You have the tools but not the insights

A Guide to Data Consolidation for Modern IT Operations Leaders

StackState
a Xebia Group Company

You have the tools but not the insights

A Guide to Data Consolidation For Modern IT Operations Leaders

Table of contents

StackState
a Xebia Group Company

1. Introduction

IT infrastructure is evolving at a breakneck pace. With the advent of virtual infrastructure and the self-service model, IT personnel can now provision resources as needed and the number of components to manage has exploded. What's more, new technologies seem to appear every day.

Over the years, organizations have done their best to adapt to each new technology generation, adopting the tools they needed to deal with its challenges. Research shows that 65 percent of larger enterprises have more than ten monitoring tools in place (source: *Enterprise Management Associates*). However, the myriad of tools in place fragments the landscape and often obstructs the big picture. When there is an issue or outage, finding the cause is like searching for a needle in a haystack. As an IT organization leader, you need a better approach. This whitepaper addresses that challenge and breaks down the solution: data consolidation.

2. The Challenge and the Solution

2.1 The challenge

The era of digital transformation has lead to paradigm shift. IT infrastructures have become continuously improving dynamic environments, with software as the significant driver for growing and competing in business.

Current monitoring and management systems are not equipped to handle today's complex, scalable and dynamic environments and the volumes of data they generate. Too much work is left to be done manually and the tools used only address specific aspects, such as applications, infrastructure or networks.

This fragmented monitoring approach limits the IT operation's ability to detect, diagnose and address performance issues and predict potential impact on other parts of an organization. Aligning metrics and closing the gap between IT and business needs and goals also remains a challenge.

2.2 The Solution

Imagine a puzzle contains an image of a code that will unlock a vault of gold. Each person across your IT organization has one piece. To solve the puzzle, you need to bring everyone into the same room to put their pieces together so you can read the code and open the vault.

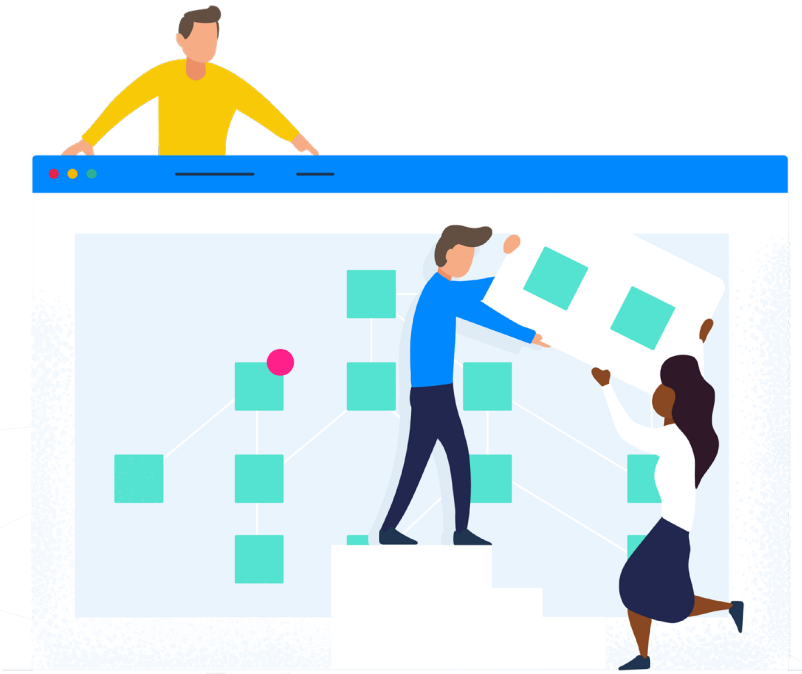
Your IT landscape is like a puzzle, and you should be able to open the vault instantly to solve or predict issues, drive business growth and achieve your goals. However, modern IT landscapes are too complex and dynamic to put the pieces together manually. It just takes too much time and effort.

The solution is to bring together all your data into one platform. On the next page, we'll discuss the benefits of data consolidation. Followed by a real-life example.

2.3 Consolidating Your Toolchain

Data containing chunks of valuable information is spread across your IT tools. To understand it, you need to bring it all together, from business applications to hardware, from legacy to microservice, and from on-premise to cloud.

In a recent report from Gartner, data consolidation is mentioned as a critical strategy for gaining more profound insights across teams and tools. (Source: *Gartner, 2018 Strategic Roadmap for IT Operations Monitoring*).



2.4 The Benefits of Data Consolidation

There are four main benefits to consolidating your data.

1. Pinpoint Issues Faster

Consolidating your data into a single platform allows you to view your IT landscape from a holistic perspective. When issues arise, you don't have to correlate data from different sources manually, which reduces your Mean Time to Discover (MTTD) and Mean Time to Remediate (MTTR) dramatically.

2. Efficient Use of Resources

With visibility across teams and tools, you can quickly uncover the root cause and discover the impact issue for different teams, making it much easier to notify the right people, at the right time, for the right problem. That means you can save time and money by having only the team working that is directly relevant for the problem to be solved.

3. Cross-Domain Visibility

No matter the cloud, application or infrastructure, consolidating your toolchain allows you to view your entire dynamic IT landscape with zero blind spots and connect to every single component.

4. Utilizing Current IT Investments

You've already invested time, money and knowledge in your current tools. Consolidating your entire toolchain into one place will truly unlock the power of your existing IT investments.

2.5 A Real-Life Scenario

There are many reasons why it's important to consolidate your IT operations toolchain. Here's one example, from a real-life scenario in a large ecommerce organization that suffers from data silos.

The problem

Each team has its perspective on the problem, but nobody understands the bigger picture. In this case, the lack of visibility across silos forced different teams from different departments to look into the issue resulting in two hours of downtime, unhappy customers and loss of revenue. The puzzle was solved way too slowly, with too many people.

Thursday - 10:00 pm - The Infrastructure team rolls out a new deployment with Kubernetes. The update was successful, but wasn't announced across teams.

Friday - 8:00 am - The Order Management team started reporting problems. They detect a higher than average error rate. Thanks to Prometheus, they see the error is related to the Payment Service team.

8:15 am - The Payment Service team starts an investigation. With their monitoring tool CloudWatch, they see the time-out but don't know why it happened.

9:15 am - A crisis team is formed with people from different teams.

9:30 am - The crisis team relates the update from last night to the problem.

10:00 am - Infrastructure team rolls back the deployment. Everything works fine again.

3. When Are You Ready to Consolidate Your Data?

Before you consider consolidation, you need to know the maturity of your IT monitoring. The following examples can help you identify if your are ready to consolidate.

You are not ready:
The majority of your monitoring is manual or not at all. IT teams spend much of their time processing the flood of alerts. Each component across the environment is monitored with tools like e.g. Nagios. Monitoring solutions at this level only report if a component is up or down.

If this sound familiar to you there's no need to start consolidating your IT operations tools.

You are ready:
You are using several solutions to monitor your systems from different perspectives. For example, one team is using Elasticsearch and Fluentd to analyze log files, while another team prefers Zabbix and CloudWatch to monitor their cloud and on-premise infrastructure. Meanwhile, the Microsoft DevOps team is using Microsoft Application Insights for application monitoring.

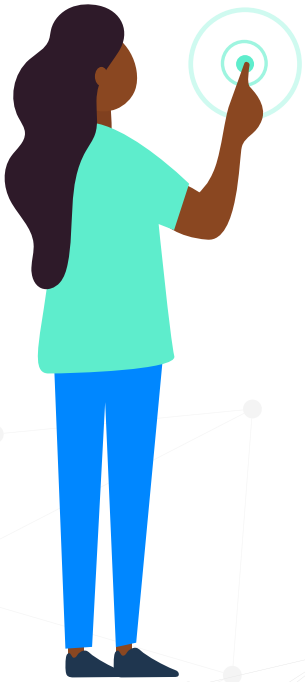
Collecting different types of data with different kinds of tools is essential, but comes with a price. When issues arise, multiple teams need to jump from tool to tool to identify root causes, then manually correlate data to understand the issue. Technological and organizational boundaries further complicate the process. Everyone has their perspective, but nobody understands the bigger picture or how his or her part of the IT landscape relates to other parts.

If these challenges sound familiar to you, then you're ready to consolidate your IT operations toolchain. We'll explain different scenarios for consolidating your IT Operations data and toolchain on the next page.

StackState

4. Different Starting Scenario's

For guidance on how to start consolidating your data, let's look at three scenarios executed by IT enterprises around the world.



4.1 Time-series database

Consolidate all your metrics and events into a time series database (TSDB). A TSDB is a solution that is optimized for time-stamped data such as server events, metrics, network data and application performance monitoring. Time-series databases are great for consolidating purposes but aren't suited for correlation purposes.

+ Metrics and events consolidated and available in one tool
+ Ask questions to your data over time
+ Open-source tooling available

– High total cost of ownership
– Doesn't capture relationships across systems
– Reactive monitoring, no automated correlations

4.2 Log Aggregators

Implement a log aggregator. A log is critical to know what is happening in your IT landscape and what your system is doing. Many enterprises consolidate their application, infrastructure, system and security logs in logs stores. Implementing a log aggregation solution allows your teams to unify their log data into a single place and gain a better understanding of your data.

+ All your different logs available into one location
+ Query the log store for easy troubleshooting
+ Open-source tooling available

– Storing and copying logs can get expensive
– Log stores are not designed to store metrics and relationships over time
– High total cost of ownership

4.3 AIOps Platform

Artificial intelligence for IT operations, or AIOps, is a platform specifically designed to consolidate data and tools to allow shared understanding and insight across teams and tools.

According to Gartner, existing monitoring tools are stressed when dealing with high volume, variety and velocity of data. More importantly, monitoring tools do not cut across the multiple data types required for extracting useful insights. This fragmented monitoring approach limits IT Operation's ability to detect, diagnose and address performance issues and predict potential impact on other critical parts of an organization. (Source: *Gartner, Market Guide for AIOps Platforms 2018*).

Gartner also writes, "domain-centric monitoring tools will continue to exist, providing data capture, analysis, and visualization for the specialist. However, they will forward their data streams to an AIOps platform, acting as a lens where the data will be focused into a single, coherent, cross-domain analysis." (Source: *Gartner, Market Guide for AIOps Platforms 2018*).

AIOps solutions are able to discover and monitor business performance, application performance, infrastructure, containers, microservices, and cloud – all in one place. In addition to this, its open character allows you to ingest different types of data such as metrics, events, logs, traces, deployments, and tickets.

+ Different types of data in one place ensures zero blind spots
+ Get cross-domain analysis
+ Get to root cause faster and reduce your MTTD and MTTR
+ Increase team efficiency
+ Understand dependencies and relationships across services, systems and teams

– Breaking down silos introduces a new way of working and transparency

4.3.1 The 4T Data Model®

To deliver comprehensive insight into past and present states of IT systems, you'll need an AIOps platform that is capable of ingesting and providing access to a broad range of data types. Processing historical and streaming data types demands a highly dynamic database.

As an example, let's take a closer look at StackState's 4T Data Model® powered by a versioned graph database, which consists of Topology, Telemetry and Tracing data and all incremental changes over Time.

Topology

For the data to be relevant and actionable, a context must be placed around the data ingested. That context is topology. Topologies in StackState are automatically updated by topology data coming from different sources. Each of these sources defines one or multiple subgraphs of the stack's topology. These topological subgraphs are automatically merged, mapped and pushed to StackState's interface.

Telemetry

StackState is able to ingest telemetry data (metrics, events and logs) from external IT systems such as monitoring, provisioning, deployment and configuration management tools or StackState's own agent.

Tracing

Tracing provides end-to-end insight in your entire IT landscape at code level. StackState Tracing capability supports all major languages, has full support for distributed traces and integrates cloud tracing technologies such as Amazon X-Ray and Azure Monitor.

Time

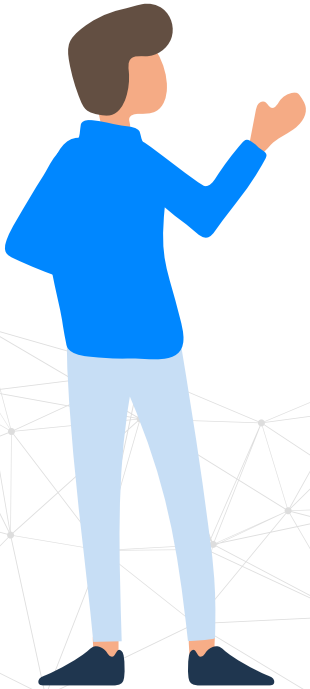
Problems in IT stacks can usually be traced back to changes. Having a change log of everything in your IT landscape is vital. To record these changes, StackState built StackGraph, a versioned graph database. StackGraph allows StackState to go back to any moment in time and to see exactly what your landscape looked like at that moment, across all data ingested.

All-in-one data model

Merging Topology, Telemetry, Tracing and Time are a way to model the configuration of what is going on in any IT system; large or small, based on microservices, containers, web services, monoliths, serverless, cloud or on-premise. It doesn't matter.

The 4T Data Model® delivers insight into the entire IT landscape by capturing every millisecond of change, from any source in real time.

5. Summary



According to Gartner, existing monitoring tools are stressed when dealing with high volume, variety and velocity of data. More importantly, monitoring tools do not cut across the multiple data types required for extracting useful insights. This fragmented monitoring approach limits IT Operation's ability to detect, diagnose and address performance issues and predict potential impact on other critical parts of an organization.

Consolidating your IT operations toolchain solves this problem and brings together information, insights, and capabilities that were previously locked into silos. There are several scenarios to consider when consolidating your IT operations toolchain:

Log aggregators: Bringing all your logs from different systems into one place allows you to troubleshoot better, but you're still relying on one data source. Log aggregators are not able to capture other types of data and thus lack the power to break down silos.

Time-series databases: This scenario allows you to consolidate events and metrics. It's a scalable solution that's great for real-time analysis, but it requires much domain-knowledge and is hard to maintain.

AIOps platform: AIOps integrates with any tool and dataset, bringing together information, insights, and capabilities that were previously locked in disconnected silos. This creates shared visibility across all tools and teams.

Any of these scenarios can be a starting point, but the most effective approach – one that StackState considers to be a best practice – is to start consolidating your IT operations toolchain with an AIOps platform. Enterprises should make a strategic investment in consolidation to realize the maximum value of current IT investments.

See how AIOps can help
your enterprise.

Try AIOps at Stackstate.com