Brought to you by:

Progress® WhatsUp® Gold

IT Infrastructure Monitoring

for dummies®
A Wiley Brand

Monitor network availability and performance

Discover everything connected to your network

Find and fix network and server problems fast

Doug Barney
Mark Towler
Larry Goldman

Progress WhatsUp Gold Edition

About Progress WhatsUp Gold

WhatsUp Gold is an IT infrastructure monitoring solution that provides complete visibility in the availability, status, and performance of applications, network devices, and servers in the cloud or on-premises. WhatsUp Gold automatically discovers anything connected to your network and generates a unique, user-friendly interactive map. Customizable alerts notify IT teams of any change to the network including devices (wired, wireless, virtual, and cloud), applications, network traffic, configurations, and device logs.

For any business in any industry, WhatsUp Gold helps IT teams proactively find and fix problems fast – usually before end-users notice. WhatsUp Gold is used by organizations around the world to maintain network uptime and diagnose network issues. Visit www.whatsupgold.com for more information.

IT Infrastructure Monitoring

Progress WhatsUp Gold Edition

by Doug Barney, Mark Towler, and Larry Goldman

for dummies®
A Wiley Brand

IT Infrastructure Monitoring For Dummies, Progress WhatsUp Gold Edition

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

ISBN: 978-1-394-20427-4 (pbk); ISBN: 978-1-394-20428-1 (ebk). Some blank pages in the print version may not be included in the ePDF version.

Publisher's Acknowledgments

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

Project Manager and Development Editor: Carrie Burchfield-Leighton

Sr. Managing Editor: Rev Mengle

Acquisitions Editor: Traci Martin

Sr. Client Account Manager: Matt Cox

Table of Contents

Introduction

A few years ago, our friend's manager at his local school system asked him to design and deploy a scalable network for all her employees and classrooms, including wireless access that was both secure and for public access. She wanted all students and their families to have access to a student's progress report online. The teachers also needed 24/7 access to the online system because they kept their students' grades in an electronic grade book, and most students' assignments would be posted in the electronic student portal. Email was also a critical system for student-teacher communication and for faculty-administration communication.

The school system had several mission-critical systems that needed to stay up and running constantly, and a recent wave of bad weather had knocked out those systems and caused quite a bit of lost data and extra employee hours. The district had one staff member with the ability and know-how to come in and bring the systems back online, and he just happened to be spending that weekend camping with his family. This staff member became a single point of failure in this instance.

At that time, our friend worked part time as the newly certified network engineer/technology manager and part time as a classroom teacher. He volunteered to install and configure an IT infrastructure monitoring (ITIM) application to monitor the school system's newly deployed network. After explaining what an ITIM application could do, he found it was an easy sell. When he was ready, he received all the needed logins and settled in to get things started.

After a few minutes of scanning the network and looking through the devices discovered on the network, he realized something important: He knew a lot about how to monitor a network; he knew many of the ins and outs of the application and how it communicated to the devices on the network and gathered data about those devices, but he didn't know the nontechnical pieces to the puzzle. He didn't know what to monitor among all those devices or which features of the ITIM application he should use.

It was a relatively small network, and he wasn't sure what was necessary and what was overkill. Did he need to monitor

everything on the network? Just the router and servers? What about the managed switches? Did he need to gather performance statistics on all those devices (and if so, for how long)? After the system was in place, who would be responsible for putting out the little fires that seem to plague all of us in the IT field?

When our friend finally gave up and stepped away from the keyboard, he decided he needed to find out more about the business side of the equation and come back with a detailed plan. He researched and researched to find the best answers, and he shared the results of all this knowledge with us, and now we share it with you.

About This Book

For this book, we define ITIM (often referred to as *network monitoring*) as watching the availability, health, and utilization of physical and virtual entities such as servers, network devices, storage, hypervisors, or Internet of Things (IoT) devices across your hybrid company infrastructure.

Modern ITIM tools also test and track the availability of essential network services, such as email, DNS, and HTTP, that can be further aggregated into business applications. ITIM tools provide both historical data analysis and trending as well as real-time insights, and they alert key staff members when something goes wrong. The point worth noting is that ITIM now encompasses much more than simply monitoring on-premises devices. Monitoring now extends to the network edge and beyond.

Although in this book we focus on the needs of small- to medium-sized businesses (SMBs), the guidance in this book is applicable to businesses of all sizes, including global enterprises.

Not surprisingly, most people who start down the path of ITIM have at least some idea of what they need to monitor and maybe even quite a bit of experience with computer networks. This book lays out the business and technical basics so anyone from any level of expertise, and from either side of the employee/management fence, can put together an effective monitoring system.

Icons Used in This Book

In the margins throughout this book, you see small pictures, known as icons. These icons have been included to guide you to important information.

The Tip icon provides quick tips for you to simplify monitoring your network and save you time.

This icon denotes certain items you want to remember.

This icon marks text that you can skip if you want, although it does contain some technical information for those who really want to know it.

Beyond the Book

There's only so much information that we can pack inside a book this size. If you'd like to learn more about how to enhance your infrastructure monitoring with confidence, then sign up for a free trial of Progress WhatsUpGold here: www.whatsupgold.com/trial.

IN THIS CHAPTER

- Discovering what ITIM means
- Recognizing who needs ITIM
- Understanding why you need ITIM
- Discovering what your ITIM system does

Chapter 1
Understanding IT Infrastructure Monitoring

If you're thinking about IT infrastructure monitoring (ITIM), also referred to as *network monitoring,* for the first time, jump into this chapter and discover the how and why on ITIM.

Defining ITIM

ITIM is designed for watching your entire network and can be configured to track related resources, as well. The monitoring solution collects the data and discovers network issues, both impending and already affecting performance or availability. These problems are made known to IT through alerts (check out Chapter 3 for more on alerts), and on a deeper — even historical — level the overall health of the network is tracked through deep reporting.

REMEMBER

A modern network is a complex and often hybrid environment, and your monitoring solution needs to examine network devices and related systems, such as servers, and have a deep view into applications and services.

Knowing Who Needs ITIM

Everyone. Everyone needs to use ITIM. Whether you're a small- or medium-sized business, a large enterprise, a local or federal government, a university or school district, a hospital, a law firm, a power plant, or energy distribution grid . . . we can go on forever, but let us just repeat that *everyone* who depends on IT systems every day can benefit from what monitoring solutions provide.

And it's not just the business owner — customers benefit, as well. If you're doing a respectable job of monitoring, your systems will have less downtime. Your customers will have a positive experience while visiting your website, instead of it not loading — just one example of the many negative consequences ITIM can help you avoid.

Knowing Why You Need ITIM

ITIM is a necessity for any business that uses connectivity technology during its day-to-day operations. Even in the smallest of businesses, avoiding the use of network technology is nearly impossible.

Your network and related application resources aren't just critical to your business; they're indispensable. When either stops working — so does your business. When a problem arises and part of your network or a critical application goes down, it is too late. The damage has already been done.

ITIM, when done right, proactively seeks out problems before they turn into outages and lets you solve them before employees get upset, customers lose confidence, and business is lost. In short, common ITIM is all about availability and performance.

Use your imagination for a moment. You're the proud owner of a brand-new, locally owned coffee shop. You're excited to advertise your free Wi-Fi to your potential customers. Your plan works — you attract a new customer by way of your advertisement.

However, when customers arrive at your business, they find they can't access the internet on your Wi-Fi. Now, put yourself in your customer's shoes. Think of how frustrated you would be if you

found the advertised service wasn't functioning. On top of that frustration, you must report it to the business owner who was unaware of the issue.

This example illustrates how important ITIM is. Regardless of whether your customer is internal or external, you want to know about any issues (or potential issues) prior to your end-users notifying you of the problem. In this same example, with ITIM, you could've been notified about your internet connection failing prior to it causing frustration for your customer. Instead, that customer may never return due to the negative experience.

Simply put, ITIM allows you to be notified about *any* problems on your network. This notification can come in various formats, which we discuss in Chapter 3.

REMEMBER

Some of the most common reasons to use ITIM include the following:

- **You can diagnose problems quickly.** What if one of your critical systems becomes unreachable? Knowing exactly where the problem is saves you time, and therefore money. Fixing problems as quickly as possible minimizes the number of losses in relation to an outage. Many businesses have specific applications, services, or servers they rely on for their employees to get their jobs done. In some scenarios, when these systems become unavailable, employees are unable to work and generate revenue for the business.
- **You can proactively solve problems.** If you can see trouble coming, you can head it off before it impacts your users. If you know applications slow down noticeably at 90 percent capacity, set your monitoring system to alert you when it hits 80 percent capacity, so you can mitigate the problem. This applies to bandwidth, storage, Wi-Fi traffic — any number of issues that can cause your network to slow down or stop working. By monitoring the infrastructure that you know is critical to your users, you can proactively deal with issues that would impact them and their ability to do their work — usually without them even knowing. As one systems administrator once told us about ITIM, "This is the Holy Grail of IT."
- **You can keep track of your customer-facing resources.** With an ITIM system, you can reduce the overall downtime of your systems, applications, and services. This monitoring is

especially critical on customer-facing resources such as a website. Reducing the potential for your customers to have a bad experience is important, whether your customers are internal or external.

- **You know what's happening.** ITIM solutions give you the information necessary to ensure your network is operating optimally. If the solution finds any issues, you can be notified immediately — you could even automate resolutions to the problems.
- **You can plan for upgrades or changes.** If a device is constantly down, a CPU on the server is overloaded during business hours, or the bandwidth to a specific subnet is constantly running near the limit, it may be time to make a change. ITIM applications allow you to easily track this type of data, simplifying the decision-making process.
- **You can show others what's going on.** Graphical reports allow for anyone to easily see and understand the health of the network(s) being monitored.
- **You know when to apply your disaster-recovery solutions.** Many more people are working from home these days, so how would you know if there was a disaster at your headquarters if you're working remotely? ITIM to the rescue. You could be notified immediately when there's any deviation from normal operations, giving you the ability to diagnose the issue quickly. Depending on the specific issue, you can fix it directly from home or decide if you need to go into the office to investigate further.


REMEMBER

If your disaster recovery plan includes an aggressive Recovery Time Objective (RTO), every second is critical to meeting that goal.

- **You can make sure your security systems are operating properly.** Companies spend huge sums of money on security software and hardware. Without an ITIM solution, you can't be sure your security devices are up and running as configured — unless you suffer through a tedious process that must be regularly repeated.
- **You're informed of your infrastructure status from anywhere.** No matter if you're responsible for one or many of your company's networks, you need to know about issues when you aren't in the office. Monitoring solutions allow you to stay informed about issues on your servers or network from anywhere in the world.

STORY TIME WITH WhatsUp GOLD

ITIM is software designed to simplify the life of IT professionals by making them aware of issues before users report the problem — therefore eliminating the random fires to fight. It has the added benefit of reducing costs for the business, while simultaneously preventing revenue loss due to system outages. Even the briefest of system outages can be costly — and not only from a revenue loss perspective but also from the user experience standpoint.

Let's put the revenue loss into context with a quick story. Your CIO tasks your team with performing a cost analysis of outages, down to the minute. You found that if one specific system were down, it would cost approximately $100,000 for every minute it was unavailable because so many full-time employees would be unable to complete their job functions. Also, the company would be unable to process payments and literally couldn't collect incoming revenue.

ITIM with WhatsUp Gold, in this specific case, helped the team reduce downtime on that system *many* times. The return on investment was instantaneous.

- **You can ensure uptime.** Network uptime is critical for your employees and business operations. And if you have customers depending on your network for their businesses, you must be sure they're up and always running as well. Would you rather know the moment a problem occurs and fix it before your customer finds out — or get that angry phone call?
- **You save money.** Monitoring cuts the total amount of downtime and the time it takes to investigate problems. This time savings translates to fewer work hours and less time with angry customers.

Understanding What Your ITIM System Does for You

Any system that can obtain an Internet Protocol (IP) address is a potential endpoint that could be monitored with an ITIM solution. This opens up a whole new world of devices, including the

Internet of Things (IoT). IP addressing gives you the ability to use one of the many standardized network protocols that depend on Transmission Control Protocol (TCP)/IP.

Every device with an IP address has the capability to respond to Internet Control Message Protocol (ICMP) requests. ICMP requests — often called a ping — allow you to test communication between two network devices. Think of it as a yes or no question; one device asks, "Are you there?" and the device on the other end responds, "Yes, I am here." And in some cases, devices don't respond at all.


REMEMBER

Verifying network connectivity by using ICMP is standard for a monitoring solution. However, ITIM goes way beyond simply verifying network connectivity. Networks of today have many different devices, applications, and services that are critical for the business. Standardized protocols make it easier to gather multiple data points from the various sources.

Take a standard computer server, for example. The server itself is a piece of hardware that runs an operating system. The operating system runs the applications on that server. The applications communicate with other systems on your network using a network switch. That switch then sends the data to a router, and so on. Don't be frightened if you're not familiar with any of those words. The big picture here is that ITIM involves many intertwined dependencies.

Your server hardware needs to be monitored. Your operating system needs to be monitored. Your applications need to be monitored. Your network infrastructure needs to be monitored. These are facts! Don't let this read as anything other than that.

Most businesses use one or more types of networks to support their business models in various ways. The most used network types are Local Area Network (LAN), Wide Area Network (WAN), and Virtual Private Network (VPN). As the names imply, LANs cover your "local" resources.

The most common real-world example of a LAN is your home internet connection. Most residential internet providers give you a "gateway" device that provides the functionality of a router, switch, wireless access point (WAP), and firewall all within this single device. Any system either directly wired to that internet gateway or connecting wirelessly to the wireless network provided by the WAP, is on your LAN.

IN THIS CHAPTER

- Discovering the key to ITIM
- Seeing the different types of monitors
- Monitoring more than just networks

Chapter 2
Grasping ITIM Fundamentals

If you want to learn the fundamentals of IT infrastructure monitoring (ITIM), jump into this chapter to discover the building blocks on which ITIM is based.

Looking into Discovery

Network discovery is the key to ITIM, defining what it is that you need to watch and allowing you to decide exactly how you want to watch it. The discovery process can be targeted to scan portions of your network or to scan your entire network. In either scenario, it will find every system with an Internet Protocol (IP) address.

After your network and endpoints are discovered, your ITIM solution can map its topology by defining all connected network assets. If you're using WhatsUp Gold's discovery, it doesn't just find your devices and their IP addresses; it also queries the device — detailing everything you need to know about that piece of equipment, who made it, the model, what the device includes such as CPUs, hard disks, fans, and so on — the operating system, and specific services.

Discovery can begin with a simple ping request that's sent out via Internet Control Message Protocol (ICMP) and listens for a response. If there is no response, WhatsUp Gold scans Transmission Control Protocol (TCP) ports looking for a response. The magic here is simple: Simple Network Management Protocol (SNMP) or Windows Management Instrumentation (WMI) do the heavy lifting and most of the gathering of information.

Agentless monitoring

Some monitoring and management solutions are agent-based, which means they install an agent (software) on each device they track. If there's no agent, the device doesn't exist as far as the monitoring/management solution is concerned. Agents are the way these systems are populated with data.

Many IT pros shy away from agent-based systems, considering them intrusive and not liking the overhead that comes with all these agents. Many devices are locked in or proprietary, so they don't allow agent installation. But agentless systems don't install little pieces of software all over the network, dropping them on all your devices. Instead, agentless ITIM *discovers* the network and devices and then gathers data using simple port checks or existing network protocols such as ICMP, SNMP, Secure Shell Protocol (SSH), or WMI.

Giving devices roles

When discovering devices, it's important not only to know that they exist but also what their function is. This is done by giving them roles. Examples include firewalls, Windows servers, printers, routers, switches, and Uninterruptible Power Supplies (UPS), among many others. The good news is that your ITIM solution should know what the device does and automatically assign the proper role.

Gathering Information with Different Types of Network Monitors

There are various types of monitors for your network. The first monitor is used during discovery (see more about discovery in the earlier section, "Looking into Discovery," in this chapter) and is

also part of defining roles for these devices. There are additional, or supplemental, monitors that gather more information.

There are three basic monitors:

- **Active monitors:** These monitors actively poll devices for availability information, such as if a service is running. As the name indicates, these monitors are active and regularly query your device services and then wait for responses that indicate the health of those services. Simply put, if the expected information is returned, the device is up and running. If there's an unexpected response or no response, the device may be down and needs attention.
- **Passive monitors:** These monitors passively listen for events on the device. In fact, they don't poll your devices as an active monitor does, and therefore are more efficient when compared to active monitors because they use fewer overall compute cycles. Passive monitors include Windows events, Syslog messages, and SNMP traps.
- **Performance monitors:** Performance monitors are designed to gather statistical data about the systems of your network. When you think of a computing device, you may think about the Central Processing Unit (CPU) utilization, memory usage, available disk space, and other criteria that define device performance. Those are the types of data performance monitors track and create reports around.

  Performance monitors gather information about the following:

  - CPU, disk and memory utilization
  - Interface traffic
  - Ping availability
  - Ping response time

Beyond this list, admins can create custom monitors to track the performance of other items they deem critical. This could be through an SNMP or WMI value, or scripting — quite literally any data that could be populated from the device.

Monitoring beyond Networks

Monitoring doesn't have to be limited to just the network. You should be able to look at servers of any type — physical servers, virtual servers, and the hypervisor itself.

With virtual server and virtual machine (VM) monitoring, sometimes offered as an option to your core ITIM solution, you can discover and map your virtual resources, set up alerts when problems arise, and then deliver reports that offer a deep understanding of your virtual infrastructure.

Windows servers

Take Windows servers. You can do an ICMP request to make sure it's responding on the network, and to look at CPU, memory, and disk utilization information. After that, you can decide what else you want to see via customization — such as monitoring specific Windows services.

Application monitoring

ITIM solutions already work across the entire network and track devices such as servers for their health, CPU utilization, memory, and performance, and if they're up and running or down, and so on. It's an easy extension, then, to also track the applications themselves, which is often an optional feature in your ITIM solution. Because the ITIM solution already knows where everything is, it's a snap to find the apps. Application monitoring isn't limited to on-premises apps, either. You can also use it for apps in the cloud.

Application monitoring sees software such as Microsoft Exchange or Microsoft SQL Server in the context of the overall network environment. It looks at the performance of the application and drills into the operation of the related server and network assets. By monitoring these related assets, you'll spot problems before they become application service outages. Done right, application performance management helps you craft and abide by service-level agreements (SLAs).

IN THIS CHAPTER

- Discovering what alerts are all about
- Turning alerts into actions
- Making time for maintenance
- Working with automation

Chapter 3
Defining Alerts and Actions

You define alerts and actions. What should the monitoring system do in response to an active monitor becoming unavailable? What happens when a performance value is higher than expected? What happens when the monitoring system receives a message from a system that indicates a problem? We help answer these questions with the information in this chapter.

Alerting

After you've discovered and begun monitoring systems (check out Chapter 2 for more about these topics), how are you going to tell people *what* you find? That's where alerts come in. But how do you send them? Is it through email, or does it need to be a text message to a phone? Is it something actionable?

With IT infrastructure monitoring (ITIM), you could accommodate every scenario, from a simple email to a corrective action. You want an ITIM solution that offers complete automated control over what alerts you receive, as well as the content of those alerts.

Putting Action in Your Alerts

You can set up alerts to be just a notification, or if it's something serious, such as when a server is down and you need to restart it, that can be made into an *actionable* process that performs a corrective action. In the latter case, IT receives the alert, but the ITIM system is already taking action to resolve the problem — wonderful news if it's happened late at night or on the weekend!

REMEMBER

Actions, as you may expect, are designed to do something such as perform a task against the device when the state of that device changes. Actions can

- Attempt to solve a problem
- Let someone know that the state of the device is changed
- Integrate with external applications, such as a ticketing system
- Be assigned to devices or monitors (see Chapter 2)

TIP

We recommend that you automate as much as you can. If you're repeatedly performing a simple task, you can automate that process and claim back all that time you would've spent doing it manually — especially something simple like restarting a service. It only takes five minutes each time, but if you have a problem with that service hundreds of times throughout the year, it adds up to hours over time. A good networking monitoring solution can help you with automation. Check out the later section in this chapter, "Customized Automated Corrective Actions."

Scheduling Maintenance

ITIM solutions should also allow for recurring maintenance schedules. Here is an example of a common situation we run across. Many organizations run their backups throughout the night, and

it takes either all their bandwidth or all their server resources. As a result, the server or network segment may get labeled as down and send you an alert because you can't legitimately reach it when it's so busy. In this scenario, IT may be getting alerts every night about the nonavailability. By creating nightly scheduled maintenance, in this case for the backup window, IT is no longer alerted because this is now a normal event.

Customized Automated Corrective Actions

Customized automated corrective actions give you the ability to define a series of steps to take to fix more complex problems. Restarting a device such as a server is the most common automated corrective action. But you can get a lot more complex if necessary — and that is where customizing and extending the ITIM solution comes in.

Say you have a web application that has an application programming interface (API) endpoint that you hit to restart a web service. Using a scripting language such as VBscript, Jscript, or PowerShell, you could customize the solution to fit your exact needs.

With WhatsUp Gold, you can really do whatever you want at the end of the day, because it supports popular scripting tools and languages. The two most common corrective actions we find are service restart and SSH actions.

ITIM customization of actions is nearly limitless. PowerShell is so extensive now that you could do anything you can think of with it, and that includes interacting with Office 365 APIs, Azure/AWS APIs, and VMware PowerShell cmdlets — just to name a few.

ITIM ALL COMES DOWN TO TIME SAVINGS

Network and IT pros are constantly stressed for time. Endlessly chasing down problems or toggling through multiple consoles is a big part of the problem. ITIM saves time when finding problems and taking corrective action and simplifies the monitoring process itself, making it efficient rather than clumsy and ponderous.

For instance, an ITIM solution can run a scheduled or ad hoc automated discovery so IT doesn't have to hunt around for new devices, segments, and network offshoots, which are often created without IT involvement or knowledge. Replacing any manual process saves time, and time equals money.

IN THIS CHAPTER

- Understanding dashboards and reports
- Observing network, configuration, and log data

Chapter 4
Reviewing Data

After you configure your IT infrastructure monitoring (ITIM) solution and have had it in place for a while, you're ready to think about trending the activity and availability of the devices on your network to see whether you have any problem areas that just won't go away. If your organization is anything like the ones we've worked at over the course of our careers, it won't be long before people in the offices with closed doors and big windows start asking, "So, what do we have to show for all that money we spent on that network thing?"

And the answer to that question is . . . valuable data.

Looking at Dashboards and Reports

Two types of important outputs you should be concerned with are dashboards and reports. In this section, we cover both.

Dashboards

Dashboards are a single interface that surface a variety of data. You can think of a dashboard as a collection of reports that you determine you need to see. There are various dashboards, but the home dashboard is generally a macro-level overview of your network,

and from there, you can drill down into more specific dashboards about devices, types of services, and more.

Default dashboards come with standard content such as which devices are down as shown by your active monitors and your top ten worst-performing devices.


TIP

Progress recommends having dashboards that show the network's overall health in its core components, such as the core network, branch offices, access points, and the server room. You may also find it helpful to have dashboards showing the health of different categories of devices, such as switches, routers, VoIP devices, and virtual machines. You can even have dashboards for specific critical devices and drill down deep into a detailed view with data gathered from multiple reports that include those devices.

Dashboards don't just give you a backward look at your data; they can also show you real-time performance and availability data. This data is important because you want to know about potential or real issues immediately, not after your end-users call you up to complain about an issue.

Reports

Reports surface through the dashboard (see the preceding section) and are ideal for spotting frequently occurring problems and finally nipping them in the bud. Let's say a server goes down 100 times a year but is fixed by whoever is around. You know it crashes a lot but don't understand the extent. A report shows the troubling truth, prompting IT to dig in and address the underlying problem, whether that's a misconfiguration, operating system problem, malware, or time for hardware replacement.

Reports should cover all the activities of your devices and key applications. This 360-degree visibility lets you completely understand and control your network.

The following reports can reveal both the good and the bad:

- **Availability reports:** These reports reveal what went up and what went down during a given period. Depending on how real-time the data is, you may be able to tell exactly when a device went down, how long it was unresponsive, and when it was brought back online. Often, you see a downtime

percentage associated with each device so you can easily tell how available the device was as a percentage of the entire time you were monitoring the device.

- **Historical logs:** Historical logs can be helpful when it comes to troubleshooting and researching outages. Many forms of logs are out there, but here are a few:
  - A log of Syslog messages
  - Windows event log
  - A log of actions that have been triggered
  - A timeline of state changes for a device or group of devices
  - A log of SNMP traps
- **Performance reports:** Performance reports track specific types of data that show how well your devices performed in each area. For example, you can track the bandwidth of a specific port on a switch over time and get a graph of how much transmitted through that port. Many applications also provide top lists, which show you the top (or worst) performers in each area.
- **Network traffic analysis reports:** It's one thing to know how much traffic is passing through your network — it's another to know what that traffic is. Network traffic analysis reports provide you with summarized information about who or what's sending data, where it's going, what protocols or ports were used, geographical information, and much more.

Viewing Network Data

Network traffic analysis collects flow exports to capture network traffic patterns and statistics from selected observation points (source devices) throughout your network. The insights from this type of data can allow you to serve the bandwidth utilization use case and set up bandwidth usage policies, maximize your return on internet service provider (ISP) costs, and ensure adequate bandwidth for critical business applications and services.

REMEMBER

Network traffic analysis provides a superset of analysis and monitoring capabilities. You can view, analyze, and share observed network traffic patterns and data by way of a suite of reports and dashboards that provide rich interactive table grid, charting, and graphing capabilities.

For more advanced traffic analysis, root cause analysis, drill downs, and security, you may need an enterprise-level network traffic monitoring solution.

For example, WhatsUp Gold offers Network Traffic Analysis Plus (NTA+), which helps network professionals gain complete visibility into network traffic structure and application performance. NTA+ helps to maintain the availability, performance, and security of your entire distributed network through a single, simple, and intuitive interface.

By tracking real-time user experiences and proactively managing network performance, NetOps teams can quickly pinpoint the root causes and resolve issues faster, helping to maintain uninterrupted business continuity. IT teams can view network status, advanced traffic analysis, and security data all in one interface to speed diagnosis and accelerate mean time to repair (MTTR).

Viewing Configuration Data

Configuration management is built around an automated task execution engine that allows network managers to dynamically gather configuration data about their network devices through configuration tasks and compare that run-time configuration with a desired state. These tasks can be scheduled to run regularly or can be manually invoked as needed to upload, download, and back up configuration files, manage device credentials, and much more.

Configuration management comes with several pre-defined configuration tasks and the option to create custom tasks. Additionally, configuration management ties into your alert center, allowing you to communicate the success or failure of a task or when changes are detected on a device.

REMEMBER

These services allow you to download and store device configuration files in an independently secured repository, keeping them readily available for comparison and restoration on a device.

Configuration management not only reduces the time and effort required to maintain device configurations and changes, but also it provides increased security, compliance, and visibility. Additionally, it reduces the risk of costly network downtime.

Viewing Log Data

Logs, when configured and used properly, are a source of truth and audit trails across the company infrastructure. *Log management* is critical for the reliable storage, classification, and analysis of logs, allowing administrators to quickly find the root cause analysis of an operational issue or investigate on threat actor activity. This is usually a daunting task because log files come from many different sources, in different formats, and in massive volumes. Just about everything in your IT environment has some kind of log.

Your ITIM solution should offer the ability to automatically collect, custom filter, alert, and display data from different types of logs, such as Windows Events Logs and System Logs (or Syslogs). Seeing log data reports and dashboard views alongside other monitoring data can help detect meta trends like log volume changes. An integrated log management and archiving function also helps your organization manage costs by avoiding tool sprawl.

REMEMBER

Log files contain a wealth of information to reduce an organization's exposure to intruders, malware, damage, loss, and legal liabilities. If your organization is required to follow regulatory compliance standards such as The Sarbanes-Oxley Act, Basel II, The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Gramm-Leach-Bliley Act (GLBA), The Federal Information Security Modernization Act of 2014 (FISMA 2014), Payment Card Industry Data Security Standard (PCI DSS), and National Industrial Security Program Operating Manual (NISPOM), you'll need to collect, store, analyze, and monitor log data.

To conform with regulatory requirements compliance, you should be able to filter and archive logs to any storage locations for any retention period and preserve historical data. You should also be able to automate the formatting, generation, and distribution of compliance reports.

IN THIS CHAPTER

- Looking at the criticality of HTTP monitoring
- Provisioning communications services
- Staying compliant
- Solving issues with ITIM
- Monitoring your website, email, and database

Chapter 5
Looking at Use Cases for IT Infrastructure Monitoring

IT infrastructure monitoring (ITIM) is an interesting animal. A good solution comes with all kinds of things you can do right out of the box. But every network is different; most networks are unique. The great news is that your ITIM solution can be adapted to your network's needs.

ITIM is like a box of paints, and your network is its canvas. The network administrator equipped with these paints and brushes is an artist who can make the ITIM solution do anything they want. That is the beauty of ITIM.

Picture yourself sitting down in the morning trying to access your email or going to your company's website, only to find your laptop isn't connecting. These types of nuisances are far less likely to happen with ITIM in place, and, if they do occur, they can be detected and resolved quickly. In the case of the website, ITIM can resolve it if it's an internal problem, or it can alert the web provider if it's a problem on their end. This is just one of many ITIM use cases. We explain this use case and others in this chapter.

Website Monitoring

Imagine you own a bicycle store — one of many in your community. You suddenly find customers aren't coming in the numbers they once did. You scratch your head and wonder until a longtime customer drops by and tells you your website is down. How much business have you already lost because people searching for bikes, parts, or services can't find you? It's hard to quantify, but it clearly adds up to lost money and customers.

Website monitoring is essential to ensure adequate performance. Having website monitoring that you own and can control and configure is a much better option for most companies than buying a service. Even better, you should have website monitoring built into a broader ITIM solution that already does the following:

- Tracks the performance of your overall network
- Creates alerts when problems are found
- Reports on overall health as well as specific areas of the network
- Offers a historical view

In this scenario, the website is just one more thing you can track. That data flows into the ITIM interface that your IT staff is already using to drive alerts and reports and to support remediation.

By adopting more advanced network traffic monitoring, such as with Progress Flowmon, you can expand the set of collected metrics to

- Network Round Trip Time
- Server Response Time
- Retransmissions

This way you can easily distinguish between network delay and application delay, or performance degradation due to connectivity issues resulting in retransmissions and degraded user experience. Through integration with WhatsUp Gold, these metrics can be consolidated in a single dashboard provided by the ITIM solution.

REMEMBER

Even a slow website will turn customers away. Too many businesses set up websites and don't monitor how they perform. Your website is too critical a resource to waste. It's increasingly core to your business because it's the main way people find you, learn more about your products and services, and interact with you once they buy something. It's the face of your business and not something about which you should adopt a laissez-faire approach.

Voice over Internet Protocol

Voice over Internet Protocol (VoIP) allows for the delivery of voice communications over Internet Protocol (IP) networks. Think of it as a replacement for traditional telephone lines. Telephony is no longer a separate set of communications infrastructures but is more often simply part of your network. Calls that crackle and break up are no way to communicate so your network must not only be available but also have the bandwidth available to handle your company's needs for professional call quality.

Fortunately, ITIM can often measure your network's quality of service (QoS) and determine if it can support the volume of calls and call quality your company demands when telephony runs across your LAN and WAN infrastructure.

If you're using WhatsUp Gold, it comes with a VoIP monitor that works with Cisco IP Service-Level Agreement (IPSLA)-enabled systems that track your infrastructure for quality and performance. The WhatsUp Gold tool can help you discover

- The level of jitter
- The amount of packet loss
- Latency
- Other performance issues

TIP

To find out more about WhatsUp Gold and VoIP monitoring, visit `www.whatsupgold.com`.

THE IMPACT OF DOWNTIME

Many organizations are unaware of the following statistics:

- After waiting as little as two seconds for a page to load, 87 percent of web visitors will abandon your website.
- The ideal load time is no more than one to two seconds.

A study by Akamai discovered that nine percent of the visitors to a website will never come back if they find that your site is down. This phenomenon is called *permanent abandonment* — something you clearly don't want to face. If you're using your website to sell products, this abandonment can account for nearly a 10 percent loss of your business.

Downtime also impacts your Google ranking. Consider these facts about Google:

- Google's goal is for its own pages to load in less than half of a second.
- If you rely on Google reviews, Google gives extremely slow websites negative rankings.
- Because Google bots can't find your site, your ranking goes down.
- While your site is down, Google will drop you from the Google index for that duration.
- If your site is down for several days, Google may de-rank your site completely, and you'll have to start your search engine optimization (SEO) journey all over again.

Auditing and Compliance

Most organizations are subject to yearly, or even quarterly, IT system audits. If you're unfamiliar with the topic, an IT audit involves hundreds to thousands of individual requirements, most of which need you to provide evidence that you're compliant. ITIM simplifies this process by providing easy-to-digest reports that serve as the required compliance evidence.

Email Monitoring

Despite the rise in text and social media, email remains the king of business communications. Without email, your business comes to a stop. There are over four billion email users globally, and people send over 300 billion emails each day. In fact, an office worker on average will send and receive over 125 emails each workday.

So, what happens if your email goes down or slows to a crawl? Not much gets done. And the longer it takes you to find out that your email is down or slow, the more business is lost — potentially for good.

Despite the rise of cloud email services, much of this email is still handled by mail applications installed on on-premises servers. As with any other business-critical applications, you should be monitoring their availability and performance. This watchful eye enables IT to spot email problems before they turn into a disaster.

Watching your email system is just one of the many things a good ITIM solution can do. The ITIM tool monitors your entire network so it already understands where the problems may lie that are impacting your email system's performance. Through action-enabled alerts, the monitoring quickly resolves these problems. When equipped with application monitoring, an ITIM solution makes sure that critical applications are performing properly, and when they aren't, the solution helps you get them up to snuff.

To maintain email availability and proper performance, you need more data than just whether the email server is up or down. A monitoring solution like WhatsUp Gold gives you a thorough view of key processes and performance indicators and alerts when a process needs attention. Visit `www.whatsupgold.com` for more information.

Database Monitoring

Databases have long been a core business application. These days, databases do even more heavy lifting — even serving as a repository for all your company's critical information. And that includes both structured and unstructured information. When a customer asks a question, you go straight to the database for an answer.

So, when that database is slow, or even worse, completely down, those questions aren't getting answered in a timely matter or at all. At the same time, employees aren't discovering product information or making sales updates. These issues can cripple your business.

More often the database is slow because of application or network issues. While not exactly crippling, this issue can cause great harm to productivity and is certainly frustrating for customers who must wait on an answer.


TIP

The solution is database monitoring, which keeps steady and detailed tabs on how the database application is operating. When your ITIM solution notices a problem, it finds out exactly where the trouble lies. The idea is to spot issues before they turn into actual failures.

Microsoft SQL Server is one of the most popular database management system (DBMS) solutions, so we use that as an example to describe the ins and outs of how database monitoring works. SQL Server monitoring keeps track of the following:

- **Monitors critical SQL parameters:** Customizable alerts are available for the state of CPUs, amount of memory free, disk utilization, page buffers, cache utilization, system processes, transactions, wait locks, and users. You can also define custom threshold parameters that apply to any performance counter you want to track.
- **Tracks SQL service availability:** Checks all SQL services for availability through a dashboard that can monitor the SQL Server database engine, reporting service, indexing and search services, and more. Alerts report on issues, while automated actions can resolve them.
- **Provides SQL query reports:** The query monitor reports on the output of SQL Server queries, showing how well the DBMS performs its job. Alerts or actions can be triggered if a query fails or comes back with an unexpected result.

Certificate Discovery and Monitoring

A single expired SSL certificate can disrupt critical services, erode customer trust, and trigger a series of avoidable issues. SSL certificates are essential for secure communication between your servers and users. However, they can be easily overlooked until they expire. When that occurs, users may see browser warnings, APIs may fail, and services may go offline. The cost? Lost revenue, damaged reputation, and a lot of stress.

This functionality is more than just a checkbox on a release note; it's a proactive safeguard designed to help you spot certificate issues before they escalate into business problems.

WhatsUp Gold has automated the process of discovering and monitoring SSL certificates across users network. This means you can

- Automatically detect devices with SSL certificates during network discovery
- Monitor certificate expiration dates and receive alerts when a certificate is about to expire
- Avoid outages caused by expired or misconfigured certificates

Say your organization operates a customer-facing portal that relies on a secure HTTPS connection. One of the backend servers has an SSL certificate set to expire in 10 days. Without proper monitoring, this could go unnoticed until the certificate expires, leading to customers facing security warnings and error messages.

With WhatsUp Gold, the SSL Certificate monitor flags the issue during its routine check. You receive an alert, renew the certificate, and the portal continues to run smoothly. No downtime. No angry calls. No lost business.

This is the kind of quiet win that IT teams love, problems resolved before they become headlines.

IN THIS CHAPTER

- Identifying the most critical business needs
- Exploring the benefits of a unified monitoring approach
- Understanding the criteria for an ITIM solution

Chapter 6
Considering Your Needs when Choosing an ITIM Solution

Your network is your business. IT infrastructure monitoring (ITIM) helps you to stay in business. The more you know about the state of your network, the more you can assure internal and external users that your whole company infrastructure can achieve performance and availability goals.

TIP

Generally, you want to look for a solution that's easy to use but also fully featured. Particularly, you want a solution that

- Lets you see the real-time status on a dashboard
- Enables secure, role-based, remote access to the system
- Has configurable alerts
- Offers full reporting features
- Allows for the automation of recurring tasks, either innately or via an application programming interface (API)

- Supports all key protocols, starting with Simple Network Management Protocol (SNMP) and Windows Management Instrumentation (WMI)

This chapter gives you the information you need when choosing an ITIM solution.

Recognizing the Top Critical Business Concerns

You want extremely happy IT shops and business owners, right? To satisfy those folks, you need to address their basic concerns. At the top of most professionals' lists are the following critical business needs:

- The need for proactive management of the overall IT infrastructure and network resources
- The need to reduce troubleshooting times
- The need to lower incident rates
- The need to raise the level of service and ensure a positive experience for all users
- The need for improved, trained, skilled, efficient, and effective workers
- The need for automation to reduce human error and workload on workers

REMEMBER

If you can meet the first four needs, but the last two are nearly impossible to attain, you may burn out the team you have and be left with no one to service your clients. Keep working toward satisfying all these needs and striving to maintain and support effective workers.

Taking Advantage of a Unified Monitoring Approach

To address critical business issues, IT teams seek flexible and unified monitoring tools to help control complexity. In a typical multi-vendor, distributed environment, nearly all IT

components support a wide range of protocols that are used to gather data. Unified IT monitoring tools use these protocols to provide end-to-end visibility of servers, storage, networks, and applications; wireless usage and its relationship to users hard-wired into the network; and the configuration of most of these devices, as well as their interrelationships.

TIP

The unified monitoring approach results in several key advantages:

- A proactive IT posture
- Much faster problem resolution
- Improved service levels
- Reduced business costs associated with
  - Licensing of essential software tools
  - Maintenance and reconfiguration of those tools
  - The costs of training and upgrading the skills of the folks who need to work with the tools

Selection Criteria for an ITIM Solution

The criteria you use to identify the right ITIM solution for your organization should contain certain line items. Use the following questions to guide you:

- For you and your organization, what's the approximate value of the intellectual property you have exposed on the network? How long could your business survive if this data was inaccessible?
- Based on the size department you have, will you be comfortable using a host of tools, or do you want a single, customizable dashboard that uses a unified approach to monitoring all your critically important resources? ***Note:*** Studies have shown that the more tools an IT team uses, the worse is their mean time to repair (MTTR).

  MTTR is the standard measure of the maintainability of repairable items representing the average time required to repair a failed system or component.

TECHNICAL STUFF

- Are you interested in automatically updating your network topology map and discovering all your assets automatically or on demand?
- Are you interested in having a regularly updated inventory of all devices with an IP address?
- Do you want to monitor all critical applications, servers, storage devices, or virtual machines (VM) on your network whether they're on-premises or in the cloud?
- Are you subject to IT audits or need to access, view, or manage device logs for root cause analysis?
- Are you required to provide your leadership or management with reports on the status of all devices on your network?
- Do you need to monitor and manage the configuration and preferences of each device?


TIP

To further help you choose criteria for your ITIM solution, check out this buyer guide: www.whatsupgold.com/resources/ebooks/it-monitoring-buyer-s-guide. You can also review these case studies:

- **Education:** `www.whatsupgold.com/danville`
- **Healthcare:** `www.whatsupgold.com/calgary`
- **Finance:** `www.whatsupgold.com/asb`
- **Government:** `www.whatsupgold.com/pleasanton`

ATTAINING BUSINESS INFORMATION WITH WhatsUp GOLD

When you're considering a solution to monitor your distributed and complex networks, take a look at WhatsUp Gold. It delivers comprehensive and easy-to-use ITIM that allows you to turn network data into actionable business information. By proactively monitoring all critical network devices, applications, and services, WhatsUp Gold reduces costly and frustrating downtime that can impact your business.

With its browser-based interface, WhatsUp Gold lets you take control of your network infrastructure and applications for the important strategic work that drives results. In a marketplace overwhelmed with complexity, WhatsUp Gold provides simple deployment, robust scalability, award-winning usability, and a fast return on investment.

WhatsUp Gold offers an easy-to-customize reporting environment. You can select from hundreds of out-of-the-box views or easily create drag-and-drop dashboards that provide a quick assessment of overall IT health — even detailed drill-down dashboards to isolate the root causes of performance problems. These dashboards can help you quickly resolve performance problems across your organization. Real-time performance monitors provide for extremely granular reporting when troubleshooting or isolating an issue. These reports can be added to any dashboard view and configured to display real-time statistics for any performance monitor.

WhatsUp Gold also features integrated inventory reporting, including hardware inventory, reports on installed software and updates, and more. These automated reports save time, decreasing year-end IT inventory activities from weeks to minutes. The reports also help you find underutilized hardware resources that can be redeployed and can identify unlicensed software to avoid expensive true-up costs.

For more in-depth information, visit `www.whatsupgold.com`.

IN THIS CHAPTER

- Using one solution
- Deploying ITIM
- Learning that less is more
- Turning alerts into actionable items
- Scheduling reports

Chapter 7
Ten ITIM Best Practices

Installing and deploying an IT infrastructure monitoring (ITIM) solution is a good start, but you still have more to do. Ongoing monitoring gives you better results when you follow some simple, common-sense best practices. Like everything else in IT, "garbage in equals garbage out." Use the best practices in this chapter as a guide to get the most out of your ITIM solution, and you'll find and fix problems before your end-users even notice.

Replace Multiple Monitors with One Solution

Having a "single source of truth" that's accessible to the entire team is crucial to the long-term success of your IT responsibilities. If the network team is using one tool, your system administrators are using another, and your application team yet another, there is certain to be conflict and finger-pointing. By consolidating all your monitoring to one solution, your various IT teams have the opportunity to build more collaboration and share accountability. In addition, having a single solution can dramatically reduce costs.

Figure Out Where to Deploy ITIM

We often get the questions "Where can I" or "Where should I" deploy my ITIM solution? Generally, if the operating system can reach the systems you want to monitor, it doesn't matter where it's deployed.

We've worked with customers that deploy their solutions inside their Amazon Web Services (AWS), Microsoft Azure, or other cloud environments. We've even worked with customers that told us their solution runs on a system under their desk.


TIP

Basically, the best advice is to deploy your monitoring solution in a place that enables it to be highly available while still being able to reach all the distributed systems you want to monitor.

Make the Tool Work for You

All ITIM solutions require some form of manual configuration. However, configuring the solution in a way where it can do as much of the work for you is critical to your long-term success. Boost your success by asking yourself these questions:

- Do you know what needs to be monitored on each device? Ensure your monitoring system knows that or can be configured so it does.
- Do you know which network segments may get new devices? Configure your monitoring solution to scan those network segments automatically.
- Do you have recurring issues that require someone to log in and fix them? Automate those with your monitoring solution.

Spend the Time and Effort to Configure It Right

The initial time and effort put into infrastructure monitoring directly translate to how well it will work for you. This seems like a contradiction to "make the tool work for you" — but it is directly related. When you begin to implement your ITIM solution, the

focus you dedicate to configuring the solution properly will translate into long-term time savings.

For example, you could manually run a discovery every morning and use your time doing so — or you could set the application to automatically schedule that same activity and only be notified if it needs your attention. Even saving five minutes a day could translate to 30 hours each year.

Know What to Monitor

In Chapter 2, we discuss what monitor types exist and how they should be applied on different infrastructure components. Here, we give you the best practice on what to monitor.


TIP

Honestly, there's no specific answer for what to monitor. Each environment is different. But in general, make sure availability, as well as performance, is looked at for any system that can cause some outage where either people can't work or you risk the business losing revenue or budget.

For example, what happens if a critical system becomes unavailable, and your employees and customers can't connect? Obviously, that's going to cost you financially because you can't process payments or perform other economic or productive functions.

Don't just have a narrow view of your network. Track switches, routers, and other dedicated network devices. But the network is far more than that. The network encompasses the web, which you may well want to monitor (we discussed this in Chapter 6). Your applications run on servers across the network, and both could be monitored effectively with your ITIM solution.


REMEMBER

Think of what's most important to your business and most critical to your operations and revenue-generating activities, and find a way to monitor it.

Less Is More when Sending Alerts

We always tell customers that in terms of a best practice for alerting, less is more. Here is a perfect example of "crying wolf." We worked with a customer who was repeating the same actions every

two minutes. When a system became unavailable, they would get an email alert when it was down for a minute. Every two minutes after that, the ITIM tool kept emailing them. They grew accustomed to that sort of pattern, and soon people just started ignoring the alerts. When there are too many alerts, people tune them out and ignore them, and if something critical comes along (the wolf) it's likely to be missed. That's just the reality.


TIP

Only send emails to people who must log in and perform a task on the system. Anything more than that is just spam. And we all know how folks feel about spam.

Performance Alerts Should Turn to Action

Make sure any performance alarm that occurs gives you something actionable. Take CPU utilization, especially in a virtual environment. Many admins want an alert if CPU usage exceeds 90 percent for 30 minutes. But that is a bad idea because it's a normal state for a well-designed infrastructure. If you're alerted at the 90 percent threshold, the natural inclination is to want to log in and take action to address that type of situation, such as stopping a process to free up more CPU. However, you're supposed to size systems in a virtual environment, so they're running at near capacity.


TIP

If a CPU is running at 99 percent or greater for 30 minutes, we recommend sending an email about that because it gives you potential action you should take. You may log in and stop a process in that scenario.


REMEMBER

The key best practice when it comes to actions is ensuring you're only notifying people when they can *do* something. Don't just notify for the sake of notification. Instead, notify to alert someone that they need to log in and fix an issue. Check out Chapter 3 for more information on alerts and actions.

Even without alerts, the ITIM solution is still gathering key information, and you still get that information when you're looking at your ITIM dashboards or reports. It's just not sending you danger alerts about doing something right away when you don't need to.

Set Up Your Reporting Rules

Setting up reports is really based on a case-by-case decision in terms of what you and your customers need to see. There's no one-size-fits-all approach, which is why the flexibility of ITIM reporting is so crucial. The good news is that ITIM reporting is a blank slate — you can do almost whatever you want with it.


TIP

Start with defining your requirements, how often you need reports, and what you want them to cover. One of the most common use cases we see is reporting on uptime for the previous month and sending that to management. In many cases, IT success is measured based on the percentage of the availability of the systems IT is responsible for.

We also see people run daily reports about network bandwidth utilization, giving them a close view of their performance and allowing them to easily spot any traffic that is outside of expectations. Others want to see the same information every day about disk space usage. It all depends on the individual, team, or scenario.

Schedule Your Reports

Properly scheduling your reports is critical. You want to be able to get the data frequently enough that you can take action and track it long enough that you can see trends. Report frequency depends on the criticality of the function and history of events and issues. Schedule the ones you *must* grab often.

Reports can also have various levels of detail. A person whose job directly involves working on the network gets more detailed reports. Then higher-up executives within the company get a less-detailed report that looks at the overall health of the network. Those reports, especially if you look back in a historical way, help guide the future architecture of the network. You can see where your company is, know it is growing a certain amount, and plan to ramp up capacity.

Make Sure ITIM Can Scale

Making ITIM scale goes hand in hand with having one solution. How can you have one solution if it does not scale? For example, an ITIM solution may be able to monitor only a certain subset of your network before requiring a separate instance. When deciding on which solution to use, it's important to figure out how well it can scale to your network's needs as well as if there are any additional costs associated with the scalability of the solution.

For example, WhatsUp Gold has various editions and deployment options available to help scale your ITIM. For most companies, a single WhatsUp Gold server is all that's needed. For larger businesses or enterprises, IT has the option of deploying multiple WhatsUp Gold servers in a distributed architecture.

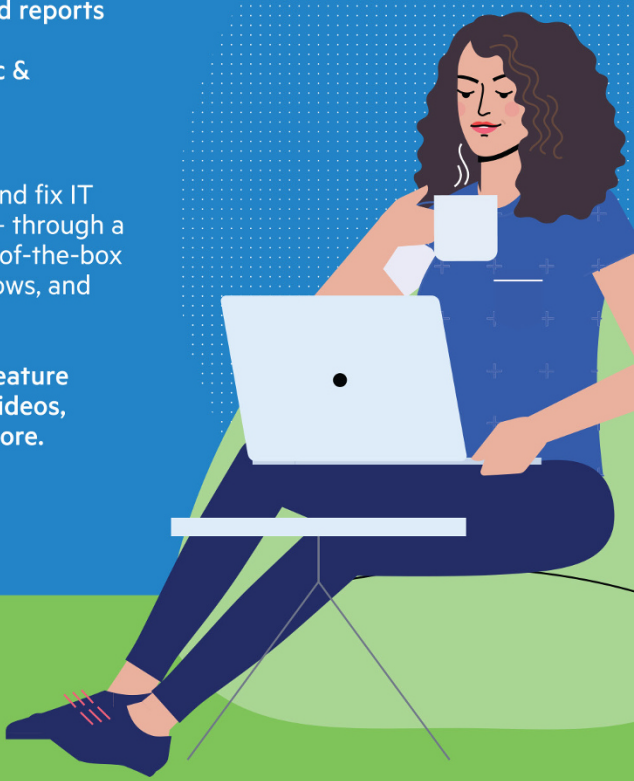
Progress® WhatsUp® Gold

Simplify the way you manage your IT infrastructure

- Automatically discover, map, & monitor device dependencies
- Quickly identify & proactively resolve issues in your hybrid network
- Improve productivity through alerts, dashboards, & scheduled reports
- Optimize network traffic & bandwidth utilization

WhatsUp Gold lets you find and fix IT infrastructure problems fast – through a powerful combination of out-of-the-box functionality, intuitive workflows, and system integrations.

Visit our website today for feature overviews, success stories, videos, demos, a trial version, and more.



www.whatsupgold.com

Monitor network availability and performance

If you're wondering about ITIM, now is the time to learn more. An ITIM solution monitors your entire network. In this book, you discover ITIM software through practical examples, abundant tips, and a breakdown of the benefits. Progress WhatsUp Gold is ITIM software that finds and fixes IT infrastructure problems through a combination of out-of-the-box functionality, intuitive workflows, and system integrations. You can see up/down availability and performance at-a-glance for everything connected to your network.

Inside...

- Understand IT infrastructure monitoring (ITIM)
- Monitor beyond networks
- Discover reporting and dashboards
- Recognize top business concerns
- Increase IT visibility

Progress® WhatsUp® Gold

Doug Barney was the founding editor of Redmond Magazine, Redmond Channel Partner, Redmond Developer News and Virtualization Review. **Mark Towler** and **Larry Goldman** have decades of experience working with hardware and software technology companies to find their customers' pain points.

ISBN: 978-1-394-20427-4
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.