Monitoring Microsoft Hub Transport Server

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

Deployed inside your Active Directory directory service forest, the Hub Transport server role handles all mail flow inside the organization, applies transport rules, applies journaling policies, and delivers messages to a recipient's mailbox. Messages that are sent to the Internet are relayed by the Hub Transport server to the Edge Transport server role that is deployed in the perimeter network. Messages that are received from the Internet are processed by the Edge Transport server before they are relayed to the Hub Transport server. If you do not have an Edge Transport server, you can configure the Hub Transport server to relay Internet messages directly. You can also install and configure the Edge Transport server agents on the Hub Transport server to provide anti-spam and anti-virus protection inside the organization.

The Hub Transport server role stores all its configuration information in Active Directory. This information includes transport rules settings, journal rule settings, and connector configurations. Because this information is stored in Active Directory, you can configure settings one time, and then those settings are applied by every Hub Transport server in the organization.

The message-processing scenarios that you can manage on the Hub Transport server role are described in the following sections.

- Internal Mail Flow

  The Hub Transport server role processes all messages that are sent inside the Exchange 2007/2010 organization before the messages are delivered to a recipient's Inbox or are routed to users outside the organization. There are no exceptions to this behavior; messages are always passed through a server that runs the Hub Transport server role.

- Messaging Policy and Compliance Features

  A collection of transport agents lets you configure rules and settings that are applied as messages enter and leave the mail flow components. You can create messaging policy and rule settings that are designed to meet different regulations and that can easily be changed to adapt to your organization's requirements. The transport-based messaging policy and compliance features include server-based rules that you configure to enforce your organization's compliance scenarios and the Journaling agent that acts to enforce message retention.

- Anti-Spam and Antivirus Protection

  The Exchange 2007/2010 Built-in Protection features provide anti-spam and antivirus protection for messages. Although these Built-in Protection features are designed for use in the perimeter network on the Edge Transport server role, the Edge Transport agents can also be configured

on the Hub Transport server. By default, these agents are not enabled on the Hub Transport server role. To use the anti-spam features on the Hub Transport server, you must register the agents in a configuration file and enable the features that you want to use by running a provided Exchange Management Shell script. You install and enable the antivirus agent in a separate operation.

The error-free functioning of the Hub Transport server is therefore essential to ensure uninterrupted mail flow within the Exchange organization and to insulate the Exchange organization from spam/virus attacks. By continuously monitoring the operations of the Hub Transport server, administrators can be promptly alerted to ineffectiveness of the anti-spam or anti-virus agents on the server and slowdowns in the processing of mail messages by the server. This can be achieved using eG Enterprise. eG Enterprise offers a specialized monitoring model for continuously monitoring the Hub Transport server to track mail flow and timely provide alert on slowdowns.

Chapter 2: How to Monitor the Microsoft Exchange 2007/2010 Server with Hub Transport Server Role Using eG Enterprise?

eG Enterprise adopts an agent-based approach to monitoring the Exchange 2007 /2010 server that corresponds to Hub Transport server role. The agent-based approach requires that you install and configure the eG agent on the Exchange 2007/2010 host (if one of the 'integrated' Exchange 2007 or Exchange 2010 models is being used) or on the host on which the server role to be monitored exists.

This internal agent, once started, periodically runs a wide variety of tests on the Exchange 2007/2010 server/server role to extract useful performance data. Some of these tests , namely – the Exchange Mailbox Status test, the Exchange Storage Group test, and the Exchange Queue Stats test – require **Exchange Administrator** privileges to execute. Therefore, prior to monitoring an Exchange 2007/2010 server/Hub Transport server role using eG Enterprise, make sure that you configure the eG agent to run with the privileges of an **Exchange Administrator**. Then, manage the Microsoft Exchange Hub Transport Server using the eG administrative interface. The procedure for achieving this is discussed in Section **2.1**.

2.1 Managing the Microsoft Exchange Hub Transport Server

The eG Enterprise cannot automatically discover the Microsoft Exchange Hub Transport Server. This implies that you need to manually add the component for monitoring. Remember that the eG Enterprise automatically manages the components that are added manually. To manage a Exchange Hub Transport Server component, do the following:

1. Log into the eG administrative interface.
2. Follow the Components -> Add/Modify menu sequence in the **Infrastructure** tile of the **Admin** menu.
3. In the **COMPONENT** page that appears next, select *Microsoft Exchange Hub Transport* as the **Component type**. Then, click the **Add New Component** button. This will invoke Figure 2.1.

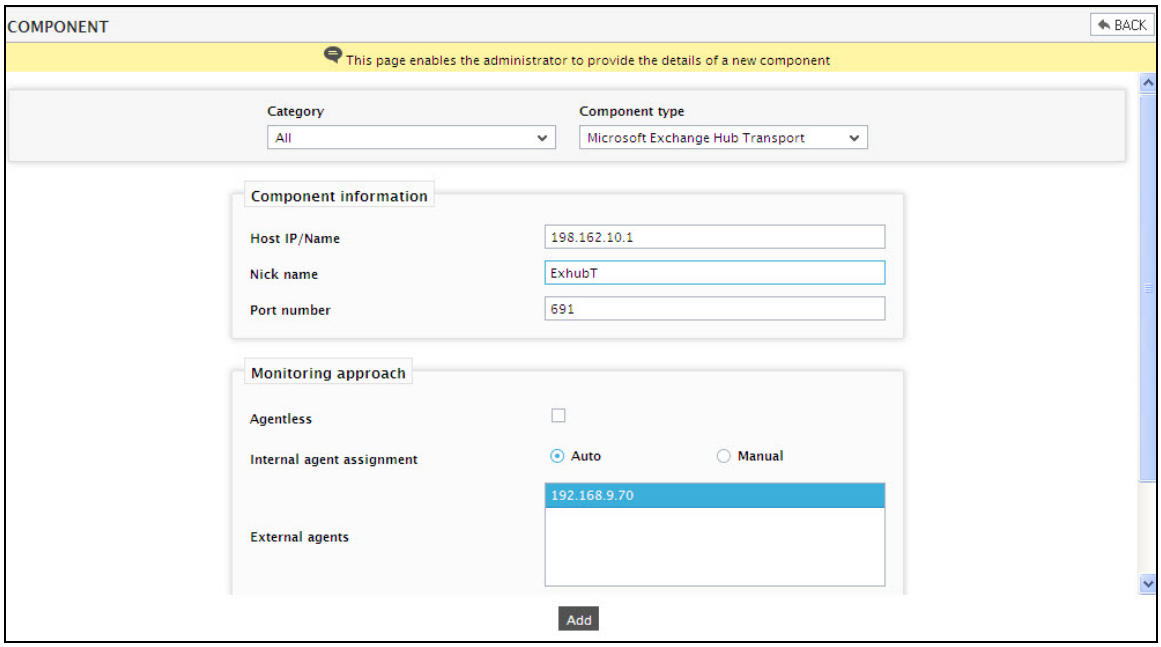

Figure 2.1: Adding an Exchange Hub Transport server

4. Specify the **Host IP** and the **Nick name** of the Exchange Hub Transport Server in Figure 2.1.
5. The **Port number** will be set as *691* by default. If the server is listening on a different port in your environment, then override this default setting.
6. Now, click on the **Add** button in Figure 2.1 and sign out of the eG administrative interface.

Chapter 3: Monitoring the Microsoft Exchange Hub Transport Server

eG Enterprise provides an Microsoft Exchange Hub Transport model that monitors the internal health of the Hub Transport server.

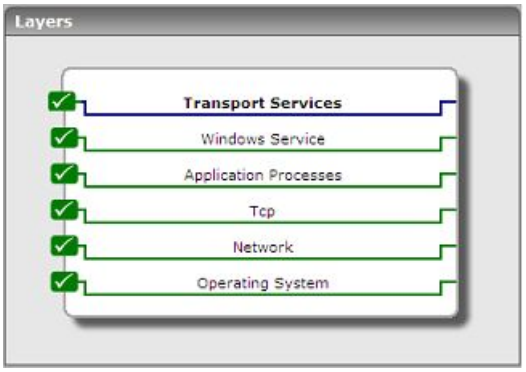

Figure 3.1: Layer model of the Microsoft Exchange Hub Transport server

The tests mapped to each layer report critical statistics that reveal the following:

- Is the server experiencing processing bottlenecks? Are there any lengthy message queues on the server? If so, which ones?
- How effective is the Recipient filter agent? How many requests per second were rejected by the Recipient Lookup and Recipient Block List data sources?
- How successful is the Sender Filter agent in evaluating and filtering out "suspect" senders?
- Is the Sender ID agent efficient?
- Has the Hub Transport server experienced latencies while connecting to the Exchange store? Which store interface can this delay be attributed to?
- How many messages are available in the delivery queue? Is the number very high?
- Do too many messages exist in the retry queue?
- Are too many messages awaiting delivery to an external recipient?
- Have messages been queued in the Unreachable queue?
- Does the poison queue contain messages?
- Which receive connector is overloaded with data and messages?

The sections to come discuss the **Transport Services** layer alone, as all other layers have been discussed elaborately in the *Monitoring Unix and Windows Servers* document.

3.1 The Transport Services Layer

The tests mapped to this layer monitor the transport services offered by the Hub Transport server.

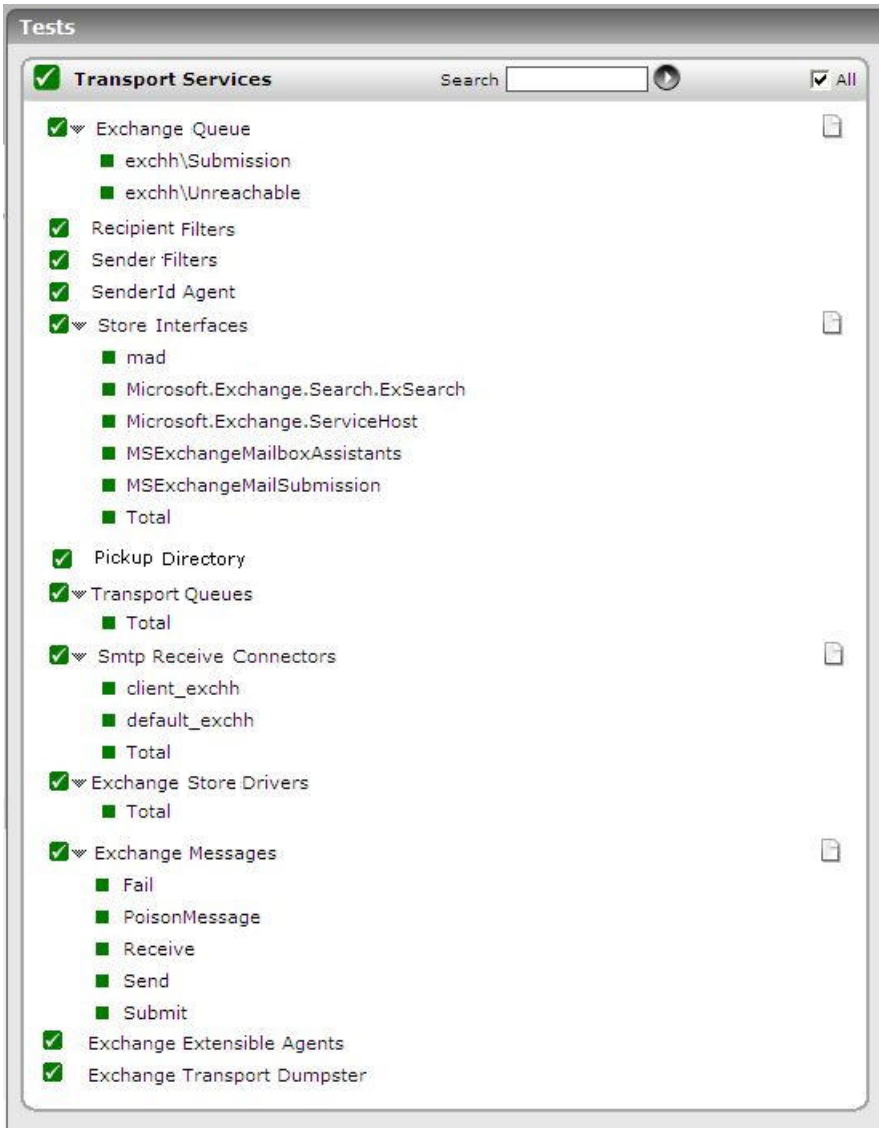

Figure 3.2: The tests mapped to the Transport Services layer

3.1.1 Exchange Queues Test

A queue is a temporary holding location for messages that are waiting to enter the next stage of processing. Each queue represents a logical set of messages that an Exchange transport server

processes in a specific order. Queues exist only on computers that have the Hub Transport server role or Edge Transport server role installed.

This test reports the length of each message queue on the Microsoft Exchange Edge Transport server or the Microsoft Exchange Hub Transport server, so that queues experiencing processing bottlenecks can be accurately identified.,

Target of the test : A server configured with the Hub Transport role

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every queue on the Hub/Edge Transport server being monitored.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	Indicates the IP address of the Hub Transport server.
Port	The port number of the Hub Transport server. By default, this is *691*.
XchgExtensionShellPath	The Exchange Management Shell is a command-line management interface, built on Windows PowerShell which enables you to administer every part of Microsoft Exchange. This test uses the Exchange management shell to run scripts and collect the desired performance metrics from the Exchange server. By default, the test auto-discovers the location of the Exchange management shell and thus, automatically loads the Exchange management shell snap-in (exshell.psc1) for script execution. This is why, the XchgExtensionShellPath is set to *none* by default.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Messages in queue	Indicates the number of messages currently found in this queue.	Number	A high number could indicate a processing bottleneck in the queue.

3.1.2 Recipient Filters Test

The Recipient Filter agent is an anti-spam agent that is enabled on computers that have the Microsoft Exchange server 2007/2010 Edge Transport server role installed.

The Recipient Filter agent blocks messages according to the characteristics of the intended recipient in the organization. The Recipient Filter agent can help you prevent the acceptance of messages in the following scenarios:

- **Nonexistent recipients**: You can prevent delivery to recipients that are not in the organization's address book. For example, you may want to stop delivery to frequently misused account names, such as administrator@contoso.com or support@contoso.com.
- **Restricted distribution lists**: You can prevent delivery of Internet mail to distribution lists that should be used only by internal users.
- **Mailboxes that should never receive messages from the Internet**: You can prevent delivery of Internet mail to a specific mailbox or alias that is typically used inside the organization, such as Helpdesk.

The Recipient Filter agent acts on recipients that are stored in one or both of the following data sources:

- **Recipient Block list**: An administrator-defined list of recipients for which inbound messages from the Internet should never be accepted.
- **Recipient Lookup**: Verification that the recipient is in the organization. Recipient Lookup requires access to Active Directory directory service information that is provided by EdgeSync to Active Directory Application Mode (ADAM).

You can use this test to monitor the effectiveness of the Recipient Filter Agent. This test reports the number of messages that were rejected based on the **Recipient Block List** and the **Recipient Lookup** data sources.

Target of the test : A server configured with the Hub Transport role

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the Hub/Edge Transport server being monitored.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	Indicates the IP address of the Hub Transport server.
Port	The port number of the Hub Transport server. By default, this is *691*.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Recipients rejected by recipient validation	Indicates the number of recipients rejected per second by recipient validation.	Rejects/Sec	One benefit of the Recipient Filter agent is the ability to verify that the recipients on an inbound message are in your organization before Exchange 2007/2010 transmits the message into your organization. The ability to verify recipients in your organization relies on a Recipient Lookup data source that is available to the Hub/Edge Transport server. The value of this measure indicates the number of recipients who were rejected by this data source.
Recipients rejected by block list	Indicates the number of recipients rejected by block list per second.	Rejects/Sec	The **Recipient Block** list is a list that is maintained by the Edge Transport server administrators. The Recipient Block list data is stored in the Edge Transport server instance of ADAM. You must enter blocked recipients on each Edge Transport server computer. You can enter the recipients that you want the Recipient Filter agent to block in the Exchange Management Console on the Blocked Recipients tab of the

Measurement	Description	Measurement Unit	Interpretation
			Recipient Filtering Properties page. You use the Set-RecipientFilterConfig command in the Exchange Management Shell to enter recipients.

3.1.3 Sender Filters Test

The Sender Filter agent is an anti-spam filter that is enabled on computers that have the Microsoft Exchange server 2007/2010 Edge Transport server role installed. The Sender Filter agent relies on the MAIL FROM: Simple Mail Transfer Protocol (SMTP) header to determine what action, if any, to take on an inbound e-mail message.

The Sender Filter agent acts on messages from specific senders outside the organization. Administrators of Edge Transport servers maintain a list of senders who are blocked from sending messages to the organization. As an administrator, you can block single senders (kim@contoso.com), whole domains (*@.contoso.com), or domains and all subdomains (*@*.contoso.com). You can also configure what action the Sender Filter agent should take when a message that has a blocked sender is found.

Using this test, administrators can determine the overall health and effectiveness of the Sender Filter agent's operations.

Target of the test : A server configured with the Hub Transport role

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the Edge Transport server being monitored.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	Indicates the IP address of the Hub Transport server.
Port	The port number of the Hub Transport server. By default, this is *691*.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Messages evaluated by sender filter	Indicates the number of messages evaluated by the Sender Filter agent per second.	Msgs/Sec	This is a good measure of the agent's processing ability.
Messages filtered by sender filter	Indicates the number of messages filtered by the Sender Filter agent per second.	Msgs/Sec	

3.1.4 SenderId Agent Test

The Sender ID agent is an anti- spam agent that is enabled on computers that have the Microsoft Exchange server 2007/2010 Edge Transport server role installed. The Sender ID agent relies on the RECEIVED Simple Mail Transfer Protocol (SMTP) header and a query to the sending system's domain name system (DNS) service to determine what action, if any, to take on an inbound message.

Sender ID is intended to combat the impersonation of a sender and a domain, a practice that is frequently called spoofing. A spoofed mail is an e-mail message that has a sending address that was modified to appear as if it originates from a sender other than the actual sender of the message.

In essence, Sender ID asks a question: "Has this e-mail message been spoofed?" If the answer is "Yes, it has been spoofed," the Sender ID filter rejects or deletes the message immediately. If the answer is "No, we can confirm the sender's authenticity," the message is assigned a Sender ID status and transmitted to Intelligent Message Filter, if Intelligent Message Filter is enabled on the server, for additional anti-spam processing.

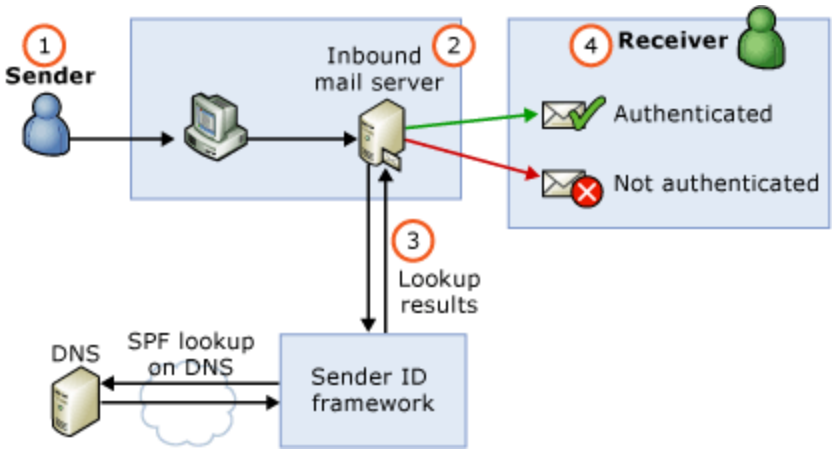

Figure 3.3: How the Sender ID filter works?

Here are the steps in the Sender ID verification process in Figure 3.3:

1. A sender sends an e-mail message to the receiver.
2. The receiver's inbound mail server receives the e-mail message and extracts the PRA.
3. The inbound mail server checks which domain claims to have sent the message, and examines the domain name system (DNS) for the sender policy framework (SPF) record of that domain. These SPF records identify authorized outgoing e-mail servers. The inbound server determines whether the sending e-mail server's IP address matches any of the IP addresses that are published in the SPF record.
4. If the IP addresses match, the e-mail message is authenticated and delivered to the receiver. If the IP addresses do not match, the e-mail message fails authentication and is not delivered.

Based on the evaluation of the Sender ID record, every message is stamped with a Sender ID status. Intelligent Message Filter considers this status for the final assignment of an SCL rating, if Intelligent Message Filter is enabled on the server and the status is also available as an output from the Sender ID filter.

This test reports statistics related to the anti-spamming activities performed by the Sender ID agent, and reveals its overall efficiency.

Target of the test : A server configured with the Hub Transport role

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the Hub/Edge Transport server being monitored.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	Indicates the IP address of the Hub Transport server.
Port	The port number of the Hub Transport server. By default, this is *691*.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Messages validated by Sender Id agent	Indicates the number of messages validated per second.	Msgs/Sec	
Messages with no PRA	Indicates the number of messages per second that were detected as not having a valid PRA.	Msgs/Sec	When you enable Sender ID, each message contains a Sender ID status in the metadata of the message. When an e-mail message is received, the Edge Transport server queries the sender's DNS server to verify that the IP address from which the message was received is authorized to send messages for the domain that is specified in the message headers. The IP address of the authorized sending server is referred to as the purported responsible address (PRA). PRA is calculated based on the following message headers: • Resent-Sender: • Resent-From: • Sender: • From: A high value of this measure indicates that the Sender ID agent has rejected many messages owing to an invalid

Measurement	Description	Measurement Unit	Interpretation
			PRA.
Messages with SoftFail result	Indicates the number of messages that were validated per second with a SoftFail result.	Msgs/Sec	Anti-spam stamps help you diagnose spam-related problems by applying diagnostic metadata, or "stamps," such as sender-specific information, puzzle validation results, and content filtering results, to messages as they pass through the anti-spam features that filter inbound messages from the Internet. The Sender ID (SID) stamp is based on the sender policy framework (SPF) that authorizes the use of domains in e-mail. The SPF is displayed in the message envelope as Received-SPF. The Sender ID evaluation process generates a Sender ID status for the message. If the status returned is SoftFail then it means that the IP address of the sender may not be in the SPF. Softfail is considered less trusted than Neutral, where the sender ID verification check is inconclusive.
Messages with a fail – non-existent domain - result	Indicates the number of messages that were validated per second with a Fail – Non-existent Domain result.	Msgs/Sec	
Messages with a fail – malformed domain result	Indicates the number of messages per second that were validated with a Fail – Malformed Domain result.	Msgs/Sec	
Messages with a Fail Not Permitted result	Indicates the number of messages per second that were validated with a Fail – Not Permitted result.	Msgs/Sec	
Messages with a	Indicates the number of	Msgs/Sec	The None result signifies that no

Measurement	Description	Measurement Unit	Interpretation
None result	messages per second that were validated with the result of None.		published SPF data exists in the sender's Domain Name System (DNS).
Messages with a TempError result	Indicates the number of messages per second that were validated with a TempError result.	Msgs/Sec	The TempError result denotes that a temporary DNS failure occurred, such as an unavailable DNS server.
Messages with a Neutral result	Indicates the number of messages per second that were validated with a Neutral result.	Msgs/Sec	The TempError result implies that Sender ID verification check was inconclusive.
Messages with a Pass result	Indicates the number of messages per second that were validated with a Pass result.	Msgs/Sec	A Pass result indicates that the IP Address and Purported Responsible Domain pair passed the Sender ID verification check.
Messages missing originating IP	Indicates the number of messages for which the originating IP could not be determined.	Msgs/Sec	
Messages with a PermError result	Indicates the number of messages per second that were validated with a PermError result.	Validates/Sec	A PermError result indicates that the DNS record is invalid, such as an error in the record format.

3.1.5 Store Interfaces Test

The core data storage repository for Microsoft Exchange server 2007/2010 is the Microsoft Exchange Information Store service. This test is useful in isolating and determining issues involving the interfaces between the Microsoft Exchange Information Store service on the Mailbox server and Edge/Hub Transport servers. Unlike Exchange Server 2003, Exchange 2007/2010 communicates with Hub Transport servers via RPC, not Simple Mail Transfer Protocol (SMTP), and therefore latency and queuing are a greater concern. This test isolates and determines issues involving the interface between the Microsoft Exchange Information Store service on the Mailbox server and Hub Transport servers.

Target of the test : A server configured with the Hub Transport role

Agent deploying the test : An internal agent

Outputs of the test : One set of results for each interface between the Exchange store and the Hub transport server being monitored.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	Indicates the IP address of the Hub Transport server.
Port	The port number of the Hub Transport server. By default, this is *691*.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Active connections to connection caches	Indicates the number of active connections in all connection caches for this interface.	Number	
Idle connections to connection caches	Indicates the current number of idle connections in all connection caches for this interface.	Number	Ideally, the value of this measure should be zero, as idle connections in a cache are only resource drainers.
Current RPC requests outstanding	Indicates the current number of outstanding RPC requests for this interface.	Number	Ideally, the value of this measure should be 0.
Data transfer over an RPC call - average	Indicates the average number of bytes, sent to the server in one RPC call via this interface.	KB	These measures serve as good indicators of the data load generated by the RPC traffic to and from the Hub transport server.
Avg. data received per RPC call	Indicates the average number of bytes, received from the server in one succeeded RPC call via this interface.	KB	
Average RPC	Indicates the average	Msecs	Average is calculated over all RPCs

Measurement	Description	Measurement Unit	Interpretation
latency	latency in milliseconds, averaged across all RPC operations in the past 1024 RPC packets.		since exrpc32 was loaded. Ideally, this value should be less than 25 ms. High RPC latencies often cause significant delays in the Mailbox server – Hub Transport server interactions, and hence need to be eliminated.
Slow RPC requests	Indicates the percentage of slow RPC requests in the RPC queue, currently.	Percent	A slow RPC request is one that has taken more than 2 seconds. Any value higher than 5% for this measure is a cause for concern.
RPC requests failed	Indicates the percentage of requests in the RPC queue that currently failed.	Percent	Ideally, this value should be 0. A non-zero value for this measure migt warrant an investigation.
RPC requests succeeded	Indicates the percentage of RPC requests in the queue that currently succeeded.	Percent	

3.1.6 Transport Queues Test

A queue is a temporary holding location for messages that are waiting to enter the next stage of processing. Each queue represents a logical set of messages that an Exchange transport server processes in a specific order. Queues exist only on computers that have the Hub Transport server role or Edge Transport server role installed.

Long winding message queues or messages with long waiting times in a queue could indicate lapses in the processing ability of the transport servers. To verify this, it is essential for the queue length to be monitored continuously.

This test monitors the active, remote, and retry queues to figure out whether or not the transport servers are experiencing processing bottlenecks.

Target of the test : A server configured with the Hub Transport role

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every queue on the Hub Transport server being monitored.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	Indicates the IP address of the Hub Transport server.
Port	The port number of the Hub Transport server. By default, this is *691*.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Messages in the active mailbox delivery queue	Indicates the number of messages currently in active mailbox queues.	Number	Mailbox queues hold messages that are being delivered to a Mailbox server that is located in the same site as the Hub Transport server. Mailbox delivery queues exist only on Hub Transport servers. One mailbox delivery queue exists for each destination Mailbox server. If the number of messages in the queue grows continuously, it could indicate a processing bottleneck. You might want to investigate this condition further.
Messages in the retry mailbox delivery queue	Indicates the number of messages currently in retry in the mailbox queues.	Number	Retry is a renewed connection attempt with the destination domain, smart host, or Mailbox server. Messages in this queue are in a retry state because an issue prevented their delivery. If the issue is transient, a subsequent reattempt to send the message may be successful. A high value for this measure could indicate any of the following: • A domain to which you send a large

Measurement	Description	Measurement Unit	Interpretation
			amount of e-mail is down or experiencing problems. • A computer on your network may be infected with a virus which is sending messages through your Exchange servers. • Your DNS server may have some issue resolving fully qualified domain names (FQDNs) to IP addresses. • There may be a network connectivity issue that is preventing your server from properly connecting to destination servers, or the internet. Some possible issues that could affect your connection are: • Router or routing issues between your server and the destination • Proxy or gateway server issues. • Internet Service providers (ISP) issues, such as a cut line, downed system, routing issues, global disturbance, or some other issue. The resolution to a high retry remote delivery queue length depends on the root cause of this problem. Try one or more of the following to identify and resolve the problem causing the high volume of messages in the remote delivery queue.: • Check the destination addresses for

Measurement	Description	Measurement Unit	Interpretation
			the messages in the retry queue. If the messages are all addressed to a single domain or small number of domains, verify that the specified domains are valid and functional. • Verify that there are no machines on your network that are infected with a virus which might be sending messages through your Exchange server(s). Take steps to remove the virus from the infected machine, or remove the machine from your network. • Check where the retry messages are being sent to, if there a large number of messages addressed to companies that you do not know, do not regularly work with, or with unusual subject lines that look to be spam in nature. • Confirm that your DNS server can resolve the FQDNs of the affected domains mail exchanger (MX) resource records to IP by using the NSLOOKUP command. Confirm that there are no network connectivity issues preventing your server from properly connecting to destination servers or the Internet.
Messages in the active remote delivery queue	Indicates the number of messages currently in active remote delivery	Number	Remote delivery queues hold messages that are being delivered to a remote domain or smart host by using the

Measurement	Description	Measurement Unit	Interpretation
	queues.		Simple Mail Transfer Protocol (SMTP). After all messages are delivered, these queues persist for three minutes and then are automatically deleted. A high value of this measure could indicate a processing bottleneck or a poor network link between the Hub Transport server and the remote domain to which messages are to be delivered.
Messages in the retry remote delivery queue	Indicates the number of messages currently in the retry remote delivery queues.	Number	Retry is a renewed connection attempt with the destination domain, smart host, or Mailbox server. Messages in this queue are in a retry state because an issue prevented their delivery. If the issue is transient, a subsequent reattempt to send the message may be successful. A high value for this measure could indicate any of the following: • A domain to which you send a large amount of e-mail is down or experiencing problems. • A computer on your network may be infected with a virus which is sending messages through your Exchange servers. • Your DNS server may have some issue resolving fully qualified domain names (FQDNs) to IP addresses. • There may be a network connectivity issue that is preventing your server from properly connecting to

Measurement	Description	Measurement Unit	Interpretation
			destination servers, or the internet. Some possible issues that could effect your connection are: • Router or routing issues between your server and the destination • Proxy or gateway server issues. • Internet Service providers (ISP) issues, such as a cut line, downed system, routing issues, global disturbance, or some other issue. The resolution to a high retry remote delivery queue length depends on the root cause of this problem. Try one or more of the following to identify and resolve the problem causing the high volume of messages in the remote delivery queue.: • Check the destination addresses for the messages in the retry queue. If the messages are all addressed to a single domain or small number of domains, verify that the specified domains are valid and functional. • Verify that there are no machines on your network that are infected with a virus which might be sending messages through your Exchange server(s). Take steps to remove the virus from the infected machine, or remove the machine from your

Measurement	Description	Measurement Unit	Interpretation
			network. • Check where the retry messages are being sent to, if there a large number of messages addressed to companies that you do not know, do not regularly work with, or with unusual subject lines that look to be spam in nature. • Confirm that your DNS server can resolve the FQDNs of the affected domains mail exchanger (MX) resource records to IP by using the NSLOOKUP command. • Confirm that there are no network connectivity issues preventing your server from properly connecting to destination servers or the Internet.
Messages in the active Non-SMTP delivery queue	Indicates the number of messages currently in the Drop directory that is used by a Foreign connector.	Number	This refers to the number of messages in the queue for which the Delivery Type has been set to NonSmtpGatewayDelivery. The messages in such a queue are typically queued for delivery to an external recipient by using a non-SMTP connector on the local server.
Messages in the retry Non-SMTP delivery queue	Indicates the number of messages currently in retry in the non-SMTP gateway delivery queues.	Number	Messages in this queue are in a retry state because an issue prevented their delivery. If the issue is transient, a subsequent reattempt to send the message may be successful. The value of this measure could rise, owing to the following reasons: • A connector that connects to the Non-

Measurement	Description	Measurement Unit	Interpretation
			SMTP mail server might not be functioning properly. • A domain that you connect to via a Non-SMTP connector might be down or unreachable. • Your DNS server may have some issue resolving fully qualified domain names (FQDNs) to IP addresses. • There may be a network connectivity issue that is preventing your server from properly connecting to destination servers or the Internet. Some possible issues that could affect your connection are: • Router or routing issues between your server and the destination • Proxy or gateway server issues. • Internet Service providers (ISP) issues, such as a cut line, downed system, routing issues, global disturbance, or some other issue.
Messages in the aggregate delivery queue	Indicates the number of messages currently queued for delivery in all queues.	Number	
Largest delivery queue length	Indicates the number of messages that are currently queued to a given Exchange Hub Transport server or Edge Transport server.	Number	When this value is high, the server cannot establish a SMTP session to the other Hub Transport or Edge Transport server. Other symptoms you may experience when this threshold is reached are reduced intra-site, inter-site,

Measurement	Description	Measurement Unit	Interpretation
			and external mail flow. This alert may be caused by one or more of the following conditions: • Problem with a specific Hub Transport server or Edge Transport server. For example, one or more required services may not be running. • Issues with network connectivity, routers, or firewalls.
Messages in the unreachable queue	Indicates the number of messages currently in the Unreachable queue.	Number	The categorizer sends messages to the unreachable queue when there is no known route to their destinations. Typically, an unreachable destination is caused by a configuration error that affects the delivery path By default, the messages in the unreachable queue have the status of Ready. Messages in the unreachable queue are never automatically resubmitted. Messages remain in the unreachable queue until they are manually resubmitted by an administrator, removed by an administrator, or the value specified in the MessageExpirationTimeOut parameter passes.
Messages in the poison queue	Indicates the number of messages currently in the poison queue.	Number	The poison message queue contains messages that are determined to be potentially harmful to the Microsoft Exchange server 2007/2010 server after a server failure. The messages may be genuinely harmful in their content and format. Alternatively, they may be the results of a poorly written agent that has caused the Exchange server to fail when it processed the supposedly bad

Measurement	Description	Measurement Unit	Interpretation
			messages. Messages remain in the poison message queue until they are manually resumed or removed by an administrator. The messages in the poison message queue are never automatically resumed or expired.
Messages in the submission queue	Indicates the number of messages currently in the submission queue.	Number	A sustained high Submission Queue Length value may indicate that an excessive amount of inbound messages have over-loaded the categorizer. It may also indicate that there is an issue with message categorization. Message resubmission sends undelivered messages back to the submission queue to be processed again by the categorizer. A sustained high Submission Queue Length may be caused by one or more of the following: • The server is being over-utilized and does not have enough resources to satisfy all of the current requests. This situation may occur if there are more messages being submitted for transport then the server can handle. Similarly, it may also occur if many messages are being resubmitted for categorization. • There is a problem with a custom event sink or rule, or a third-party event sink or rule.

3.1.7 SMTP Receive Connectors Test

Smtp Receive connectors are configured on computers that are running Microsoft Exchange server 2007/2010 and that have Hub Transport and Edge Transport server roles installed. The Smtp Receive Connector represents a logical gateway through which inbound messages are received. This test monitors the statistics of smtp receive connectors.

Using this test, you can periodically observe the traffic conducted by the Receive connectors, and be promptly alerted when the connector rejects messages.

Target of the test : A server configured with the Hub Transport role

Agent deploying the test : An internal agent

Outputs of the test : One set of results for each receive connector on the Hub Transport server being monitored.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	Indicates the IP address of the Hub Transport server.
Port	The port number of the Hub Transport server. By default, this is *691*.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Current SMTP connections to the server	Indicates the current number of outbound connections from the SMTP Receive connectors.	Number	
Messages received by the server	Indicates the number of messages received by the SMTP Receive connector each second.	Msgs / Sec	This is a good indicator of the load on the Receive connector.
Data received by SMTP server	Indicates the number of bytes received per	Bytes/Sec	This is a good indicator of the load on the Receive connector.

Measurement	Description	Measurement Unit	Interpretation
	second.		
Messages refused due to size limit	Indicates the number of messages that were rejected currently because they were too big.	Number	Ideally, this value should be 0.
Avg. size of messages	The average number of message bytes per inbound message received.	Bytes / Msg	
Avg. recipients per message	Indicates the average recipients per message handled by this SMTP Receive connector.	Recipients/Msg	
Avg. data transfer per connection	Indicates the average number of bytes received per connection.	Bytes/Conn	
Avg. messages per connection	Indicates the average number of message bytes per inbound message received.	Msgs/Conn	

3.1.8 Exchange Store Drivers Test

The Store driver on the Hub Transport server places messages from the transport pipeline into the appropriate mailbox. The Store driver on the Hub Transport server also adds messages from the Outbox of a sender on the Mailbox server to the transport pipeline.

This test monitors the overall health of each of the Store Drivers.

Target of the test : A server configured with the Hub Transport role

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the Hub Transport server being monitored.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	Indicates the IP address of the Hub Transport server.
Port	The port number of the Hub Transport server. By default, this is *691*.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Inbound data delivered	Indicates the number of requests processed from clients during the last measurement period.	KB	
Inbound failed recipients	Indicates the number of failed deliveries during the last measurement period.	Number	Ideally, this value should be 0. A non-zero value requires further investigation.
Inbound succeeded recipients	Indicates the number of successful deliveries during the last measurement period.	Number	
Inbound local delivery calls	Indicates the number of local delivery attempts per second during the last measurement period.	Calls/Sec	
Inbound message delivery attempts	Indicates the number of attempts for delivering messages per second during the last measurement period.	Attempts/Sec	
Inbound delivering threads	Indicates the number of threads used in delivery currently.	Number	
Inbound recipients delivered	Indicates the number of recipients to whom messages were delivered per second.	Recipients/Sec	

Measurement	Description	Measurement Unit	Interpretation
Outbound submitted mail items	Indicates the number of mail messages per second being submitted for delivery.	Mails/Sec	

3.1.9 Pickup Directory Test

By default, the pickup directory exists on every Microsoft Exchange server 2007/2010 computer that has the Hub transport server role or the Edge Transport server role installed. Correctly formatted e-mail message files that you copy to the Pickup directory are submitted for delivery. The Pickup directory is used by administrators for mail flow testing or by applications that must create and submit their own messages. This test monitors the performance of the Pickup directory and reveals whether or not it has been able to submit all messages it contains for delivery.

Target of the test : A server configured with the Hub Transport role

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the Hub Transport server being monitored.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	Indicates the IP address of the Hub Transport server.
Port	The port number of the Hub Transport server. By default, this is *691*.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Messages submitted to the pickup directory	Indicates the number of messages that were successfully submitted for delivery by the Pickup directory during the last measurement period.	Number	

Measurement	Description	Measurement Unit	Interpretation
Messages to the pickup directory that caused NDR creations	Indicates the number of messages processed by the Pickup directory that caused NDRs to be created during the last measurement period.	Number	A correctly-formatted message file together with a valid sender that can't be successfully submitted for delivery by the Pickup directory generates a non-delivery report (NDR). Malformed content or Pickup directory message restriction violations could also cause the Pickup directory to generate an NDR. When an NDR is generated during Pickup directory message processing, the original message file is attached to the NDR message, and the message file is deleted from the Pickup directory. A correctly formatted message that is submitted by the Pickup directory may later experience a delivery failure and be returned to the sender with an NDR. This kind of failure may be caused by transmission issues that are unrelated to the Pickup directory, such as messaging server failures or routing failures along the delivery path of the message.
Badmailed messages to the pickup directory	Indicates the number of messages that were submitted to the Pickup directory but were classified as badmail and not delivered, during the last measurement period.	Number	A message that is classified as badmail has serious problems that prevent the Pickup directory from submitting the message for delivery. The other condition that causes badmail is when the message is formatted correctly, but the recipients are not valid, and an NDR message can't be sent to the sender because the sender is not valid. Message files that are determined to be badmail are left in the Pickup directory and are renamed from <filename>.eml to <filename>.bad. If the <filename>.bad file already exists, the file is renamed to <filename><datetime>.bad. If badmail exists in the Pickup directory, an event log error is generated, but the same

Measurement	Description	Measurement Unit	Interpretation
			badmail messages do not generate repeated event log errors.

3.1.10 Exchange Messages Test

This test tracks the flow of messages through an Exchange 2007/2010 organization, and reports the number and size of messages that pertain to every key event type handled by the Exchange 2007/2010 server. These types include the following:

Type	Description
SEND	A message sent by Simple Mail Transfer Protocol (SMTP) to a different server.
RECEIVE	A message received and committed to the database.
SUBMIT	A message submitted by an Exchange 2007/2010 computer that has the Mailbox server role installed to an Exchange 2007/2010 computer that has the Hub Transport server role or Edge Transport server role installed.
POISON	A message added to the poison message queue or removed from the poison message queue.
FAIL	Message delivery failed

Whenever a user complaints of not being able to send or receive mails, the metrics reported by this test and the detailed diagnosis information provided therein will enable administrators to accurately determine the current status of the email sent by the user.

If need be, administrators can configure this test to additionally report the total number of messages on the Exchange 2007/2010 server and their total size, regardless of event type. Apart from the event types discussed above, this total will also include messages that belong to the following event types:

Type	Description
BADMAIL	A message submitted by the Pickup directory or the Replay directory that cannot be delivered or returned
DELIVER	A message delivered to a mailbox
DEFER	A message for which delivery was delayed

Type	Description
DSN	A message for which a delivery status notification (DSN) was generated
EXPAND	A distribution group was expanded
FAIL	Message delivery failed
REDIRECT	A message redirected to an alternative recipient after an Active Directory directory service lookup
RESOLVE	A message for which recipients were resolved to a different e-mail address after an Active Directory lookup
TRANSFER	Recipients were moved to a forked message because of content conversion, message recipient limits, or agents

Exchange administrators can use this total to accurately assess the overall message traffic on the server and the ability of the server to handle the inflow/outflow of messages.

Target of the test : A server configured with the Hub Transport role

Agent deploying the test : An internal agent

Outputs of the test : One set of results for each of the following event types: SEND, RECEIVE, FAIL, POISON, SUBMIT.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	Indicates the IP address of the Hub Transport server.
Port	The port number of the Hub Transport server. By default, this is *691*.
XchgExtensionShellPath	The Exchange Management Shell is a command-line management interface, built on Windows PowerShell which enables you to administer every part of Microsoft Exchange. This test uses the Exchange management shell to run scripts and collect the desired performance metrics from the Exchange server. By default, the test auto-discovers the location of the Exchange management shell and thus, automatically loads the Exchange management shell snap-in (exshell.psc1) for script execution. This is why, the XchgExtensionShellPath is set to *none* by default.
AllEvents	By default, this flag is set to **false**, indicating that this test will report metrics for only the following event types by default: SEND, RECEIVE, SUBMIT, FAIL,

Parameters	Description
	POISON. If you want the test to additionally report metrics across all event types – i.e., support an additional *All* descriptor, which will report the total number of emails handled by the server and their total size – then, set this flag to **true**.
DDForSendMessage	In large, highly active Exchange environments, hundreds of emails may be sent by the Exchange server within a short period of time. In such environments, the frequent collection of detailed diagnosis information related to the sent emails may increase the processing overheads of the eG agent, and may even choke the eG database. To avoid this, the DDForSendMessage flag is set to **No** by default; this implies that the test will not provide the detailed diagnosis for the SEND descriptor – i.e., for the sent messages – by default. To view detailed diagnosis for these messages as well, set this flag to **Yes**.
DDForSubmitMessage	In large, highly active Exchange environments, hundreds of emails may be submitted to the transport pipeline within a short period of time. In such environments, the frequent collection of detailed diagnosis information related to the submitted emails may increase the processing overheads of the eG agent, and may even choke the eG database. To avoid this, the DDForSubmitMessage flag is set to **No** by default; this implies that the test will not provide the detailed diagnosis for the SUBMIT descriptor – i.e., for the sent messages – by default. To view detailed diagnosis for these messages as well, set this flag to **Yes**.
IsPassive	If the value chosen is **Yes**, then the Exchange server under consideration is a passive server in an Exchange cluster. No alerts will be generated if the server is not running. Measures will be reported as "Not applicable" by the agent if the server is not up.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Number of emails	Indicates the number of emails of this event type detected during this measurement period.	Number	By default, this measure provides detailed diagnosis for the FAIL and POISON messages only. Using the detailed diagnosis of these descriptors, you can view the complete details of the failed and poison messages. Optionally, users can turn on detailed diagnosis generation for the

Measurement	Description	Measurement Unit	Interpretation
			RECEIVE, SEND, and SUBMIT messages as well, so as to view the complete details of such messages. The **All** descriptor, even if displayed, will not provide detailed diagnosis information.
Total traffic	Indicates the total size of messages of this event type, during the last measurement period.	Number	Since the value of this measure includes the size of attachments, an unusually high value could indicate that one/more messages carry large attachments. A high value could also indicate the availability of a large number of messages of a particular type.

3.1.11 Exchange Extensible Agents Test

Transport agents let you install custom software, created by Microsoft, by third-party vendors, or by your organization, on a computer that is running Microsoft Exchange server 2007/2010. This software can then process e-mail messages that pass through the transport pipeline on a Hub Transport server or Edge Transport server. Custom transport agents provide additional functionality to Exchange 2007/2010, such as anti-spam or antivirus programs or any transport function that your organization may require.

Delays in e-mail processing by the transport agents and flaws while performing anti-spam /anti-virus activities may affect the stability and security of Exchange. By periodically checking how the agents process e-mail messages, you can easily spot processing bottlenecks and security lapses. This test does just that.

Target of the test : A server configured with the Hub Transport role

Agent deploying the test : An internal agent

Outputs of the test : One set of results for theHub Transport server being monitored.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	Indicates the IP address of the Hub Transport server.
Port	The port number of the Hub Transport server. By default, this is *691*.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Agent processing time	Indicates the time taken by the transport agent per event for processing e-mail messages.	Secs	Ideally, the value of this measure should be low. A high value indicates that the agent is taking too long a time to process e-mail messages. The reason for this needs to be investigated. Sustained higher latencies may indicate a hung agent.
Total agent invocations	Indicates the total number of agent invocatins since last restart.	Number	

3.1.12 Exchange Transport Dumpster Test

The transport dumpster is a feature of the Hub Transport server role that submits recently delivered mail after an unscheduled outage. The transport dumpster should always be turned on when using CCR or local continuous replication (LCR). The transport dumpster is enabled organization wide by setting the amount of storage available per storage group and setting the time to retain mail in the transport dumpster. If either of these settings are violated in real-time, then the transport dumpster starts deleting mails.

Using this test, you can closely monitor the transport dumpster and the mails within, determine how often the Exchange server experienced outages, and also figure out whether any critical mails were lost during downtime.

Target of the test : A server configured with the Hub Transport role

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the Hub Transport server being monitored.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	Indicates the IP address of the Hub Transport server.
Port	The port number of the Hub Transport server. By default, this is *691*.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Overall size of the Dumpster	Indicates the total size of the mail items(in bytes) that are currently in the transport dumpster on this server.	Bytes	A low value is typically desired for this measure. A very high value or a value that increases consistently could reveal a prolonged outage. If the value exceeds or is dangerously close to the value of the MaxDumpsterSizePerStorageGroup parameter, it could mean that mails will soon be deleted from the dumpster.
Dumpster inserts rate	Indicates the rate at which mails were inserted in the dumpster.	Inserts/Sec	
Number of current items	Indicates the total number of mail items that are currently available in the transport dumpster on this server.	Number	A low value is typically desired for this measure. A very high value or a value that increases consistently could reveal a prolonged outage.
Dumpster deletions rate	Indicates the rate at which items were deleted from the dumpster.	Deletes/Sec	A high rate of deletion is typically indicative of the frequent violation of the MaxDumpsterSizePerStorageGroup and/or the MaxDumpsterTime setting. These parameters have been discussed below: • **MaxDumpsterSizePerStorageGroup**: This parameter specifies the maximum size of the transport dumpster queue for

Measurement	Description	Measurement Unit	Interpretation
			each storage group. It is recommended that you set this to a size that is 1.5 times the size of the maximum message that can be sent in the organization. If the organization has no size limits, we recommend you configure the MaxDumpsterSizePerStorageGroup parameter to a size that is 1.5 times the size of the average message size sent in the organization. For example, if the maximum size for messages is 10 megabytes (MB), you should configure the MaxDumpsterSizePerStorageGroup parameter with a value of 15 MB. • **MaxDumpsterTime**: This parameter specifies how long an e-mail message should remain in the transport dumpster queue, to a value of 07.00:00:00, which is 7 days. This amount of time is sufficient to allow for an extended outage to occur without loss of e-mail. When using the transport dumpster feature, additional disk space is needed on the Hub Transport server to host the transport dumpster queues. The amount of storage space required is approximately equal to the value of MaxDumpsterSizePerStorageGroup multiplied by the number of storage groups. If you do not configure the transport dumpster, the default values are used. The default value for the

Measurement	Description	Measurement Unit	Interpretation
			MaxDumpsterSizePerStorageGroup parameter is 18 MB and the default value for the MaxDumpsterTime parameter is 7 days. If either the size limit or time limit is reached, messages are removed from the transport dumpster queue by order of first in, first out.

3.1.13 Exchange Email Traffic Test

Periodic workload monitoring is imperative to evaluate the processing ability of the Exchange 2010 server and to proactively detect potential overload conditions. By continuously monitoring the email traffic to and from the Exchange server, this test turns a spotlight on the workload of the Exchange server, helps detect overload conditions, and also points you to the source of the overload – mails sent/received by users in the intranet? Or mail traffic over the internet?

Target of the test : A server configured with the Hub Transport role

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the Mailbox server being monitored.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	Indicates the IP address of the Hub Transport server.
Port	The port number of the Hub Transport server. By default, this is *691*.
XchgExtensionShellPath	The Exchange Management Shell is a command-line management interface, built on Windows PowerShell which enables you to administer every part of Microsoft Exchange. This test uses the Exchange management shell to run scripts and collect the desired performance metrics from the Exchange server. By default, the test auto-discovers the location of the Exchange management shell and thus, automatically loads the Exchange management shell snap-in (exshell.psc1) for script execution. This is why, the XchgExtensionShellPath is set to *none* by default.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed

Parameters	Description
	measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Internal mails received	Indicates the number of mails received by the Exchange server from the intranet.	Number	In the event of an overload, you can compare the value of this measure with the value of the Internal mails sent, External mails received, and External mails sent measures to determine what could have contributed to the overload – is it because of incoming or outgoing mail traffic? Is it because of the exchange of mails over the intranet or the internet? To know the email IDs that received the emails, the number of emails that each ID received, and the total size of the emails to an ID, use the detailed diagnosis of this test.
Internal mails received size	Indicates the total size of the mails received by the	KB	

Measurement	Description	Measurement Unit	Interpretation
	Exchange server from the intranet.		
Internal mails sent	Indicates the number of mails sent by the Exchange server to the intranet.	Number	In the event of an overload, you can compare the value of this measure with the value of the Internal mails received, External mails received, and External mails sent measures to determine what could have contributed to the overload – is it because of incoming or outgoing mail traffic? Is it because of the exchange of mails over the intranet or the internet? To know the email IDs that sent the emails, the number of emails that each ID sent, and the total size of the emails from an ID, use the detailed diagnosis of this test.
Internal mail sent size	Indicates the total size of the mails sent by the Exchange server to the intranet.	KB	
External mails received	Indicates the number of mails received by the Exchange server from the internet.	Number	In the event of an overload, you can compare the value of this measure with the value of the Internal mails received, Internal mails sent, and External mails sent measures to determine what could have contributed to the overload – is it because of incoming or outgoing mail traffic? Is it because of the exchange of mails over the intranet or the internet? To know the email IDs that received the emails, the number of emails that each ID received, and the total size of the emails to an ID, use the detailed diagnosis of this test.
External mail	Indicates the total size of	KB	

Measurement	Description	Measurement Unit	Interpretation
received size	the mails received by the Exchange server from the internet.		
External mails sent	Indicates the number of mails sent by the Exchange server to the internet.	Number	In the event of an overload, you can compare the value of this measure with the value of the Internal mails sent, Internal mails sent, and External mails received measures to determine what could have contributed to the overload – is it because of incoming or outgoing mail traffic? Is it because of the exchange of mails over the intranet or the internet? To know the email IDs that sent the emails, the number of emails that each ID sent, and the total size of the emails from an ID, use the detailed diagnosis of this test.
External mail sent size	Indicates the total size of mails sent by the Exchange server to the internet.	KB	

Use the detailed diagnosis of the *Internal mails received* measure to know the internal email IDs that received the emails, the number of emails that each ID received, and the total size of the emails received by an ID. This way, you can quickly identify the email ID that received the maximum number of emails and that which received mails of the maximum size.

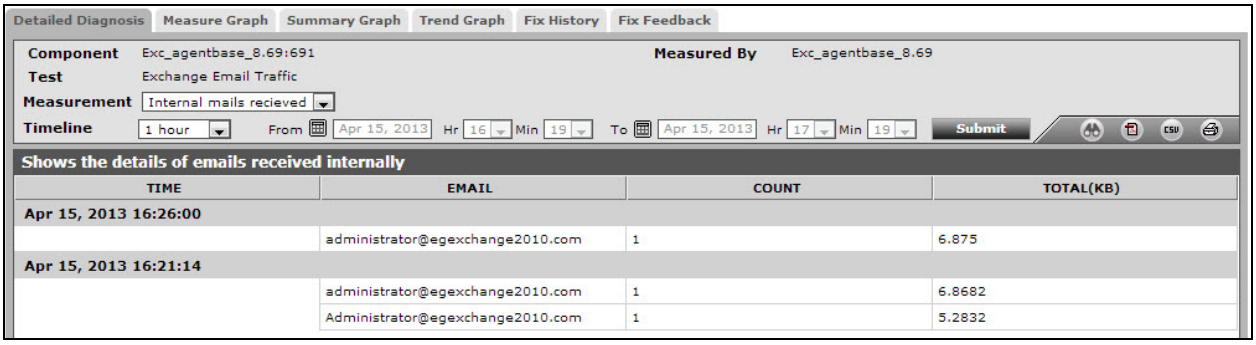

Figure 3.4: The detailed diagnosis of the Internal mails received measure

Use the detailed diagnosis of the *Internal mails sent* measure to know the internal email IDs that sent the emails, the number of emails that were sent from each ID, and the total size of the emails sent from an ID. This way, you can quickly identify the email ID that sent the maximum number of emails and that which sent mails of the maximum size.

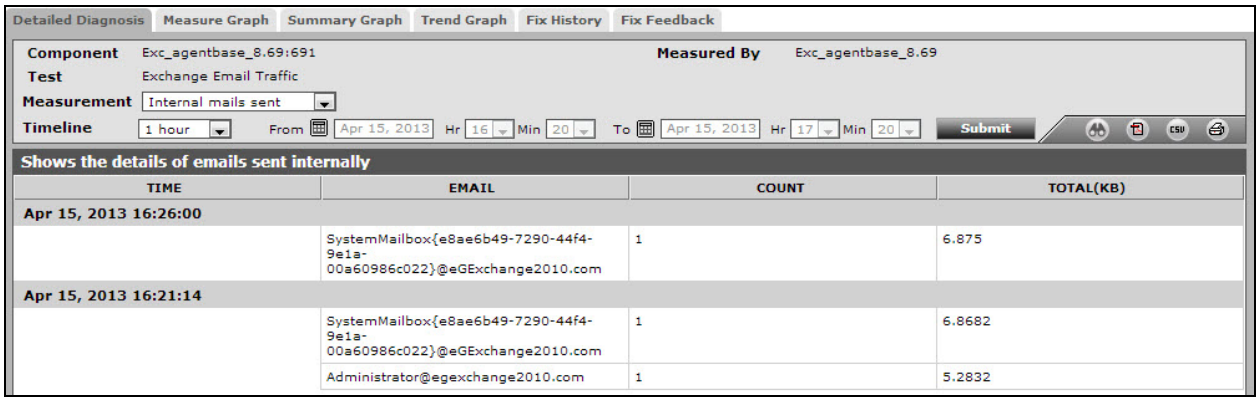

Figure 3.5: The detailed diagnosis of the Internal mails sent measure

About eG Innovations

eG Innovations provides intelligent performance management solutions that automate and dramatically accelerate the discovery, diagnosis, and resolution of IT performance issues in on-premises, cloud and hybrid environments. Where traditional monitoring tools often fail to provide insight into the performance drivers of business services and user experience, eG Innovations provides total performance visibility across every layer and every tier of the IT infrastructure that supports the business service chain. From desktops to applications, from servers to network and storage, from virtualization to cloud, eG Innovations helps companies proactively discover, instantly diagnose, and rapidly resolve even the most challenging performance and user experience issues.

eG Innovations is dedicated to helping businesses across the globe transform IT service delivery into a competitive advantage and a center for productivity, growth and profit. Many of the world's largest businesses use eG Enterprise to enhance IT service performance, increase operational efficiency, ensure IT effectiveness and deliver on the ROI promise of transformational IT investments across physical, virtual and cloud environments.

To learn more visit www.eginnovations.com.

Contact Us

For support queries, email support@eginnovations.com.

To contact eG Innovations sales team, email sales@eginnovations.com.