recovery Operations

As IT infrastructure and workloads continue to shift, the need for the backup and recovery process to be equally agile is paramount to a successful data protection strategy. The benefits of centralizing the monitoring, analysis, and reporting of the data protection technology stack to include assistive issue remediation into Microsoft SCOM can be extended when you add in the ability to also control backup and recovery management operations.

Data Protector Management Pack helps IT administrators analyze the edge of the backup and recovery network to identify clients not being protected so they can add the client to the infrastructure by binding it to a backup target via a defined backup specification. Extending the management and control of the clients includes the ability to isolate problematic clients into a sandboxed state to prevent performance impacts while root cause analysis and issue remediation is performed. In addition, IT administrators can assess the clients’ current Data Protector Component installations to validate and compare version levels and make sure the clients are at consistent patch levels. Finally, as issues arise that may affect the backup operation, with Data Protector Management Pack, IT administrators can monitor current backup operations and, if interrupted, can manage the backup restart process from within the SCOM interface.

Extending the need to build a dynamically responsive backup and recovery architecture, Data Protector Management Pack provides administrative tools to enable the installation of the management pack agent as well as its removal when assets are retired. Reports can be executed to validate that the components of the backup and recovery infrastructure being monitored have the latest agent installed and can be started and stopped, as necessary. Finally, IT administrators have granular control over the agent polling/reporting intervals, as well as the level of alerting/debugging the agents generate and report on.

In addition to the real-time monitoring and analytics capabilities of the Data Protector Management Pack, IT administrators can also take advantage of the integration’s reporting features to determine the Recovery Point Objectives the infrastructure is currently achieving, and audit their Data Protector infrastructure to make certain they are properly licensed for their backup set sizes. Additionally, the IT administrator can use the Management Pack to perform backup-related actions such as mounting backup sets, discovering unmanaged Data Protector servers and deploying SCOM monitoring agents to them, and checking the health of the Data Protector environment on each deployed server.
About the Data Protection Suite

Data Protector Management Pack for Microsoft System Center Operations Manager is a companion product in the Data Protection Suite, an enterprise class, data centric backup and disaster recovery solution for hybrid IT. The Suite enables centralized protection of backup data across hybrid environments, from the core data center and remote offices to the private and public cloud, across modern and legacy platforms.

Learn More
To learn more about the features and capabilities of the Data Protection Suite, go to www.microfocus.com/dataprotector

Figure 12. Deal with backup and recovery infrastructure changes within Microsoft SCOM