

A black horizontal banner with a white arrow-like shape on the left side pointing towards the text.

## Monitoring Microsoft Exchange with PATROL - A Best Practices Guide

<b>INTRODUCTION</b> .....	<b>3</b>
<b>MONITORING THE WINDOWS OPERATING SYSTEM</b> .....	<b>3</b>
CPU Utilization .....	4
Memory .....	4
Disk .....	4
Network .....	5
<b>MONITORING THE EXCHANGE SERVICES</b> .....	<b>5</b>
<b>MONITORING THE EXCHANGE PROCESSES</b> .....	<b>6</b>
<b>MONITORING MESSAGE FLOW</b> .....	<b>7</b>
Information Store .....	7
Routing Engine .....	7
SMTP .....	8
Queues .....	9
<b>MONITORING E-MAIL SYSTEM USAGE</b> .....	<b>9</b>
<b>MONITORING TOP CONSUMERS</b> .....	<b>10</b>
<b>MONITORING END USER PERSPECTIVE AVAILABILITY</b> .....	<b>11</b>
<b>MONITORING DATA ACCESS</b> .....	<b>11</b>
<b>PARAMETER SUMMARY</b> .....	<b>13</b>
<b>SOURCES</b> .....	<b>16</b>
Books .....	16
Online Books .....	16
Articles .....	16
Websites .....	17
Software .....	17
Online Help Systems .....	17
Helping You Maintain Advantage .....	17

## INTRODUCTION

Mail and messaging applications are mission-critical tools in today's business environments. Business productivity and effective communication require that these applications offer 24X7 availability and perform in real time. Microsoft Exchange is the leading collaboration tool offering e-mail and messaging capabilities. Now, more than ever, Exchange is being deployed in the most demanding environments including large organizations with thousands of users.

In order for an administrator to guarantee availability and performance to these thousands of users, monitoring Exchange environments is key. Monitoring aids in the rapid detection of poor performance or failures; furthermore, the detailed information provided helps with problem resolution. Additionally, through proactive monitoring, potential problems can be predicted, service outages prevented, and service level agreements met.

While every Exchange environment is unique, there are certain practices that you can follow to ensure the overall availability of your environment. While reviewing this document, please keep in mind that every Exchange environment is different and that you may need to refine our recommendations or take your own baselines in order to determine what is best for your environment.

While there are many components which may touch your Exchange environment such as anti-virus software, backup software, and Internet Information Services, this white paper discusses the critical components of a typical Exchange 2000 or Exchange 2003 environment that you should consider monitoring with PATROL KM for Microsoft Windows Operating System (OS KM) and PATROL for Microsoft Exchange Servers (Exchange KM). In addition, it makes some recommendations as to the thresholds you should set. We will focus on the most basic areas to consider in monitoring Exchange including

- > Windows Operating System
- > Exchange Services
- > Exchange Processes
- > Message Flow
- > E-mail System Usage
- > Top Consumers
- > End User Perspective Availability
- > Data Access

## MONITORING THE WINDOWS OPERATING SYSTEM

The performance and availability of applications and databases are intimately tied to the operating systems on which they run; without a healthy operating system, no application (for example, Exchange) will perform as expected. There are four primary areas related to the operating system that should be monitored: Central Processing Unit (CPU), memory, disk, and the network.

### CPU Utilization

Monitoring CPU utilization is important because Exchange may perform slowly or not respond at all if CPU utilization is too high.

**PATROL application class:** NT\_CPU

**Thresholds:** Because this application class collects data related to the time that the processor is running, it is a good indicator of processor activity. Generally speaking, if a processor demonstrates that it is being used close to 0 percent of the time, you should be concerned that the services are down. On the other hand, if a processor presents data that shows it is being used 90 percent of the time or more, you should be concerned that the processor is being overworked and may shut down. Be sure to set an alarm for when a processor exceeds 90 percent for 5 minutes or longer to prevent service outages.

### Memory

Memory plays a key part in server availability. Applications and users will consume memory and sometimes make a server perform sluggishly. Monitoring memory usage can help you isolate problems and performance issues before they become critical.

**PATROL application classes:** NT\_MEMORY, NT\_CACHE, NT\_PAGEFILE

**Thresholds:** In the NT\_MEMORY application class, pay special attention to the ratio of Committed bytes to the Committed limit; you should configure PATROL to trigger an alert if your virtual memory exceeds 80 percent to avoid potential service impacts. In the NT\_PAGEFILE application class, be sure to pay attention to the PAGEpgUsagePercent parameter. Experts consider the paging file to be healthy between 15 and 35 percent, and usage above 60 percent may indicate an issue such as too little RAM or a memory leak. Windows will automatically increase the size of the paging file once it reaches 90 percent, as this can be considered a critical situation. However, this will cause negative impacts to performance; thus, you should set an alarm between 60 and 80 percent in order to address any possible issues before they escalate.

### Disk

One of the key resources that can affect a server's availability is the disk being in use excessively. When the disks are spending the majority of their time reading or writing, or there is very little free space, performance will be degraded or a database may be dismounted. Monitoring the disks can help you ensure that you address possible issues before performance becomes degraded or a store is dismounted and service is interrupted.

**PATROL application class:** NT\_LOGICAL\_DISKS, NT\_PHYSICAL\_DISKS

**Thresholds:** Recommended thresholds for these application classes are discussed in detail in the *Monitoring the Microsoft Windows Server System with PATROL - a Best Practices Guide* white paper.

### PATROL Benefit



The PATROL KM for Microsoft Windows OS is pre-programed to trigger an alarm when disk space utilization is between 69 and 100 percent.



The Exchange KM provides the FreeDBSpaceAvailForDefrag parameter that tells you how much disk space you have available for defragmentation; this parameter can help you manage your disk space more efficiently. With this feature, you can choose your threshold, and the Exchange KM initiates an automated recovery action that defragments the disk and helps improve performance.

### Network

Regardless of how well your Exchange servers are working, if the network has problems, your Exchange servers may not be able to send or receive any information. Therefore, it is important to monitor network components so that you understand what kind of impact they may have or are having on the performance and availability of your Exchange environment.

**PATROL application class:** NT\_NETWORK

**Thresholds:** In a properly functioning network, the number of errors either outbound or inbound should be zero. Be sure to set an alarm of at least 1 so that you will be notified as soon as a your network is compromised. In addition, be sure to monitor the NETniBytesTotalPerSec parameter. This counter will tell you whether or not you are experiencing a performance bottleneck. Depending on your environment, you should observe a threshold between 8.75 and 11.25 MB/sec. If you observe this metric to be increasing, collisions are probably occurring, and network efficiency is decreasing. You need to take corrective action.

## MONITORING THE EXCHANGE SERVICES

Services are application types that run in the system background. Services provide core operating system features such as Web serving, event logging, file serving, help, support, printing, cryptography, and error reporting. To provide core system features to its users, Exchange provides a number of services. Of these services, the following components should be monitored:

- > Microsoft Exchange Information Store (IS)
- > Microsoft Exchange Routing Engine
- > Microsoft Exchange System Attendant
- > Simple Mail Transport Protocol (SMTP)
- > World Wide Web Publishing

**PATROL application class:** NT\_SERVICES

**Thresholds:** The two most important parameters to monitor for each service are ServiceStatus and SvcDown. The ServiceStatus parameter indicates whether or not the Exchange service has been started and whether or not clients can make connections. The SvcDown parameter indicates the opposite.

### PATROL Benefit



The OS KM monitors all services out of the box so there is little configuration necessary to achieve service monitoring. If any of the Exchange services enters a precarious state of between 1 and 5, you will receive a warning. If the state should escalate to between 5 and 12, PATROL is preconfigured to send an alarm, as this can be detrimental to the mail flow in your organization.

## MONITORING THE EXCHANGE PROCESSES

In addition to service monitoring, you should monitor the processes that run on behalf of an application. Exchange has critical processes that should be watched to determine their availability and resource usage. Exchange processes include

- > **store.exe** (Information Store Service)
- > **inetinfo.exe** (IIS, Routing Engine)
- > **mad.exe** (System Attendant)
- > **emsmta.exe** (MTA Stacks Service)

**PATROL application class:** NT\_PROCESS

**Thresholds:** The two most important parameters to consider are PROCDown and PROCProcessorTimePercent. If the PROCDown parameter indicates that a process is down or the PROCProcessorTimePercent parameter is at zero, your processes may not be running, which is detrimental to mail flow. **inetinfo.exe**, **store.exe**, **emsmta.exe**, and **mad.exe** normally consume 90 percent of the processor time combined. However, if you observe these processes to be running at 100 percent for a sustained period of time, one of these processes has a problem that needs to be diagnosed and resolved. Set an alarm between 90 and 100 percent, depending on your environment.

### PATROL Benefit



The PROCDown parameter for each of these processes is preconfigured to alarm in the case where its value equals 1, indicating that the process is not running.



When used with the OS KM, the Exchange KM automatically monitors Exchange Server processes that are initiated at startup. You can also configure PATROL to monitor additional Exchange Server processes where necessary.

### MONITORING MESSAGE FLOW

To understand the performance of your Exchange systems, you should monitor parameters related to message flow. These will allow you to understand the speed at which the IS, Routing Engine, SMTP, and Queues are processing requests and whether or not there is a bottleneck.

#### Information Store

Monitoring the IS is critical as this is the repository that Exchange uses to manage and process all of its information including mail, attachments, calendar appointments, and querying Active Directory to authenticate users.

**PATROL application classes:** MSEXCH\_DB\_Private, MSEXCH\_DB\_Public

**Thresholds:** The MSEXCH\_DB\_Public\RecvQueueSize and MSEXCH\_DB\_Private\RecvQueueSize parameters monitor Exchange server performance for user mailboxes and the public folders store and will tell you the number of messages in the receive queue waiting to be processed by the IS. If the parameter value is high or increasing, you may need to load balance your server or consider other issues. The same limits that apply to the SendQueueSize parameter apply to the RecvQueueSize parameter.

**Tips:** If you suspect that the private or public send queue is experiencing a bottleneck, use one of the following actions to correct the problem:

- > Move some or all of the mailboxes to another server
- > Configure the public folders to another server
- > Use multiple disk controllers
- > Limit the amount or type of e-mail that users may send
- > Add more disks to the stripe set
- > Add one or more caching disk controllers that cache read and write operations

#### PATROL Benefit



For the State parameter, the Exchange KM has a preconfigured threshold of 2 to 3 for a warning to be issued, and a threshold of 1 for an alarm.



The Exchange KM is preconfigured to alarm at a threshold of 30 minutes or more for the AvgDeliverTime parameter.

#### Routing Engine

The function of the routing engine or message transfer agent is to deliver messages once the IS has searched the directory to determine the destination of a message. Thus this component should be closely monitored, as any problems will impact the rate or ability of clients to send and receive messages.

**PATROL application class:** MSEXCH\_MTA

**Thresholds:** The WorkQueueLength parameter displays the total number of messages currently in the MTA queue. This number includes inbound and outbound messages for the IS, the Directory, and any MTA connectors. If the QueueLength parameter is large or increasing, you have a problem that may impact performance. The cause could be

- > the receiving MTA may be failing
- > a network communication failure
- > a performance problem on the sending or receiving machine

The parameter value should remain between 0.5 and 1.0 percent of connected users or vary somewhere between 0 and 50 normally. If the queue length is above these values for a sustained period of time or if the queue length is rising, you may have a problem with one of your Exchange components, a connector, or a remote Exchange MTA. Set an alarm for any value of 100 or greater.

**Tips:** To improve performance, you can remove messages from the MTA queue that were generated by the directory service, system attendant, or the public IS. These messages often accumulate when a WAN link fails or when a server is offline, interfering with the delivery of user-generated messages.

If the queue is larger than normal, determine the destination server of the first message in the queue and then verify that the destination server or connector is configured properly. You may also want to search the application event log generated by the MTA connection or the destination server.

### PATROL Benefit



If the MTA cannot contact a domain controller, it may frequently shut down. If it does, the Exchange KM has a recovery action that will automatically restart the service for you.

### SMTP

Although Exchange 5.5 used X.400 as the Internet protocol of choice, this protocol has since been replaced by SMTP. Exchange 2003 now uses this protocol for all communication between Exchange servers within a site, thus monitoring its availability is critical to ensure message flow. In addition, queue traffic is a direct result of the clients in use.

**PATROL application class:** MSEXCH\_SMTP\_Server

**Thresholds:** If you observe the values of the parameters in the SMTP application class increasing, specifically the LocalQueueLength parameter, you should be concerned that messages are not being passed between Exchange servers. This suggests that a connector is not working properly or that there is a problem with the network.



### Queues

As messages are passed from one process or component to another in the Exchange environment, these messages may be queued while waiting for the next process to perform its function (for example, look up in Active Directory or routing). Monitoring the number of messages in these queues is one of the most effective means of determining whether or not there is a message flow problem. While you may sometimes receive a *false positive* from a hang up in the queue due to a spike in the number of messages being sent or a large message in the queue, monitoring these queues for such events can help avert potential service problems.

**PATROL application class:** MSEXCH\_Queues

**Thresholds:** In the MSEXCH\_Queues application class, focus on the State and IncreasingTime parameters. If you notice that the State parameter is constantly in Frozen mode, your network is having delivery problems that need to be addressed. Be sure to set an alarm for when the state of this parameter changes to Frozen. Also, pay close attention to the IncreasingTime parameter. This parameter will give you a good indication if your performance is suboptimal due to problems with the Web Storage system or contacting the Domain Controller in the case of an Active Directory lookup. The Exchange KM has a preprogrammed threshold of 10 unprocessed messages per minute or more for an alarm to trigger.

**Tips:** Additional parameters that may help you determine message traffic flow and productivity are the MSEXCH\_Sent\_Mail\SentMsgs and MSEXCH\_Sent\_Mail\RecvMsgs parameters (the message tracking logs must be enabled for these parameters to be active). These parameters tell you the number of messages sent and received within a site, among sites in your organization, local to the server, and to external servers. You can use this data to balance server load and to ensure that you are using network bandwidth effectively. Furthermore, the MSEXCH\_Sent\_Mail\_Containers\TotalMsgSent and MSEXCH\_Sent\_Mail\_Containers\TotalMsgReceived parameters show you the sum of all the message traffic on a particular server on your network.

### PATROL Benefit



The Exchange KM discovers the queues being used on the server and will generate an application class instance for each type of queue.

## MONITORING E-MAIL SYSTEM USAGE

As with any server or application, the number of users or clients connecting to it creates increased load and resource consumption. Though these are not parameters that you need to monitor closely from day to day, from a planning perspective you should monitor these parameters over time to determine whether or not your current infrastructure can continue to support your messaging needs.

**PATROL application class:** MSEXCH\_IS

**Thresholds:** Thresholds for the UserCount and ConnectionCount parameters should be set at zero, as this may be helpful for indicating possible problems with clients being able to connect.

**Tip:** There are two IS-related performance counters that are worthwhile to monitor. These are:

- > MSExchangeIS\RPC Requests counter - indicates the number of MAPI RPC requests serviced by the Exchange store. 100 simultaneous requests is the store's limit. However, this value should normally be quite small, though it can vary over a day. Start by setting a threshold of between 10 and 15 requests and adjust as necessary.
- > MSExchangeIS\RPC Operations/sec counter - indicates the rate at which the Exchange store is servicing user requests.

These two metrics help you determine problems with processing client requests before or after Exchange processing begins. A problem before Exchange processing and message flow exists if the RPC Requests are low and the RPC Operations/sec is 0. Anything other than this scenario indicates a problem during or after Exchange processing. You should set an alarm when the RPC Operations/sec drops below normal for a sustained period of time.

### PATROL Benefit



You can use the PATROL Wizard for Microsoft Performance Monitor and WMI provided by the PATROL for Microsoft Windows Servers product to bring in any performance counters of interest, such as those listed above, for monitoring.

## MONITORING TOP CONSUMERS

While monitoring the top consumers is not critical to ensure the overall health of the Exchange system, it does allow an administrator to make refinements based on observed resource requirements that can help improve overall Exchange performance. For example, an administrator may be able to better allocate storage resources based on demonstrated need or shift certain high volume mailboxes or public folders to servers with less traffic or a higher capacity.

**PATROL application classes:** MSEXCH\_Top\_Senders, MSEXCH\_Top\_Recipients, MSEXCH\_Top\_Folders, MSEXCH\_Top\_Mailboxes

**Thresholds:** Thresholds do not typically apply here as the intention is simply to monitor a specified number of top consumers (please note that message tracking must be enabled to use this functionality). The Exchange KM monitors five consumers by default and can monitor no more than 50 consumers in any one of the above application classes. While this value may seem low, you must consider the impact that such monitoring could have on your resources and network. We have artificially set this limit with the intention of preventing any adverse impact that monitoring of an extensive number of users could have.

However, if you are concerned about limiting public folder sizes, you can set a threshold here based on the needs of your organization using the `MsgSize` parameter.

**Tips:** The Exchange KM has a feature that allows you monitor specified users in the `MSEXCH_Watched_Users` application class. This could be advantageous if you need to monitor a particular user (for example, the CEO) in order to ensure that they experience optimal performance and availability of Exchange or if you need to ensure that users stay within their quota limits.

You can also configure PATROL to watch for suspect mail. The Exchange KM uses a dummy mailbox to monitor for suspect mail that could contain viruses. This dummy mailbox uses a bogus name and is not a member of any distribution list, so it should never send or receive e-mail. If it does, an e-mail virus may be present.

### PATROL Benefit



You can configure the Exchange KM to perform recovery actions such as automatically notifying the top senders, receivers, or mailbox users of their usage. You can also specify whether to use the number of messages or the total message size to determine the top senders, receivers, mailboxes, and folders.



If you choose to use the Watched User function to monitor for suspect mail, the Exchange KM knows that the dummy mailbox should never send or receive e-mail. In the event that it does, a built-in recovery action will automatically shut down the Message Transfer Agent to prevent further spread of the virus.

## MONITORING END USER PERSPECTIVE AVAILABILITY

When developing a best practices monitoring plan for Exchange, you should not only monitor end userload, but also end user perspective. Users depend on Exchange to be available and responsive; therefore, understanding how the Exchange server responds to typical client usage will help determine its availability to your users. Please refer to the *Best Practices for Monitoring Roundtrip Response Times in Microsoft Exchange with PATROL for Microsoft Exchange Servers* whitepaper for details on how to use this feature.

## MONITORING DATA ACCESS

DSAccess is one of the core components of Exchange 2000 and 2003 that controls how Exchange accesses the Active Directory. For example, a user or Exchange Server can initiate an Active Directory query to look up an e-mail address. These results are stored in a cache called DSAccess. Because Exchange always searches this cache before submitting a query, this helps reduce network traffic and process performance by eliminating redundant queries and allows Exchange to be more scalable.

In addition, because the MTA, IS, Exchange routing, and other components require DSAccess for processing, monitoring the availability of data access is key to the availability of the Exchange environment.

**PATROL application class:** MSEXCH\_DSAccess\_Cache, MSEXCH\_DSAccess\_Processes

**Thresholds:** If any of the parameters in this application class are high or rising and the message delivery rate is decreasing, Active Directory is having problems.

**Tip:** If your server houses a large number of mailboxes, you may be able to improve performance by increasing the cache size. Microsoft sets the default user and configuration cache size at 25MB. Depending on your hardware, you may be able to increase the user cache size to 90MB and the configuration size to 5MB.

## PARAMETER SUMMARY

Table 1 shows you all of the parameters discussed in this paper. To learn more about these parameters, see the PATROL KM for Windows OS online Help, the PATROL for Microsoft Exchange Servers online Help, or the *PATROL Parameter Reference Manual*, which contain descriptions and attributes for all of the parameters.

**Table 1 Monitoring Exchange in Summary (Part 1 of 3)**

Exchange Area	Application Class\Parameters
Exchange Services > Microsoft Exchange Information Store > Microsoft Exchange MTA Stacks > Microsoft Exchange Routing Engine > Microsoft Exchange System Attendant > Simple Mail Transport Protocol > World Wide Web Publishing Service	NT_SERVICES\SvcDown NT_SERVICES\ServiceStatus
Exchange Processes > <b>store.exe</b> (Information Store Service) > <b>inetinfo.exe</b> (IIS, Routing Engine) > <b>mad.exe</b> (System Attendant) > <b>emsmta.exe</b> (MTA Stacks Service)	NT_PROCESS\PROCDDown NT_PROCESS\PROCProcessorTimePercent
Events from Sources > IMAP4Svc > MS-ExchangeAL > MExchangeIS\System > MExchangeIS\Mailbox > MExchangeIS\Public Folder > MExchangeSRS > MExchangeTransport > MExchangeMTA > MExchangeSA > POP3SVC	NT_EVENTLOG\Application\eventFilter\ELMError

Table 1 Monitoring Exchange in Summary (Part 2 of 3)

Exchange Area	Application Class\Parameters
Client Load > client load > top mail senders and mail receivers > top mailbox users and public folders	MSEXCH_Top_Senders\MsgSize MSEXCH_Top_Senders\MsgCount MSEXCH_Top_Senders\AvgMsgsPerHour MSEXCH_Top_Recipients\MsgSize MSEXCH_Top_Recipients\MsgCount MSEXCH_Top_RecipientsAvgMsgsPerHour MSEXCH_Top_Mailboxes\MsgSize MSEXCH_Top_Mailboxes\MsgCount MSEXCH_Top_Folders\MsgSize MSEXCH_Top_Folders\MsgCount MSEXCH_Watched_Users\AttachmentSize MSEXCH_Watched_Users\MsgCount MSEXCH_Watched_Users\MsgSize MSEXCH_Watched_Users\SuspectMsgCount
End User Perspective Availability > sending round-trip messages to the Exchange Server > logging on and off the Exchange Server > opening messages > creating messages > sending messages > deleting messages	MSEXCH_Roundtrip_Client\CreateMsgTime MSEXCH_Roundtrip_Client>DeleteMsgTime MSEXCH_Roundtrip_Client>LastMsgTime MSEXCH_Roundtrip_Client>LastNMsgTime MSEXCH_Roundtrip_Client\LogoffTime MSEXCH_Roundtrip_Client\LogonTime MSEXCH_Roundtrip_Client\MaxMsgTime MSEXCH_Roundtrip_Client\OpenMsgTime MSEXCH_Roundtrip_Client\SendMsgTime MSEXCH_Roundtrip_Client>Status
Data Access > DS Access > Address List	MSEXCH_DSAccess_Cache\AsyncReadsPending MSEXCH_DSAccess_Cache\AsyncSearchesPending MSEXCH_DSAccess_Processes\LdapReadTime MSEXCH_DSAccess_Processes\LdapSearchTime MSEXCH_Address_List\AddressListQueueLength
Message Traffic - Protocol Queues > Protocol Queues > Sent/Received > Client Connections	MSEXCH_Queue\IncreasingTime MSEXCH_Queue\State MSEXCH_Sent_Mail\RecvMsgs MSEXCH_Sent_Mail\SentMsgs MSEXCH_Sent_Mail_Containers\TotMsgSent MSEXCH_Sent_Mail_Containers\TotMsgReceived
Message Traffic - Routing Engine	MSEXCH_MTA\WorkQueueLength MSEXCH_MTA_Connections\QueueLength
Message Traffic - Information Store	MSEXCH_DB_Private\RecvQueueSize MSEXCH_DB_Public\RecvQueueSize MSEXCH_DB_Private\SendQueueSize MSEXCH_DB_Public\SendQueueSize
Message Traffic - SMTP	MSEXCH_SMTP_Server\LocalQueueLength

## Parameter Summary

**Table 1 Monitoring Exchange in Summary (Part 3 of 3)**

Exchange Area	Application Class\Parameters
Store > ExIPC > DB Private and DB Public	MSEXCH_ExIPC\ClientQueLen MSEXCH_ExIPC\StoreQueLen MSEXCH_DB_Private\SendQueueSize MSEXCH_DB_Public\SendQueueSize MSEXCH_DB_Private\MsgSentPerMin MSEXCH_DB_Public\MsgSentPerMin MSEXCH_DB_Private\RecvQueueSize MSEXCH_DB_Public\RecvQueueSize
User and Client Connections	MSEXCH_IS\UserCount MSEXCH_IS\ConnectionCount Perfmon:MSEXchangeIS\RPC Requests Perfmon:MSEXchangeIS\RPC Operations/sec

### SOURCES

#### Books

- > Daugherty, Mike. *Monitoring and Managing Microsoft Exchange Server 2003*. Burlington: Digital Press, 2004.
- > Gerber, Barry. *Mastering Exchange Server 2003*. Alameda: SYBEX Inc., 2003.
- > Microsoft Corporation. *Microsoft Exchange 2000 Server Resource Kit*. Redmond: Microsoft Press, 2000.

#### Online Books

- > *Active Directory Operations Guide Version 1.5*; available from <http://www.microsoft.com/downloads/details.aspx?displaylang=en&familyid=4a82eccc-76d6-4431-aac4-1ef1ba11d8ea>
- > *Exchange 2000 Operations Guide*; available from <http://www.microsoft.com/technet/prodtechnol/exchange/2000/maintain/opsguide.msp>
- > *PATROL for Microsoft Exchange Servers Getting Started*; available from <http://documents.bmc.com/supportu/documents/72/09/47209/47209.pdf>
- > *PATROL for Microsoft Windows Servers Getting Started*; available from <http://documents.bmc.com/supportu/documents/93/43/49343/49343.pdf>
- > *PATROL Parameter Reference Manual*; available from <http://documents.bmc.com/supportu/documents/66/39/26639/26639.pdf>
- > *Troubleshooting Exchange 2000 Performance*; available from <http://www.microsoft.com/downloads/details.aspx?displaylang=en&familyid=bd16ee6a-c4ee-4ab0-aaf0-27705465154e>
- > *Understanding and Troubleshooting Directory Access*; available from <http://www.microsoft.com/downloads/details.aspx?displaylang=en&familyid=c976433f-f979-4745-b7a6-9d8446ef6409>

#### Articles

- > Pierre Bijaoui and Tony Redmond, "3 Basics of Exchange Server Performance," in *Windows 2000 Magazine*; available from <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnw2kmag01/html/ExchangeServer.asp>



- > "Designing Monitoring and Maintenance Procedures" in the *Exchange 2000 Planning Guide* white paper. Available from [http://www.microsoft.com/technet/prodtechnol/exchange/2000/deploy/upgrademigrate/series/planningguide/p\\_07\\_tt1.mspx](http://www.microsoft.com/technet/prodtechnol/exchange/2000/deploy/upgrademigrate/series/planningguide/p_07_tt1.mspx)

### Websites

- > <http://support.microsoft.com>
- > <http://www.microsoft.com>

### Software

- > PATROL KM for Microsoft Windows Operating System in PATROL for Microsoft Windows Servers
- > PATROL for Microsoft Exchange Servers

### Online Help Systems

- > PATROL KM for Microsoft Windows Operating System Help v3.8. Available from [http://filedownload.bmc.com/bmc/onlinehelpfiles/pwkkm\\_3.8.02/pwkkm/epssnav1.htm](http://filedownload.bmc.com/bmc/onlinehelpfiles/pwkkm_3.8.02/pwkkm/epssnav1.htm)
- > PATROL for Microsoft Exchange Servers Help v5.0. Available from [http://filedownload.bmc.com/bmc/onlinehelpfiles/pkx\\_5.0.00.05/pkx/epssnav1.htm](http://filedownload.bmc.com/bmc/onlinehelpfiles/pkx_5.0.00.05/pkx/epssnav1.htm)

#### About BMC Software

BMC Software, Inc. [NYSE:BMC], is a leader in enterprise management. The company focuses on Assuring Business Availability® for its customers by helping them proactively improve service, reduce costs, and increase value to their business. BMC Software solutions span enterprise systems, applications, and databases. Founded in 1980, BMC Software has offices worldwide and is a member of the S&P 500, with fiscal year 2002 revenues of approximately \$1.3 billion. Visit [www.bmc.com](http://www.bmc.com) to learn more.

#### Helping You Maintain Advantage

BMC Software Professional Services helps your company maintain its competitive advantage through a comprehensive suite of services that includes service level management consulting, installation, implementation, configuration, and customization. Our professional services and education offerings are designed to ensure the ongoing availability of critical business applications, maximize product potential, reduce project risk, deliver IT value to your business, and improve your operations. For more information about BMC Software Professional Services, visit <http://www.bmc.com/profserv>.



#### About BMC Software

BMC Software, Inc. [NYSE:BMC], is a leading provider of enterprise management solutions that empower companies to manage their IT infrastructure from a business perspective. Delivering Business Service Management, BMC Software solutions span enterprise systems, applications, databases, and service management. Founded in 1980, BMC Software has offices worldwide and fiscal 2004 revenues of more than \$1.4 billion. For more information about BMC Software, visit [www.bmc.com](http://www.bmc.com).



50088