bmc

TECHNICAL WHITE PAPER

Operations Management and AIOps: 7 Key Capabilities

Explore the technology that powers
BMC Helix Operations Management

Table of Contents

03 Executive summary

05 Key capability #1: Service-centric probable cause analysis

08 Key capability #2: Event noise reduction

10 Key capability #3: Anomaly detection

12 Key capability #4: Dynamic service modeling

13 Key capability #5: Real-Time incident correlation

15 Key capability #6: Major incident prediction

17 Key capability #7: Proactive problem management

Executive summary

Artificial intelligence for IT Operations, or AIOps, is a paradigm shift that allows machines to solve IT issues without requiring human assistance. It is a multi-layered technology that enhances the operations of IT by using machine learning and analytics to analyze big data sets obtained via different tools. This allows the solution to quickly detect and react to IT issues.

How can organizations benefit from AIOps? AIOps not only helps address complex IT challenges, it also helps you manage the exponential growth of data. AIOps automates the entire operations process across hybrid environments and builds an accurate inventory of CIs to be managed. It applies AI and machine learning to detect patterns and reduce noise, saving time, labor, and lowering MTTR.

BMC has taken AIOps even further by making it "open." BMC Helix AIOps can ingest data from other solutions, including those from third parties, to extend visibility across the organization and add context. According to Gartner, this combination of big data and machine learning helps organizations ingest and manage "the ever-increasing volume, variety and velocity of data generated by IT."

With open AIOps, you can improve IT Operations response times and reduce the time and money spent identifying and correcting IT issues. Let's take a closer look.

Powering digital transformation: How AIOps overcomes four critical challenges

Digital transformation is essential for competitive differentiation and growth. If companies aren't already introducing the new digital services and business models that consumers demand, they're working quickly to do so. This puts unprecedented pressure on IT to play a more strategic role in the organization -- and introduces significant challenges.

AIOps can solve many of the common issues experienced by IT teams as they navigate digital transformation and expand their strategic role. With an open AIOps approach, you can:

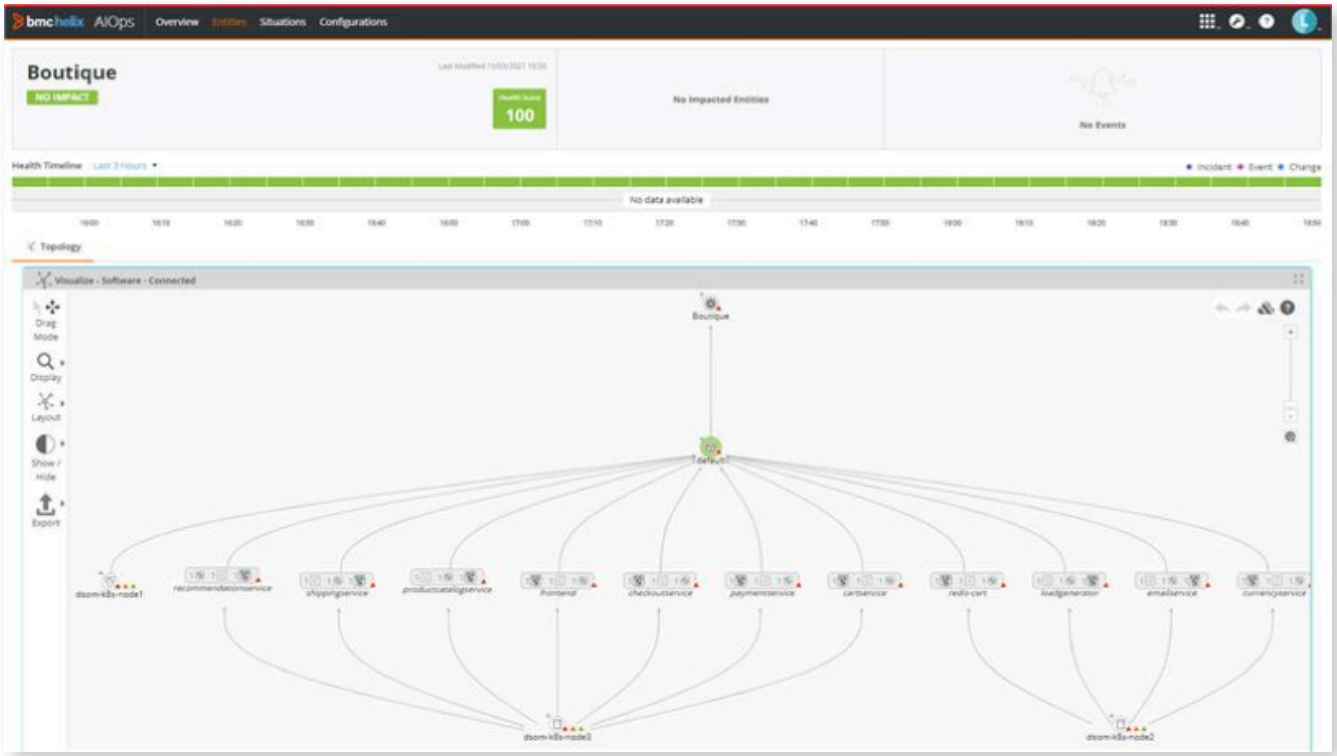
- **Break down data silos**
  For many organizations, the inability to manage large chunks of data is a key reason they haven't been able to monitor events and systems effectively in their environments. With AIOps, data is ingested in the form of logs, events, and metrics and taken through a set of algorithms that select specific data points. Once those data points are chosen, a correlation or set of patterns is identified and inferences are drawn, which pass into a collaborative work environment.
- **Eliminate IT operational noise**
  If you are a part of an IT Ops team, IT operational noise is a major concern. IT noise creates problems because it hides the source of a problem and increases MTTR, which causes higher operating costs, performance and availability issues, and risks to enterprise digital initiatives. AIOps-powered tools reduce event noise by correlating incidents and providing visibility to the true source(s) of the problem.
- **Deliver a seamless customer experience**
  Ensuring a seamless customer experience with predictive analytics is an important business objective. AIOps makes complex automated decisions by collecting and analyzing data. By leveraging this data, it can predict future events that may affect availability and performance and help ensure proactive problem solving.
- **Overcome monitoring and analytics challenges**
  Data collection is the primary step in enabling AIOps; you must collect and correlate data from multiple sources to effectively analyze it. AIOps and digital experience monitoring can deliver analytics and visibility across the domains underlying a service, reducing the need to use multiple monitoring tools.

An effective AIOps approach includes a number of capabilities necessary to maximize the use of this technology.

Key capability #1: Service-centric probable cause analysis

Service-centric probable cause analysis is a key differentiator for BMC Helix Operations Management. With it, Operations teams can view the top scored causal configuration items and related events for any impacted service to determine the most likely root cause(s) of a potential problem or issue. The analysis is extensive and factors in time, metrics, events, and topology. Operations teams can also view how the probability has changed over time and drill down into the details of the probable cause analysis.

- View the top scored causal CIs and related events for any impacted service.
- Determine probability based on time, metrics, events, and topology.
- Change the time window to view how the probability has adjusted over time.
- Drill down into full analysis details including events, metrics, and topology.



How It Works: Identifying Probable Cause with the PCA Algorithm

One of the ways that AIOps performs service-centric probable cause analysis is through the PCA (Probable Cause Analysis) algorithm.

The PCA algorithm is based on correlating data from service and operations management systems (like events, incidents, and change requests) across time, criticality, text, service model, and uses machine learning to determine probable causes of a situation where an IT service is affected.

The algorithm works in 3 phases:

1. **Collect.** First, it collects all the relevant data such as events, metrics, logs, incidents, and change requests across the topology in the dynamic service model. Change integration with ITSM is built into the solution.

2. **Rank.** Next, it runs a ranking algorithm that uses criticality, time proximity, graph depth, and cardinality factors to determine the causality rank order of nodes and events.

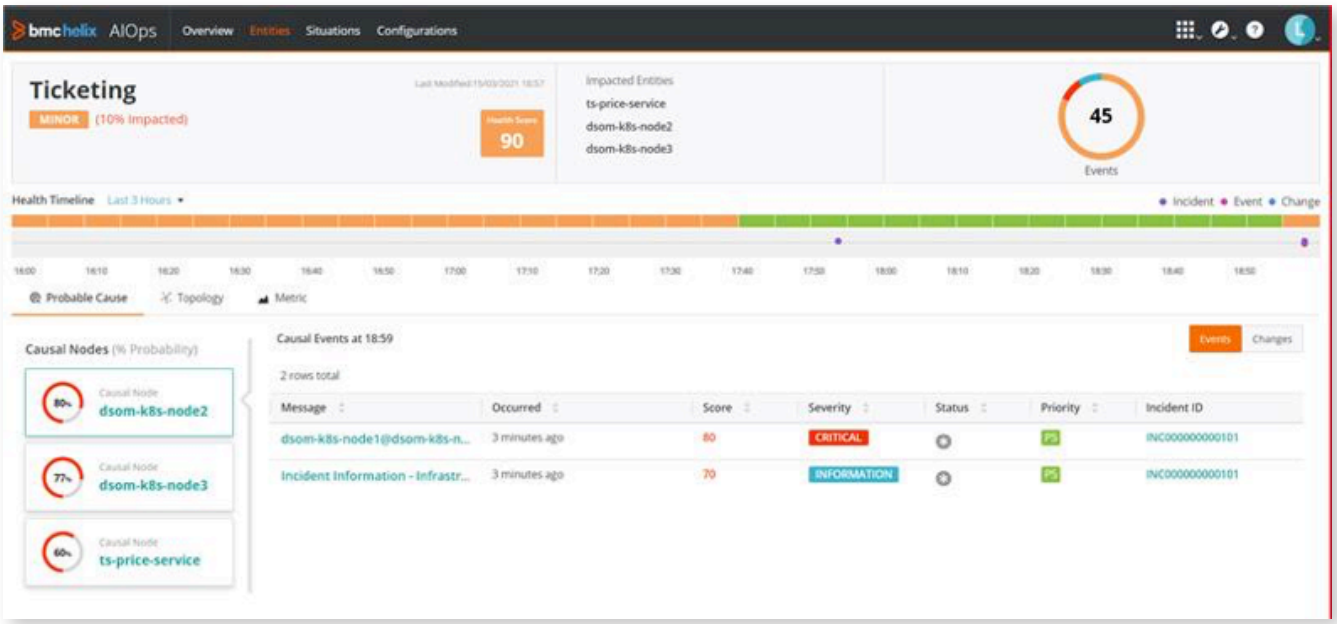
3. **Learn.** Finally, it uses machine learning and statistical models built based on feedback and historical causality analysis to classify nodes and events that are causal. This provides improved accuracy for both the probable causes and their statistical probability.

Each of these phases impacts how the system identifies an accurate probable cause.

Topology

The topology for a technical/application service clarifies the relationships between infrastructure, applications, and services. The correlation includes millions of data points that include topology, performance metrics, events, logs, and baselines. Nodes that are "deepest" or "lowest" in the graph of a service will usually have a higher causality than upstream nodes closer to the service mode. For example, database or network devices that are typically the deepest nodes in the service model would have a higher rank than the other dependent nodes above them.

The second aspect of topology is understanding the cardinality of relationships from each node, usually called centrality in graph theory. The higher the number of relationships from a node, the higher the probability that it is a causal node.



Ranking

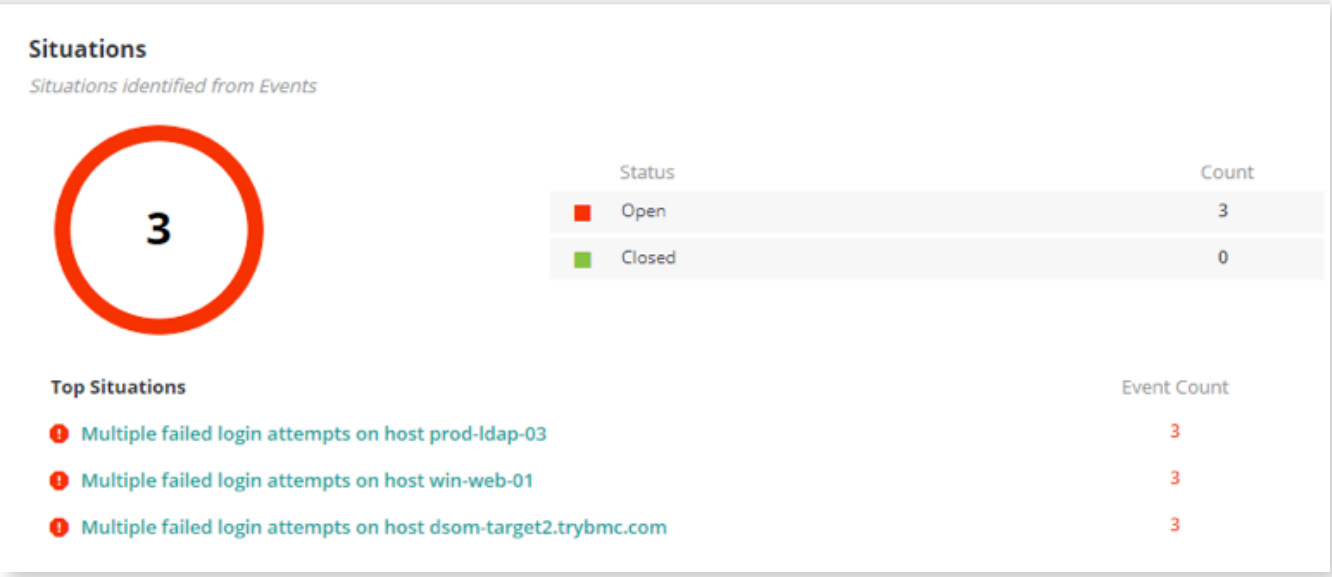
The ranking algorithm in BMC Helix AIOps takes a multi-dimensional factor approach that evaluates each node and event across factors such as time, priors, and graph parameters like depth and cardinality to get an accurate score. Usually, events and changes that are closer to the service degradation have a higher causality than events that happened several hours or days earlier. A weighted score based on numerous experiments accounts for these factors.

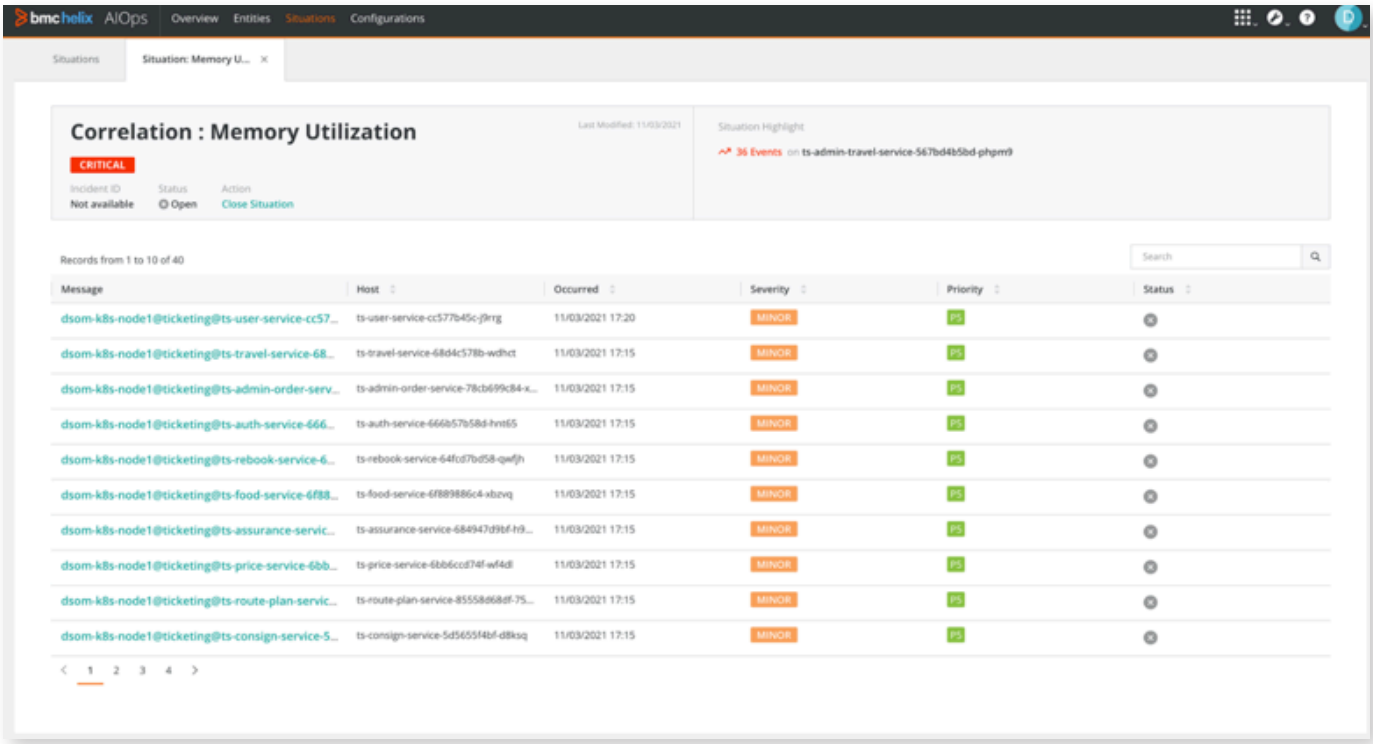
Feedback and historical cause analysis (future)

Using probabilistic methods on historic data, BMC Helix AIOps analyzes the past patterns of causality and outages for each node and identifies the "most causal" or "most failure prone" nodes. The feedback from the past event patterns is used as ground truth for training a classifier to determine whether a given event on a node is causal. Combining this with the ranking algorithm provides enhanced accuracy for identifying root causes.

Key capability #2: Event noise reduction

BMC Helix Operations Management relies on AI and machine learning to correlate and analyze events to reduce event noise, and provide visibility to the key issues that are creating an event storm. It uses automation to save time and labor, improve productivity, and help identify business-critical issues. BMC Helix Operations Management reduces costs by eliminating the need to analyze thousands of events and transforms large amounts of data into actionable information.





How It Works: The Situations Algorithm
BMC Helix AIOps uses machine learning algorithms to correlate events into meaningful situations based on patterns of textual similarity, time-based proximity, topology context, and multi-dimensional attribute level matching among events. For example, it can group events by service, topological proximity, temporal proximity, events co-occurrence, host and textual similarity in a situation. The events used for generating situations can originate from multiple sources, such as applications, networks, or infrastructure.

The algorithm works in 5 phases:

1. **Group.** As events are ingested, they are first combined into distinct groups based on "group by" fields. These "group by" fields can be a service field or any other categorical field. This allows users to have control over the scope of events to which the clustering algorithm will be applied and ensures that clusters stay within certain boundaries (e.g. only within same service).

2. **Embed.** Next, the system generates a vector representation of the event using advanced embedding techniques that can include text, TF-IDF, Google BERT or graph or contextual knowledge driven embedding techniques. Its uses offline methods to learn embeddings based on historical data.

3. **Search.** It compares the vector representation of the new event with the representations of the other events in situations to determine cluster membership. This step can result in new situations or evolving existing ones where a situation can continuously have new events added to it.

4. **Title generation.** The system generates meaningful titles for the clusters based on topic modeling algorithms.

5. **Situation lifecycle state management.** As events change state, or get added to a situation or time elapses, the state and severity of the situation changes along with it. For example, a situation will get closed when all events in the situation are closed. A situation can also close after a configurable period of time if no new events are added to the situations. Using both time and state of events influences the state and severity of a situation.

Key capability #3: Anomaly detection

With BMC Helix AIOps, you can proactively remediate issues before any service impact to meet SLAs, optimize customer experience, increase productivity, and reduce the number of incidents generated from events.

- Trigger events and notifications based on a group of metrics behaving abnormally.
- Trigger events and notifications based on a single metric behaving abnormally.
- Reduce event noise using sensitivity controls to manage the detection.
- Generate events with detailed graphs showing the anomalous metric or metrics.
- Use the Random Cut Forest (RCF) unsupervised algorithm to generate anomalies.

How It Works: The Anomaly Detection Algorithms

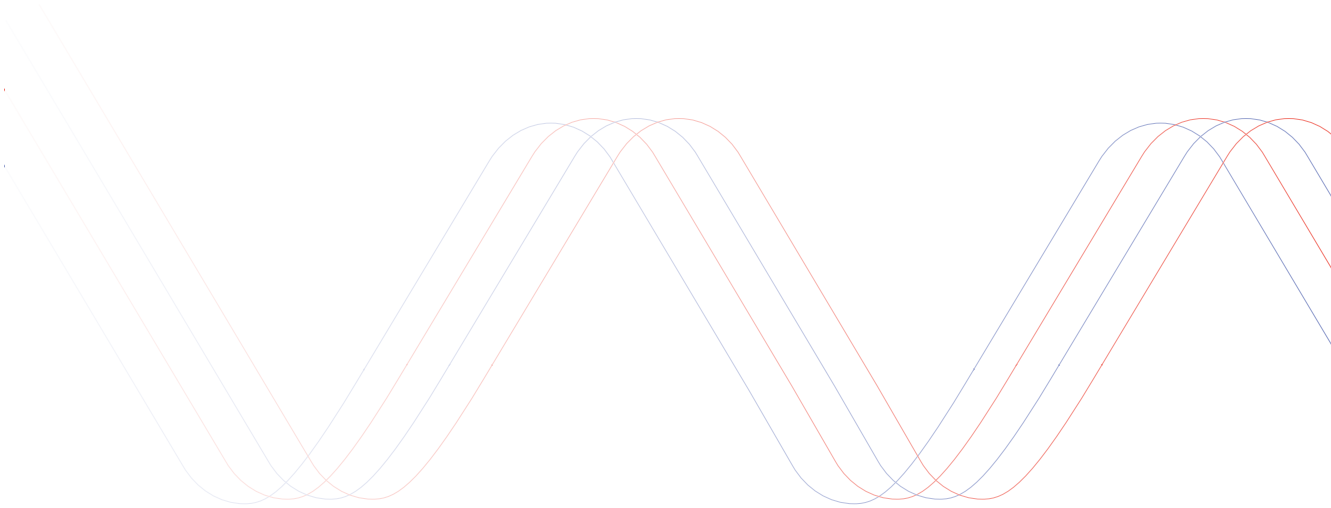
BMC Helix AIOps uses statistical and unsupervised machine learning algorithms to detect anomalies in time series. The anomaly detection first discovers patterns of "normal" behavior in the data to build a model and then uses that model to identify outliers – those data points that fall outside of what is normal.

The system leverages two different algorithms for anomaly detection. One is a highly efficient and scalable univariate anomaly detection algorithm for single metrics. The second is a robust multi-variate anomaly detection algorithm that builds a model for a group of related metrics. Multi-variate anomaly detectors are computationally more complex as they model a group of metrics, such as all key service metrics or entity metrics, but can also surface interesting interactions among different metrics.

Univariate metrics enable the system to learn the distribution of each seasonal time series for each hour time slot (e.g. Monday 9AM–10AM, 10AM–11AM, etc.) and use this to detect anomalies. When the current value of the metric is substantially in the tail of this distribution (such as > 99.5 percentile), then an anomaly is raised. This approach is better than simpler statistics such as mean or medians because the data distribution is captured for a time series and combined to produce anomalies that lie outside of the normal distribution of data. This approach can also scale better than others, as it uses unique digests for accurately estimating extreme quantiles with limited memory usage.

For multivariate metrics, AIOps allows defining systems of related metrics such as a KPI group and detects anomalies that capture the relationships and interactions among these metrics. It uses the Random Cut Forest anomaly detection algorithm to enable this capability.

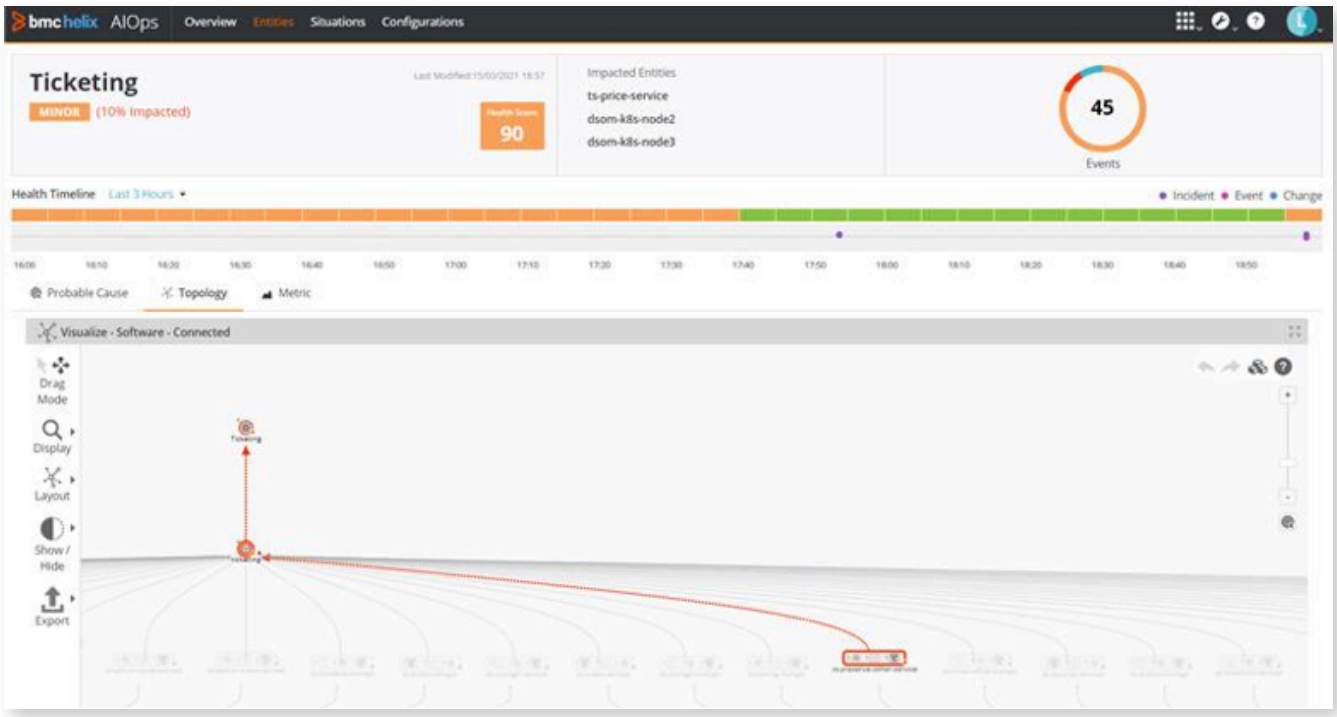
Finally, BMC Helix AIOps also has a set of rules that allows it to reduce false positives such as sustained anomaly detection.



Key capability #4: Dynamic service modeling

BMC Helix AIOps leverages a single dynamic service model across the BMC Helix Platform. This model is a unique datastore for assets and relationships. It allows 3rd party data ingestion and contains rich visualization, search, impact analysis as well as a rules-based engine to correlate, analyze, combine data into a unified topology view.

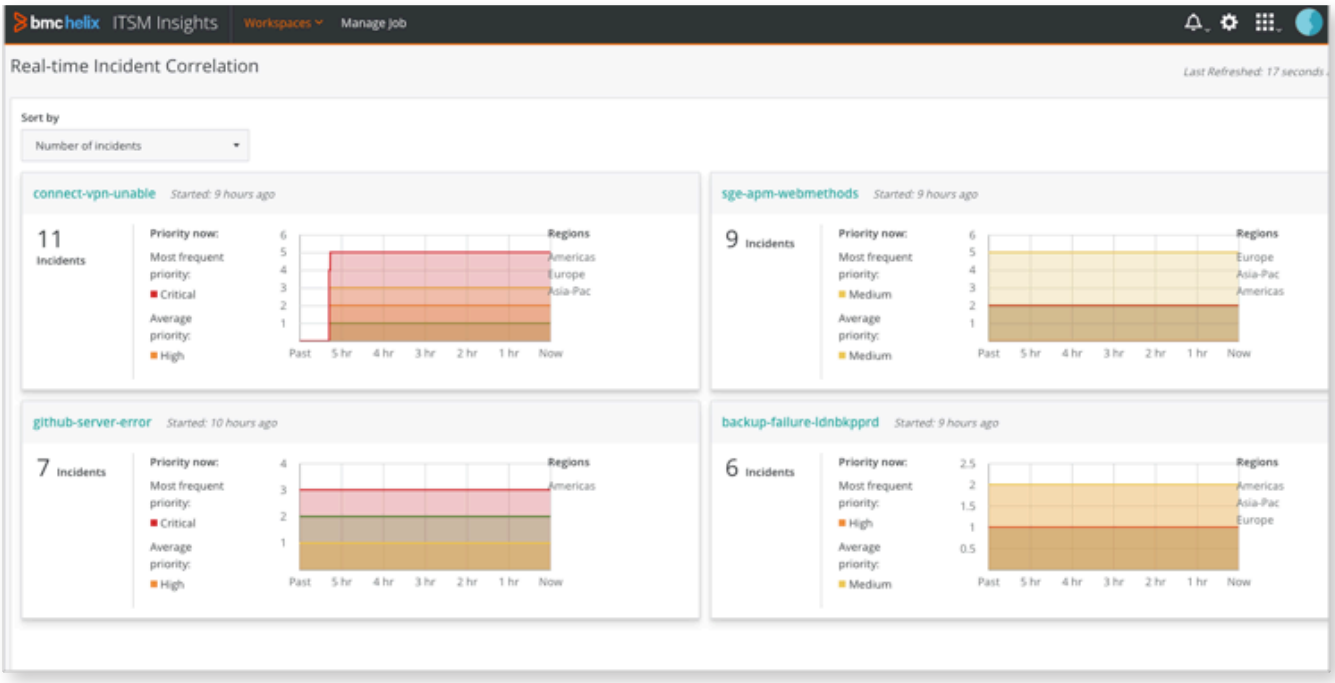
- Acts as a unique datastore across the BMC Helix Platform for assets and relationships
- Allows 3rd party data ingestion
- Streamlines dynamic service model updates and usage for ITSM and ITOM
- Provides rich visualization, search, and impact analysis
- Correlates, analyzes, and combines data into a unified topology view through a rules-based engine
- Supports creating business service models



Key capability #5: Real-Time incident correlation

In organizations with a large inflow of incidents to the service desk from multiple channels, major incident managers or service desk supervisors struggle to see the big picture. They often need to rely on "word of mouth" to detect if a set of incidents reflects the same (emerging) situation of an impacted IT service. It's also a significant effort to manage all incidents related to this situation.

Automatically identifying clusters of incoming incidents that are related to the same situation in real time helps major incident managers or service desk supervisors identify major incidents or other significant disruptions quickly, enabling them to rapidly reduce down time and negative customer impact. Incident correlation also reduces work for service desk agents by eliminating duplicate incidents. This frees up resources for higher value work like swarming on major incidents.



How It Works: Real-time Incident Correlation Algorithm

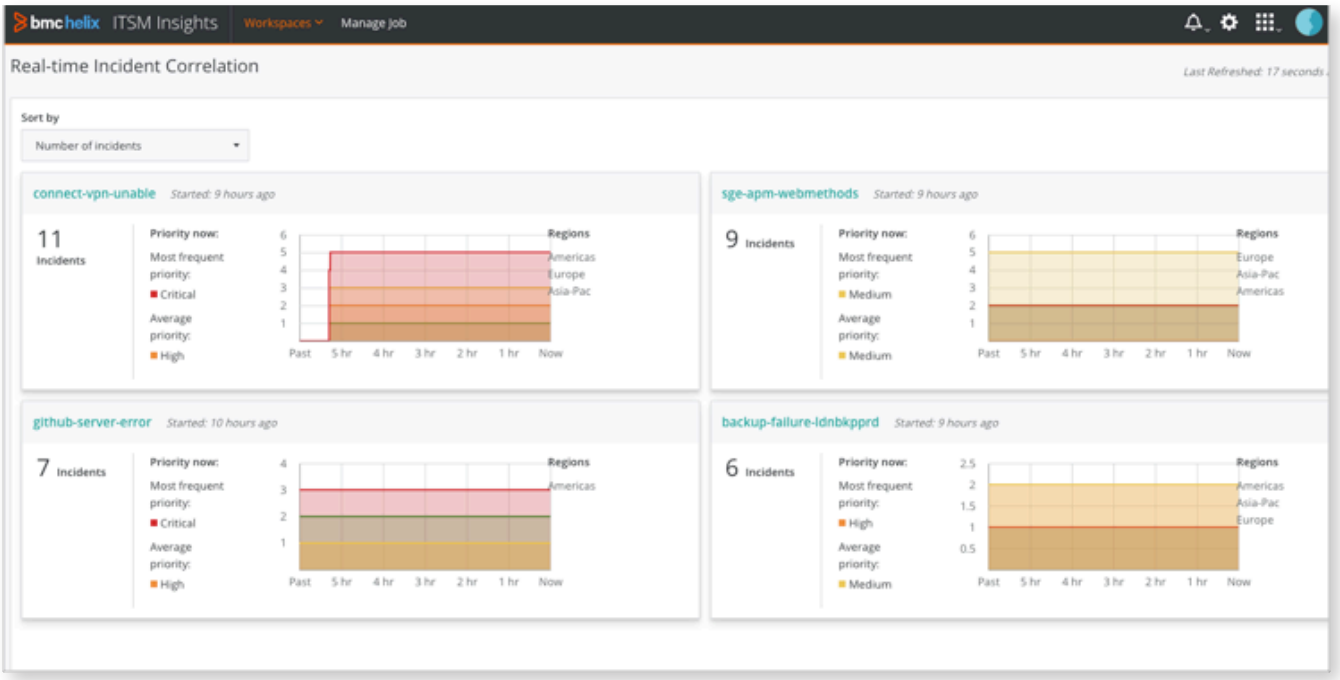
BMC Helix AIOps uses machine learning algorithms to group incidents together based on semantic similarity of incidents and generate a meaningful caption. If you have two incidents with similar texts -- "I cannot connect to Teams" and "Fail to connect with Teams" for example -- they will be clustered together into a group/cluster because the intent of these two incidents is the same. If you have configured the proactive service resolution (PSR) feature to create incidents from events in AIOps, then you can also see event-based clusters.

The algorithm works in 5 phases:

1. **Group.** As incidents are created, they are combined first into distinct groups based on "group by" fields. These "group by" fields can be service field or any other categorical field. This allows users to have control over the scope of incidents to which the clustering algorithm will be applied, ensuring clusters stay within certain boundaries (e.g. only within same service).
2. **Embed.** Next, AIOps generates a semantic representation of the incident using advanced NLP models such as Google BERT. These vector representations capture the meaning of text in the incident.
3. **Search.** The system compares the vector representation of the new incident with the representations of the other incidents using cosine similarity and kNN search. If it has a high match, then it adds to an existing cluster. If not, it creates a new one.
4. **Title generation.** AIOps generates meaningful titles for the clusters based on topic modeling algorithms.
5. **Lifecycle state management.** The system manages the lifecycle of the clusters based on recently added incidents such as which clusters should be closed.

Key capability #6: Major incident prediction

With BMC Helix AIOps, you can predict major incidents by analyzing multiple parameters, including events, metrics, incidents, and change requests.



How It Works: Predicting Major Incidents Algorithm

BMC Helix AIOps predicts major incidents for a technical/business service using deep learning and statistical models. The algorithm works on finding leading indicators that can correlate well with an impending service degradation, outage, or major incident. The models look for these correlations to predict major incidents by using combined data from monitoring and service management solutions.

The algorithm has offline and online phases.

Offline training phase:

1. The system uses 3–12 months of historical data for metrics and events for each service and looks for patterns that indicate a strong correlation between past data and future major incidents. Deep learning models such as LSTM are trained and evaluated for their precision/recall to determine whether these models can be used for prediction. If they have high accuracy, they will be deployed for online inference.
2. Short-term forecasting models are built for selected time series data. Algorithms for forecasting may include simple regression to more complex models. These may include Holt-Winters; Box-Jenkins (a.k.a. SARIMA with automatic trend regression and prediction); linear (ordinary and robust); polynomial trend with seasonal component; multiplicative exponential trend with seasonal component; and exponential damping.

Online inference phase:

1. As real-time data flows in, the deep learning models, real-time incident correlation, and forecasting models are evaluated to generate leading indicator scores from each model.

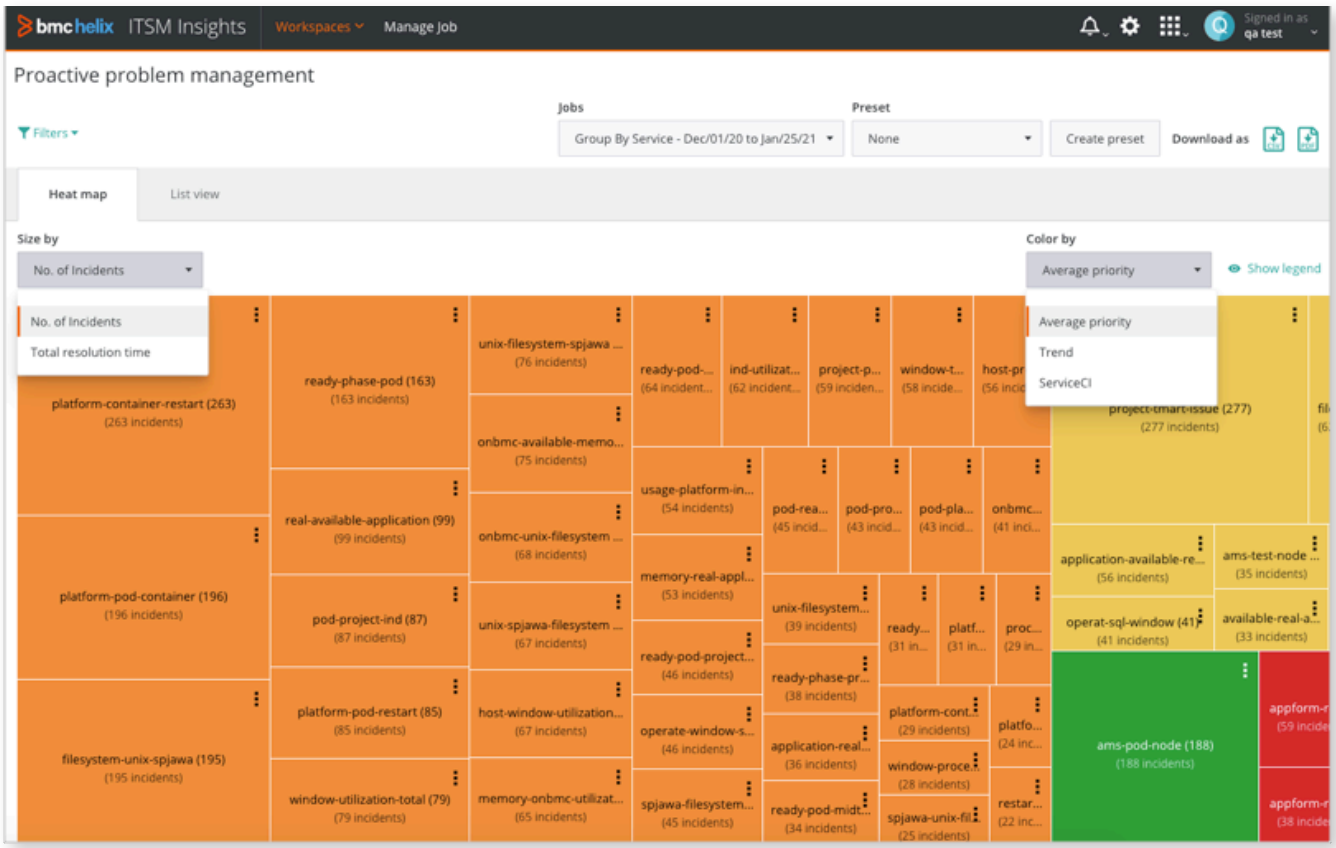
2. Using an ensemble of these leading indicator scores, a major incident is predicted. If a major incident was already predicted for this service in the previous evaluation period, then the state of the service is updated with the new prediction.

Key capability #7: Proactive problem management

Problem investigations are expensive. Between incident analysis, the investigation itself, and remediation, costs add up. Even with the help of reports, large sets of incidents have to be manually reviewed once or twice per week because key info is in free text fields.

Due to these costs, organizations can often only conduct problem investigations for a few, most impactful sets of recurring incidents. It's therefore critical to correctly identify which sets of incidents are most impactful (i.e. which ones generate the most work for the service desk). In large sets of incidents with lots of free text descriptions, this is a difficult exercise.

BMC Helix AIOps allows you to automate the identification of recurring incidents and problem investigation recommendations to improve efficiency.



How It Works: Proactive Problem Management Algorithm

The clustering algorithm is applied to resolved and closed incidents to identify interesting clusters which are candidates for "problem investigations."

The algorithm has 5 phases:

1. **Data pipeline.** A data pipeline is driven by job configuration that specifies a lookback period of historic incident data to use for the clustering algorithm, number of clusters (k), and fields. During the job execution, incident data is extracted from ITSM and processed through a data pipeline where tokenization, cleaning, stemming, lemmatization, stop-word removal and vectorization takes place. The vectorization can be done by TF-IDF or by Google BERT or other language models.
2. **Clustering algorithm.** Next, a machine learning clustering algorithm (k-means) is used to group the incident data into clusters that group most similar incidents together using distance-based metrics.
3. **Cluster quality evaluation.** The system evaluates the cluster quality using industry standard benchmarks for cohesiveness such as Silhouette score. If cluster quality is not acceptable, it automatically fine tunes parameters (Auto ML) to get better quality clusters.
4. **Optimal k.** An optimal k algorithm is run that finds the optimal k to optimize the cluster quality.
5. **Title generation.** Each cluster of incidents is given a caption based on topic modeling algorithms.

AIOps for today's complex hybrid environments

To succeed in today's competitive environment, IT Operations teams must adopt a holistic operations management strategy driven by intelligence and AI/ML across their entire hybrid IT environment. This includes building monitoring into digital and cloud transformation processes to eliminate visibility and control gaps.

Deploying an AIOps strategy empowers IT Ops to manage the increasing volume, variety and velocity of data, which has grown beyond human scale across an increasingly complex and fast-moving IT landscape. Machine learning and analytics are also key in cloud-native technology environments that comprise many more components than traditional apps, like microservices and containers, and emit much larger volumes of operational data.

At the same time, IT Ops needs a solution that is flexible, easy to deploy and upgrade, and supports fast value realization to meet the constantly changing needs of a quickly moving organization. These requirements make a SaaS deployment model ideal for rapid onboarding and cost optimization across any environment.

The solution? BMC Helix Operations Management for full, end-to-end operations and systems management. BMC Helix Operations Management is a SaaS-based solution based on a microservices, containerized architecture that provides fast deployment and scalability in an easy-to-use environment. It contains all the key capabilities detailed in this white paper alongside continued innovation that ensures it can always meet your needs and solve your challenges.

Accelerate digital transformation and harness the power of AIOps from BMC.

For more information
To learn more about BMC Operations Management with Open AIOps please visit **bmc.com/operations-management**

About BMC
BMC works with 86% of the Forbes Global 50 and customers and partners around the world to create their future. With our history of innovation, industry-leading automation, operations, and service management solutions, combined with unmatched flexibility, we help organizations free up time and space to become an Autonomous Digital Enterprise that conquers the opportunities ahead.

www.bmc.com

529058