Brought to you by

servicenow

AIOps & Visibility

for dummies®

A Wiley Brand

ServiceNow Special Edition

Address today's IT complexity

Drive operational efficiencies and IT productivity

Significantly reduce time to repair

Tony Branton

Ted Coombs

About ServiceNow

ServiceNow makes work, work better for people. Our cloud-based platform and products streamline and simplify how work gets done. We deliver digital experiences that help people do their best work fast, creating great employee and customer experiences. ServiceNow (NYSE: NOW) works for you. To learn more, visit **servicenow.com**.

AIOps & Visibility

ServiceNow Special Edition

by Tony Branton and Ted Coombs

for dummies®
A Wiley Brand

AIOps & Visibility For Dummies®, ServiceNow Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN: 978-1-119-65681-4 (pbk); ISBN: 978-1-119-65683-8 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Editor: Carrie Burchfield-Leighton

Editorial Manager: Rev Mengle

Business Development Representative: Karen Hattan

Production Editor: Tamilmani Varadharaj

Special Help: Hakan Işık and Lisa Wolfe, writing and graphics contributors; Gerard Berthet, editing contributor

Table of Contents

Introduction

Artificial Intelligence for IT Operations (AIOps) is the use of artificial intelligence (AI) to manage the digital complexity of modern organizations. Modern IT complexity comes from

- Data volume, variety, and speed of ingestion
- Cloud and on-premises architectures
- Virtualized and cloud-native applications
- Containers and serverless computing

This complexity is further compounded because of siloed monitoring tools and the never-ending stream of events being directed at the operations teams in different formats.

AIOps represents a set of capabilities that helps you sort through this complexity, automate the analysis of symptoms, and expedite the decision-making process to remediate a problem in your infrastructure, applications, and services. AIOps can suggest certain tasks to automate by learning patterns from past remediation actions, further improving your operations team's effectiveness. AIOps becomes the necessary helper working for you in the background.

AIOps lets you remain in control of your operations, regardless of complexity. Using AIOps directly translates into customer satisfaction and increased revenue.

About This Book

This book gives you the basics of AI and how it has become an essential part of managing the complex challenges that face most IT departments. *AIOps & Visibility For Dummies*, ServiceNow Special Edition, shows you how using a Configuration Management Database (CMDB) is essential to managing your entire IT ecosystem in today's modern enterprise. A CMDB brings visibility to how your IT infrastructure supports business, making it a game changer.

In this book, you find out the challenges AIOps helps you overcome and learn some of the strategies for a successful implementation

of an AIOps platform in your organization. Discover how the tools you already use can lead to better insights and enhance IT Operations. Finally, find out more about ServiceNow, a thought leader and provider of AIOps capabilities dedicated to the success of your business through the application of AIOps.

Icons Used in This Book

Throughout this book, you find special icons that call attention to important information. Those icons are as follows:


TIP

The Tip icon gives you suggestions for successfully implementing AIOps.


REMEMBER

Information here highlights tidbits you should remember for future reference.


WARNING

Be aware of the information here that may be costly, cause headaches, or give you a reason to pause in your pursuits.

Beyond the Book

This book helps you discover more about AIOps, but you can find more resources beyond what this book offers at

- bit.ly/2rW8zn1**:** Deliver high-performance business services with visibility and AIOps.
- bit.ly/2Mw0sFd**:** Download a copy of *Configuration Management & CMDB For Dummies,* ServiceNow Special Edition.
- bit.ly/3604iOc**:** Discover how a healthy CMDB helps you deliver great business service quality.
- bit.ly/2Yc6waC**:** Learn how a healthy CMDB helps you deliver great service quality.
- bit.ly/34REMdT: Take five steps to successfully deploying a healthy CMDB.

IN THIS CHAPTER

- Looking at the challenges facing IT operations
- Overcoming problems of traditional approaches with AIOps
- Assessing AIOps outcomes

Chapter 1
Making the Case for AIOps

In an era of disruptions of various kinds, the enterprises need to be able to move faster than ever if they want to come out ahead. Luckily, through their journey, they have a secret best friend who can help them with potential challenges they may face both in terms of keeping the lights on and innovating for tomorrow: "Their IT."

IT, as the intelligence engine of business, can help the enterprises answer their questions and take decisions and actions much faster. While keeping up that critical duty, IT also needs to overcome its own challenges and deal with an ever-increasing complexity both in terms of components to manage and data to process and interpret.

In this chapter, we discuss the main challenges modern IT organizations face and how they can leverage frameworks like AIOps to achieve desired visibility and agility through automation.

Looking at the Challenges Facing IT Operations

IT Operations today can be summed up in two words: complex and decentralized. Whether this means virtual servers spinning up and down, or containers sharing operating systems and providing microservices, or just the general exponential increase in IT complexity brought about by mobile devices, Internet of Things (IoT), cloud storage, Software as a Service (SaaS), Platform as a Service (PaaS), and more, it boils down to one thing — the ability to manage this complexity, shown in Figure 1-1, requires a technology capable of handling this level of complexity.

Enter AIOps.

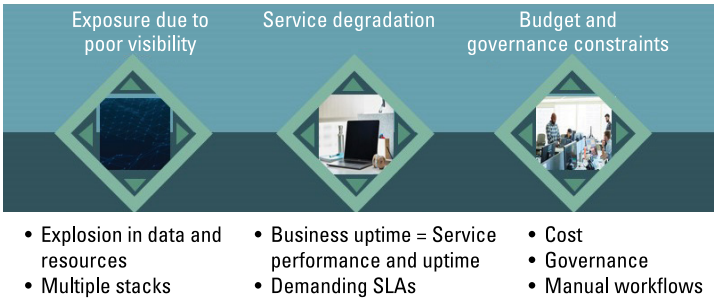

FIGURE 1-1: The complexity of modern IT can be overwhelming.

This complexity didn't just happen one day. It has developed over years. The tools that monitor these applications, network services, and storage environments have also increased over time leading to an overwhelming number of siloed monitoring tools generating events in different formats, often for the same issue. It isn't unusual to find companies having at least 20 to 30 distinct monitoring tools.

To deal with the ever-increasing complexity, IT has invested more money and people into operations teams and increased infrastructure resources. This approach hasn't been able to keep up with the rate of change occurring in today's complicated and

DevOps-driven digital world. Adding more resources has only increased organizational and operational complexity at a time when complexity needs to be reduced and operations streamlined.

The complexity is further compounded by

- A lack of visibility and insight into the IT environment due to siloed data sources and processes
- Inefficiency due to lack of automation
- A lack of business context due to a disconnect between IT resources and how they map to and support business services

Don't forget about customer and employee experience — the top priority driving digital transformation today. Customers and employees expect enterprise IT to be highly responsive, available, and as easy to use as their consumer devices. They don't have the patience to wait on slow or interrupted applications in their personal or work lives.

Overcoming the Problems of Traditional Approaches with AIOps

IT teams have traditionally been buried in unplanned work reactively addressing service degradations and priority 1 (P1) outages with manual processes and siloed tools. Determining the cause of an outage can take hours, and it can take even longer to identify impacted services and remediate issues.

Traditional IT tools have been siloed, making IT slow and unresponsive (see Figure 1-2). For example, think about a service outage when there are separate IT Service Management (ITSM) and IT Operations systems that don't share data. This situation can cause significant delays at the worst possible time. When it comes to fixing the outage, critical information such as alerts, service topologies, and previous incidents and changes are spread over two systems or more, making it even harder to quickly restore service.

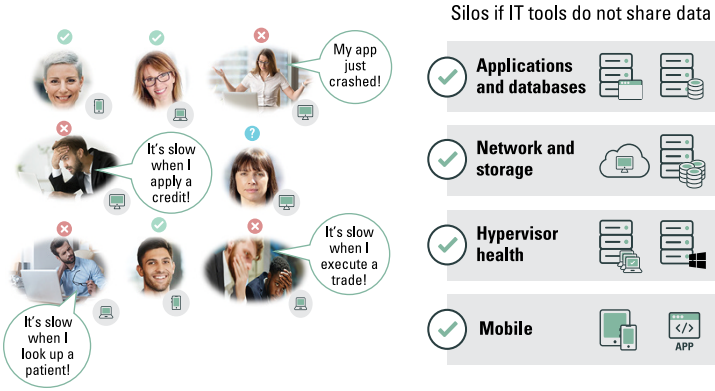

FIGURE 1-2: Challenges exist in companies using manual processes and siloed tools.

WARNING

To increase speed and alleviate traditional IT shortcomings, employees are simply bypassing IT altogether and managing their own services by grabbing cloud resources. Grabbing cloud resources increases the speed that business units and development teams require today, but this strategy creates additional problems for IT and impedes its ability to quickly pinpoint and fix issues. In addition to the difficulties in diagnosing problems, out-of-control costs can arise when cloud resources are not managed effectively.

Achieving accurate service visibility

IT has also been challenged with being able to see the relationships between infrastructure and the services provided to the business. When problems strike, IT struggles to understand how the problem impacts the business, determining whether a single service or multiple services are affected, if the issue is in an on-premises data center or in the cloud, and what changes may have been made before the problem occurred.

To determine the impact of an IT problem or service degradation, one of the solutions has been to create maps of IT infrastructure to the related services. These service maps provide the visibility needed to understand the impact of change and infrastructure on services. However, these maps are often manually created, quickly out of date, prone to error, and costly.

But, maintaining the accuracy of service maps is possible through automation. By using special software, IT infrastructure and its individual components can be automatically discovered and documented as configuration items (CIs) and stored in a Configuration Management Database (CMDB). See Chapter 5 for more info on a CMDB.

For example, it isn't unusual for ServiceNow customers to discover hundreds of thousands to millions of CIs across hundreds of services. Figure 1-3 shows the ServiceNow CMDB, where common data that's required for digitizing services, processes, and workflows lives. The CMDB brings order out of chaos.

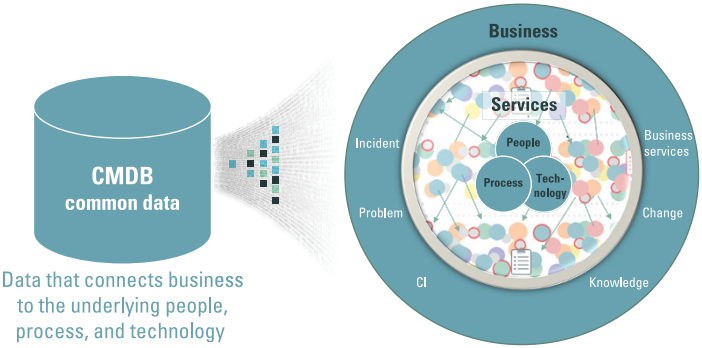

FIGURE 1-3: A CMDB brings a new level of order to a complex IT environment.

The creation and updating of service maps stored in a CMDB can be automated. Best of all, updates to the CMDB can be driven directly from changes occurring in cloud and microservices infrastructure. Armed with these powerful maps, IT is provided the visibility needed to accurately detect service issues, analyze the impact on your business, pinpoint root causes, and fix the issues for good — in near real time. Check out Chapter 5 for more information about how a CMDB is vital to modern IT operations.

Chapter 2 goes into greater detail about AIOps. One of the things it can provide is real-time complete assessment of a problem when given knowledge of how computing resources are interconnected and which business services are running on these resources. Not only can AIOps identify which business service or services are affected by a failure, but also it can detect patterns across a set

of CIs. For example, if a previous occurrence of a MySQL database running on a Windows server had a past memory limitation, causing increased latency that slowed down end-user response time, an AIOps system can infer the same issue for an Oracle database on a Linux server, given similar alerts.

Collecting and analyzing the data

All the different technologies and data sources in your on-premises data centers and public clouds produce massive amounts of data. IT needs to be able to extract insights hidden within all that data and correlate event and metric data with other types of data, such as knowledge base articles or incidents, problems, and change records, and do all of this at the speed of today's digital business — which is impossible with traditional manual processes and siloed IT tools that don't share data.

When there's an outage or service degradation, it's a herculean task to efficiently detect issues, determine the root cause, and resolve problems quickly. For instance, assume all VPN access is down for the West Coast; a critical alert is generating thousands of events flooding in from siloed monitoring systems for the routers, servers, and applications related to this outage. Your IT operations teams managing these siloed monitoring systems then begin the manual process to sort through thousands of events coming from these many systems to pinpoint the root cause — much like finding a needle in a haystack.

AIOps, on the other hand, can apply machine learning techniques to correlate current and historical data that operators can't realistically envision with traditional manual processes and siloed tools. AIOps helps reduce *event noise* by grouping alerts based on previously found patterns and types of CIs. Machine learning techniques can identify the primary alert that needs to be investigated reducing the number of alerts operators need to look at.

REMEMBER

A complete AIOps system should also provide operators with historical information that can help pinpoint the root cause faster. An AIOps system can identify previous similar alerts on the same CI or on CIs related to the main CI. It can also identify similar past incidents and past changes from an ITSM system and correlate them with relevant knowledge base articles, providing valuable information for operators to more quickly assess and remediate a problem.

Automating remediation

When service problems strike, IT is in a race against the clock to identify the source of the issue, the root cause, and apply a fix to restore the service to a healthy state. AIOps helps identify the suggested remediation to the problem and dramatically reduce the time it takes to restore service. An AIOps system can mine knowledge base articles, using natural language processing (NLP), to identify remediation recommendations for the same or similar alerts. In addition, AIOps can analyze past scenarios of successful remediation for similar situations and present the most relevant scenario to the Operations team.

When enough confidence is determined, the AIOps system can trigger remediation automatically, relieving the operations teams to address other priority issues.


TIP

Being able to correlate different types of records, such as events, changes, incidents, problems, and bringing current ITOM and ITSM historical records together, enables you to overcome many of the difficulties associated with manual remediation, automating traditional steps in the process. An AIOps system can learn from this historical information and automatically suggest a remediation action, or even automate the remediation action without operator intervention.

Imagine a scenario where your order processing system performance has suddenly crashed to the point of being unusable because a storage disk is full. The systems impacted by this failure all start sending events to the operator. Before AIOps, discovering which of these events were critical and then researching the root cause and the methods of resolution was extremely time consuming, often involving reading many unrelated log files, knowledge base articles, and manually correlating data from several monitoring applications. Now, an AIOps system can perform many of these steps in the background and present the outcome to operators. Resolutions are a click away or can even take place automatically, which allows you to run your operations at digital speeds, as shown in Figure 1-4, required of IT departments today.

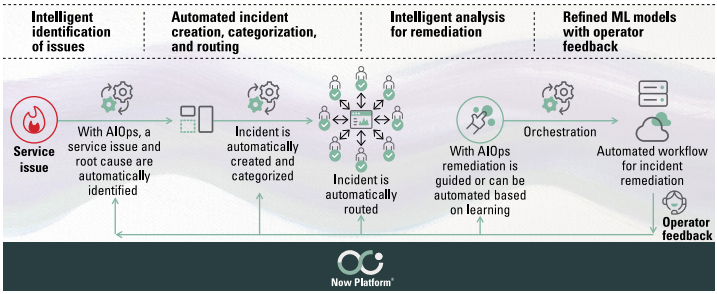

FIGURE 1-4: Process improvements with AIOps.

Assessing AIOps Outcomes

When looking for reasons to justify implementing AIOps, take a look at the new set of capabilities it can provide to your team and to the overall business. This section gives you the Key Performance Indicators (KPIs) you may want to consider.

Greater user satisfaction

AIOps proactively helps reduce the amount of time needed to detect, diagnose, and fix issues that lead to an increase in the quality of the services provided. The main outcome is that IT can deliver end-users with great experiences, meeting and exceeding their expectations. The steps to improving customer experience with AIOps and automation are covered in Chapter 4.

With AIOps leveraging service visibility, reducing alert noise, and performing problem analysis, the expected outcomes are reduced: Mean Time to Identify (MTTI) the root cause of a problem and overall Mean Time to Repair (MTTR) to get a service back up and running in near real time.

Greater IT cost savings

One of the cost justifications for AIOps is that it can help organizations increase operational efficiency, which saves time and money while improving employee experience through improved analysis, automation, and better collaboration in resolving problems.

Not all businesses have the same complexity or overhead, but on the low end, downtime can cost around $140,000 an hour, while the average is around $300,000 an hour. It can run as high as $540,000 an hour. Introducing AIOps significantly reduces the number or outages in your operations. You get a pretty good picture of your cost savings.

Enabling IT as a business partner

The IT department, while seen as essential, is often not seen as one of the primary business departments that directly supports the company mission and goals. Traditionally, an IT team is busy fighting fires, with little or no time to do anything else.

AIOps frees up time spent by IT teams to take corrective actions, allowing them to be more involved by integrating new and updated technology. In a world that advances daily, IT departments are now the ones most in-tune with modern technological advancements in how business is done in a digital world, best positioning them to support the business in adopting those changes.

IN THIS CHAPTER

- Learning a bit about AIOps and what it can do
- Discovering the power of machine learning
- Managing with AIOps
- Improving user experience and meeting organizational needs

Chapter 2
Introducing AIOps

Artificial Intelligence for IT Operations (AIOps) is a relatively new term for a technology approach that's changing IT Operations. Uncertainty about what it takes to implement artificial intelligence (AI) and a lack of knowledge of the benefits of AIOps have resulted in slower than expected adoption but just like cloud computing, AIOps is a game-changing concept. In this chapter, you discover how AIOps can get your organization running at digital speed.

Getting to Know AIOps

AIOps isn't a specific off-the-shelf product. It's a set of capabilities that enables the processing of big data and real-time events and metrics by using AI and a branch of AI known as machine learning. Put simply, AIOps capabilities provide insights to IT operators in near real time, resulting in unprecedented speed and efficiency.

AIOps doesn't replace existing IT management tools. Rather, it sits on top of them and further analyzes data coming from these tools using AI and machine learning techniques. By analyzing and correlating the data from all these tools, a cohesive image or behavioral model is formed, and new insights are developed. New

abilities to automate an ever-changing environment are enabled, with the result that companies experience fewer failures and significantly reduced time spent determining the root cause and remediating failures when they do occur.

REMEMBER

The more familiar you become with the benefits of AIOps the faster you see how it transforms the way IT Operations can move from reactive to proactive and from proactive to preventive.

Imagine how effective your team could be if you had a system that proactively indicated when problems arose so you could take care of those issues as soon as they happened and even prevent them before they happened, too, continuing to deliver an excellent experience. Getting to the root cause of a failure faster, and with fewer resources, gives your team more time to focus on important business goals and lowers your overall operating expenses. You can deliver high-performing services with visibility and AIOps, as shown in Figure 2-1.

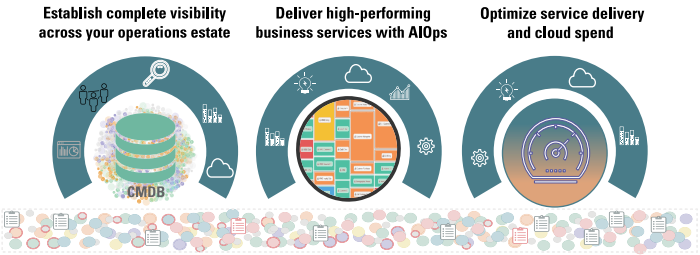

FIGURE 2-1: Using AIOps improves how you manage your IT environment.

Using Machine Learning

Machine learning is a branch of AI that uses the ability of computers to learn by analyzing data and improving answers to questions posed to it autonomously. This conception contrasts with the idea that the only way a machine gets smarter is if a human adds to its programming by giving it a new rule from which to make decisions. Machines can now make those rules on their own by digesting data fed to them, both initially and over time by input from people trying to improve results. Today, machine learning is used in everything from answering questions to operating your smartphone to medical diagnostics and self-driving cars.

Learning is done by giving a machine learning system some training data to decide its best algorithm. With feedback on previously provided responses, such as "Oh, so you think that's the answer? Here is a better answer," the computer remembers the feedback and next time provides a better response. Machine learning systems learn in three different ways: supervised, unsupervised, and reinforced learning.

Supervised learning

A *supervised learning model* uses structured data and a computer cheat sheet. The learning algorithm checks its answers to evaluate how well it's done and makes the necessary adjustments iteratively to arrive at the best answer. Unlike simple calculations you may expect from a computer, AI is going to give you its "best" answer based on what it has seen before.

Unsupervised learning

Unsupervised learning is a method of machine learning that uses data that doesn't have a corresponding expected outcome. In this case, the machine learning system must first examine the data in order to create its own function for further analyzing the data.

Two kinds of problems are normally solved by unsupervised learning: clustering and association. *Clustering* is where you want machine learning to find groupings in your data. For example, when looking at log data, it can find common occurrences of log events. *Associations* can find links between events. For example, when cloud virtual instances reach a certain threshold, the instance crashes.

In the case of AIOps, machine learning is used to find patterns for alert correlation, root cause analysis, dynamic thresholding, anomaly detection, and similarity matching.

Reinforced learning

A third type of machine learning is known as *reinforced learning*. Answers it provides are given feedback, and the machine learning system learns to give better answers in the future by adjusting the algorithm it used to arrive at its provided insight. Operators train the model by providing their knowledge and expertise in evaluating the answers provided by the computer. In this way, the model is trained and it continually becomes a better tool.

AUTOMATED ANALYTICAL MODEL BUILDING

Ever build a model as a kid? You took all those pieces and glued them together, and eventually all those pieces started to look like your expected car, plane, boat, or whatever your goal happened to be. Computers see data the same way. They take all the pieces, and as the pieces are put together, a model is built that allows an image of the goal.

Machine learning is a way to automate the model building through data analysis. In the past, knowledge workers spent a lot of time constructing complicated models of data — a great example is weather modeling. Considering barometric pressure, temperature, wind speeds, and change over time, models could forecast the weather. Okay, maybe not that well.

In today's machine learning environment, models can be built automatically and sometimes in novel ways humans had never considered. The same is also true in an IT environment. The data is complex and vast, and the ability to create analytical models automatically saves vast amounts of time and resources. The more data you can provide to the AI the better machine learning is at building analytical models.

Managing what you can see

One of IT's most important operational requirements is being able to "see" what's going on in every part of your organization's IT environment — it's critical to managing services supporting your business successfully. A successful approach includes the ability to visualize the current state of the IT environment almost in real time. AIOps can use information stored in a configuration management database (CMDB) to keep a handle on the unpredictable nature of an organization's digital world by using machine learning to draw insights. Chapter 5 goes into detail regarding the benefits of maintaining an accurate CMDB.

Discovering what you need to manage

Knowing what you need to manage is a prerequisite to successfully managing anything, particularly a complex IT environment. It may take some time to comb through your organization to find all the hidden data stores, departmental servers, cloud operations, containers, applications, mobile devices, and even Internet of Things (IoT)-connected devices. Each of these needs to be managed for

- Security
- Asset management
- Root-cause analysis
- Change management
- Impact analysis
- Capacity management
- Performance and availability management, and more

Finding all the "IT" components supporting your business services is a great first step in terms of achieving the visibility you need to keep your business healthy. To complete that visibility, you also need to understand the dependencies between those components.

Mapping services is the traditional method for keeping track of the dependencies between IT infrastructure components and the services they support. But service maps are difficult to maintain. When done manually, it's almost impossible to visualize, keep up to date, and preserve accuracy. On top of items you track in a service map, you also track incidents, events, network and application efficiency, and changes. These tracking tasks are manpower intensive.

WARNING

Attempting to build service maps manually in today's environment leads to out-of-date and inaccurate maps.

One of the benefits of automating discovery is you can more easily and accurately detect and track configuration changes to services and know who's affected by a change.

Managing what you discover

After you've discovered all the things you can manage with AIOps, it can also help you manage the IT health of your organization by

- Advanced event suppression, with tight integration into problem identification and resolution processes
- Knowledge and use of historical incident and problem data
- Use of machine learning to detect anomalies, reduce event noise, and provide service health information

Interacting with a good configuration management database and the output of various monitoring tools empowers AIOps to automatically update service maps so they're always seen as trusted and accurate.


TIP

One of the great capabilities of AIOps is the ability to group alerts based on machine learning review of the correlated data. An example of how this works is when the operator views a dashboard displaying events and sees that a primary and severe alert has occurred in web services. The alert displayed is actually a group of alerts with the most severe being displayed first. After viewing the knowledge base articles and log data that are automatically displayed related to that alert, the operator can choose an automated response. This may resolve all the related alerts. For instance, if the degradation in web services was being caused by a cyberattack, there may be cybersecurity related alerts. After resolution and patching the security vulnerability, the web services return to normal, and the cybersecurity alerts stop appearing. This attack may have been the result of a developer update. The machine learning system remembers that in the future and looks for that possibility should similar alert patterns arise.

ITSM and the importance of having a single data model

One of the key components to modern IT Service Management (ITSM) is continual improvement. ITSM supports customer experience and service quality through several software tools. The data collected by these applications is key in managing IT Operations and Customer Support.

An important goal in adopting AIOps is silo-busting, where monitoring tools are located in ways that they can't communicate with each other or be accessed by another set of services such as AIOps. Using a single solution that consolidates your IT tools and processes into a single data model allows you to gain visibility, automate your workflows, and provide a better experience that improves your team's productivity.

Consolidating your IT tools into one data model not only automatically simplifies your IT processes but also improves the ability of machine learning to provide insights to IT staff and automated remediation of well-known problems. This greatly improves staff productivity by freeing them from problem resolution research and automating the mundane tasks.

Engaging with People and Processes

The ability for an IT team to effectively manage the growing complexity is largely based on better communication. In this section, you see how working with AIOps becomes simpler when you utilize the communication tools your team already uses to collaborate among the impacted teams and individuals.

Omnichannel, chatbots

Omnichannel refers to a unified communication experience for users across multiple channels. This approach allows users to have a seamless experience as content is optimized for each channel and device where organizations allow them to migrate from channel to channel in a consistent and seamless way.

For example, you may offer solutions such as voice response, text response, live human chat, email support, Facebook support, or some other social media support. Providing a means to integrate all these so the customer can easily move between them seamlessly is what omnichannel support is all about. Providing chat support without using a human can provide one more method of client support.

Chatbots are one of the earliest and most enduring AI applications. Initially, they were simple responses to key words. Today, with natural language processing (NLP), which is an area that's a confluence of AI and linguistics, chatbots can have real and

meaningful conversations, making them perfect for providing customer support.


REMEMBER

Today's end-users want immediate gratification, and when it comes to support, they're already impatient. They aren't willing to fill out a lengthy ticket submission form and then wait for someone to respond to their support request.

Chatbots can provide basic user support and help triage larger problems. Removed from the burden of answering routine questions, or providing simple solutions, IT service staff becomes increasingly efficient. Chatbots are available 24/7 and equipped with machine learning so they continually get smarter.

Omnichannel creating seamless support response and chatbots providing continual customer support around the clock are technologies that continually improve ITSM.

Operator notifications

AIOps capabilities can be set up to send context-aware notifications to all the required IT stakeholders. Rather than receiving a plethora of events from which operators must draw inferences, they receive detailed notices of impending or actual problems, a list of the systems and services that are impacted, and suggested methods of remediation. In this way, AIOps becomes an intelligent partner with the operators. It isn't the goal of AIOps or AI to replace humans; instead, it acts as intelligent partners in meeting complicated human needs.

Getting It Done Automatically

While automated tools in IT Operations are nothing new, AIOps allows for another level of intelligence and ability in automating tasks. Machine learning can look into the past to see what tasks were automated and in so doing can assist in recommending new tasks for automation based on what it learned.

Task creation and assignment

Creating and assigning tasks to the right people/groups automatically is essential for an organization to be able to move at the speed of the modern digital world. Proper task assignment not

only allows your staff members to focus on the right things, save their valuable time, and keep them motivated, but also it reduces time to resolution and keeps the users happy.

Let the IT staff oversee the AI and improve its ability to do the job, while intelligent algorithms learn the history of how tasks have been created and assigned to automate those steps.

Omnichannel notifications

Collaboration has driven businesses to move far beyond email. Applications, both desktop and mobile, are now used to facilitate better team communication. Being able to communicate via Microsoft Teams, Slack, and other mobile applications brings new abilities in working together.

AIOps can use its NLP capabilities to interact with omnichannels and ChatOps, which are chatbots, chat clients, and other real-time communication software. ChatOps applications, such as Qbot and Hubot, deliver operator tasks through chat style interactions. This style of interaction also provides an easy way to expose certain capabilities to audiences like DevOps audiences. It isn't necessary to leave your collaboration environment of preference in order to be made aware of or respond to alerts and tasks.

Taking action

Going beyond simply automating tasks, diagnostic and corrective actions can also be automated. AIOps can provide you with expert diagnosis automatically based on previous patterns it learned. Diagnostics are automatically executed to enrich information beyond the simple alert. This can include collecting log files that have additional data to further diagnose and triage a problem getting your services back to a healthy state. It can also suggest remediation actions based on previous situations.

Providing Continuous Insights

One of the great assets about computers in general and AI specifically is that it's always there and always on top of the latest information. New insights are drawn from real-time analysis of various data sources/types such as event data, metric data,

remediation solutions, and incident/problem/change records that are being tracked by your integrated configuration management database.

REMEMBER

Keep track of how you're achieving your goals by measuring Mean Time to Repair (MTTR), incident assignment time, and service level agreement (SLA) attainment. When AIOps helps you, it gives you the most relevant assistance in attaining your goals by offering continuous insights.

One of the difficult factors in IT Operations in using old methods is drawing insights by integrating otherwise siloed information. Your ITSM applications are great sources of insight. Machine-generated data on everything from application response times to storage levels is also important for staying ahead of the game in a proactive manner rather than responding when limits are hit. Of course, change management is key, and tying this altogether in a machine learning system provides powerful and continuous insights.

Improving Operator Experience

Reducing the noise that comes from events originating from users, services, applications, and the cloud by using event correlation algorithms improves operators' experiences. Rather than being barraged by every single event, operators receive a proactive notification, relevant knowledge articles, similar issues that have happened in the past, and a suggested remediation. In some cases, the remediation is automated. The operators see a description and timeline of the event, the services impacted, and remediation task recommendations. This makes life much simpler for operators and improves their performance and experience.

IN THIS CHAPTER

- Detecting anomalies in performance metrics
- Solving issues faster
- Mining corporate data for better answers
- Improving operational efficiency

Chapter 3
Exploring Key AIOps Use Cases

Artificial Intelligence for IT Operations (AIOps) employs machine learning to process vast amounts of information from IT services, processes, applications, and infrastructure to primarily

- Identify behaviors and anomalies in performance data without relying on manually defined and managed thresholds
- Correlate alerts by finding patterns in alert data instead of using manually defined rules
- Find root causes of service impacting issues

Machine learning can also be applied to categorizing and assigning tasks and analyzing historical data in context of current issues, which reduces the time it takes to submit an incident for resolution. AIOps has many use cases, and we cover a few in this chapter.

Managing Thresholds

IT monitors the performance of infrastructure by using monitoring tools that periodically check metrics like how much work the CPU on a server is performing, the amount of memory being used, the volume of data sent and received on a network adapter, or how long a website takes to respond. IT operators are interested in the performance data, or *metrics,* but sitting in front of a screen watching charted metrics isn't productive. Instead, thresholds for metrics are set in monitoring tools so IT operators receive alerts when a threshold is breached. Practically every monitoring tool works this way and *has* worked this way for decades. While this saves IT operators from having to continuously watch screens, managing thresholds has remained a time-consuming task.

Why should you manage thresholds in the first place? A threshold is set to alert you when a service is operating outside of its operating parameters. Refining these thresholds improves the efficiency of your monitoring system. Thresholds may initially be set too high or low and trigger false alerts. A threshold set for monitoring a CPU workload may generally work but not for specific servers. You may adjust the threshold to find some common ground and end up with false positives. Or you could create separate monitoring policies that apply different sets of thresholds to different monitored systems — but now you have *more* thresholds to manage.

Another problem with thresholds is they're static. Once set, they stay that way unless manually adjusted. Metrics can — and do — periodically exceed thresholds, and this behavior is sometimes expected. Static thresholds don't see it that way and raise an alert to which IT operators need to respond. Static thresholds don't adjust for *seasonality*.

These problems are magnified with infrastructure growth and the addition of more monitoring tools. Instead of manually managing hundreds or thousands of thresholds, what if the machine could automatically analyze metrics to learn normal behavior and spot abnormal conditions, or *anomalies?* Machine learning can be applied to do just that.

Figure 3-1 shows a graph of thresholds for disk space. From this example, you can see how an alert would be generated when the disk space suddenly drops off precipitously. It's easy to see the normal operating parameters, the machine learning generated thresholds, and the return to normal after the problem has been resolved. In this case, an alert was sent when the order entry system went down. AIOps recommended several solutions, one being to change the disk partition size. The operator chose that resolution, the disk was repartitioned, and the problem was resolved.

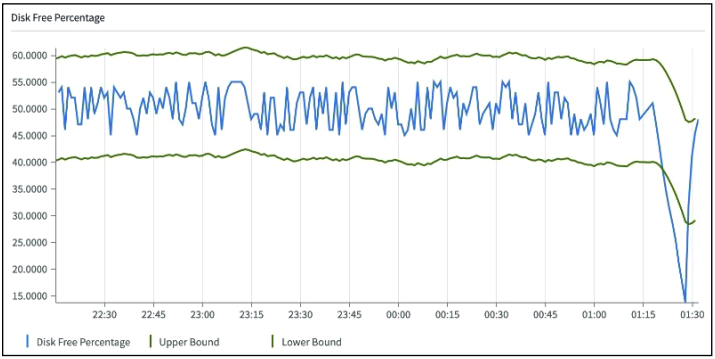

FIGURE 3-1: AIOps learns behavior of individual metric streams and detects anomalies automatically.

Anomaly detection is a key AIOps capability that uses machine learning to analyze metrics, fit the data to a model, automatically learn thresholds for normal behavior, and isolate statistical outliers. Machine learning can adjust the learned thresholds for seasonal behavior, such as a cinema website experiencing higher visits when new movies are released every Thursday. New metrics can then be compared to the learned thresholds and an alert automatically raised when a significant deviation is detected — an anomaly.

Unlike manually managed static thresholds and policies, machine learning can learn the behavior of metrics and find anomalies as they *uniquely* apply to *different* systems. IT gets a boost in productivity from no longer managing thresholds, benefits from getting early warnings of impending problems, and is now able to scale monitoring to meet future growth and increased complexity in the infrastructure and services they manage.

Allowing Machine Learning to Find Patterns in Alert Data

IT operators can spend a lot of time analyzing individual alerts only to find that some are related and are often symptoms of one alert. When this occurs, IT operators may manually link the alerts together, or create a *correlation rule* that automatically links the alerts together as a group. Correlation rules can be difficult to get right, typically are result of an IT operator identifying patterns or similarities between alerts, and often need to be updated as the IT environment changes.

Machine learning has proven to be effective at finding patterns and similarities in data. Applied to alerts, machine learning can identify patterns in alert data (see Figure 3-2), taking into account information mutually shared between alerts, the proximity of alerts occurring in time, and potentially relationships between the configuration items (CIs) the alerts originated from. Rather than manually defining and managing correlation rules, machine learning can create patterns that group alerts. And if needed, IT operators can provide feedback to machine learning to refine automatically detected patterns. Now when new alerts arrive that match the pattern, they're automatically grouped.

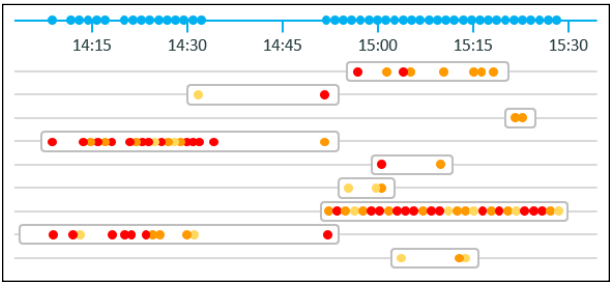

FIGURE 3-2: Patterns in alert data are easy to find by AI.

REMEMBER

Pattern recognition is one of the key strengths of artificial intelligence (AI). Chances are high that patterns can be found in your alert data by a machine learning algorithm. Correlate these patterns with other key data, such as change data, and you have a powerful triage system, spotting problems before they happen.

When they do happen, the alert appears as a single alert, rather than a series of individual unrelated alerts.

Pattern recognition can assist in a number of ways:

- Proactive alerting
- Event noise reduction
- Root cause identification
- Automated remediation

This list is by no means exhaustive. As historical data, infrastructure relationships, personnel information, real-time alert data, change data, and more are fed to the machine learning algorithm, its abilities will continue to grow.

Automating responses to correlated AIOps alerts further reduces the workload on the IT team and speeds resolution. Even the most skilled humans may not see the pattern in complex alerts, particularly if they happen over a long period of time.

Pinpointing the Cause of Service Issues

When service issues occur, IT is tasked with pinpointing and fixing the root cause as fast as possible. Known as root cause analysis (RCA), causes may cross a variety of IT disciplines, security, storage, networking, cloud resources, and databases. AIOps can help pinpoint system failures and then assist in making suggestions on how these should be remediated. Rather than sifting through alerts or digging through problems in siloed systems, correlation is key in getting to the root cause.

AIOps can provide data from past incidents, historical metrics, and insights with alert notifications. This guides the operator to the condition of the underlying root cause. AIOps spans multiple departments, multiple tools, and multiple processes, creating better insights and saving a great deal of time and money. Figure 3-3 shows an example of a service map facilitating root cause and service/change impact analysis processes bringing health and configuration data together.

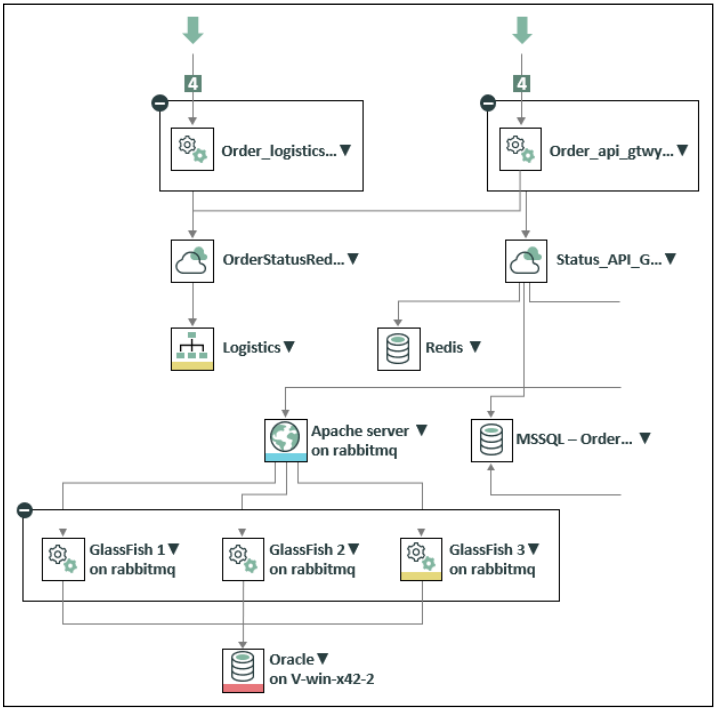

FIGURE 3-3: A service map brings health and configuration data together.

When change occurs at digital speed, it's tough to find problems that may appear transitory at first, but later prove to be symptoms of larger problems. Letting AIOps assist the operator in spotting service issues frees the operator to do more than just keep the lights on. AIOps further enables IT Service Management (ITSM) by reducing alert noise and removing duplicate alerts.

REMEMBER

Sometimes alerts are spread out over a long period of time, and a human operator may not notice the steady trend toward potential failure or system degradation. AIOps capabilities ensure that temporal alert patterns are readily seen and responded to. That also gives IT the ability to prevent issues before they even happen.

Using Natural Language Processing to Uncover the Past

One of the most significant advances in AI in the last few years has been natural language processing (NLP). Not only can you now have conversations with AI, but also you can read text and draw inferences. In other words, after reading something, AI has a pretty good idea of what was said and what it means.

NLP gives AIOps the ability to correlate additional forms of data to uncover insights into problems and their remediation. Trouble tickets, shown in Figure 3-4, describe a problem, and their resolutions describe what was done to fix them. Read through enough of these and you have a pretty good idea of how similar problems were fixed in the past. This is a powerful feature of AIOps that shortcuts a great deal of research and trains the machine learning model to suggest solutions based on past experience.

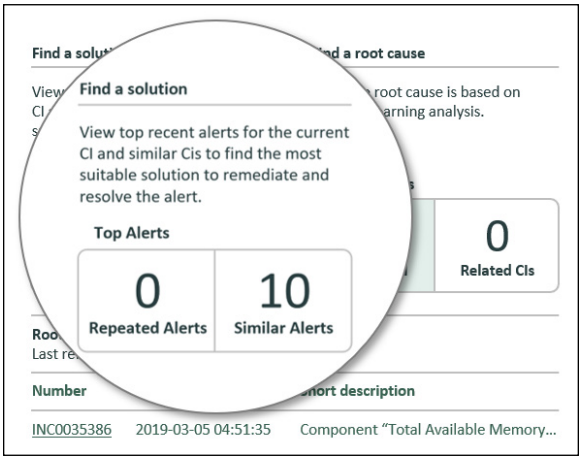

FIGURE 3-4: NLP can find and suggest past solutions in knowledge base articles, blogs, and announcements.

More than trouble tickets, given the connection and access, an AI can read any number of knowledge base articles, blog posts, security announcements, and any other type of published articles and correlate the information into useful suggestions even when your organization has never faced a particular problem in the

past. The great thing about this is that the second something is published, AI has already read it and included the information into its ability to provide assistance.

REMEMBER

Knowledge base articles are an important part of the problem management process. A number or articles capture the knowledge about how to solve problems and then can be used by staff to help troubleshoot and solve problems, closing alerts. While knowledge base articles are important, they can be time consuming to read and even more difficult sometimes to come up with a solution to the problem. AI can read them instead using NLP and derive insight in order to propose solutions to the operator. The proposed solution may involve manual steps you should take or an automated action recommended by the knowledge base article.

Faster Categorization and Assignment

One of the great advantages provided by AIOps is its ability to categorize an alert and assign it to the right team, group, or person. This doesn't replace the problem manager and the problem management process. Instead, machine learning builds patterns of behavior from historical data and helps with categorizing tasks based on how they were tasked in the past. The challenge of finding the right assignment group is reduced by making the task more specific. You can leverage CI and business service data to improve machine learning's accuracy.

This process frees up time for the problem manager responsible for problem categorization and assignment. Then, he can spend his time training and refining the machine learning process based on his experience.

Acting on AI's Operational Insights

Routine problems are best handled by instantaneous and automated routines. While companies generally build libraries of automated routines, allowing the AI to provide the solution means it's no longer necessary to program the automated response. Canned responses are for canned problems, and today, things change too fast to keep up with the number of "things"

that can and should be automated. AI can handle events or adjust workflows and configurations.

Machine learning can also learn from the automated corrective actions that have been applied previously and begin providing insights to operators on what automated actions should be applied to an alert. Because not everything can be automated, humans are still required to handle a great deal of the IT management workload. AIOps can provide operational insights to speed and improve the response times of human operators.

REMEMBER

Operational efficiency can be improved when processes, such as discovery of new resources, are automated. Also, AIOps generally leads to a shared understanding of how data and resources lead to increased efficiency across teams and departments. Operational efficiency leads to both cost and time savings, improving the efficiency of the team and cost effectiveness of the overall business.

Whether your organization subscribes to an Information Technology Infrastructure Library (ITIL) methodology or has other business practices, continuous improvement is part of any strategy with a goal of success. Examining organizational data gives organizations the ability to benefit from the data that's being captured and analyzed. This allows new operational efficiencies to be achieved.

IN THIS CHAPTER

- Discovering the benefits of ServiceNow's holistic approach to AIOps
- Providing a system of engagement for AIOps with ITSM
- Measuring the outcomes of AIOps

Chapter 4
Delivering AIOps with ServiceNow

When it comes to adopting Artificial Intelligence for IT Operations (AIOps) capabilities for your IT organization, looking to an industry thought leader and innovator can accelerate and lead to your successful adoption of AIOps. ServiceNow is a leader in delivering real-world AIOps capabilities. Working with the largest enterprises across the globe to transform IT, ServiceNow has experience in delivering industry-leading software solutions and AIOps capabilities to meet the industry's toughest IT challenges.

In this chapter, you look at how ServiceNow approaches AIOps.

The Benefits of ServiceNow's Holistic Approach to AIOps

AIOps encompasses a number of capabilities that work together to deliver insights that enhance IT operations. Key capabilities include

- Big data
- Machine learning

- Monitoring
- Automation
- Analytics

In an ideal AIOps world, big data would be a single "bucket" where all events, log messages, performance metrics, and traces from monitoring tools and systems are stored. In reality, data is stored separately by each monitoring tool in its own database, which isn't ideal for AIOps. This chaos is shown in Figure 4-1.

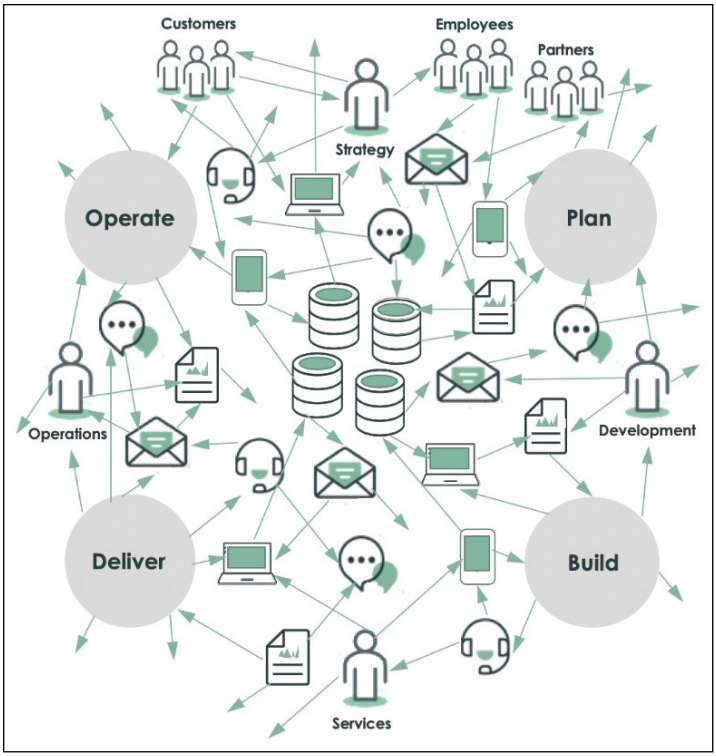

FIGURE 4-1: Data stored in silos creates chaos.

Taking all the data in a variety of formats, normalizing it and storing it in one place, and then managing the growth, performance, and retention of this data is a herculean task. This

management task can be reduced by limiting the data to that which is operationally relevant, consolidated from the originating monitoring tools and applications. This has the effect of reducing noise at the source.

Focusing only on "machine data," there's not much business relevance that can be achieved. For example, an event may contain the IP address for a server with a CPU issue, but with that information alone it's virtually impossible to know whether the server is supporting an important business service such as your general ledger or HR services. Suppose you now take events from different monitoring tools that contain the same IP address. With more information available, you may be able to figure out what applications with issues are running on the server, but there's still uncertainty about the services those applications may be supporting.

Service desk systems capture an enormous amount of data related to IT Service Management (ITSM) processes such as incidents, change requests, and problems. These processes benefit from a Configuration Management Database (CMDB) that provides information about configuration items (CIs), such as the CI type (for instance, a Windows server), the CI owner, support group, and most important the relationships to other CIs. Being able to associate this information provides business context to the machine data and provides improved meaningful insights for IT.

One area ITSM focuses on is managing service availability. Services are often composed of applications running on IT infrastructure. Managing availability starts with providing IT operations teams with accurate and comprehensive views of how applications and IT infrastructure map to services, regardless of whether the service components reside on-premises or in the cloud. These views also need to be dynamically updated to ensure that changes to applications and IT infrastructure are captured to maintain the accuracy of these service maps.

The next step involves combining application health data such as events and metrics from monitoring tools with the components making up the service maps. Maps of this "big data" can be further related to services and importantly, the infrastructure on which the services are dependent. This consolidated data gives

machine learning algorithms additional comprehensive information with which to learn patterns of behavior and detect problems.

When problems are detected, operations teams need to pinpoint root causes and take action quickly, taking advantage of captured knowledge and automation. ServiceNow provides a holistic approach to AIOps by combining key capabilities from its IT Operations Management (ITOM) and ITSM solutions delivered on a single platform where data is seamlessly shared.

ServiceNow provides a holistic approach to AIOps by combining key capabilities from ITOM and ITSM solutions delivered on the Now Platform, shown in Figure 4-2, where data, machine learning, and automation are seamlessly shared without any process level integrations.

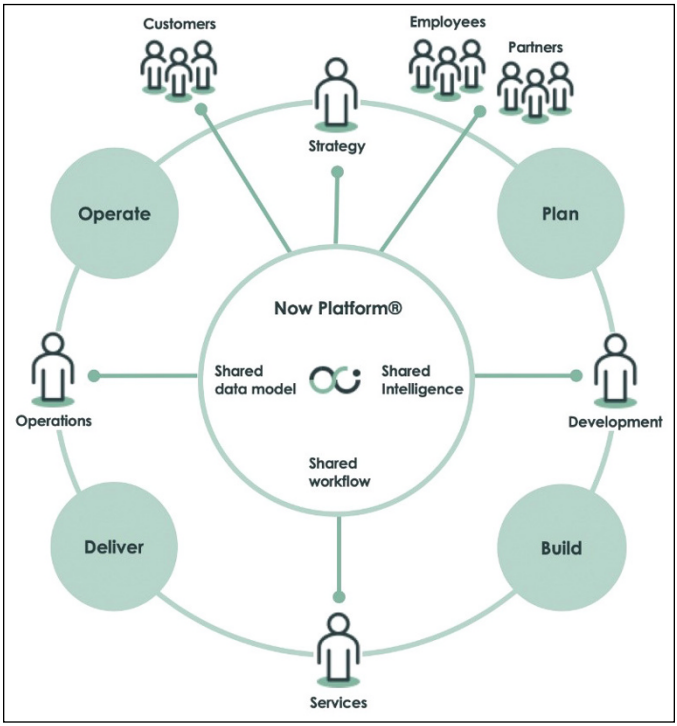

FIGURE 4-2: The Now Platform includes a shared data model, shared intelligence, and shared workflows.

With its common service data model, native platform intelligence, and cross enterprise workflows, the Now Platform can be automatically populated and kept up to date in real time and also acts as an intelligent automation engine, allowing organizations to automate steps in their processes such as root cause analysis. That kind of a strong foundation is essential for any digital transformation initiatives supporting your business, including AIOps and more.

With the Now Platform's AIOps capabilities, organizations can automate steps that include such things as

- Prediction of issues before they impact users and the business
- Detection, prioritization, and assignment of issues when they happen
- Diagnosing and fixing issues for good

Visibility

AIOps starts with obtaining visibility into the services and infrastructure that IT is managing. Step one is gaining actionable insights from gathered data from varying sources. This process is shown in Figure 4-3.

FIGURE 4-3: Discover and automatically add data.

It's no longer feasible to manually map or find all the devices and programs that make up a complex IT environment. It is best to automate that process.

ServiceNow Discovery, shown in Figure 4-4, scans networks and public and private clouds to find IT infrastructure and applications and stores that configuration information in the ServiceNow CMDB.

ServiceNow Service Mapping uses a "top-down" approach to create topology maps that relates services to supporting IT infrastructure, analyzing actual infrastructure configurations and storing the maps in the CMDB. This approach is shown in Figure 4-5.

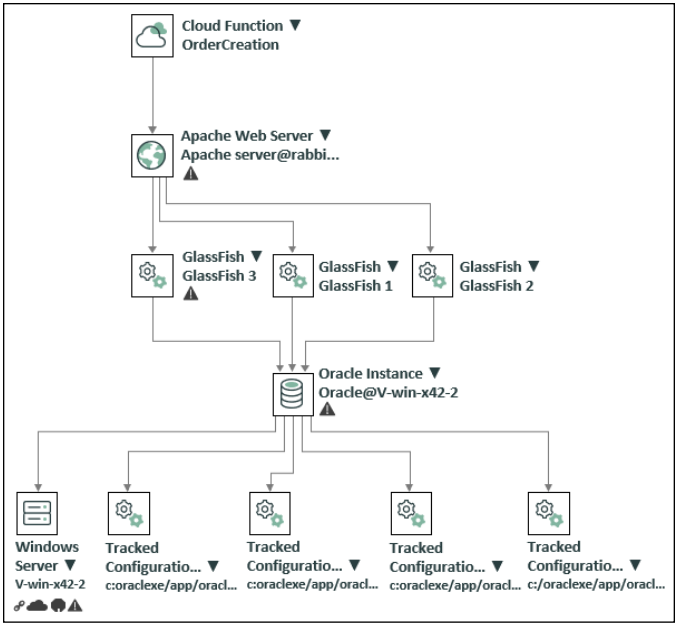

FIGURE 4-4: ServiceNow Discovery creates a dependency map.

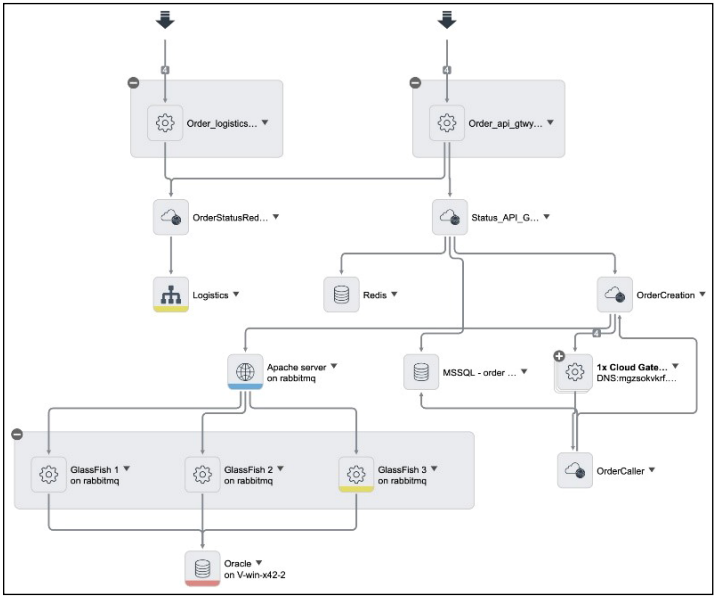

FIGURE 4-5: A typical order processing topology map.

REMEMBER

Changes are a significant cause of IT related issues. Regular rediscovery of infrastructure and services not only keeps the CMDB up to date but also tracks changes, which is valuable information to have when diagnosing problems.

Health

Monitoring service health requires analyzing events and metrics being generated by the tools monitoring the related IT infrastructure, including cloud resources. When AIOps discovers issues, it creates the incident and routes it to the correct responsible person or group. This step is shown in Figure 4-6.

FIGURE 4-6: AIOps locates issues, creates the incident, and intelligently routes it.

The right business context provided within the ServiceNow's Operator Workspace allows IT to not only observe the health of every single business service supporting the business in a single dashboard, but also gives IT the right focus highlighting issues that matter the most to the business with the right prioritization, as shown in Figure 4-7.

The same service maps contain impact relationships that, when fed by alerts, can indicate the overall health of a service (see Figure 4-8).

ServiceNow AIOps collects events from monitoring tools, processes them to create alerts, and applies machine learning to automatically group, or correlate, alerts. In addition, grouped alerts can be treated as a single phenomenon, allowing actions to be taken on the group, such as opening an incident. See Figure 4-9. When used with service maps, alert groups can also be used to identify a root cause alert.

ServiceNow Operational Intelligence is designed to detect system behavior that falls outside normal parameters or not captured by raw events coming from monitoring tools. Analyzing performance data coming from any environment, including your on-premises

data centers, public cloud environments, and any third-party data sources, machine learning algorithms model metric behavior to automatically identify operational thresholds, adjusting for seasonality where relevant. This removes the burden of manually adjusting thresholds for hundreds or thousands of metrics. Even with thresholds being set automatically, you still have the ability to override these thresholds.

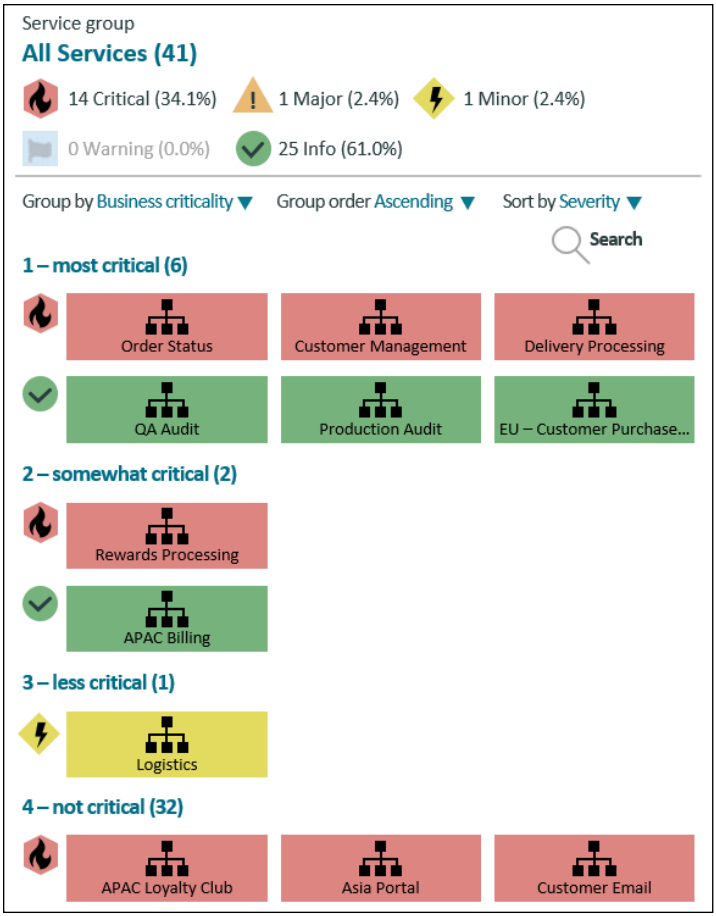

FIGURE 4-7: Put your IT data in business context.

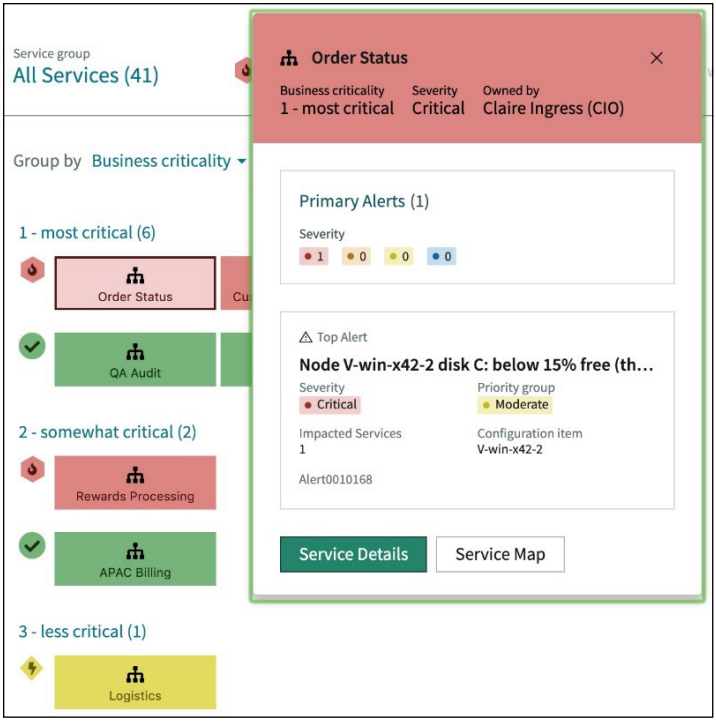

FIGURE 4-8: Service details show details of the service along with active alerts.

FIGURE 4-9: Grouped alerts reduce noise creating greater efficiency.

When metrics are received, ServiceNow Operational Intelligence compares its data points to the normal ranges it learned for every single metric stream to identify and score anomalies that indicate a major threshold breach and that an infrastructure item may be at risk of causing a service outage. A qualified anomaly generates an IT alert, which is shown on the alert console and event management dashboard to help with root cause analysis. You can see these thresholds in Figure 4-10 and the anomaly information in Figure 4-11.

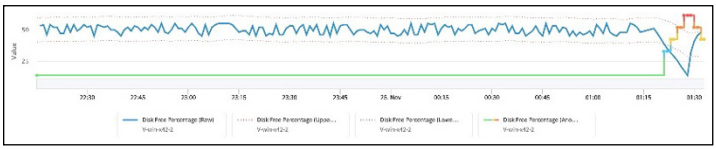

FIGURE 4-10: Disk availability with thresholds and anomaly.

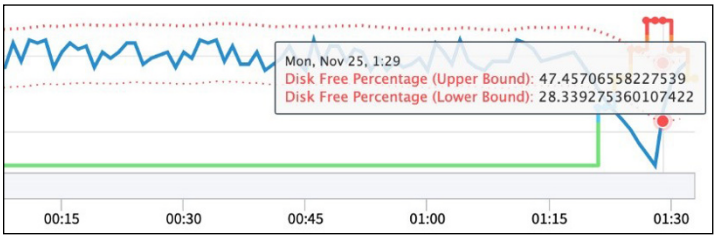

FIGURE 4-11: The details of the disk availability anomaly.

REMEMBER

Machine learning can turn a massive number of events into actionable service health information.

ServiceNow doesn't just apply machine learning to real-time data; it also uses historical data, service context, and human responses as well as feedback from human operators to oversee the health of the services supporting the business. Companies using the ServiceNow ITOM solutions have realized a significant decrease in outages, high-priority incidents, and MTTR improvements.

Automation

Automation features heavily in AIOps, from collecting and processing IT data to providing insights to performing automated actions. Step 3 is to create workflows across ITOM, ITSM, DevOps, and SecOps, shown in Figure 4-12.

FIGURE 4-12: Create workflows to achieve KPIs.

Automation is a core feature of the ServiceNow platform and is used extensively by the ITOM, ITSM, and other applications. Discovery and Service Mapping features provide automated updates to the CMDB. Event management performs automated responses to alerts such as opening, updating, or closing an incident, or running a corrective action on a remote system to restore service health. See some of the options listed for actions in Figure 4-13.

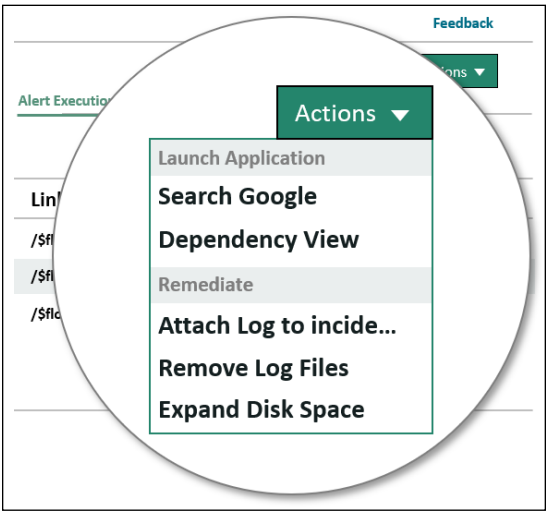

FIGURE 4-13: Drop-down action menus allow you to trigger any automation flow.

The automation engine is available to all ServiceNow applications and can be used to automate business processes (workflows), such as provisioning cloud services, onboarding and offboarding activities, managing IT records and configuration, and so on. See Figure 4-14 to see a flow diagram of automated actions.

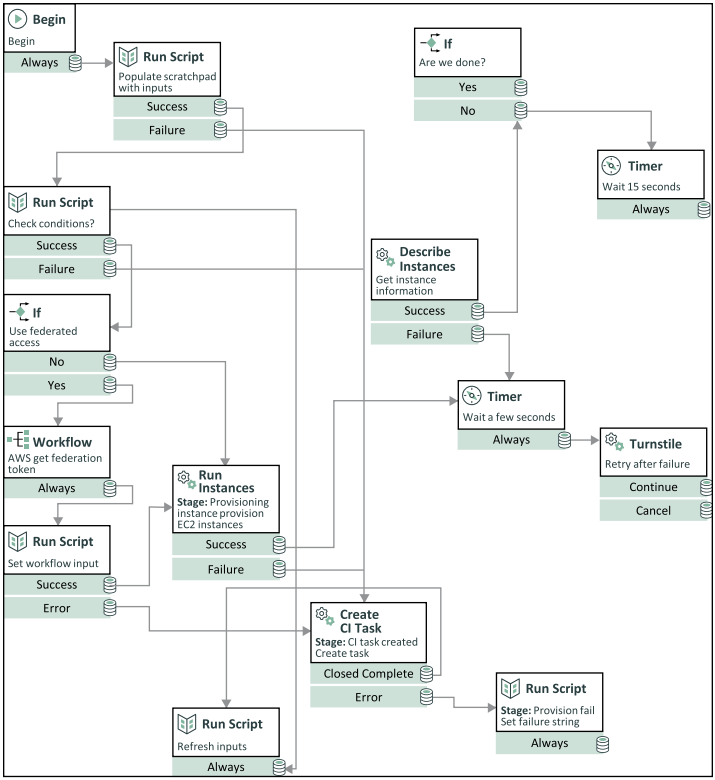

FIGURE 4-14: A flow diagram showing automated actions.

ITSM

ITSM encompasses planning, creating, delivering, supporting, and managing IT services. It's a monumental task that grows as complexity grows. The ServiceNow platform connects the two worlds of ITOM and ITSM, traditionally treated as two siloed operational departments. ServiceNow ITOM works hand in hand with the ServiceNow ITSM applications to provide contextual and historical access to service management data such as incidents, problems, and change requests.

IT generates a wealth of data; however, its usefulness is often limited to short-term and immediate operational needs. When ITOM data is combined with historical data from ITSM and the CMDB, valuable insights can be derived, allowing business service owners

and IT to easily identify trends and drive continual improvement. Actions can be measured against identifiable goals.

ServiceNow bridges the ITOM and ITSM worlds through its unique single platform and extensive automation and provides capabilities that include

- Mobile support for users on the move
- Seamless integration with the notification and collaboration tools your organization uses
- Intelligent and interactive virtual agents, or chatbots

ServiceNow realizes that AIOps is meant to benefit people and combines these capabilities with the ITOM and ITSM applications to provide an effective system of engagement.

Measuring AIOps Outcomes

Most IT professionals understand the qualitative benefits of AIOps. This includes intelligent event correlation to reduce noise, improved problem identification to find the root cause in near real time, and automated ticketing to speed time to resolution. See some of the value provided by AIOps in Figure 4-15.

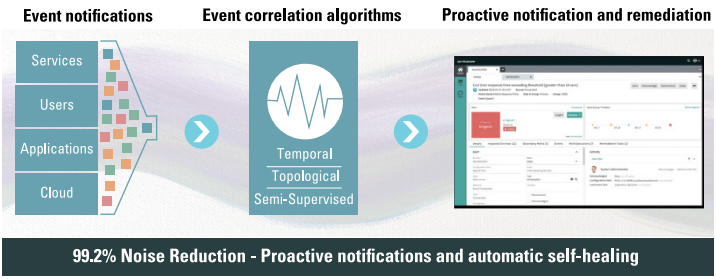

FIGURE 4-15: Value propositions provided by AIOps.

For quantifying the business impact of AIOps, there are typically two broad types of costs: soft-costs and hard-costs. Soft-cost benefits tend to be more abstract such as maintaining brand integrity or improving customer satisfaction where the improvement can be measured: for example, with Net Promoter Scores. While these are critical, putting numbers to the risk impact or revenue potential is difficult because the estimates tend to be very subjective.

TIP

One way to measure AIOps outcomes and attain better business intelligence is by using performance analytics. Performance analytics is a business intelligence feature of the ServiceNow platform and is used by organizations to better align IT with business objectives, make data-driven decisions, manage change more effectively, and spot trends faster — key enablers for delivering continuous insights for AIOps. By using performance analytics, you can define and track KPIs, perform text analytics, apply predictive forecasting, set thresholds on business KPIs, and share insights on interactive dashboards.

While hard-cost savings are easier to quantify, it still takes effort and IT expertise to make it valuable. ServiceNow has worked with several of its customers to help justify the benefit of IT operations management (ITOM) and AIOps. These examples can help you in calculating your own potential savings for implementing AIOps.

To help you get started quantifying savings and calculating ROI, follow these suggestions:

- Determine what problem(s) you want to solve and how AIOps can help.
- Pick digestible chunks to evaluate.
- Baseline your current environment and situation.
- Calculate (or estimate) the expected change when AIOps is implemented.
- Validate assumptions with multiple people within your team — don't do it alone.
- Be realistic in your assumptions and estimates — err on the side of caution.
- Get your calculator and see the results.

REMEMBER

While IT benefits directly from AIOps, many indirect benefits can extend to your enterprise-wide organization. Your organization can expect to see quantifiable improvements from AIOps so it's important to be able to measure, track, and share business-relevant KPIs.

USE CASE: QUANTIFYING AIOps OUTCOMES

The UK-based National Air Traffic Services (NATS) consolidated over 170 different screens for its Control and Monitoring requirements to a single unified platform with AIOps from ServiceNow. Before ServiceNow, the incident resolution time for priority 1 (P1) incidents — the most business critical incidents — typically ranged from 15 minutes to several hours or days. By leveraging ITOM Health capabilities, including Event Management, NATS has been able to reduce the resolution time to less than 5 minutes.

A better than 67 percent reduction sounds great, but how do you quantify it? Time to break out your dusty elementary school math book.

For example, let's say NATS had 200 P1 incidents a day where typically two engineers worked on each incident, and their average salary is $84,000 (which equals approximately $126,800 loaded with benefits or $66 per hour). Let's be conservative and say the engineers only saved 10 minutes per incident, which doesn't include the massive time savings experienced to resolve complex issues.

With these assumptions and calculations, NATS saves $801,176 per year on just reducing the time to solve P1 incidents. This doesn't include all the other benefits and savings, such as reducing engineering validation time for new starters from 1 year to 6 months or keeping the skies safer and planes on time with better quality of service.

ServiceNow's IT team uses AIOps as well to solve problems that save money. One example that likely resonates with other enterprises is a spike in VPN outages that impacts employee productivity and IT troubleshooting time. After implementing AIOps, VPN outages were reduced by 900 hours per year, which gave more than 1,000 hours in employee productivity back to the company.

Factoring in both the saved employee salary and the reduction in time in troubleshooting the VPN issues, the organization saved over $150,000.

These are just two examples of how to quantify the benefits associated with AIOps when you can reduce noise, improve productivity, and provide better service.

IN THIS CHAPTER

- Discovering why a CMDB is essential for AIOps
- Making a CMDB the configuration system of record
- Learning from CMDB use cases
- Building a CMDB for the modern enterprise
- Keeping the CMDB healthy and trusted

Chapter 5
Giving AIOps Visibility with a Configuration Management Database

One of the key elements of Artificial Intelligence for IT Operations (AIOps) involves capturing the availability and performance of IT infrastructure from monitoring tools and then inferring from all this information the state of what's being monitored. *Observability*, sometimes associated with this aspect of AIOps, is a measure of how well the state can be inferred from external data. And configuration information is essential for providing AIOps visibility of the IT domain being monitored.

A Configuration Management Database (CMDB) provides AIOps the most accurate and comprehensive view of IT infrastructure, applications, and related business services. When business services are mission-critical, a CMDB updated through *direct observation* gives AIOps the highest visibility.

A CMDB is a purpose-built system for storing configuration information about your IT infrastructure and the relationship of one infrastructure item to another. But the CMDB not only contains information about your IT environment, but also it puts business context around it and helps IT organizations become service oriented.

With so much of the modern enterprise powered by IT, visibility into IT infrastructure is mission critical. But as IT infrastructure continues to grow and become more complex due to multi-cloud environments, serverless computing, and containerization, providing AIOps accurate and comprehensive visibility of business services and the supporting infrastructure seems like a mountain too hard to climb.

For IT to gain visibility, it faces the challenge of consolidating, maintaining, and understanding complex configuration data. Often this data is found in many different repositories (silos), making it even harder for IT to find business service issues arising as a result of infrastructure or application changes. In other words, when problems arise because of changes in programs or devices, they're not easily identified or isolated.

The CMDB consolidates disparate IT management systems into a single system of action. Many organizations struggle with the CMDB because they treat it as a project and fail to realize the value CMDBs provide. CMDB projects have a reputation for failed starts, lengthy implementations, and ongoing maintenance challenges. This chapter provides you with the fundamentals to help ensure that your configuration data management process and the resulting CMDB are a success.

Opening New Value Streams with a CMDB

Enterprises use a CMDB as a foundation for IT service management, but the value doesn't end there. The CMDB is the foundation for IT Operations Management, Asset Management, and Security Operation Management and provides Audit/Compliance capabilities.

When a CMDB becomes the configuration system of record, organizations see benefits such as

- Reduced incident volume
- Reduced number of system outages
- Improved vulnerability response
- Increased automation to respond to issues faster

Increasingly, the CMDB is evolving from being applicable for Information Technology Infrastructure Library (ITIL) to now being relevant for DevOps. IDC states that 48 percent of organizations with DevOps deployed will release new code monthly or weekly. These activities are powered by Kubernetes and other container orchestration engines as Platform as a Service (PaaS) or public cloud environments. A healthy CMDB is the foundation to manage changes in these dynamic environments.

TIP

Use a CMDB to understand the complex relationships among infrastructures supporting critical business services.

Exploring CMDB Use Cases

Any organization's IT functions can benefit from adopting a CMDB. Some of the primary use cases include the following:

- **IT Service Management (ITSM) is more efficient with a CMDB.** Configuration items (CIs) provide a common reference point. Incidents, change requests, and problems are able to be related to the correct CI. Using a common CI record, a change request can be raised to resolve an incident without fear of using duplicate or inaccurate CI information. ITSM is more efficient because you're using the right information the first time, every time, which leads to greater customer satisfaction and reduces the load on the service team.
- **Understanding the impact of a change.** Change is a major cause of service outages, and yet, IT infrastructure undergoes change daily. With a healthy CMDB, you can evaluate the impact of these daily changes and respond to them properly to quickly fix or prevent service outages.

The CMDB records details about CIs, including configuration information *and* relationships to other CIs. This allows a CI to also be related — or mapped — to business services. If a change is proposed for a CI, service maps are invaluable for getting visibility of the business services that will be impacted. Service owners, business partners, and IT are on the same page, and you can plan accordingly. Visibility from the CI to the service lets you instantly understand the impact of a change and reduce the risk of service disruptions — one less problem for AIOps to deal with.

- **Manage system outages in a better way.** Service maps are great for understanding the impact of a change and are even more valuable when they can be used to understand the impact of IT infrastructure issues on business services. IT operations teams get immediate visibility of the business services affected by an IT infrastructure issue, and AIOps can use the relationships in the CMDB to pinpoint the root cause. With AIOps guiding IT operations teams to root causes, business service availability can be responded to faster, potentially avoiding outages. IT Operations can use automation to remediate issues that impact services, using the CMDB to ensure the correct action is applied to the right CI identified as the root cause. Each corrective action can be recorded against a CI in the CMDB, which provides an opportunity to gain valuable insights into preventing future occurrences. In an environment equipped with machine learning, this history leads to greater insights.
- **Save more with software asset management.** Asset management is usually considered a financial function. A configuration management platform can be used to track physical assets, software assets, and consumables. If you can have software asset data in the same place where you manage IT, your IT teams can track the location of all installed assets and their utilization in a single platform.
- **Respond to security vulnerabilities faster.** A single source of truth — the CMDB — is likewise a valuable tool for security management teams. The CMDB offers easy access to data, which is useful to security management. Security

teams can leverage the CMDB to map threats and security incidents, and discover vulnerabilities in your IT infrastructure.

Practically every organization in every industry today is subject to various regulatory requirements such as Sarbanes–Oxley (SOX), Health Insurance Portability and Accountability (HIPAA), and Payment Card Industry Data Security Standard (PCI DSS). Additionally, many organizations are subject to federal government regulations and certification programs. Although these various regulations differ in their requirements, they all share the common goal of ensuring that sensitive data and systems are appropriately secured, and proper governance and accountability are established. The CMDB is an essential strategic resource that helps organizations meet their audit and compliance needs.

REMEMBER

Use the power of a CMDB and its abilities to assist your organization in meeting stringent government and certification requirements.

Building a CMDB for the Modern Enterprise

The fundamental building block of a CMDB is the CI. A CI represents an item under configuration management, such as a router, a server, an application, or even a logical construct such as a business service. And the CMDB manages data in a technology, brand, and architecture agnostic way for both on-premises and cloud environments.

For example, the CMDB can create CIs from cloud resources such as virtual machines, containers, or cloud data centers to accommodate for the complex and dynamic environments of today's IT Operations. A properly maintained CMDB allows IT to have insight into the critical business services that run on the IT infrastructure. This visibility lets organizations better engage customers, drive revenues, increase efficiency, create new business insights, and innovate more. Service maps are essential to

give IT this visibility within a business context using the data and relationships in CMDB. They visualize the CIs that support a particular business service and how these CIs are related to improve visibility of your products and services. These service maps are derived from CIs held directly in your CMDB, connecting your business services to your infrastructure. Then you can use AI processes such as machine learning, advanced analytics, and actionable intelligence to benefit from this visibility of your business services.

Historically, configuration was added to a CMDB manually. But manually entering information about CIs is time-consuming and can be error-prone. Even in a small organization, too many changes take place, and you can't depend on manual entry for long. Yet, many organizations start out using this method to establish their CMDBs before automating the process.

REMEMBER

ServiceNow Discovery scans networks and public and private clouds to find IT infrastructure and applications and stores that configuration information in the ServiceNow CMDB.

Automated technologies that can discover CIs and their relationships/dependencies are the most efficient, repeatable, and accurate method for populating the CMDB. This way, the CMDB can ensure that the most recent and accurate profile of a CI is loaded. Mature automated technologies also can map the relationship between business services and underlying infrastructure. But some data can't be gathered automatically, such as business and organizational information. Information about people or the revenue lost for each hour of downtime can't be gathered by a scan of the network and must be entered manually or automatically pulled from other business databases.

TIP

Your configuration management platform should have the capability to regularly poll for or receive events from cloud resources, to automatically create and update CIs, and manage their life cycles as appropriate.

CMDB SUCCESS WITH CONSUMER CREDIT REPORTING

A global consumer credit reporting company with thousands of employees in many countries began its CMDB journey in 2016 with a migration from an existing technology asset repository to a ServiceNow CMDB. It leveraged service automation and orchestration opportunities by using this platform and expanded the reach of a CMDB by building an automated federated model, sourcing data from Qualys, Tanium, FireEye, and other authoritative sources. The company then leveraged the CMDB to build robust and automated business service maps to further facilitate impact and risk assessment for internal and client-facing products. Next came development of an automated method of identifying and eliminating duplicate configuration records to help further reduce manual processes. Adding cloud management with support for account inventory management, along with normalization of its discovery methods, was the final step.

Keeping the CMDB Healthy and Trusted

A configuration management team should be created to manage the CMDB and govern the configuration management process. The configuration management team should be relentless in challenging the IT organization to improve CI data quality. Technology and processes must be put in place to ensure that the data within your CMDB is accurate and the level of detail supports business needs. Correcting bad data in the CMDB can be exponentially more costly than preventing it in the first place — invest time to ensure only good data reaches the CMDB. This process involves creating identification rules for a CI and attribute population and reviewing every automation method that updates the CMDB. Regular verification and audit reviews led by the configuration management team should be performed to look for data quality issues such as duplicate and incomplete CIs.

An open channel must exist between the users and the configuration management team to communicate incorrect CI data. A process (preferably automated) must exist to handle such

corrections. Most important, you don't want to just fix the errors; you need to fix the process that allowed the errors to occur in the first place.

REMEMBER

Many processes and people downstream of the CMDB depend on the quality and accuracy of the data in the CMDB to do their jobs. When inaccurate data affects the success of those processes, those people lose trust in the CMDB and the configuration management team.

Configuration management is an ongoing discipline in any organization. Changes come from the evolution of corporate strategies that are then translated into technology decisions that then need to be implemented. Regularly measure your effectiveness and benefit to the organization. You should collect metrics on the following:

- Number of configuration management queries that are fulfilled
- CMDB defects identified and fixed
- Number of CIs missing key attributes, recommended attributes
- Monitoring and maintaining the number of CI classes in the CMDB
- Number of incidents and changes placed on items where there's no corresponding CI
- List of IT use cases for which the CMDB is being utilized with detailed metrics on each

With tools and processes in place for managing your CMDB, your next task is to keep it healthy and resolve issues as they arise. The best way to do this is to monitor your CMDB using a CMDB health dashboard. With it you can monitor CMDB key performance indicators (KPIs), including completeness, compliance, and correctness. In addition to aggregate scorecards, the dashboard can be used to drill into details for specific business services and individual CIs, allowing you to pinpoint CMDB problems and take corrective action.

A healthy and service-aware CMDB equips you with capabilities to better diagnose service issues, allow AIOps to detect root causes quickly, fix problems, and reduce the mean time to resolve (MTTR). Real-world enterprises have seen results such as

- Over 50 percent reduction in major incidents in spite of huge IT growth
- A decrease of 30 percent in false positive incidents
- Major outages reduced by 22 percent

REMEMBER

Implementing a CMDB is essential to the success of any large IT environment, but it's also essential as one of the underpinning technologies to the successful implementation of AIOps.

IN THIS CHAPTER

- Building your team and creating a plan
- Gaining visibility with a trustworthy CMDB
- Monitoring the health of your services
- Optimizing service health through automation
- Sharing your success with the enterprise

Chapter 6
Your AIOps Journey

Start your Artificial Intelligence for IT Operations (AIOps) journey with an area in the business that can dramatically improve your employee and customer experience. This allows you to effect the greatest change with a minimal amount of risk. Crawl before you walk and run. Pick one source of siloed data and apply AIOps to that and create gradual and measurable achievement. This will assist you in getting further buy-in from other departments when seeing the success within your organization.

Build Your AIOps Team

Implementing an AIOps strategy may be as much of a culture shift as it is a technical implementation. Unless your business *is* data science, your IT operations team shouldn't need a data scientist. Your AIOps solution should operate without the need for deep mathematical skills and present results in ways that don't require a new way of thinking.

REMEMBER

AIOps will only maximize the effectiveness of your IT Operations, not totally revamp it. It's an evolution, not a revolution. Develop a core team of individuals that understands the need to build a solid foundation for AIOps to be successful. A good place to find members of the AIOps team is with key ITOps staff — stakeholders in departments heavily impacted by IT efficiency and people who are used to thinking outside the box.

Define Your AIOps Use Cases

Defining use cases is an important step in implementing any new technology. Ask yourself how the technology will be used to meet business goals. What challenges will be addressed, and what problems will the technology help solve? Does the new technology have dependencies on other business processes or systems? Who are the users and how will they interact with the new technology? Answering these questions will be one of the keys in selecting members of the AIOps team.

Defining your use cases for AIOps involves collecting information from executive leadership (for example, the CIO and the CTO), IT operations team members, IT Service Management (ITSM) team members, service owners and application SMEs, or DevOps team members. Engaging people from these disciplines brings together tribal knowledge such as which systems, infrastructure types, and applications comprise a service. Do critical points of failure exist in the service? Is there a history of related known errors? How is the service monitored today? Are services being developed using cloud and microservices platforms? What's the business impact if a particular service experiences a disruption? Are the services wholly supported internally or are external service providers involved?

To visualize the process of figuring out the right use-cases/questions, check out Figure 6-1. Capturing the answers to the kinds of questions shown in Figure 6-1 allows use cases to be identified and also profiles your business services, current and future technology platforms, monitoring tools and data, and how services are supported.

FIGURE 6-1: Questions can arise from a number of different people and entities.

When use cases are aligned to business goals, you can also identify Key Performance Indicators (KPIs) to measure improvements. KPIs may include Mean Time To Detect (MTTD), Mean Time To Acknowledge (MTTA), Mean Time To Repair (MTTR), Monthly Availability, number of outages due to planned or unplanned changes, and more.

Establish Implementation Principles

Before you embark into new technology, define guidelines on what's acceptable and what's not. For example, you may want to minimize the number of integrations between multi-vendor products, agree on configuration, but minimize customization to reduce the life cycle complexity of your IT Operations. For example, while it might be easy to code one small extension today, it may become problematic during product upgrades, which creates indefinite technical debt.

Create Your AIOps Technology Plan

After you've assembled your AIOps team, a successful implementation hinges on technology and good governance. Part of creating a successful AIOps technology plan includes selecting vendors that meet your implementation principles. Careful selection helps you be successful with upfront training and customer success teams over time. Chapter 5 details how ServiceNow is considered one of those vendors.

Establish Visibility with a Trustworthy CMDB

The importance of an accurate and trusted Configuration Management Database (CMDB) can't be overstated. Chapter 5 details the importance of using a CMDB. In order to maximize the effectiveness of AIOps, accurate information about the configuration of IT infrastructure and how it has changed over time and its relationship to business services is vital. Chapter 4 goes into detail about how ServiceNow Discovery can automatically keep your CMDB up-to-date. Figure 6-2 gives you an idea of how a healthy CMDB is populated and maintained.

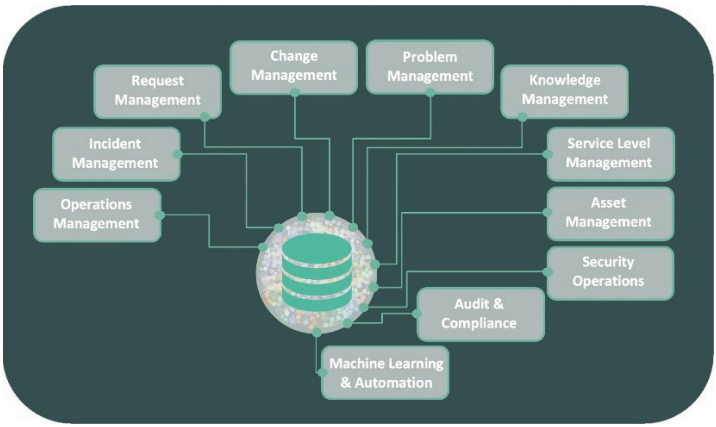

FIGURE 6-2: In the heart of IT, a healthy CMDB supports various IT and business processes.

REMEMBER

Keeping the CMDB up to date manually is impractical. It requires an automated approach. The best way to keep your CMDB accurate is to use automated discovery. Discovery can run on a scheduled basis to periodically scan networks to find IT infrastructure and applications, or in some cases be triggered by events occurring such as a virtual server in the cloud undergoing a configuration or state change. Not only does this approach keep the CMDB up to date, but also it helps you identify *what's* changed.

Because ITSM is focused on managing *services*, the next step is to map discovered IT infrastructure and applications to business services. Using automation for this task ensures you have *accurate* maps and you can also identify any *changes* to the service topology, which is a huge benefit for operators when diagnosing issues.

You may be wondering if you need to discover *every* configuration item (CI) and map *every* service for AIOps to be successful. Not at all. Start with one critical service, its related infrastructure, and applications and use it as a pilot. Crawl before you walk or run. The experience you gain from discovering and mapping that service helps you with the next one, gradually completing your service-aware CMDB.

Finally, you need to have a way of identifying any issues within your CMDB. AIOps is adversely impacted if your CMDB contains duplicate CIs, inaccurate or incomplete CI information, or stale, wildly out of date, information.

Monitor the Health of Your Services

The next step in your AIOps journey involves understanding the health of the IT infrastructure and services being managed. In order to do that, you need to connect the data coming from the tools and feeds monitoring the IT infrastructure and applications to CIs in the CMDB. Correlating this data allows you to quickly identify root causes or head off impending issues, as shown in Figure 6-3.

TIP

Make sure your AIOps solution is able to fully exploit a CMDB to use CI, relationship, and service map information.

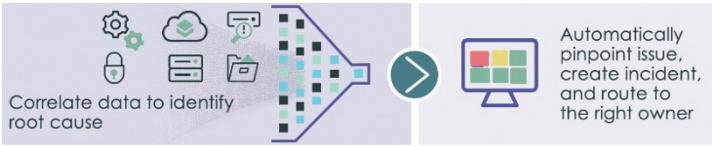

FIGURE 6-3: Correlating data from a CMDB allows you to rectify problems faster.

Monitoring service health involves combining monitoring data with the CMDB. This starts with collecting relevant events and performance metrics from monitoring tools. Deciding on which events and metrics to collect can be guided by the services you choose to monitor first. Use a service map to identify any instrumentation gaps. Consider choosing metrics that are the best indicators for application-oriented issues — "golden metrics." If possible, filter events at the source. Consolidating collected events and metrics on the same platform as your CMDB and ITSM systems will help avoid costly integration efforts and allow easy access to data for AI/ML.

Link an alert to a CI that's part of a service map and you instantly get an indication of its service health. If that same CI supports multiple services, then you instantly recognize *all* the impacted services. Impact relationships define the extent that a CI's alert contributes to the service state. For example, a critical severity alert for a CI may be downgraded to a major severity because the CI is in a cluster with redundant members.

AIOps can also use these service maps to identify and diagnose probable root causes using AI/ML techniques. Operators can examine the CI in the map to determine whether a recent configuration change occurred, thanks to your automated CMDB. Operators get a further boost in triaging a root cause when AIOps digs into the past history of incidents, problems, and change requests tracked through ITSM. It's possible that a detected configuration change associated with an alert is related to a recent change request.

Changes are typically scheduled to be performed in a maintenance window for a CI, so if AIOps can take advantage of this information, any alerts occurring while the change is performed can be automatically suppressed.

TIP

IT Operations are provided the best insights when AIOps can take advantage of active and historical ITSM records.

Optimize Service Health through Automation

Next up in your AIOps journey involves *acting* on service health issues. In the past, this may have been a manual task whereby a luckless operator would spot an alert on a monitoring console, spin around on a squeaky swivel chair to an incident management console, and raise an incident ticket. More fortunate operators would see a monitoring tool *automatically* create an incident ticket — a straightforward and important step in the right direction! Eventually someone steps in and fixes the issue, usually logging into a server to run commands, apply a patch, or perform other corrective actions.

Implementing workflows leads to rapid issue remediation, which allows you to quickly overcome outages, recover from malware and vulnerabilities, and detect software license issues. This process is shown in Figure 6-4.

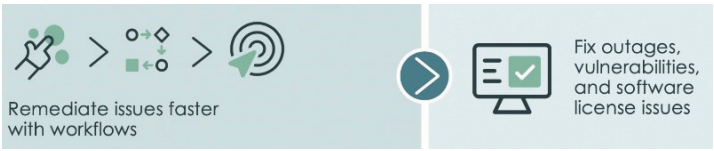

FIGURE 6-4: Workflows allow for faster problem remediation.

One of the aims of AIOps is to apply extensive automation that applies corrective actions in response to service degradations or outages. Automation can help in several ways:

- Automatically create an incident in response to an alert
- Automatically associate a known error knowledge article created through problem management with an alert — in effect, a runbook instruction for operators

- Automatically perform a diagnostic action on a CI to collect more information, such as a log file or command output
- Automatically run a corrective action, such as restarting a service or process, restarting a server, installing software, and so on

Automated corrective actions, or remediation, can be presented to operators for manual triggering, or for well-understood alert conditions fully automated triggering. Identifying automation candidates can be as simple as examining past incidents to identify common problems reported by monitoring tools. Filter the list of resolved incidents for those that involved manual fixes and identify whether any of those fixes can be automated. Next, automate the steps taken to apply the fix using a workflow, script, or tool. With a reliable automated fix in place, you can configure a rule to trigger the fix based on a specific alert condition.

Whether choosing to implement automated corrective action or operator action assisted by AIOps, the use of another type of AI known as natural language processing (NLP) provides AIOps with the capability of reading all past incident reports, knowledge base articles, journal articles, or logs to quickly provide additional insight. NLP now has the ability to understand what it's reading through a process called *deep learning*.


REMEMBER

AIOps can automatically set operational thresholds. Build a library of remediations and look for opportunities to reuse remediations in other more complex remediations. Track the execution of remediations to identify failures that may indicate required improvements, or CIs requiring manual intervention. Remember that each remediation gains you productivity.

Review and Learn for Continuous Improvement

Throughout all the steps in this chapter, you're capturing what's happened (alerts), who's been involved (incidents), what's needed to be done (change requests), the corrective actions that were performed (remediation tasks), and validated changes applied (CIs updated by discovery). Figure 6-5 shows the stages of problem resolution.

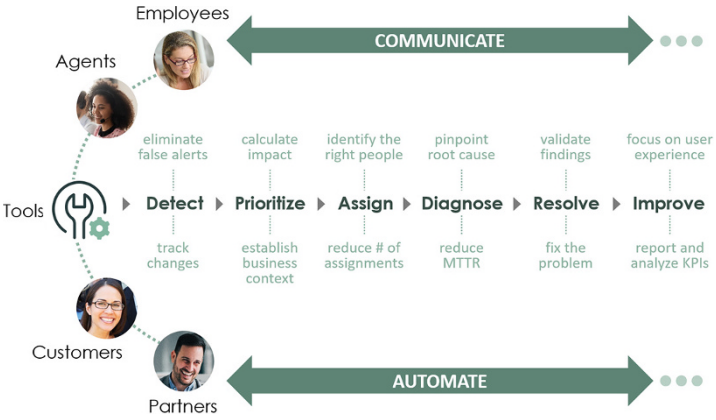

FIGURE 6-5: Successful stages of problem resolution.

The entire resolution process presents a ton of valuable information perfect for obtaining insights into potential improvements. Make sure to review and learn from this information for continuous improvement. Some examples of the insights you can gain include the following:

- Service architecture, identifying redesign opportunities based on frequent root causes
- Infrastructure, such as replacing legacy systems with cloud resources
- Instrumentation, adding/replacing/tuning monitoring
- Remediation, identifying more efficient sequences or methods
- Process, changing the way certain activities are performed

Because you defined KPIs for your AIOps use cases near the start of your journey, you can use the information being captured through AIOps to track and report on progress.

Plan monthly reviews to figure out how you could do things differently and how new services can leverage the expertise gained from existing services and be brought online faster and more reliably.

Share Your Success with the Enterprise

The final step in your AIOps journey is sharing your success with the business. You and your IT team may think you're successful, but does your management chain know it? Develop dashboards for the KPIs tied to the business priorities you identified and publish those dashboards periodically, or better yet, have them available online. From there on, your operational success is assured.

REMEMBER

Once again, don't overwhelm yourself. Crawl before you walk and run. Pick one source of siloed data and apply AIOps to that and create gradual and measurable achievement. This will assist you in getting further buy-in from other departments when seeing the success within your organization.

IN THIS CHAPTER

- Understanding what you want to achieve
- Knowing what to expect
- Learning about learning
- Gaining greater visibility with a CMDB
- Seeing how ITSM is essential for AIOps
- Learning the essential of mapping your services
- Automating your way to success
- Taking baby steps on your journey
- Utilizing machine learning for continuous improvement
- Extending the benefits of AIOps beyond IT

Chapter 7
Ten Considerations for Implementing AIOps

Today, IT operations must oversee a number of applications, resources, and data sources. Implementing AIOps requires a carefully planned strategy and patience, but the result is a proactive IT operations team that meets the corporate mission through data-driven KPIs. In this chapter, you discover key points to think about when implementing AIOps with ServiceNow.

Understand Your Goals and Objectives

It may sound obvious, but before you embark on your journey be sure you have a clear understanding of the goals and objectives for implementing AIOps (see Chapter 1). Be sure to identify KPIs that you can use to measure improvements delivered by AIOps to ensure you're on track to achieve your goals and objectives (Chapter 6).

Have Realistic Expectations

If you think AIOps will auto-magically solve all your IT Operations challenges, think again. AIOps applies extensive automation and statistical analysis to event, performance metrics, log, and trace data collected from monitoring tools to learn behaviors, identify anomalies, correlate alerts, reduce noise, and pinpoint root causes.

When it comes to prediction, AIOps deals with probabilities — receiving a notification that an issue currently unfolding has a high confidence of leading to an outage is realistic. Being told that a service outage is going to occur in the next 27 minutes and 34 seconds is less realistic.

TIP

Understand the techniques used in AIOps so you have realistic expectations on what it can and can't do (see Chapter 2).

Give Machines Time to Learn, Too

If you expect instantaneous results from AIOps, you'll likely be disappointed. Like humans, machines need time to learn, too. Have realistic expectations for the time machine learning needs to analyze data, build and train models, and begin providing insights, such as performance anomalies, grouped alerts, and identifying root causes. For example, identifying weekly seasonality requires at least a couple of weeks of observation.

The similarity doesn't end there: Just like getting feedback from a teacher marking your school work, feedback from IT Operations allows AIOps to identify whether what it learned was useful and

the reasons why. Given time and feedback, AIOps will provide IT Operations more accurate insights, allowing better decisions to be made.

Use CMDB to Give AIOps Visibility

Don't underestimate the benefit AIOps and IT Operations obtain from the visibility provided by a service-aware Configuration Management Database (CMDB). Ensuring the CMDB stays healthy and trusted significantly increases the accuracy of the insights AIOps can provide IT. See Chapter 5 for more details on how the CMDB improves visibility for AIOps.

Remember That ITSM Is Essential for AIOps

IT Service Management (ITSM) is the system of engagement between the business and IT and provides AIOps with critical information including change requests, incidents, problems, and knowledge base articles. Change requests can be correlated with alerts to help identify changes that led to a system failure. Past incidents may be used to identify an issue experienced across multiple instances of the same application. Problems with known errors documented as knowledge articles can be automatically surfaced to IT as recommended solutions. In addition to providing information, ITSM is also used by AIOps to coordinate responses to detected issues. Auto-creating and assigning an incident, triggering notifications to impacted users and service stakeholders, triggering a major incident management process, and raising an emergency change request are just a few examples of how AIOps engages ITSM. Chapter 4 gives you more information on why ITSM is essential for AIOps.

Map Your Services

Bring in your service owners and enterprise architects to help map your infrastructure and applications to the business services IT is managing. Using the automated approach ServiceNow

Service Mapping offers enables service maps to be kept up-to-date, and any changes to the map and its components can be tracked in the CMDB — AIOps becomes *service-aware*.

Respond Faster with Automation

After you reach a steady state in your AIOps operations, meaning that you're delivering on your original outcomes, start thinking about optimizing your operations through automation. With knowledge of past failures captured by ITSM, you can analyze root causes and how they were resolved to identify potential candidates for automation. IT operators can be armed not just with knowledge that AIOps surfaces by using natural language processing (NLP) but also automated corrective actions to remediate issues.


REMEMBER

For well-understood issues with highly reliable automated actions, AIOps can take over and provide fully automated remediation. In either case, the end result is faster responses to issues detected through AIOps.

One Size Doesn't Fit All

Achieving a single AIOps platform that can do everything is challenging, but ServiceNow's AIOps capabilities and platform come close and can consolidate and process alerts, performance metrics, collect CMDB and ITSM data, trigger business processes, and automate corrective actions, which all reduce integrations and the associated technical debt for maintaining them.

Be realistic about how much data can be — or should be — consolidated in one place. Your AIOps solution may involve a combination of tools and platforms suited for specific tasks such as network monitoring, transaction tracing, or log analytics. Specialized tools like these typically have highly optimized database and processing logic that would be difficult to consolidate on a single platform.

Expect your AIOps solution to share some similarities to those used by other organizations — such as those using ServiceNow — but also expect differences resulting from your organization's unique environment.

Build the Right Team

As with anything that requires more than one person, developing the right team to get the job done helps ensure your success. Your AIOps team should be made up of people familiar with what artificial intelligence and machine learning bring to the table when attempting to keep your business running at today's digital speed and massive complexity.

Stakeholders from various departments most impacted by technology infrastructure will be excited to participate when they learn about how AIOps reduces the amount of downtime they experience, improves business efficiency, and increases customer satisfaction.

Plan Big, Start Small, and Iterate Fast

You may have a grand vision for AIOps in your organization and probably are eager to get started. Rather than attempting to do everything in one massive undertaking, start small. That gives you the chance to learn from your accomplishments, validate and fine-tune your approach, acquire and build on capabilities, and achieve all-important quick wins for your organization. Chapter 6 provides guidance on how to get started on your AIOps journey.

REMEMBER

Taking on too much at once can lead to disappointments and may lead to poor business adoption. Take small steps that allow your team and the software to grow together.

Continually Improve

One of the great beauties of machine learning is that it continually learns. Of course, the old computer adage of garbage in-garbage out still applies. That's why automated discovery and a healthy CMDB are so important.

AIOps improves things on several fronts. Its ability to continually gain insight using NLP to read through updated logs, knowledge bases, prior alert resolutions, and operator feedback makes it perfect for improving operations situational awareness. The other

thing it improves is the ability for an IT team to become a more proactive part of your business. A solid IT team, when not burdened with continual firefighting, can provide a valuable ability to stay current with new technologies as they're developed, helping your company to innovate and remain competitive.

Extend the Benefits of AIOps beyond IT

AIOps directly benefits IT; however, it can also benefit other areas of an organization. For example, AIOps may detect an issue with a service supplied to one or more customers. While an incident may be opened for IT to resolve the issue, a customer case record can be proactively opened and the customer notified of the issue and updated on their status — that's proactive customer service management.

Take DevOps as another example: Suppose software recently released by a DevOps team results in an issue detected by AIOps. AIOps can automatically open a defect, notify the DevOps team, and recommend an emergency change to roll back the software to a previously known good release. Each step and configuration change are recorded and tracked in the CMDB.


TIP

ServiceNow's unique single platform allows organizations to connect AIOps to business processes outside of IT, extending its benefits to areas including — but not limited to — Customer Service Management, DevOps, SecOps, Risk and Governance, HR, and Operational Technology (OT).

Notes

Notes

Run IT at digital speed with AIOps

This book gives you the basics for AIOps – Artificial Intelligence for IT Operations. AIOps capabilities automate IT operations functions, prevent issues before they become problems to the user or the business, and improve customer and employee experiences. You also discover how a Configuration Management Database (CMDB) is essential for running IT at the speed of today's digital business.

Inside...

- Prevent issues before they impact users or the business
- Significantly reduce the time to remediate issues
- Remediate a problem in your infrastructure, applications, and services with AIOps
- Keep your business services up and running

servicenow

Tony Branton, Sr. Product Manager at ServiceNow focused on AIOps, has 15+ years' experience helping organizations align business and technology to solve challenges in IT Operations. **Ted Coombs** is a multidisciplinary scientist and futurist with 37 years of programming experience, beginning his AI work in the early 1980s.

ISBN: 978-1-119-65681-4
Not For Resale

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.