

Application Playbook: **Exchange Monitoring** for IT Pros



APPLICATION PLAYBOOK: EXCHANGE MONITORING FOR IT PROS






Applications make up the backbone of every business, from small companies to large corporations. Countless internal applications enable these businesses to function. There are applications used by employees, and application servers hosted by IT teams that deliver business and IT services. IT teams in every organization are responsible for keeping applications and the supporting infrastructure readily available and performing optimally.

This is not an easy job. All IT professionals have been there. They've received the dreaded help desk call from an end-user wondering why email is running slow, or reporting an outage (every IT pro's nightmare).

IT teams are responsible for keeping email, Web applications, and other internal applications, like SharePoint®, up and running. This eBook will discuss the best practices for monitoring Microsoft® Exchange™ to help you troubleshoot performance issues faster.



TABLE OF CONTENTS

	When IT Becomes a Reactive Service	4
	How to be Proactive	4
	What to Monitor in the Exchange Environment	6
	How to Set Up Effective Monitoring	9
	How SolarWinds Can Help	11



IT AS A REACTIVE SERVICE

As we grapple with Exchange issues every day, the two questions most of us want the answers to are, “What is the root cause?” and “How do we prevent this from happening again?”

Historically, IT has been a reactive service. Unfortunately, the IT team often reacts to issues rather than preventing them. Most IT departments are short-staffed with an ever-increasing workload, which forces most IT pros to behave more like fire fighters. We just put out fires, and barely have enough time to take on any truly innovative projects. So, let’s take a step back and think about this a minute. Obviously, it would be more efficient in the long run to be proactive. If we were able to take a proactive approach, it would free up time for us to focus on important projects. It would be great to know about the fire before the dreaded help desk call comes. Getting a head start on addressing the fire while it’s still just a spark could help minimize any negative impact on the business.



HOW TO BE PROACTIVE

There is a way to be proactive. It’s by utilizing the various monitoring and alerting tools that are currently available. Each has pros and cons, depending on what your budget and scope is. Anybody can download and set up monitoring software alerts. However, to get real value from these tools you need to assess your needs. Ask yourself the following questions:

- What are you monitoring and alerting for? Be specific.
- What key indicators or triggers do you need to be alerted about?
- What are the thresholds, if any?
- Who needs to be notified, and how soon and often?

The assessment process can take days and even months to fine tune. If you set all your alerts without any fine-tuning, you will get overwhelmed with alerts that become virtual white noise. If you aren’t getting enough alerts you could miss an opportunity to avoid an issue, which presents no value to the monitoring

tool. What's the point of alerting if you are not paying attention? The key is finding the right balance to be successful in a proactive IT shop. Your monitoring tool should be able to provide you with flexibility and customization to set up alerts that will only trigger based on advanced conditions, such as:

- Correlated events happening for correlated events (only when X and Y events happen simultaneously).
- Group-based alerts (only when all objects of the group go down).
- Only when an error exists for a sustained period of time.

Monitoring is more than making sure that your server is ping-able. Monitoring and alerting are not only about the server, but also about knowing what that application running on the server is doing. It involves viewing the whole picture, inside and out, to help you keep and maintain your SLA.

IT pros need to understand what the applications are doing, when they're doing it, and why.

- Why are RPC requests taking so long on a mailbox server?
- Is it a network issue or disk issue?
- Why did my scheduled SQL query fail overnight?

With application monitoring, we can receive alerts when these issues happen and correlate them with other events that may have happened on the server. This keeps those fires from happening, and helps the team determine root cause.

Understanding the behaviors and patterns of our servers and applications may even help predict what will happen. For instance, predictive analysis can help detect failing disk drives for servers and storage arrays. There are even monitoring tools that will predict how much storage growth you will have, and when you will run out of storage, based on your usage patterns. Predictive analysis can examine workload trends, CPU/hardware utilization, and application errors/warnings and correlate them to determine if there will be an outage. Predicting a potential issue can prevent unwanted outages, which means fewer headaches for the IT team.

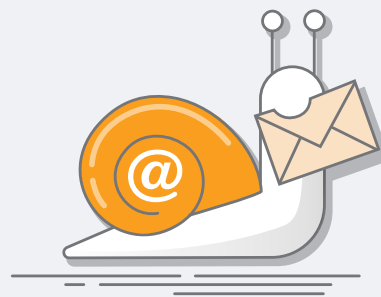


WHAT TO MONITOR IN THE EXCHANGE ENVIRONMENT

When troubleshooting any issue, regardless of the application or system, you should always check your application and system logs. These should be the first places you go to check for warnings and errors. Often, application and systems errors will be captured as warnings and errors in the event logs. If your monitoring tool has the ability, you can even trigger it to alert you on specific event IDs. These event IDs are the first indications that you may have a possible issue.

Answering the million-dollar question: Why is the email slow?

When you get the help desk call demanding to know why email is slow, it's frustrating. Almost anything can cause email to run slow. It could be the local computer. It could be network latency, or a server side issue.



When troubleshooting a complex issue such as this, always check the performance counters that you are monitoring. These counters will indicate if there are latency or performance issues. Knowing the right key performance counters to look at will help you determine whether the issue is on the client or the server side.

Here are some key metrics that you may want to monitor and receive alerts about if they exceed defined thresholds:

- **MSExchangeIS\RPC Requests** (lower than 70): Indicates how many threads are currently in use.
- **MSExchangeIS\RPC Operations/sec** (Always higher than RPC Requests): Number of operations the server received in the past second.
- **If MSExchangeIS\RPC Requests** is increasing fast and the MSExchangeIS\RPC Operations/sec stays stable: Indicates that the server cannot process client operations fast enough, or is having performance issues. This points to the exchange server as the source of slow running email. When all RPC threads have been exhausted, clients are not unable to submit new requests to the server until all threads are released.

- **When MExchangeIS\RPC Requests and MExchangeIS\RPC Operations/sec** are either low or at zero: Indicates that the exchange server is not the source of the problem. Instead, it is most likely coming from an external source, such as Active Directory®, the network or a client-side issue.

You also will want to look at additional counters, such as memory and disk activity. For example, if the disk performance counters are above the thresholds, the exchange server could be suffering from disk issues. You could have failing hardware or simply not enough spindles.

- **Database disks**
 - PhysicalDisk\Average Disk sec/Read – less than 20ms.
 - PhysicalDisk\Average Disk sec/Write – less than 20ms.
- **Transaction logs disk**
 - PhysicalDisk\Average Disk sec/Read – less than 5ms, spikes no higher than 50.
 - PhysicalDisk\Average Disk sec/Write – less than 10ms, spikes no higher than 50ms.
- **Log buffer**
 - Database\Log Record Stalls/sec – below 10 per sec, no higher than 100 per sec.

If you are seeing high CPU utilization for your Client Access Servers, this can also be causing the problem. The RPCClientAccess.Service.exe process consumes excessive CPU resources. This can be caused by many things, such as a bad iOS code on mobile devices, or 3rd-party archiving software that is integrated with Exchange. Sometimes it's as simple as antivirus scanning on the exchange servers that is causing the overconsumption of resources.

When you've ruled out client-side configurations, network latency, and Exchange server-side as the source of issue, you should look at Active Directory.

Exchange depends on Active Directory (AD). It uses the Global Catalog domain controllers. When there is an issue on the Active Directory side, this can negatively impact Exchange. As part of your troubleshooting, you should investigate

CPU, disk, and memory bottlenecks on the Active Directory servers. But there are also AD-related counters on the Exchange servers. To determine if there is an Active Directory issue affecting Exchange, use these counters found on the Exchange servers performance monitor:

- **SMTP Server\Categorizer Queue Length** should not be greater than 10. This shows how SMTP is processing LDAP lookups against global catalog servers. If the value is greater than 10, and is increasing, this can point to slow global catalog servers. Keep in mind that this value can go slightly high if large distribution lists are being expanded.
- **MSExchangeDSAccess Process\LDAP Read Time** (for all processes) shows how long an LDAP read request takes to be fulfilled. The average value is around 50ms and should not exceed 100ms.
- **MSExchangeDSAccess Process\LDAP Search Time** (for all processes) shows LDAP search request takes to be fulfilled. Similar to the LDAP Read Time, the average value is around 50ms and should not exceed 100ms.



HOW TO SET UP EFFECTIVE MONITORING

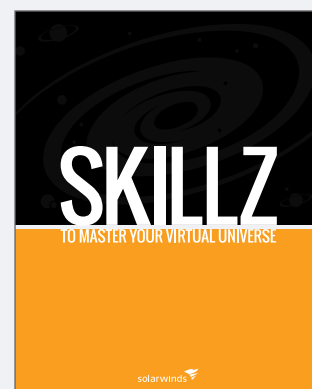
Now that we have seen why you have to monitor Exchange, and what you have monitor to be alerted of performance issues, let's look at how to actually set up this monitoring. You cannot anymore resort to manually building scripts or investing considerable time customizing open source technology and free tools as a workaround. The opportunity cost is very high with free tools. You will end up spending more time managing the tool than actual Exchange administration and troubleshooting.

Based on your IT budget, evaluate and select an application monitoring tool that not only monitors Exchange, but also monitors other critical applications that run in your environment. The standout feature should be ready value, automation, and, more importantly, less manual intervention. You want a monitoring tool that hits the ground running, one you don't have to constantly meddle with.

Make sure your monitoring solution supports the latest version of Microsoft Exchange. You may never know when you will have to upgrade to a newer version. Your monitoring tool should be able to support that. Whether you have Exchange deployed on a physical server or a virtualized server, if the monitoring tool can provide visibility into the health of the underlying infrastructure, it'll make Exchange troubleshooting much easier.

Once you have selected the tool you need for the job, you have to make sure you set it up and let it run in such a fashion that it won't require your constant intervention, or send you hundreds of alerts about things you really don't care about. This can be achieved by looking at monitoring as a discipline.

There are four ways to break monitoring down. As Kong Yang, Head Geek® at SolarWinds, explained in the eBook, **Skillz to Master Your Virtual Universe**, you can look at implementing the DART framework. This is a very simple, but highly streamlined and effective discipline of setting up monitoring. It only involves four steps:



- 1. Discovery:** This can be achieved if your monitoring tool supports automated and scheduled application discovery. As your IT environment grows and configurations change, there will be many applications and servers on your network that you won't monitor on a daily basis. Without having to find them and add to the monitoring tool every now and then, you have to program the monitoring tool to do this automatically.
- 2. Alerting:** This is a very important part of monitoring. You cannot build all alerts from scratch. A lot of this depends on the out-of-the-box value of the monitoring tool you choose. What is important is the flexibility you have in customizing these alerts according to your alerting conditions. You may choose to get alerted only when a certain condition exists, or when a specific error has sustained a threshold time period. This is what is going to prompt you to respond to a situation, or proactively warn you that something looks like it's going to break or go bad.
- 3. Remediation:** Remediation cannot be separated from application monitoring. With the evolution of monitoring tools, there are many remediation actions built into monitoring tools that allow you to remotely address infrastructure issues. What if you could reboot the server remotely, or terminate some runaway processes in the server running Exchange? It's possible with monitoring.
- 4. Troubleshooting:** This is needed to get the service and supporting applications up and running. To do this quickly, you need deep performance insight to be able to isolate the root cause of the issue that impacted the application in the first place. If monitoring is intelligently set up to help you pinpoint the root cause quickly, troubleshooting goes much quicker.





HOW SOLARWINDS CAN HELP

SolarWinds® Server & Application Monitor (SAM) is an affordable tool to monitor the health, availability, and performance of your applications and servers (physical and virtual). Benefit from out-of-the-box support for **over 200 applications**, including Exchange, AD, SharePoint, Windows, Linux®, VMware®, and more.

Exchange Monitoring with SAM



Deep monitoring of Microsoft Exchange. Supports various Exchange versions, including 2013, 2010, and 2007.



Identify mailbox issues, such as high RPC requests, RPC averaged latency, database I/O read & write, information store issues, replication status of database availability group.



Receive automatic alerts when specific users' mailboxes reach allocated usage space.



Use ready, built-in templates to monitor the health metrics of client access role, hub transport role, edge transport role, and mailbox role.



Monitor critical Exchange processes and services, and explore event log messages for further insight.



Diagnose network traffic packets to analyze if there is any network latency reported for email traffic (SMTP, POP3, IMAP, etc.).



Visualize contextual dependency and relationship of Exchange with other applications, databases, and underlying physical server and virtual infrastructure.



Monitor server performance, response time, hardware health, and resource capacity metrics.

“This product is reliable, easy to use, and provides a whole lot of features at my fingertips!”

John Shook,
IT/Systems
Administrator, ACSI

“When our production mail server node went down, the SolarWinds SAM helped us find where the bottleneck was—in the cluster or in the application.”

Purushothaman Samikannu,
Consultant,
Telekom Brunei
Limited

[DOWNLOAD FREE TRIAL](#)
[LEARN MORE](#)
[VIEW INFOGRAPHIC](#)

Fully Functional for 30 Days