Using Application Response to Monitor Microsoft Outlook

Microsoft® Outlook® is one of the primary e-mail applications used today. If your business depends on reliable and prompt e-mail service, you need to know about changes in service and performance that may impact your users. You can use Application Response to monitor and manage Outlook performance using data based on actual end-user response times. If you choose to enhance Application Response with eHealth Live Health, you can be notified of problems with real-time alarms.

Benefits

This section provides a high-level summary of the benefits that Application Response provides for managing the performance of Microsoft Outlook. The “Value” sections that follow elaborate on these points and provide sample eHealth reports and Live Status Displays.

Quickly Identify Degradations in Outlook Performance.
When you configure Live Health for Application Response, you can establish levels of alarms from normal to critical. With these levels in place, Application Response automatically notifies IT personnel when Outlook performance begins to degrade through a Live Status diagram (shown on page 3). This warning gives your IT staff time to identify and fix problems before users notice slow response time.

Accelerate Diagnosis of Problems. When Application Response identifies a problem, you can easily determine whether the Outlook slowdown is due to the client, the network, or the server. You can direct the efforts of your IT staff to the appropriate area quickly. In addition, Application Response can identify whether a problem is restricted to a particular user, group, or location, further helping to focus the efforts of IT staff. Drill-down reports (shown on page 4) provide additional troubleshooting details that you can use to investigate the source of the problem. With this information readily available, IT staff can improve the mean time to repair (MTTR) and keep your Outlook users productive with minimal disruption.
Establish Thresholds for Response Time. You can set thresholds for the response time of specific Outlook transactions. Application Response will send an alert and Live Status will display an alarm whenever performance degrades below acceptable levels. To do this, use the response time data that Application Response collects as a basis for determining realistic service goals for Outlook. These service thresholds appear in eHealth reports so you can easily compare current performance to the goal. You can set thresholds to send alerts when performance degrades slightly, when users barely recognize the slowed response time. You can also set higher thresholds for critical alarms, when response time delays are very noticable to users.

Measure The Impact of a Virus on Outlook. The proliferation of e-mail viruses poses a serious threat to Outlook performance, user productivity, and business profitability. By monitoring the current level of new e-mails and comparing it with a baseline of normal behavior, Application Response can warn you of suspicious e-mail activity. This alert gives you time to investigate the problem and act before the virus affects Outlook performance across your organization. During a virus attack, you can use Application Response to measure the impact of the virus on your Outlook users, including who is affected, the number of failed transactions, and the degradation to Outlook response time.

Compare Current versus Historical Performance. You can quickly compare current and historical performance to answer user questions about perceived slowness in their Outlook response times. Application Response records Outlook response times for actual end-user activity, not simulated test results, to provide insight to the end-user experience. You no longer need to rely on anecdotal feedback or perceptions from users who complain that Outlook is “too slow” or that performance seems “worse today than last week.” You can organize the data and reports by user groups, locations, and transaction types to compare the performance over a time range and for similar users or transactions. With this data readily available, you can make decisions and address performance questions based on data, not guesses or personal impressions.

Monitor Outlook Performance When Making Infrastructure Changes. When you make significant changes to your infrastructure, such as upgrading Microsoft Exchange® software, adding users, and increasing network bandwidth, you can use Application Response to compare current performance with past performance to determine how those changes affect Outlook. For example, if you upgrade Microsoft Exchange to a new version or upgrade the server to a new hardware model, you can use Application Response to determine whether the change has improved or degraded response time for Outlook users. You can also use Application Response to monitor Outlook performance after implementing firewalls, installing anti-virus software, or making changes to your network infrastructure (interfaces, routers/switches, and quality of service [QoS] policies).

Improve Capacity Planning. You can improve capacity planning by projecting new equipment needs based on historical trends in Outlook performance degradations. Capacity planners can use this trend information to predict and plan for upgrades to the application infrastructure. For example, if Application Response indicates that server time for Outlook transactions increases when you add new users, you can plan to add an Exchange server to increase capacity.

Value 1: Identify Degradations in Outlook Performance Before Users Notice

Together with Live Health, Application Response can identify and alert you to Outlook performance degradations, providing your IT staff time to investigate and repair problems before users start to notice slow response time. You can set thresholds to send alerts for IT staff when performance degrades slightly, before the decreased response time is very noticable to users. IT staff can investigate and correct the problem promptly.
Receive Immediate Notification of Developing Problems. After you set response thresholds for Outlook, you can use Live Health to monitor its performance. Live Health raises an alarm when Outlook performance factors begin to approach (or exceed) your service thresholds.

When Outlook does exceed an established response threshold, the Live Exceptions notifier automatically sends e-mail or pager messages to the Outlook manager (or the on-call IT staff person). The following sample e-mail is from the notifier, alerting the user to a major alarm for response time.

From: NetHealth User [mailto:george@company.com]
Sent: Thursday, November 06, 2003 8:28 AM
To: outlookAdmin@company.com
Subject: Alarm major Response Time approaching threshold;
service alert orden-pc-Outlook-Reply-Default-Exchange-AP

response 255.255.255.255
eHealth Event Data:
-------------------
[Severity]: major
[Start Time(UTC)]: 1068124980
[Element Name]: orden-pc-Outlook-Reply-Default-Exchange-AP
[Rule Message]: Response Time approaching threshold
[Tech Type]: response
[Variable]: Avg. Response Time
[Problem Start Time]: 11/06/2003 13:23:00
[Problem Start Time(UTC)]: 1068124980

At the same time, icons on your Live Status diagram change color (yellow, orange, or red depending on the alarm severity), alerting you to the severity of the problem.

Figure 1. Sample Live Status Diagram for Outlook

By configuring Live Status to show the components of your Outlook application, you can observe the effect and scope of performance problems. With a quick glance at Live Status, you can determine whether problems affect the application servers, users, client sets (groups of users), and application tasks. A pattern of icons changing color can yield valuable information about the affected resources. You can determine whether an alarm indicates a problem for one or more users, groups, or locations, which business is impacted, and to what degree.

The diagram in Figure 1 shows alarms for a client set, as well as the users in Atlanta and their Outlook tasks. The Application Server group does not show any alarms, so the problem is unlikely to be related to the server. In this case, you should investigate the Atlanta client users first, as described in the next section.
Value 2: Accelerate Diagnosis of Problems

When Application Response indicates a degradation in Outlook performance, you can take full advantage of eHealth diagnostic capabilities to quickly pinpoint the problem. Drill-down reports can identify whether the problem is due to the client, the network, or the server, and whether the problem is limited to a particular application, location, or user group. With this information at hand, you can quickly direct the appropriate IT resources to investigate and resolve the issue quickly, so that users are impacted as little as possible.

Drill Down for Details. The Live Status diagram shown in Figure 1 indicates a problem with Atlanta client sets. From Live Status, right-click a problem icon to drill down to an At-a-Glance report to diagnose the problem. For example, drill down from a response client set icon to investigate the problem for all clients in that set.

In the At-a-Glance report, review the Average Response Observed chart to determine how average response time has changed. Look for a sudden spike in response time or a recent steady increase. The following sample chart shows a steady increase in network response time for the past few hours.

This trend may be the result of a recent problem in the network; perhaps the router connecting the Atlanta users to the application server is having trouble. The clients that use the router are showing increases in network time as a result.

A sudden increase or spike in response time may indicate a failure or recent change in the network. Use the chart to determine when the spike occurred, and look for other system events that occurred at that time.

Also review the Transactions Observed chart of the At-a-Glance report to check for a change in application activity. The following sample chart shows that the transaction rate is decreasing steadily, which is likely to be a result of the increasing network time. Outlook users are probably starting to slow down because they are waiting longer for transactions; this problem is starting to impact user productivity in Atlanta.

While the At-a-Glance report shows the performance of the client set, you should also identify how many users are affected. From any chart on the At-a-Glance report, drill down to a Top N report for a list of the Outlook users who were active during this time and affected by the network slowdown.

The Top N report can help you to determine whether the Outlook problem is affecting one or two users in the client set, or all of its users. This information can help you to further identify the
Using Application Response to Monitor Microsoft Outlook

scope of the problem and can point to the area to examine next.

The following sample Top N report shows that the network response time is high for most users in the Atlanta office. Therefore, you can conclude the problem is not related directly to a specific user but is a problem with the network link between the Atlanta office and headquarters.

Now that you have identified a problem in network response time for the Atlanta office users, you can investigate the network to look for the source of the problem. Use other eHealth products and reports to identify whether the problem is on a router or a specific line between the clients and application servers. For example, you can run a Health report for LAN/WAN or router groups to check for exceptions and situations to watch.

**Value 3: Establish Thresholds for Outlook and Alarm When Performance Degrades**

For the Outlook transactions that you monitor, you can use eHealth to establish service thresholds for response time and other performance criteria. You can set different performance thresholds for each type of Outlook transaction. When the performance crosses those thresholds, eHealth can alert you to the problems.

**Establish Thresholds.** First, create reports that show trends in the performance metrics for each Outlook transaction, such as Outlook-Read, Outlook-Reply, and Outlook-New. Use a report period that shows a reasonable amount of time, such as several weeks or a month.

Run the report for a client set so that you can see the overall performance for a group of related users. Review the report to determine the typical upper and lower boundaries of the data. Look for the pattern of typical behavior, as well as spikes or unusual data points.

For example, the following chart from an At-a-Glance report for a client set shows average response time for the Outlook-Read transaction.

![Average Response Time Chart](chart.png)

For your report, determine the typical response time (shown as the pink line on the chart). You may want a *major* alarm whenever response time exceeds that value.

Also look at the upper extremes or spikes in the data (shown as the red line on the chart). You may want a *critical* alarm when response time exceeds that value.

When you determine these values for each transaction type, use them as the service thresholds in your response service profiles (for reports) as well as your Live Exceptions profiles. This ensures consistent monitoring by Live Health displays and eHealth reports.

**Receive Alarms from Thresholds.** After you set thresholds for Outlook transactions, Live Exceptions uses these thresholds to send alerts whenever response time approaches or exceeds a threshold. Live Exceptions displays an alarm that indicates the severity of the problem (warning, minor, major, or critical) and can send e-mail or pager messages to appropriate personnel to notify them immediately of the problem. Icons on the Live Status display also change color to indicate developing problems. These mechanisms ensure that you receive instant notification of degrading Outlook performance.
Using Application Response to Monitor Microsoft Outlook

**Value 4: Measure the Impact of a Virus on Outlook**

Computer viruses can take many shapes and forms. While many anti-virus programs—and IT personnel—work to identify and stop virus programs before they enter the network, e-mail viruses still find ways to infiltrate organizations.

Virus programs can vary, but most e-mail viruses have a common behavior: they cause a significant increase in new e-mails sent from the infected computer. This increase is usually intended to propagate the virus and create a traffic load that impacts Outlook performance.

Application Response can identify sudden and unexpected changes in the level of new e-mail activity. This capability helps your IT staff to take action before a virus spreads too far and affects Outlook performance. During or after an attack, you can use eHealth reports to evaluate the impact of the virus on application services.

**Detect More New E-Mails Than Normal.**

When a virus attacks, a typical symptom is a significant increase in new e-mail activity. eHealth automatically assesses normal behavior for your Outlook users based on historical data. You can use Live Health to develop rules that look for deviations in behavior from the norm.

For example, by configuring Live Health to raise a warning alarm when new e-mail activity is three times the normal rate, eHealth can alert IT staff to a potential virus.

Likewise, you can configure Live Health to raise a critical alarm when new e-mail transactions are more than five times the norm. You can also configure Live Health to send an e-mail or pager message when the alarm is raised.

**Investigate Potential Virus Attacks.** To investigate an alarm pointing to a possible virus, run a Trend report for new e-mail transactions during the past week. The following sample Trend report shows that the rate of new e-mail transactions (over 0.6 per minute) is more than three times the trend from the baseline (0.2 per minute).

Run the report again after a minute or two. If the high rate continues, investigate the client system for a potential virus.

To further investigate the possibility of a virus, run an At-a-Glance report for the Exchange server and look for changes in behavior for Average Response Time, Transactions, and Bytes (load on the network). If you have the eHealth AIM for Microsoft Exchange on your servers, you can run a more detailed performance report for the server to determine whether the number of messages sent and received has increased sharply. Use Live Status to determine whether the virus is affecting all Outlook users or isolated groups.

**Evaluate the Impact of a Virus.** If an e-mail virus is attacking your organization, use eHealth to determine its impact on Outlook. When the Live Status diagram is configured to reflect your organization, you can quickly determine which areas of your business are impacted and take steps to protect the most critical areas. For example, if Live Status indicates that the virus is affecting Outlook response time for the sales team and the research team, you may decide to focus efforts on the sales team first because the effect of the virus there will directly impact sales and profitability. By receiving alerts of possible viruses early and having the tools to investigate quickly, you can avoid major impact on your business.

**Value 5: Compare Current and Historical Performance To Answer User Questions**

Users sometimes complain that an application feels slower than normal or performance is worse than usual. Application Response can help you to diagnose user perceptions of slow Outlook response and can provide reports that show
whether performance has changed and, if so, how much it has changed.

**Investigate User Complaints.** For example, if a user reports long delays in reading new e-mail, you can run a Trend or At-a-Glance report for the Outlook-Read transaction for the past week. Review the report to look for increases in response time.

![Graph showing trend in response time](image)

In the sample Trend report, response time has a few spikes to 80 milliseconds (less than one-tenth of a second), but this is not a noticeable response delay. In this case, the one-week Trend report does not indicate a significant problem with response time for Outlook-Read transactions.

Running the same Trend report over a longer time period may help to identify a long-term trend in response times. The following sample Trend report for the Outlook-Read transaction over several weeks shows a trend for increasing response time, and much larger spikes in response time.

![Graph showing trend in response time](image)

Now run the At-a-Glance report for the user’s client set to determine whether the performance problem is limited to this one user or is affecting all users in the client set. This report will also show the breakdown of Outlook response time into client, network, and server time so you can further diagnose the problem.

**Make Reports Available to Users.** As with all eHealth reports, you can schedule Application Response reports to run on a regular basis (daily, weekly, monthly, and so on) and make these reports available to specified users. For example, you can configure eHealth to run an At-a-Glance report showing the past week’s Outlook response time for the Atlanta client set every Monday morning. This report can then be e-mailed to the Atlanta branch manager automatically, posted on your corporate intranet where the manager can access it, or made available through the eHealth Web interface. This provides application managers, department managers, and others with up-to-date information about their end users’ experiences with Outlook.

**Value 6: Monitor Outlook Performance When Making Infrastructure Changes**

Application Response can help you to identify how changes to your Outlook infrastructure (such as adding a remote office) impact response time. This involves the following process:

- Review historical Outlook performance.
- Make the change on a small scale or in a test environment.
- Test the impact of the change.
- Implement the change across the organization.
- Monitor Outlook performance over the next week to ensure that response time does not degrade.
**Review Historical Performance.** Run the Application Response Service Performance report (an eHealth Service Level report) to determine average response time over the past month, as well as current response thresholds.

![Graph showing average response time](image1)

In this sample report, average response time is one to three seconds on weekdays, with sub-second response time on weekends.

**Make the Change on a Small Scale.** Implement your infrastructure change on a small scale or in a test environment. For example, if you are adding users from a new branch office, add a small set of them before adding all of them. This gives you a chance to test its impact and correct any problems before committing the entire change.

**Test the Impact of the Change.** After making the test change (such as adding users from the new office), test Outlook performance by asking a few new and existing users to use Outlook for awhile to generate response data. Run a Trend report for each group or an At-a-Glance report for each client set to compare current performance with historical performance and the performance of the new remote site with that of local users. This check allows administrators to make any necessary adjustments to the Exchange server or network before implementing the change across the organization.

The following charts show Trend reports for a group of existing users and a group of new remote users.

![Graph showing existing users' response times](image2)

![Graph showing new remote users' response times](image3)

For the two user groups, the reports show that Outlook response times are generally the same; however, the new users are experiencing greater network time than existing users.

Suppose that your IT staff diagnoses the problem and makes a network change over the weekend. Then they run an At-a-Glance report for the new client set and examine the Average Response Observed chart to check Outlook response time before and after the network change. The first peak in the following chart shows a large amount of network time (yellow) for Outlook activity. The second peak shows a significant reduction in the amount of server time experienced by the new remote users.

![Graph showing network change impact](image4)

**Implement the Change Across the Organization.** When you are confident that you have made necessary adjustments (exposed by your preliminary test) and that Outlook performance will not degrade, implement your infrastructure change across the organization.
Monitor Outlook Performance. After making the change, continue to run reports, such as the Application Response Service Performance report, to monitor Outlook performance. Compare these reports with the reports that you generated before the change and look for changes in Outlook performance.

Usage patterns and response times for applications can differ greatly based on the day of the week. These differences can be masked by weekly average response times. For existing users, run the Service Customer report to review Outlook performance each day to ensure that response time is not degrading for that day.

An increase in the number of transactions over 100% of threshold (shown in purple) indicates degradation in response time. The following report shows average response time for the group over the past three weeks, with the last week reflecting the addition of the remote office. The report shows that the number of transactions over 100% of threshold is relatively consistent, with prior weeks indicating that response time has not significantly been impacted.

![Daily Response Limit Distribution](image)

Value 7: Improve Capacity Planning

Application Response can help you perform capacity planning to support your application infrastructure. With this information, you can plan ahead for upgrades to Exchange servers, client systems, and network components to support the desired level of Outlook performance. Because Application Response identifies the infrastructure areas that are significantly impacting Outlook performance, you can plan to use your capital budget where it is needed most.

Capacity Planning for Outlook. For Outlook, capacity planning refers the process of ensuring that the infrastructure can support the total number of Outlook users performing peak Outlook loading at the desired service level. For example, if your current infrastructure supports 1,000 Outlook users at the agreed-on service level and you plan to add 500 new users due to a recent acquisition, you need to know whether you must add an Exchange server to maintain service goals. You also want to know whether your network will require additional capacity to support the increase in network traffic.

Look for Trends. To perform capacity planning with Application Response, use the At-a-Glance report for a client set. A client set is typically a group of users who perform the same types of functions (for example, all tellers at all bank branches) or who reside at the same location (for example, all bank employees at one branch location, including tellers, loan officers, and branch managers). By running the At-a-Glance report for each client set over a long time period, you can get a sense of how the needs of each client set is changing over time, or how their end-user experiences are changing. Using this information, you can predict when client systems, network components, or Exchange servers need to be added or upgraded to support their Outlook needs, and plan appropriately.

For example, Figure 2 shows the first two charts of an At-a-Glance report for the Atlanta client set.

![Figure 2. Two Charts of an At-a-Glance Report](image)

In the Average Response Observed chart, look for trends showing a steady increase in overall response time. Check whether the increased response time is due to the client, the network, or the server. The sample chart above shows a sudden but persistent increase in server time.
Also check the Transactions Observed chart. An increase in overall response time may be due to an increase in the total number of Outlook transactions. Total transactions may increase when existing users begin to use Outlook to more or when you add users to the client set. If response time is increasing as the number of transactions increases, you may need to increase capacity to support your Outlook users.

**Investigate Trends.** When you identify a trend in the At-a-Glance report, investigate it to determine whether the trend is due to a problem or a need for additional capacity. In most cases, you can take advantage of eHealth’s end-to-end capabilities, using other eHealth reports to identify the source of the trend.

To investigate a trend showing increased server response time (as shown in Figure 2), consult the application manager or other IT staff to determine whether more Outlook users have been added recently, or whether users are using Outlook to do more work. These changes may indicate that you need to increase the capacity of your Exchange servers.

Also, run an At-a-Glance report for your Exchange servers, on which the eHealth for Microsoft Exchange AIM is installed. Check Exchange metrics for CPU utilization, disk space, log size, and total number of users. For the Message Transfer Agent (MTA), check the numbers of bytes and messages sent and received, and its work queue length. If the report indicates a problem area, run a Trend report to investigate it further. If the server is at or near capacity, make plans to add a new Exchange server or upgrade the existing server.

This chart from an At-a-Glance report for an Exchange server shows that CPU utilization is close to 100% most of the time. You may need to add a server to support Outlook.

**Where to Go from Here**

When you are ready to use Application Response to monitor Outlook, read *Configuring Application Response to Monitor Microsoft Outlook* for an overview of the process and step-by-step instructions.