OMi Management Pack for Microsoft Skype for Business Server

Software Version: 1.00

For Operations Manager i for Linux and Windows® operating systems

Reference Guide

Hewlett Packard Enterprise

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Documentation Updates

To check for recent updates or to verify that you are using the most recent edition of a document, go to: https://softwaresupport.hpe.com/.

This site requires that you register for an HPE Passport and to sign in. To register for an HPE Passport ID, click **Register** on the HPE Software Support site or click **Create an Account** on the HPE Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HPE sales representative for details.

Support

Visit the HPE Software Support site at: https://softwaresupport.hpe.com/.

Most of the support areas require that you register as an HPE Passport user and to sign in. Many also require a support contract. To register for an HPE Passport ID, click **Register** on the HPE Support site or click **Create an Account** on the HPE Passport login page.

To find more information about access levels, go to: https://softwaresupport.hpe.com/web/softwaresupport/access-levels.

HPE Software Solutions Now accesses the Solution and Integration Portal website. This site enables you to explore HPE product solutions to meet your business needs, includes a full list of integrations between HPE products, as well as a listing of ITIL processes. The URL for this website is https://softwaresupport.hpe.com/km/KM01702731.

Contents

Chapter 1: OMi MP for Microsoft Skype for Business Server Collection and Metrics

This chapter provides information about the OMi MP for Microsoft Skype for Business Server collections, metrics, and data store tables which can be used to configure the data-collection process.

Each collection contains a number of metrics which are listed under the related collection.

Field	Description
Schedule Task policy	Defines schedule for the collection
Config File	Contains definition for schedule. Maps collection to schedule task policy.
Aspect	Contains all the policies required for the collection.
CIT	Instance to which you can deploy Aspect.
Data source / data class	Database where the data is logged.
Source/ Collection Def	Following are the possible source and collection definition for OMi MP for Microsoft Skype for Business Server: Performance Counter / Object Windows Services/ Service Name Powershell / powershell command SQL / SQL query Port / port url/url
Metric	Metric label
Description	Metric description
Metric Spec	CODA column
Metric field	Metric that is monitored.
Alarm	If true, events are generated. Details about the cause, impact, and solution is mentioned. If false, metric will only log data.

Collection and Metrics

ChkLyncReplicaReplicatorAgentServStat

The policy contains the metric definition XML which will get used by Microsoft Collector to collect metrics.

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / NA

Source / Collection Definition: SERVICECHECK / Replica

Metric: LyncReplicaServname

> **Description**: Name of the Service
>
> **Metric SpecName**: SERVNAME
>
> **Metric Field Name**: Service_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: LyncReplicaDisplayName

> **Description**: Display Name of the Service
>
> **Metric SpecName**: SRVDISPNAME
>
> **Metric Field Name**: Service_Displayname
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: LyncReplicaServStatus

Description: Status of the Service

Metric SpecName: SERVSTATUS

Metric Field Name: Service_Status

Data type: TEXT

Alarm: FALSE

Metric: LyncReplicaServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_LyncReplicaServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

ChkFrontEndOnlineLogRetentionServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SERVSTAT

Source / Collection Definition: SERVICECHECK / RTCLRSVC

Metric: FERTCLRSVCServName

> **Description**: Name of the Service
>
> **Metric SpecName**: SERVNAME
>
> **Metric Field Name**: Service_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FERTCLRSVCServDisplayName

> **Description**: Display Name of the Service
>
> **Metric SpecName**: SRVDISPNAME
>
> **Metric Field Name**: Service_Displayname
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FERTCLRSVCServStatus

> **Description**: Status of the Service
>
> **Metric SpecName**: SERVSTATUS
>
> **Metric Field Name**: Service_Status
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FERTCLRSVCServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_FERTCLRSVCServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): Lync Online Log Retention Service' Windows Service is stopped.

Potential Impact: NA

Suggested Action(s): Lync Online Log Retention Service' Windows Service is stopped. Please restart the service.

Collect_Edge_DataProxy_Client_Connections

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / LSDATAPROXY

Source / Collection Definition: PERFMON / LS:DATAPROXY - 01 - Client Connections(*)

Metric: EdgeDataProxyClientInstance

Description: instance of perfmon object LS:DATAPROXY - 01 - Client Connections

Metric SpecName: DPCLIENTINSTANAME

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: Clientsdisconpersecduetoinvalidcookiedata

Description: number of clients disconnected in a second because of invalid cookie data.

Metric SpecName: CLIENTDISCONNDINVALDCOOKIDATA

Metric Field Name: DATAPROXY - 012 - Clients disconnected per second due to invalid cookie data

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 100

Policy: MSBS_Clientsdisconpersecduetoinvalidcookiedata

Message text: The value of the counter 'Clients disconnected per second due to invalid cookie data' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: Clientsdisconpersecduetoinvalidcookietimstmp

Description: number of clients rejected in a second because of invalid timestamps.

Metric SpecName: CLIENTDISCONNDINVALDCOOKITIMESTMP

Metric Field Name: DATAPROXY - 008 - Clients disconnected per second due to invalid cookie timestamp

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 100

Policy: MSBS_Clientsdisconpersecduetoinvalidcookietimstmp

Message text: The value of the counter 'Clients disconnected per second due to invalid cookie timestamp' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Collect_Monitoring_CDR Service_READ

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / NA

Source / Collection Definition: PERFMON / LS:CDR Service - 01 - READ(*)

Metric: MonitoringCDRServiceReadInstance

Description: instance of perfmon object LS:CDR Service - 01 - READ

Metric SpecName: MONCDRSERVCEREADINSTANCE

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: MonitoringDroppedmessagesfromMQ

Description: number of messages that are dropped from the MSMQ queue.

Metric SpecName: DROPPEDMSGFRMMQ

Metric Field Name: CDR Service - 006 - Dropped messages from MQ

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20

Policy: MSBS_MonitoringDroppedmessagesfromMQ

Message text: The value of the counter 'CDR Service - 006 - Dropped messages from MQ' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: MonitoringMessagesthatfailedvalidation

Description: number of messages that failed the validation process.

Metric SpecName: MSGFAILDVALIDATION

Metric Field Name: CDR Service - 002 - Messages that failed validation

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20

Policy: MSBS_MonitoringMessagesthatfailedvalidation

Message text: The value of the counter 'CDR Service - 002 - Messages that failed validation' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: MonitoringTransactionsaborted

Description: number of transactions that are aborted.

Metric SpecName: TRANSACTIONABORTED

Metric Field Name: CDR Service - 010 - Transactions aborted

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20

Policy: MSBS_MonitoringTransactionsaborted

Message text: The value of the counter 'CDR Service - 010 - Transactions aborted' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

SimplePortWatcher5066

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / Port5066

Source / Collection Definition: PORTCOL / PORTCHECKER

Metric: SimpleWatcherPort5066

Description: Used for outbound Enhanced 9-1-1 (E9-1-1) gateway.

Metric SpecName: SimpleWatcherPort5066

Metric Field Name: SimpleWatcherPort5066

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort5066

Message text: The Port No:5066 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

Metric: SimpleWatcherPort5066

Description: Used for outbound Enhanced 9-1-1 (E9-1-1) gateway.

Metric SpecName: SimpleWatcherPort5066

Metric Field Name: SimpleWatcherPort5066

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_SimpleWatcherPort5066

Message text: The Port No:5066 is down

Instructional Text:

Probable Cause(s): The watcher node does not have the required permissions. The DNS client side cache has a stale entry. The DNS infrastructure is not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available.

Potential Impact: Connection to port cannot be established.

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

> **Description**: This is the key for metric
>
> **Metric SpecName**: HOSTNAME
>
> **Metric Field Name**: HOSTNAME
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

ConferenceFailurePercentage

The policy contains the metric definition XML which will get used by Microsoft Collector to collect metrics.

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / CONFERENCEFAILURE

Source / Collection Definition: SQLDB / select isnull(cast(100.0 * cast((SUM(CASE WHEN CS.ResponseCode != 200 THEN 1 ELSE 0 END)) as float) / cast((SUM(CASE WHEN CS.ResponseCode is NOT NULL THEN 1 ELSE 0 END)) as float) as decimal(4, 1)),0) as ConferenceFailurePercentage,SERVERPROPERTY('MACHINENAME') AS 'ServerName' from [LcsCDR].[dbo].ConferenceSessionDetails CS LEFT OUTER JOIN [LcsCDR].[dbo].SessionDetails SD ON SD.SessionIdTime = CS.SessionIdTime where CS.SessionIdTime >= dateadd (MINUTE,@Duration,GETUTCDATE())

Metric: ConferenceFailurePercentage

Description: This metric captures call failures periodically from the CDR database and raises an alert whenever call failures exceed the specified "threshold" percentage value. When a Conference call fails, this failure is reported to the Monitoring Server database (Call Detail Records database).

Metric SpecName: ConferenceFailPer

Metric Field Name: ConferenceFailurePercentage

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 40, Major / 70, Warning / 40, Major / 70

Policy: MSBS_ConferenceFailurePercentage

Message text: The current value of Percentage Conference Failure is <VALUE> which exceeds the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): This issue may occur if the Audio Video Conferencing server is overloaded, or is not getting enough CPU resources to process audio in real time.

Potential Impact: Users face issue in establishing a conference

Suggested Action(s): To resolve this issue, please check the affected machine for overall CPU consumption and remove any unnecessary competing processes. If there are no competing issues, and there is a large number of users due to which Audio Video Conferencing Server is unable to process audio in real time, consider adding more hardware to service the usage with acceptable quality.

Metric: ServerName

Description: This is the key for metric

Metric SpecName: ServerName

Metric Field Name: ServerName

Data type: TEXT

Alarm: FALSE

Metric: ConferenceFailurePercentage

Description: This metric captures call failures periodically from the CDR database and raises an alert whenever call failures exceed the specified "threshold" percentage value. When a Conference call fails, this failure is reported to the Monitoring Server database (Call Detail Records database).

Metric SpecName: ConferenceFailPer

Metric Field Name: ConferenceFailurePercentage

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 40, Major / 70, Warning / 40, Major / 70

Policy: MSBS_ConferenceFailurePercentage

Message text: The current value of Percentage Conference Failure is <VALUE> which exceeds the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): This issue may occur if the Audio Video Conferencing server is overloaded, or is not getting enough CPU resources to process audio in real time.

Potential Impact: Users face issue in establishing a conference

Suggested Action(s): To resolve this issue, please check the affected machine for overall CPU consumption and remove any unnecessary competing processes. If there are no competing issues, and there is a large number of users due to which Audio Video Conferencing Server is unable to process audio in real time, consider adding more hardware to service the usage with acceptable quality.

Metric: ServerName

Description: This is the key for metric

Metric SpecName: ServerName

Metric Field Name: ServerName

Data type: TEXT

Alarm: FALSE

Collect_Monitoing_QMS_QoEMonitoringServer

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / NA

Source / Collection Definition: PERFMON / LS:QMS - 00 - QoEMonitoringServer(*)

Metric: MonitoringQMSQoEMonitoringServerInstance

> **Description**: instance of perfmon object LS:QMS - 00 - QoEMonitoringServer
>
> **Metric SpecName**: MONQMSQOEINSTANCE
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: NofMSMQmsgsrecivdwithincorcttypeorversn

Description: number of discarded MSMQ messages that are not of the expected type or version.

Metric SpecName: NOFMSMQMSGRECIVDWINCORRTYPORVER

Metric Field Name: QMS - 004 - Number of MSMQ messages received with an incorrect type or version

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20

Policy: MSBS_NofMSMQmsgsrecivdwithincorcttypeorversn

Message text: The value of the counter 'Number of MSMQ messages received with an incorrect type or version' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: Totnofreportsdropdduetodbinsertionfail

Description: number of reports dropped because of database insertion failure. The transaction was committed prematurely because of an unrecoverable database error.

Metric SpecName: TOTNOFREPDROPDBINSFAIL

Metric Field Name: QMS - 003 - Total number of reports that were dropped due to database insertion failure

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20

Policy: MSBS_Totnofreportsdropdduetodbinsertionfail

Message text: The value of the counter ' Total number of reports that were dropped due to database insertion failure' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

ChkFrontEndApplicationSharingServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SERVSTAT

Source / Collection Definition: SERVICECHECK / RTCASMCU

Metric: FERTCASMCUServName

Description: Name of the Service

Metric SpecName: SERVNAME

Metric Field Name: Service_Name

Data type: TEXT

Alarm: FALSE

Metric: FERTCASMCUServDisplayName

Description: Display Name of the Service

Metric SpecName: SRVDISPNAME

Metric Field Name: Service_Displayname

Data type: TEXT

Alarm: FALSE

Metric: FERTCASMCUServStatus

Description: Status of the Service

Metric SpecName: SERVSTATUS

Metric Field Name: Service_Status

Data type: TEXT

Alarm: FALSE

Metric: FERTCASMCUServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_FERTCASMCUServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): Lync Server Application Sharing' Windows Service is stopped.

Potential Impact: NA

Suggested Action(s): Lync Server Application Sharing' Windows Service is stopped. Please restart the service.

Collect_Edge_SIP_Routing

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / NA

Source / Collection Definition: PERFMON / LS:SIP - 05 - Routing(*)

Metric: MsgsDropdDueToOtherRoutingFail

Description: The total number of messages dropped due to a routing failure that is not covered by any of the other counters. For further information, enable DIAGNOSTIC tracing in the administrator log and examine the text and result code of each event.

Metric SpecName: MSGDROPPEDDOTHRROUTERROR

Metric Field Name: SIP - 021 - Messages Dropped Due To Other Routing Failure

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 10, Major / 20

Policy: MSBS_MsgsDropdDueToOtherRoutingFail

Message text: The value of the counter 'Messages Dropped Due To Other Routing Failure' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: EdgeSIPMessagesDroppedDueToInternalError

Description: The number of messages dropped due to an internal server error.

Metric SpecName: MSGDROPPEDDINTERERROR

Metric Field Name: SIP - 022 - Messages Dropped Due To Internal Error

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 10, Major / 20

Policy: MSBS_EdgeSIPMessagesDroppedDueToInternalError

Message text: The value of the counter 'Messages Dropped Due To Internal Error' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: EdgeSIPRoutingInstance

Description: instance of perfmon object LS:SipEps - 00 - Sip Dialogs(_Total)

Metric SpecName: INSTANCENAME

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

NetworkInterface

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / KHINETINTER

Source / Collection Definition: PERFMON / Network Interface(*)

Metric: OutputQueueLength

> **Description**: This policy monitors indiciator of how busy a network interface is.
>
> **Metric SpecName**: OutputQueueLen
>
> **Metric Field Name**: Output Queue Length
>
> **Data type**: UINT32
>
> **Alarm**: TRUE
>
> **Category** : MSSkype
>
> **Severity / Threshold** : Major / 0, Major / 0
>
> **Policy**: MSBS_OutputQueueLength
>
> **Message text**: The current value of OutputQueueLength is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:
>
> **Instructional Text**:
>
> **Probable Cause(s)**: The following may cause a high Output Queue Length: Outdated network card driver, though such a problem normally manifests itself in other ways than just an increased output queue length statistic. Receive Side Scaling (RSS) is disabled, if you went to Windows Update, the likely hood that you had RSS disabled is 100%. You should look for a problem with a network card or some other piece of network hardware. There is too much load on the server.
>
> **Potential Impact**: 1)Upgrade the NIC driver and firmware 2)Upgrade the NIC teaming software (or Break the NIC teaming) 3) Re-enable RSS •HKEY_LOCAL_ MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters •Right-click EnableRSS, and then click Modify. •In the Value data box, type 0, and then click OK. Note: it requires a reboot for the change to occur 4) For testing purpose, replace the Network Card with a different manufacturer Network Card that is a server class. 5) If NIC is does not support the maximum bandwidth of your network, upgrade the NIC to support a faster bandwidth. An application or multiple applications are causing sudden elevated network usage patterns. Reduce the load on the server. You can do this by moving the load to a server that is utilized less. If it is required, add an additional server to your environment.
>
> **Suggested Action(s)**: Network downtime

Metric: PacketsOutboundDiscarded

Description: This policy monitors packet loss indicator

Metric SpecName: PacketsOutDiscar

Metric Field Name: Packets Outbound Discarded

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 100, Major / 100

Policy: MSBS_PacketsOutboundDiscarded

Message text: The current value of PacketsOutboundDiscarded is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.

Potential Impact: Check the cabling to the device.Perform any vendor specific hardware tests on the device to determine if the device's hardware is functioning properly.Raise the threshold on the monitor. This will allow for better "tuning" of the application to your environment. Take care no to raise the threshold too much as this could allow important events to go unnoticed.

Suggested Action(s): Packet Loss could lead to poor Media calls

Metric: PacketsReceivedDiscarded

Description: This policy monitors packet loss indicator

Metric SpecName: PacketsRecDiscar

Metric Field Name: Packets Received Discarded

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 100, Major / 100

Policy: MSBS_PacketsReceivedDiscarded

Message text: The current value of PacketsReceivedDiscarded is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.

Potential Impact: Check the cabling to the device.Perform any vendor specific hardware tests on the device to determine if the device's hardware is functioning properly.Raise the threshold on the monitor. This will allow for better "tuning" of the application to your environment. Take care no to raise the threshold too much as this could allow important events to go unnoticed.

Suggested Action(s): Packet Loss could lead to poor Media calls

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: OutputQueueLength

Description: This policy monitors indiciator of how busy a network interface is.

Metric SpecName: OutputQueueLen

Metric Field Name: Output Queue Length

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 0, Major / 0

Policy: MSBS_OutputQueueLength

Message text: The current value of OutputQueueLength is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): The following may cause a high Output Queue Length: Outdated network card driver, though such a problem normally manifests itself in other ways than just an increased output queue length statistic. Receive Side Scaling (RSS) is disabled, if you went to Windows Update, the likely hood that you had RSS disabled is 100%. You should look for a problem with a network card or some other piece of network hardware. There is too much load on the server.

Potential Impact: 1)Upgrade the NIC driver and firmware 2)Upgrade the NIC teaming software (or Break the NIC teaming) 3) Re-enable RSS •HKEY_LOCAL_ MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters •Right-click EnableRSS, and then click Modify. •In the Value data box, type 0, and then click OK. Note: it requires a reboot for the change to occur 4) For testing purpose, replace the Network Card with a different manufacturer Network Card that is a server class. 5) If NIC is does not support the maximum bandwidth of your network, upgrade the NIC to support a faster bandwidth. An application or multiple applications are causing sudden elevated network usage patterns. Reduce the load on the server. You can do this by moving the load to a server that is utilized less. If it is required, add an additional server to your environment.

Suggested Action(s): Network downtime

Metric: PacketsOutboundDiscarded

Description: This policy monitors packet loss indicator

Metric SpecName: PacketsOutDiscar

Metric Field Name: Packets Outbound Discarded

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 100, Major / 100

Policy: MSBS_PacketsOutboundDiscarded

Message text: The current value of PacketsOutboundDiscarded is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.

Potential Impact: Check the cabling to the device.Perform any vendor specific hardware tests on the device to determine if the device's hardware is functioning properly.Raise the threshold on the monitor. This will allow for better "tuning" of the application to your environment. Take care no to raise the threshold too much as this could allow important events to go unnoticed.

Suggested Action(s): Packet Loss could lead to poor Media calls

Metric: PacketsReceivedDiscarded

Description: This policy monitors packet loss indicator

Metric SpecName: PacketsRecDiscar

Metric Field Name: Packets Received Discarded

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 100, Major / 100

Policy: MSBS_PacketsReceivedDiscarded

Message text: The current value of PacketsReceivedDiscarded is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.

Potential Impact: Check the cabling to the device.Perform any vendor specific hardware tests on the device to determine if the device's hardware is functioning properly.Raise the threshold on the monitor. This will allow for better "tuning" of the application to your environment. Take care no to raise the threshold too much as this could allow important events to go unnoticed.

Suggested Action(s): Packet Loss could lead to poor Media calls

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Collect_FrontEnd_HostedMigrationService

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / LSHOSTEDMGR

Source / Collection Definition: PERFMON / LS:HostedMigrationService - HostedUserMigration(*)

Metric: HostedMigrationInstance

> **Description**: Instance of perfmon object LS:HostedMigrationService - HostedUserMigration
>
> **Metric SpecName**: HOSTEDMGRINSTANCE
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: COMMethodFailures

Description: Hosted User Migration Service front-end DCOM connection failures

Metric SpecName: COMMETHODFAILURE

Metric Field Name: HostedMigration - COM method failures

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 2, Major / 10

Policy: MSBS_COMMethodFailures

Message text: The value of HostedMigration - COM method failures for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Active directory is not accessible.

Potential Impact: NA

Suggested Action(s): Check if active directory is still accessible.

Metric: ADReadWriteFailures

Description: Hosted User Migration Service AD Sync failures

Metric SpecName: ADREADWRITEFAILURE

Metric Field Name: HostedMigration - AD read-write failures

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 2, Major / 10

Policy: MSBS_ADReadWriteFailures

Message text: The value of HostedMigration - AD read-write failures for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Active directory is not accessible.

Potential Impact: NA

Suggested Action(s): Check if active directory is still accessible.

Metric: HostedMigrationUnexpectedFailures

Description: Hosted User Migration Service unhandled exception failures

Metric SpecName: UNEXPECTEDFAILURE

Metric Field Name: HostedMigration - Unexpected failures

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 1, Major / 2

Policy: MSBS_HostedMigrationUnexpectedFailures

Message text: The value of HostedMigration - Unexpected failures for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): An unexpected failure has occurred

Potential Impact: NA

Suggested Action(s): Notify Lync Server team with the alert detail.

Collect_FrontEnd_Process_RTCSrv

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / CS_PROCESS

Source / Collection Definition: PERFMON / Process(RTCSrv)

Metric: FERTCSRVrInstance

Description: instance of RTCSrv process

Metric SpecName: INSTANCENAME

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: FERTCSRVPercentprocessorTime

Description: Percentage Processor Time is the percentage of elapsed time that all of process threads used the processor to execution instructions.

Metric SpecName: PCTPROCESSORTIME

Metric Field Name: % Processor Time

Data type: UINT32

Alarm: FALSE

Metric: FERTCSRVWorkingSet

Description: Working Set is the current size, in bytes, of the Working Set of this process. the Working Set is the set of memory pages touched recently by the threads in the process. If free memory in the computer is above a threshold, pages are left in the Working Set of a process even if they are not in use. When free memory falls below a threshold, pages are trimmed from Working Sets. If they are needed they will then be soft-faulted back into the Working Set before leaving main memory.

Metric SpecName: WORKINGSET

Metric Field Name: Working Set

Data type: UINT32

Alarm: FALSE

Metric: FERTCSRVPageFaultsPerSec

Description: Page Faults/sec is the average number of pages faulted per second. It is measured in number of pages faulted per second because only one page is faulted in each fault operation, hence this is also equal to the number of page fault operations. This counter includes both hard faults (those that require disk access) and soft faults (where the faulted page is found elsewhere in physical memory.) Most processors can handle large numbers of soft faults without significant consequence. However, hard faults, which require disk access, can cause significant delays.

Metric SpecName: PAGEFAULTS

Metric Field Name: Page Faults/sec

Data type: UINT32

Alarm: FALSE

Metric: FERTCSRVPrivateBytes

Description: Private Bytes is the current size, in bytes, of memory that this process has allocated that cannot be shared with other processes.

Metric SpecName: PRIVATEBYTES

Metric Field Name: Private Bytes

Data type: UINT32

Alarm: FALSE

Metric: FERTCSRVThreadCount

Description: the number of threads currently active in this process. An instruction is the basic unit of execution in a processor, and a thread is the object that executes instructions. Every running process has at least one thread.

Metric SpecName: THREADCOUNT

Metric Field Name: Thread Count

Data type: UINT32

Alarm: FALSE

Metric: RTCSRVrInstance

Description: instance of RTCSrv process

Metric SpecName: INSTANCENAME

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: RTCSRVPercentprocessorTime

Description: Percentage Processor Time is the percentage of elapsed time that all of process threads used the processor to execution instructions.

Metric SpecName: PCTPROCESSORTIME

Metric Field Name: % Processor Time

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 90

Policy: MSBS_RTCSRVPercentprocessorTime

Message text: The value of the counter '% Processor Time' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: RTCSRVWorkingSet

Description: Working Set is the current size, in bytes, of the Working Set of this process. the Working Set is the set of memory pages touched recently by the threads in the process. If free memory in the computer is above a threshold, pages are left in the Working Set of a process even if they are not in use. When free memory falls below a threshold, pages are trimmed from Working Sets. If they are needed they will then be soft-faulted back into the Working Set before leaving main memory.

Metric SpecName: WORKINGSET

Metric Field Name: Working Set

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20000000

Policy: MSBS_RTCSRVWorkingSet

Message text: The value of the counter 'Working Set' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: RTCSRVPageFaultsPerSec

Description: Page Faults/sec is the average number of pages faulted per second. It is measured in number of pages faulted per second because only one page is faulted in each fault operation, hence this is also equal to the number of page fault operations. This counter includes both hard faults (those that require disk access) and soft faults (where the faulted page is found elsewhere in physical memory.) Most processors can handle large numbers of soft faults without significant consequence. However, hard faults, which require disk access, can cause significant delays.

Metric SpecName: PAGEFAULTS

Metric Field Name: Page Faults/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 100

Policy: MSBS_RTCSRVPageFaultsPerSec

Message text: The value of the counter 'Page Faults/sec' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: RTCSRVPrivateBytes

Description: Private Bytes is the current size, in bytes, of memory that this process has allocated that cannot be shared with other processes.

Metric SpecName: PRIVATEBYTES

Metric Field Name: Private Bytes

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20000000

Policy: MSBS_RTCSRVPrivateBytes

Message text: The value of the counter 'Private Bytes' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: RTCSRVThreadCount

Description: the number of threads currently active in this process. An instruction is the basic unit of execution in a processor, and a thread is the object that executes instructions. Every running process has at least one thread.

Metric SpecName: THREADCOUNT

Metric Field Name: Thread Count

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 150

Policy: MSBS_RTCSRVThreadCount

Message text: The value of the counter 'Thread Count' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Collect_FrontEnd_Provision

This Policy monitors the performance of Skype Business Server Provisioning

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Provisioning_Performance_Conf

Aspect: Skype Provisioning Performance

CIT: Front End Server

Data source / Data class: LYNC / LSPROVISION

Source / Collection Definition: PERFMON / LS:Provision - Provision(*)

Metric: ProvisionInstance

Description: instance of perfmon object LS:Provision - Provision

Metric SpecName: PROVISIONINSTANCE

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: ContactProvisionLatency

Description: the latency of provision Contact

Metric SpecName: CONTPROVLATENCY

Metric Field Name: - Contact Provision latency (ms)

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 1000, Major / 3000

Policy: MSBS_ContactProvisionLatency

Message text: The value of Contact Provision latency (ms) for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Contact provision latency is high.

Potential Impact: NA

Suggested Action(s): Check if the Provisioning Service is still working well. And notify Lync Server team with the alert detail.

Metric: DCReplicaLatency

Description: the latency of AD replication

Metric SpecName: DCREPLICALATENCY

Metric Field Name: - DCReplica latency (ms)

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 120000, Major / 300000

Policy: MSBS_DCReplicaLatency

Message text: The value of DCReplica latency (ms) for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): The latency for two domain controller replicating data is high.

Potential Impact: NA

Suggested Action(s): Check if active directory is still working well. And notify Lync Server team with the alert detail.

Metric: GetChangesLatency

Description: the latency of calling GetChanges from MSODS

Metric SpecName: GETCHNAGESLATENCY

Metric Field Name: - GetChanges latency (ms)

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 5000, Major / 60000

Policy: MSBS_GetChangesLatency

Message text: The value of GetChanges latency (ms) for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): The latency of calling MSODS web service is too high.

Potential Impact: NA

Suggested Action(s): Check if MSODS web service is still available. And notify Lync Server team with the alert detail.

Metric: ContactProvisionFailures

Description: Number of provision contact failures

Metric SpecName: CONTPROVFAILURES

Metric Field Name: - Contact provision failures

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 225, Major / 450

Policy: MSBS_ContactProvisionFailures

Message text: The value of Contact provision failures for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Contact provision failed.

Potential Impact: NA

Suggested Action(s): Notify Lync Server team with the alert detail.

Metric: CookiePersistenceFailures

Description: Number of cookie persistence failures

Metric SpecName: COOKEPERSFAILURES

Metric Field Name: - Cookie persistence failures

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 6, Major / 10

Policy: MSBS_CookiePersistenceFailures

Message text: The value of Cookie persistence failures for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): The incoming cookie data is invalid or active directory is not reachable.

Potential Impact: NA

Suggested Action(s): Check if active directory is still accessible and incoming cookie format is valid. And notify Lync Server team with the alert detail.

Metric: FailedPublishCalls

Description: Failed to publish objects status to MSODS

Metric SpecName: FAILEDPUBCALLS

Metric Field Name: - Failed publish calls

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 2250, Major / 4500

Policy: MSBS_FailedPublishCalls

Message text: The value ofFailed publish calls for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Microsoft online directory service returned the publication result failure.

Potential Impact: NA

Suggested Action(s): Notify Lync Server team with the alert detail.

Metric: SyncToADFailures

Description: Number of failure to apply the synced changes to AD

Metric SpecName: SYNCTOADFAILURES

Metric Field Name: - Sync to AD failures

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 30, Major / 50

Policy: MSBS_SyncToADFailures

Message text: The value of Sync to AD failures for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Incoming data is invalid or active directory is not reachable.

Potential Impact: NA

Suggested Action(s): Check if active directory is still accessible and incoming data format is valid. And notify Lync Server team with the alert detail.

Metric: TenantProvisionFailures

Description: Number of tenant provision failures

Metric SpecName: TENANTPROVFAILURES

Metric Field Name: - Tenant provision failures

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 225, Major / 450

Policy: MSBS_TenantProvisionFailures

Message text: The value of Tenant provision failures for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Tenant provision failed.

Potential Impact: NA

Suggested Action(s): Notify Lync Server team with the alert detail.

Metric: UserProvisionFailures

Description: Number of user provision failures

Metric SpecName: USRPROVFAILURES

Metric Field Name: - User provision failures

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 2250, Major / 4500

Policy: MSBS_UserProvisionFailures

Message text: The value of User provision failures for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): User provision failed.

Potential Impact: NA

Suggested Action(s): Notify Lync Server team with the alert detail.

Metric: PICWebServiceLatency

Description: the latency of calling PIC web service

Metric SpecName: PICWSLATENCY

Metric Field Name: - PIC web service latency (ms)

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 5000, Major / 60000

Policy: MSBS_PICWebServiceLatency

Message text: The value of PIC web service latency (ms) for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): The latency of calling Public provider web service is high.

Potential Impact: NA

Suggested Action(s): Check if Public provider web service is still working well. And notify Lync Server team with the alert detail.

Metric: PublishLatency

Description: the latency of calling Publishing to MSODS

Metric SpecName: PUBLISHLATENCY

Metric Field Name: - Publish latency (ms)

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 5000, Major / 60000

Policy: MSBS_PublishLatency

Message text: The value of Publish latency (ms) for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): MSODS web service response latency is high.

Potential Impact: NA

Suggested Action(s): Check if MSODS web service is still available. And notify Lync Server team with the alert detail.

Metric: SaveLatency

Description: the latency of saving objects in AD

Metric SpecName: SAVELATENCY

Metric Field Name: - Save latency (ms)

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 1000, Major / 3000

Policy: MSBS_SaveLatency

Message text: The value ofSave latency (ms) for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): The latency of saving objects in active directory is high.

Potential Impact: NA

Suggested Action(s): Check if active directory is still working well. And notify Lync Server team with the alert detail.

Metric: TenantProvisionLatency

Description: the latency of provision Tenant

Metric SpecName: TENAMYPROVLATENCY

Metric Field Name: - Tenant Provision latency (ms)

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 3000, Major / 30000

Policy: MSBS_TenantProvisionLatency

Message text: The value of Tenant Provision latency (ms) for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Tenant provision latency is high.

Potential Impact: NA

Suggested Action(s): Check if the Provisioning Service is still working well. And notify Lync Server team with the alert detail.

Metric: UserProvisionLatency

Description: the latency of provision User

Metric SpecName: USERPROVLATENCY

Metric Field Name: - User Provision latency (ms)

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 1000, Major / 3000

Policy: MSBS_UserProvisionLatency

Message text: The value of User Provision latency (ms) for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): User provision latency is high.

Potential Impact: NA

Suggested Action(s): Check if the Provisioning Service is still working well. And notify Lync Server team with the alert detail.

Collect_FrontEnd_Director

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / LSPROCESSOR

Source / Collection Definition: PERFMON / Processor(_Total)

Metric: ProcesserInstance

> **Description**: instance of perfmon object Processor Total
>
> **Metric SpecName**: PROCESSORINST
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: SystemPercentProcessorTime

> **Description**: Percentage Processor Time is the percentage of elapsed time that all of process threads used the processor to execution instructions.
>
> **Metric SpecName**: SYSPCTPROCESSORTIME
>
> **Metric Field Name**: % Processor Time
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

SimplePortWatcher5086

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / Port5086

Source / Collection Definition: PORTCOL / PORTCHECKER

Metric: SimpleWatcherPort5086

Description: SIP port used by Mobility Services internal processes

Metric SpecName: SimpleWatcherPort5086

Metric Field Name: SimpleWatcherPort5086

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_SimpleWatcherPort5086

Message text: The Port No:5086 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

SimplePortWatcher445

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / Port445

Source / Collection Definition: PORTCOL / PORTCHECKER

Metric: SimpleWatcherPort445

Description: Used to push configuration data from the Central Management store to servers running Lync Server.

Metric SpecName: SimpleWatcherPort445

Metric Field Name: SimpleWatcherPort445

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_SimpleWatcherPort445

Message text: The Port No:445 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

> **Description**: This is the key for metric
>
> **Metric SpecName**: HOSTNAME
>
> **Metric Field Name**: HOSTNAME
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: SimpleWatcherPort445

Description: Used to push configuration data from the Central Management store to servers running Lync Server.

Metric SpecName: SimpleWatcherPort445

Metric Field Name: SimpleWatcherPort445

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_SimpleWatcherPort445

Message text: The Port No:445 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

Local500Responses

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / LOCAL500RESPONSES

Source / Collection Definition: PERFMON / LS:SIP - Responses(*)

Metric: Local500Responses

Description: This metric captures The total number of 500 responses generated by the server.

Metric SpecName: Local500Responses

Metric Field Name: SIP - Local 500 Responses

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 50

Policy: MSBS_Local500Responses

Message text: The number of Local 500 Responses by server is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): The server is encountering unexpected errors. The problem may be related to low memory conditions

Potential Impact: This might be a temporary condition. If the problem persists and is not related to low memory conditions please check diagnostic headers of the 500 responses in the protocol logs.

Suggested Action(s): Users face issue in sharing desktop or other applications

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

ChkPersistentChatServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SERVSTAT

Source / Collection Definition: SERVICECHECK / RTCCHAT

Metric: PersistentChatRTCCHATServName

> **Description**: Name of the Service
>
> **Metric SpecName**: SERVNAME
>
> **Metric Field Name**: Service_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: PersistentChatRTCCHATServDisplayName

> **Description**: Display Name of the Service
>
> **Metric SpecName**: SRVDISPNAME
>
> **Metric Field Name**: Service_Displayname
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: PersistentChatRTCCHATServStatus

> **Description**: Status of the Service
>
> **Metric SpecName**: SERVSTATUS
>
> **Metric Field Name**: Service_Status
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: PersistentChatRTCCHATServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_PersistentChatRTCCHATServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): Lync Server Persistent Chat' Windows Service is stopped.

Potential Impact: NA

Suggested Action(s): Lync Server Persistent Chat' Windows Service is stopped. Please restart the service.

Collect_FrontEnd_CAAPlanning

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / LSCAA

Source / Collection Definition: PERFMON / LS:CAA - Planning(*)

Metric: CAAPlanningInsatnceName

Description: Instance of perfmon object LS:CAA - Planning

Metric SpecName: CAAINSTANCE

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: TotApplEndPointCreationFailure

Description: Platform Endpoint Creation

Metric SpecName: TOTAPPLEPCREFAILURE

Metric Field Name: CAA - Total Application Endpoint creation failures

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 5, Major / 10

Policy: MSBS_TotApplEndPointCreationFailure

Message text: The value of Total Application Endpoint creation failures for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): The application has not been properly activated or the contact object was deleted.

Potential Impact: NA

Suggested Action(s): Deactivate and then activate the application for this pool.

SimplePortWatcher5072

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / Port5072

Source / Collection Definition: PORTCOL / PORTCHECKER

Metric: SimpleWatcherPort5072

Description: Used for incoming SIP requests for Attendant (dial in conferencing).

Metric SpecName: SimpleWatcherPort5072

Metric Field Name: SimpleWatcherPort5072

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort5072

Message text: The Port No:5072 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

Metric: SimpleWatcherPort5072

Description: Used for incoming SIP requests for Attendant (dial in conferencing).

Metric SpecName: SimpleWatcherPort5072

Metric Field Name: SimpleWatcherPort5072

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort5072

Message text: The Port No:5072 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

> **Description**: This is the key for metric
>
> **Metric SpecName**: HOSTNAME
>
> **Metric Field Name**: HOSTNAME
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Collect_AVEdge_TCP_Logging

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / CS_AVEDGETCP

Source / Collection Definition: PERFMON / LS:A/V Edge - TCP Counters(_Total)

Metric: AVEdgeTcpInstance

> **Description**: instance of perfmon object LS:A/V Edge - TCP Counters(_Total)
>
> **Metric SpecName**: CSTCPINSTANAME
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: AVEdgeTCPAuthFailurPerSecLogging

Description: Authentication Failures/sec over TCP

Metric SpecName: TCPAUTHFAILURES

Metric Field Name: A/V Edge - Authentication Failures/sec

Data type: UINT32

Alarm: FALSE

Collect_Edge_SIP_AccessEdge_Server_Messages

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / ACCEDGEMSG

Source / Collection Definition: PERFMON / LS:SIP - Access Edge Server Messages(*)

Metric: EdgeServerMessageInstance

Description: instance of perfmon object LS:SIP - Access Edge Server Messages

Metric SpecName: EDGEINSTNAME

Metric Field Name: Instance_Name

Data type: UINT32

Alarm: FALSE

Metric: EdgeSIPMessageDroppedDueToUnknownDomain

Description: the per-second rate of messages that could not be routed because the message domain is not configured and does not appear to belong to a federated partner.

Metric SpecName: MSGDROPPEDUKDOM

Metric Field Name: SIP - Messages/sec Dropped Due To Unknown Domain

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 5, Major / 10

Policy: MSBS_EdgeSIPMessageDroppedDueToUnknownDomain

Message text: The value of SIP - Messages/sec Dropped Due To Unknown Domain for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): The Access Edge Server received SIP messages with an unknown domain.

Potential Impact: NA

Suggested Action(s): If the number is high then the Access Edge Server may be under attack.

Metric: EdgeServerMessageInstance

Description: instance of perfmon object LS:SIP - 09 - Access Edge Server Messages

Metric SpecName: EDGEINSTNAME

Metric Field Name: Instance_Name

Data type: UINT32

Alarm: FALSE

Metric: ExMsgsDrpdDueToUnresolvedDom

Description: rate at which the number of messages is dropped at the external edge, as DNS SRV failed to resolve the domain.

Metric SpecName: MSGDROPPEDDUNRDOM

Metric Field Name: SIP - 063 - External Messages/sec Dropped Due To Unresolved Domain

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 40

Policy: MSBS_ExMsgsDrpdDueToUnresolvedDom

Message text: The value of the counter 'External Messages/sec Dropped Due To Unresolved Domain' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: ExMsgsDrpdDueToBlkdIMSrvcProviderDom

Description: rate of messages dropped at the external edge, in a second, because of DNS SRV resolving the domain to a server blocked in the IM Service Providers table.

Metric SpecName: MSGDROPPEDDBLKDIMSDOM

Metric Field Name: SIP - 065 - External Messages/sec Dropped Due To Blocked IM Service Provider Domain

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 40

Policy: MSBS_ExMsgsDrpdDueToBlkdIMSrvcProviderDom

Message text: The value of the counter 'External Messages/sec Dropped Due To Blocked IM Service Provider Domain' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: ExMsgsDrpdDueToIncompatibleMsgDom

Description: rate at which the messages are dropped per second at the external edge, as the previous messages are not compatible with the federation type of domain.

Metric SpecName: MSGDROPPEDDINCMPTBLEMSGDOM

Metric Field Name: SIP - 077 - External Messages/sec Dropped Due To Incompatible Message Domain

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 40

Policy: MSBS_ExMsgsDrpdDueToIncompatibleMsgDom

Message text: The value of the counter 'External Messages/sec Dropped Due To Incompatible Message Domain' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: ExMsgsDrpdDueToBlkdDom

Description: number of messages which are dropped at the external edge as their domain is in the blocked list, in one second.

Metric SpecName: MSGDROPPEDDKLKDDOM

Metric Field Name: SIP - 033 - External Messages/sec Dropped Due To Blocked Domain

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 40

Policy: MSBS_ExMsgsDrpdDueToBlkdDom

Message text: The value of the counter 'External Messages/sec Dropped Due To Blocked Domain' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

ChkFrontEndWWWebPublishingServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SERVSTAT

Source / Collection Definition: SERVICECHECK / w3svc

Metric: FEw3svcServName

Description: Name of the Service

Metric SpecName: SERVNAME

Metric Field Name: Service_Name

Data type: TEXT

Alarm: FALSE

Metric: FEw3svcServDisplayName

Description: Display Name of the Service

Metric SpecName: SRVDISPNAME

Metric Field Name: Service_Displayname

Data type: TEXT

Alarm: FALSE

Metric: FEw3svcServStatus

Description: Status of the Service

Metric SpecName: SERVSTATUS

Metric Field Name: Service_Status

Data type: TEXT

Alarm: FALSE

Metric: FEw3svcServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_FEw3svcServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): World Wide Web Publishing Service' Windows Service is stopped.

Potential Impact: NA

Suggested Action(s): World Wide Web Publishing Service' Windows Service is stopped. Please restart the service.

MediationServerCounter

This policy maintains the information about the status for the different services

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_ConferenceProcPerform_2010_Conf

Aspect: Skype Conference Processing Performance

CIT: Mediation Server, Front End Server, Edge Server

Data source / Data class: SKYPE / TTLFAILCALUNEXPINTPX

Source / Collection Definition: PERFMON / LS:MediationServer - Global Counters(*)

Metric: TotalFailedCallsCausedByUnexpectedInteractionFromTheProxy

Description: This metric captures Total Failed Calls Caused By Unexpected Interaction From The Proxy

Metric SpecName: TtlFailCalUnexpIntPx

Metric Field Name: - Total Failed Calls Caused By Unexpected Interaction From The Proxy

Data type: UINT32

Alarm: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: TotalFailedCallsCausedByUnexpectedInteractionFromTheProxy

Description: This metric captures Total Failed Calls Caused By Unexpected Interaction From The Proxy

Metric SpecName: TtlFailCalUnexpIntPx

Metric Field Name: - Total Failed Calls Caused By Unexpected Interaction From The Proxy

Data type: UINT32

Alarm: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Collect_FrontEnd_Process_ClsAgent

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / CS_PROCESS

Source / Collection Definition: PERFMON / Process(ClsAgent)

Metric: FERTCCLSAGTInstance

> **Description**: instance of ClsAgent object
>
> **Metric SpecName**: INSTANCENAME
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FERTCCLSAGTPercentprocessorTime

> **Description**: Percentage Processor Time is the percentage of elapsed time that all of process threads used the processor to execution instructions.
>
> **Metric SpecName**: PCTPROCESSORTIME
>
> **Metric Field Name**: % Processor Time
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Metric: FERTCCLSAGTWorkingSet

Description: Working Set is the current size, in bytes, of the Working Set of this process. the Working Set is the set of memory pages touched recently by the threads in the process. If free memory in the computer is above a threshold, pages are left in the Working Set of a process even if they are not in use. When free memory falls below a threshold, pages are trimmed from Working Sets. If they are needed they will then be soft-faulted back into the Working Set before leaving main memory.

Metric SpecName: WORKINGSET

Metric Field Name: Working Set

Data type: UINT32

Alarm: FALSE

Metric: FERTCCLSAGTPageFaultsPerSec

Description: Page Faults/sec is the average number of pages faulted per second. It is measured in number of pages faulted per second because only one page is faulted in each fault operation, hence this is also equal to the number of page fault operations. This counter includes both hard faults (those that require disk access) and soft faults (where the faulted page is found elsewhere in physical memory.) Most processors can handle large numbers of soft faults without significant consequence. However, hard faults, which require disk access, can cause significant delays.

Metric SpecName: PAGEFAULTS

Metric Field Name: Page Faults/sec

Data type: UINT32

Alarm: FALSE

Metric: FERTCCLSAGTPrivateBytes

Description: Private Bytes is the current size, in bytes, of memory that this process has allocated that cannot be shared with other processes.

Metric SpecName: PRIVATEBYTES

Metric Field Name: Private Bytes

Data type: UINT32

Alarm: FALSE

Metric: FERTCCLSAGTThreadCount

> **Description**: the number of threads currently active in this process. An instruction is the basic unit of execution in a processor, and a thread is the object that executes instructions. Every running process has at least one thread.
>
> **Metric SpecName**: THREADCOUNT
>
> **Metric Field Name**: Thread Count
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Collect_AvConf_AVMCU_HealthandPerformance

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / NA

Source / Collection Definition: PERFMON / LS:AVMCU - 04 - MCU Health And Performance

Metric: AvConfAVMCUHealthandPerformanceInstance

> **Description**: instance of perfmon object LS:AVMCU - 04 - MCU Health And Performance
>
> **Metric SpecName**: AVCONFHEALTHNPERFMINSTANCE
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: AvConfHTTPStackload

Description: time taken in HTTP stack to process all pending transactions. It is measured in milliseconds

Metric SpecName: HTTPSTACKLOAD

Metric Field Name: AVMCU - 000 - HTTP Stack load

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 30000, Major / 120000

Policy: MSBS_AvConfHTTPStackload

Message text: The value of the counter 'AVMCU - 000 - HTTP Stack load' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: AvConfMCUHealthState

Description: Current Health of AVMCU is monitored by this policy . A value 0 signifies normal ,1 signifies loaded ,2 signifies full and 3 signifies unavailable of MCU

Metric SpecName: MCUHEALTHSTATE

Metric Field Name: AVMCU - 005 - MCU Health State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 1, Major / 2

Policy: MSBS_AvConfMCUHealthState

Message text: The value of the counter 'AVMCU - 005 - MCU Health State' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

ChkEdgeAudioVideoServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SERVSTAT

Source / Collection Definition: SERVICECHECK / RTCMEDIARELAY

Metric: EdgeRTCMEDIARELAYServName

Description: Name of the Service

Metric SpecName: SERVNAME

Metric Field Name: Service_Name

Data type: TEXT

Alarm: FALSE

Metric: EdgeRTCMEDIARELAYServDisplayName

Description: Display Name of the Service

Metric SpecName: SRVDISPNAME

Metric Field Name: Service_Displayname

Data type: TEXT

Alarm: FALSE

Metric: EdgeRTCMEDIARELAYServStatus

Description: Status of the Service

Metric SpecName: SERVSTATUS

Metric Field Name: Service_Status

Data type: TEXT

Alarm: FALSE

Metric: EdgeRTCMEDIARELAYServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_EdgeRTCMEDIARELAYServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): Lync Server Audio/Video Edge' Windows Service is stopped.

Potential Impact: NA

Suggested Action(s): Lync Server Audio/Video Edge' Windows Service is stopped. Please restart the service.

ActiveRegisteredEndpoints

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / ACTREGISTERENDPOINT

Source / Collection Definition: PERFMON / LS:USrv - Endpoint Cache(*)

Metric: ActiveRegisteredEndpoints

> **Description**: This metric captures Active Registered End points connected to the server
>
> **Metric SpecName**: ActRegisterEndpoint
>
> **Metric Field Name**: USrv - Active Registered Endpoints
>
> **Data type**: REAL64
>
> **Alarm**: FALSE

Metric: Instance_Name

> **Description**: This is the key for metric
>
> **Metric SpecName**: Instance_Name
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

EmergencyCallRouting

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / KHIEMERCALLROU

Source / Collection Definition: PERFMON / LS:RoutingApps - 01 - Emergency Call Routing(*)

Metric: Numberofincomingfailureresponses

Description: This policy monitors the number of times an Emergency Call failure response was received from Gateway.

Metric SpecName: Noofincfailresp

Metric Field Name: RoutingApps - 002 - Number of incoming failure responses

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 0, Major / 0

Policy: MSBS_Numberofincomingfailureresponses

Message text: The current value of Numberofincomingfailureresponses is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): This Performance Counter represents the number of Emergency Services calls where the Gateway has responded with a 4xx/5xx SIP response code.

Potential Impact: If you have configured the Centralized Logging Service (CLS) CacheFileNetworkFolder, it may be possible to query CLS for the more data.

Suggested Action(s): Unable to contact Emergency Services

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: Numberofincomingfailureresponses

Description: This policy monitors the number of times an Emergency Call failure response was received from Gateway.

Metric SpecName: Noofincfailresp

Metric Field Name: RoutingApps - Number of incoming failure responses

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 0, Major / 0

Policy: MSBS_Numberofincomingfailureresponses

Message text: The current value of Numberofincomingfailureresponses is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): This Performance Counter represents the number of Emergency Services calls where the Gateway has responded with a 4xx/5xx SIP response code.

Potential Impact: If you have configured the Centralized Logging Service (CLS) CacheFileNetworkFolder, it may be possible to query CLS for the more data.

Suggested Action(s): Unable to contact Emergency Services

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

WEBDistributionList

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: SKYPE / WEBDISTRIBUTIONLIST

Source / Collection Definition: PERFMON / LS:WEB - 00 - Distribution List Expansion(*)

Metric: AverageActiveDirectoryFetchTimeInMilliseconds

> **Description**: This metric captures Average Active Directory Fetch Time In Milliseconds
>
> **Metric SpecName**: AvgActDireFetchTmMS
>
> **Metric Field Name**: WEB - 005 - Average Active Directory Fetch time in milliseconds
>
> **Data type**: REAL64
>
> **Alarm**: FALSE

Metric: Instance_Name

> **Description**: This is the key for metric
>
> **Metric SpecName**: Instance_Name
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: AverageMemberPropFetchTimeMillisec

> **Description**: This metric captures Average Member Properties Fetch Time In Milliseconds
>
> **Metric SpecName**: AvgMbrPropFetchTmMS
>
> **Metric Field Name**: WEB - 008 - Average member properties fetch time in milliseconds
>
> **Data type**: REAL64
>
> **Alarm**: FALSE

Metric: SopException

Description: This metric captures Soap Exceptions

Metric SpecName: SopException

Metric Field Name: WEB - 014 - Soap Exceptions

Data type: REAL64

Alarm: FALSE

Metric: TimedOutActiveDirectoryRequestsPerSec

Description: This metric captures Timed Out Active Directory Requests Per Sec

Metric SpecName: TimOutActDireReqPS

Metric Field Name: WEB - 011 - Timed out Active Directory Requests/sec

Data type: REAL64

Alarm: FALSE

Metric: TimedOutRequestsThatFetchMemberPropertiesPerSec

Description: This metric captures Timed Out Requests That Fetch Member Properties Per Sec

Metric SpecName: TimReqFtchMbrPropPS

Metric Field Name: WEB - 013 - Timed out Requests that fetch member properties/sec

Data type: REAL64

Alarm: FALSE

Metric: ValidUserRequestsPerSec

Description: This metric captures Valid User Requests Per Sec

Metric SpecName: ValidUserRequestsPS

Metric Field Name: WEB - 001 - Valid User Requests/sec

Data type: REAL64

Alarm: FALSE

Metric: AverageActiveDirectoryFetchTimeInMilliseconds

Description: This metric captures Average Active Directory Fetch Time In Milliseconds

Metric SpecName: AvgActDireFetchTmMS

Metric Field Name: WEB - Average Active Directory Fetch time in milliseconds

Data type: REAL64

Alarm: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: AverageMemberPropFetchTimeMillisec

Description: This metric captures Average Member Properties Fetch Time In Milliseconds

Metric SpecName: AvgMbrPropFetchTmMS

Metric Field Name: WEB - Average member properties fetch time in milliseconds

Data type: REAL64

Alarm: FALSE

Metric: SoapExceptions

Description: This metric captures Soap Exceptions

Metric SpecName: SoapExceptions

Metric Field Name: WEB - Soap Exceptions

Data type: REAL64

Alarm: FALSE

Metric: TimedOutActiveDirectoryRequestsPerSec

Description: This metric captures Timed Out Active Directory Requests Per Sec

Metric SpecName: TimOutActDireReqPS

Metric Field Name: WEB - Timed out Active Directory Requests/Sec

Data type: REAL64

Alarm: FALSE

Metric: TimedOutRequestsThatFetchMemberPropertiesPerSec

Description: This metric captures Timed Out Requests That Fetch Member Properties Per Sec

Metric SpecName: TimReqFtchMbrPropPS

Metric Field Name: WEB - Timed out Requests that fetch member properties/Sec

Data type: REAL64

Alarm: FALSE

Metric: ValidUserRequestsPerSec

Description: This metric captures Valid User Requests Per Sec

Metric SpecName: ValidUserRequestsPS

Metric Field Name: WEB - Valid User Requests/Sec

Data type: REAL64

Alarm: FALSE

SimplePortWatcher5060

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / Port5060

Source / Collection Definition: PORTCOL / PORTCHECKER

Metric: SimpleWatcherPort5060

Description: Optionally used by Standard Edition servers and Front End Servers for static routes to trusted services, such as remote call control servers.

Metric SpecName: SimpleWatcherPort5060

Metric Field Name: SimpleWatcherPort5060

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort5060

Message text: The Port No:5060 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

> **Description**: This is the key for metric
>
> **Metric SpecName**: HOSTNAME
>
> **Metric Field Name**: HOSTNAME
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: SimpleWatcherPort5060

Description: Optionally used by Standard Edition servers and Front End Servers for static routes to trusted services, such as remote call control servers.

Metric SpecName: SimpleWatcherPort5060

Metric Field Name: SimpleWatcherPort5060

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort5060

Message text: The Port No:5060 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

> **Description**: This is the key for metric
>
> **Metric SpecName**: HOSTNAME
>
> **Metric Field Name**: HOSTNAME
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Collect_Mediation_Outbound Calls

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / NA

Source / Collection Definition: PERFMON / LS:MediationServer - 00 - Outbound Calls(*)

Metric: MedOutboundCallsInstance

> **Description**: instance of perfmon object LS:MediationServer - 00 - Outbound Calls
>
> **Metric SpecName**: MEDOUTBOUNDINSTANCE
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: MedTotalRejectedDueToLoad

Description: number of SIP INVITEs from proxy which were rejected immediately because of server load.

Metric SpecName: TOTREJCTDDTLOAD

Metric Field Name: Total Rejected Due to Load

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 5, Major / 10

Policy: MSBS_MedTotalRejectedDueToLoad

Message text: The value of the counter 'Total Rejected Due to Load' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

UCWA

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / KHIUCWA

Source / Collection Definition: PERFMON / LS:WEB - UCWA

Metric: HTTP5xxResponsespersec

Description: This policy monitors the per second rate of responses with HTTP 5xx code

Metric SpecName: HTTP5xxResppersec

Metric Field Name: UCWA - HTTP 5xx Responses/Second

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Minor / 0

Policy: MSBS_HTTP5xxResponsespersec

Message text: The current value of HTTP5xxResponsespersec is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): Configuration errors Server/Component is down for maintenance. Network/connectivity issues Component specific errors.

Potential Impact: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution errors or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view.

Suggested Action(s): HTTP server errors increase.

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Collect_Mediation_Process_ReplicaReplicatorAgent

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / CS_PROCESS

Source / Collection Definition: PERFMON / Process(ReplicaReplicatorAgent)

Metric: MedREPLICAInstance

> **Description**: instance of ReplicaReplicatorAgent process
>
> **Metric SpecName**: INSTANCENAME
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: MedREPLICAPercentprocessorTime

> **Description**: Percentage Processor Time is the percentage of elapsed time that all of process threads used the processor to execution instructions.
>
> **Metric SpecName**: PCTPROCESSORTIME
>
> **Metric Field Name**: % Processor Time
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Metric: MedREPLICAWorkingSet

Description: Working Set is the current size, in bytes, of the Working Set of this process. the Working Set is the set of memory pages touched recently by the threads in the process. If free memory in the computer is above a threshold, pages are left in the Working Set of a process even if they are not in use. When free memory falls below a threshold, pages are trimmed from Working Sets. If they are needed they will then be soft-faulted back into the Working Set before leaving main memory.

Metric SpecName: WORKINGSET

Metric Field Name: Working Set

Data type: UINT32

Alarm: FALSE

Metric: MedREPLICAPageFaultsPerSec

Description: Page Faults/sec is the average number of pages faulted per second. It is measured in number of pages faulted per second because only one page is faulted in each fault operation, hence this is also equal to the number of page fault operations. This counter includes both hard faults (those that require disk access) and soft faults (where the faulted page is found elsewhere in physical memory.) Most processors can handle large numbers of soft faults without significant consequence. However, hard faults, which require disk access, can cause significant delays.

Metric SpecName: PAGEFAULTS

Metric Field Name: Page Faults/sec

Data type: UINT32

Alarm: FALSE

Metric: MedREPLICAPrivateBytes

Description: Private Bytes is the current size, in bytes, of memory that this process has allocated that cannot be shared with other processes.

Metric SpecName: PRIVATEBYTES

Metric Field Name: Private Bytes

Data type: UINT32

Alarm: FALSE

Metric: MedREPLICAThreadCount

> **Description**: the number of threads currently active in this process. An instruction is the basic unit of execution in a processor, and a thread is the object that executes instructions. Every running process has at least one thread.
>
> **Metric SpecName**: THREADCOUNT
>
> **Metric Field Name**: Thread Count
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Collect_FrontEnd_PersistentChat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / LSPROCESSOR

Source / Collection Definition: PERFMON / Processor(_Total)

Metric: ProcesserInstance

> **Description**: instance of perfmon object Processor Total
>
> **Metric SpecName**: PROCESSORINST
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: SystemPercentProcessorTime

> **Description**: Percentage Processor Time is the percentage of elapsed time that all of process threads used the processor to execution instructions.
>
> **Metric SpecName**: SYSPCTPROCESSORTIME
>
> **Metric Field Name**: % Processor Time
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Collect_Edge_Process_MediaRelaySvc

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / CS_PROCESS

Source / Collection Definition: PERFMON / Process(MediaRelaySvc)

Metric: EdgeMediaRelaySvcWorkingSet

Description: Working Set counter available in the Audio/Video Edge service.

Metric SpecName: WORKINGSET

Metric Field Name: Working Set

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20000000

Policy: MSBS_EdgeMediaRelaySvcWorkingSet

Message text: The value of the counter 'Working Set' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: EdgeMediaRelaySvcThreadCount

Description: Thread Count counter available in the Audio/Video Edge service.

Metric SpecName: THREADCOUNT

Metric Field Name: Thread Count

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 150

Policy: MSBS_EdgeMediaRelaySvcThreadCount

Message text: The value of the counter 'Thread Count' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: EdgeMediaRelaySvcProcessorTime

Description: the % Processor Time counter available in the Audio/Video Edge service.

Metric SpecName: PROCESSORTIME

Metric Field Name: % Processor Time

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 90

Policy: MSBS_EdgeMediaRelaySvcProcessorTime

Message text: The value of the counter '% Processor Time' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: EdgeMediaRelaySvcPrivateBytes

Description: Private Bytes counter available in the Audio/Video Edge service.

Metric SpecName: PRIVATEBYTES

Metric Field Name: Private Bytes

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20000000

Policy: MSBS_EdgeMediaRelaySvcPrivateBytes

Message text: The value of the counter 'Private Bytes' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: EdgeMediaRelaySvcPageFaultsPersec

Description: Page Faults/sec counter available in the Audio/Video Edge service.

Metric SpecName: PAGEFAULTPERSEC

Metric Field Name: Page Faults/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 100

Policy: MSBS_EdgeMediaRelaySvcPageFaultsPersec

Message text: The value of the counter 'Page Faults/sec' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: EdgeMediaRelaySvcInstance

Description: instance of perfmon object Process(MediaRelaySvc)

Metric SpecName: MEDIARELAYSVCINSTANCE

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Collect_FrontEnd_WebSchedulerHandler

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / LSWEBSCHHANDLER

Source / Collection Definition: PERFMON / LS:WebScheduler - Web Scheduler Handler(*)

Metric: WebschedulerHandlerInstance

> **Description**: instance of perfmon object LS:WebScheduler - Web Scheduler Handler
>
> **Metric SpecName**: WEBSCHINSTANCE
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: NumberofFailedAddressBookLookupsFailed

> **Description**: Number of address book resolution failures
>
> **Metric SpecName**: FAILEDADDRBKLKUP
>
> **Metric Field Name**: WEBSCHEDULER - Number of failed Address Book lookups that failed
>
> **Data type**: UINT32
>
> **Alarm**: TRUE
>
> **Category** : MSSkype
>
> **Severity / Threshold** : Warning / 10, Major / 20
>
> **Policy**: MSBS_NumberofFailedAddressBookLookupsFailed
>
> **Message text**: The value of WEBSCHEDULER - Number of failed Address Book lookups that failed for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>
>
> **Instructional Text**:
>
> **Probable Cause(s)**: Web Scheduler not able to connect to ABWQ web service
>
> **Potential Impact**: NA
>
> **Suggested Action(s)**: Check that ABWQ is up and running. Confirm that the machine hosting Web Scheduler is able to connect to machine hosting ABWQ.

Metric: RequestForWhichResponseStatusisNotSuccess

Description: Total number of requests for which response status is not Success

Metric SpecName: WSUNSUCRESSTATUS

Metric Field Name: WEBSCHEDULER - Requests for which Response Status is not Success

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 10, Major / 20

Policy: MSBS_RequestForWhichResponseStatusisNotSuccess

Message text: The value of WEBSCHEDULER - Requests for which Response Status is not Success for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Bad requests coming from the client or malicious attempt.

Potential Impact: NA

Suggested Action(s): Check logs to detect malicious attempts, perform IIS reset to reset the state of web scheduler.

Collect_FrontEnd_DataCollection_Exchange_ Archive_Adapter

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / LSDCEXCHADAPT

Source / Collection Definition: PERFMON / LS:DATACOLLECTION - Exchange Archiving Adaptor
(*)

Metric: DataCollectionInstance

> **Description**: instance of perfmon object LS:DATACOLLECTION - Exchange Archiving
> Adaptor
>
> **Metric SpecName**: DATACOLLINSTANCE
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: UDCNumberofUndeliverableItems

> **Description**: the number of undeliverable items due to continuing failures.
>
> **Metric SpecName**: NUMUNDELITEMS
>
> **Metric Field Name**: UDC - Number of Undeliverable Items
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Metric: UDCNumberofExchangeArchivingFailures

> **Description**: the number of failed Exchange I/O completions.
>
> **Metric SpecName**: NUMEXCHARCHFAILURES
>
> **Metric Field Name**: UDC - Number of Exchange Archiving Failures
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Metric: UDCNumberofDroppedSessions

> **Description**: Number of Exchange Archiving sessions dropped due to continuing failures.
>
> **Metric SpecName**: NUMDROPPEDSESSIONS
>
> **Metric Field Name**: UDC - Number of Dropped Sessions
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

UnifiedContactStore

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_LOW

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SYNRPCUNICONSTR

Source / Collection Definition: POWERSHELL / Test-CsUnifiedContactStore -TargetFQDN {fqdn}

Metric: UnifiedContactStore

Description: This metric gathers the information which confirms that users are able to access unified contact store

Metric SpecName: UnifiedCntSt

Metric Field Name: UnifiedContactStore

Data type: TEXT

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Minor / 1

Policy: MSBS_UnifiedContactStore

Message text: The Unified Contact Store is down

Instructional Text:

Probable Cause(s): 1. User configuration must not have done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: New users cannot be registered

Suggested Action(s): 1. Configuration errors: Most common issues are: Test user password is invalid or expired, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availability: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution errors or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responded to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Metric: TargetFqdn

Description: This is the key for metric

Metric SpecName: TargetFqdn

Metric Field Name: TargetFqdn

Data type: TEXT

Alarm: FALSE

Metric: UnifiedContactStoreLatency

Description: This metric will capture latency in receipt of confirmation that users are able to access unified contact store

Metric SpecName: UnifiedConStoLat

Metric Field Name: UnifiedContactStoreLatency

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Minor / 1000

Policy: MSBS_UnifiedContactStoreLatency

Message text: The value of Unified Contact Store Latency is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): 1. User configuration must not have done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: New users cannot be registered

Suggested Action(s): 1. Configuration errors: Most common issues are: Test user password is invalid or expired, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availibility: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution errors or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responded to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

ChkMonitoringQualityMonitoringServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / NA

Source / Collection Definition: SERVICECHECK / RtcQms

Metric: MonitoringRtcQmsServname

> **Description**: Name of the Service
>
> **Metric SpecName**: SERVNAME
>
> **Metric Field Name**: Service_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: MonitoringRtcQmsDisplayName

> **Description**: Display Name of the Service
>
> **Metric SpecName**: SRVDISPNAME
>
> **Metric Field Name**: Service_Displayname
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: MonitoringRtcQmsServStatus

Description: Status of the Service

Metric SpecName: SERVSTATUS

Metric Field Name: Service_Status

Data type: TEXT

Alarm: FALSE

Metric: MonitoringRtcQmsServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_MonitoringRtcQmsServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

MCUHealthStateChanged

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: SKYPE / MCUHELTHSTATCHANGCNT

Source / Collection Definition: PERFMON / LS:ImMcu - 02 - MCU Health And Performance(*)

Metric: MCUHealthStateChangedCount

> **Description**: This metric captures MCU Health State Changed Count
>
> **Metric SpecName**: MCUHelthStatChangCnt
>
> **Metric Field Name**: IMMCU - 007 - MCU Health State Changed Count
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Metric: Instance_Name

> **Description**: This is the key for metric
>
> **Metric SpecName**: Instance_Name
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: MCUHealthStateChangedCount

> **Description**: This metric captures MCU Health State Changed Count
>
> **Metric SpecName**: MCUHelthStatChangCnt
>
> **Metric Field Name**: DATAMCU - MCU Health State Changed Count
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Metric: Instance_Name

> **Description**: This is the key for metric
>
> **Metric SpecName**: Instance_Name
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

SimplePortWatcher5080

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / Port5080

Source / Collection Definition: PORTCOL / PORTCHECKER

Metric: SimpleWatcherPort5080

Description: Used for call admission control by the Bandwidth Policy service for A/V Edge TURN traffic.

Metric SpecName: SimpleWatcherPort5080

Metric Field Name: SimpleWatcherPort5080

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort5080

Message text: The Port No:5080 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

AppSharingCallFailurePercentage

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / APPSHARINGFAILURE

Source / Collection Definition: SQLDB / select isnull(cast(100.0 * cast((SUM(CASE WHEN SD.ResponseCode != 200 THEN 1 ELSE 0 END)) as float) / cast((SUM(CASE WHEN SD.ResponseCode is NOT NULL THEN 1 ELSE 0 END)) as float) as decimal(4, 1)),0) as AppSharingCallFailurePercentage,SERVERPROPERTY('MACHINENAME') AS 'ServerName' from [LcsCDR].[dbo].SessionDetails SD LEFT OUTER JOIN [LcsCDR].[dbo].Media M ON SD.SessionIdTime = M.SessionIdTime LEFT OUTER JOIN [LcsCDR].[dbo].MediaList ML ON M.MediaId = ML.MediaId Where ML.MediaId = 4 AND SD.SessionIdTime >= dateadd (MINUTE,@Duration,GETUTCDATE())

Metric: AppSharingCallFailurePercentage

Description: This metric captures call failures periodically from the CDR database and raises an alert whenever call failures exceed the specified "threshold" percentage value. When an Application Sharing call fails, this failure is reported to the Monitoring Server database (Call Detail Records database).

Metric SpecName: AppShareCallFailPer

Metric Field Name: AppSharingCallFailurePercentage

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 40, Major / 70, Warning / 40, Major / 70

Policy: MSBS_AppSharingCallFailurePercentage

Message text: The current value of Percentage App Sharing Call Failure is <VALUE> which exceeds the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Failure to do an app sharing event may be because of policy violation, processing error, network overload, server overload etc

Potential Impact: Users face issue in sharing desktop or other applications

Suggested Action(s): Defining appropriate policy, troubleshoot network etc

Metric: ServerName

Description: This is the key for metric

Metric SpecName: ServerName

Metric Field Name: ServerName

Data type: TEXT

Alarm: FALSE

Collect_FrontEnd_Process_ReplicaReplicatorAgent

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / CS_PROCESS

Source / Collection Definition: PERFMON / Process(ReplicaReplicatorAgent)

Metric: FEREPLICAInstance

> **Description**: instance of ReplicaReplicatorAgent process
>
> **Metric SpecName**: INSTANCENAME
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FEREPLICAPercentprocessorTime

> **Description**: Percentage Processor Time is the percentage of elapsed time that all of process threads used the processor to execution instructions.
>
> **Metric SpecName**: PCTPROCESSORTIME
>
> **Metric Field Name**: % Processor Time
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Metric: FEREPLICAWorkingSet

Description: Working Set is the current size, in bytes, of the Working Set of this process. the Working Set is the set of memory pages touched recently by the threads in the process. If free memory in the computer is above a threshold, pages are left in the Working Set of a process even if they are not in use. When free memory falls below a threshold, pages are trimmed from Working Sets. If they are needed they will then be soft-faulted back into the Working Set before leaving main memory.

Metric SpecName: WORKINGSET

Metric Field Name: Working Set

Data type: UINT32

Alarm: FALSE

Metric: FEREPLICAPageFaultsPerSec

Description: Page Faults/sec is the average number of pages faulted per second. It is measured in number of pages faulted per second because only one page is faulted in each fault operation, hence this is also equal to the number of page fault operations. This counter includes both hard faults (those that require disk access) and soft faults (where the faulted page is found elsewhere in physical memory.) Most processors can handle large numbers of soft faults without significant consequence. However, hard faults, which require disk access, can cause significant delays.

Metric SpecName: PAGEFAULTS

Metric Field Name: Page Faults/sec

Data type: UINT32

Alarm: FALSE

Metric: FEREPLICAPrivateBytes

Description: Private Bytes is the current size, in bytes, of memory that this process has allocated that cannot be shared with other processes.

Metric SpecName: PRIVATEBYTES

Metric Field Name: Private Bytes

Data type: UINT32

Alarm: FALSE

Metric: FEREPLICAThreadCount

Description: the number of threads currently active in this process. An instruction is the basic unit of execution in a processor, and a thread is the object that executes instructions. Every running process has at least one thread.

Metric SpecName: THREADCOUNT

Metric Field Name: Thread Count

Data type: UINT32

Alarm: FALSE

Metric: REPLICAInstance

Description: instance of ReplicaReplicatorAgent process

Metric SpecName: INSTANCENAME

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: REPLICAPercentprocessorTime

Description: Percentage Processor Time is the percentage of elapsed time that all of process threads used the processor to execution instructions.

Metric SpecName: PCTPROCESSORTIME

Metric Field Name: % Processor Time

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 90

Policy: MSBS_REPLICAPercentprocessorTime

Message text: The value of the counter '% Processor Time' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: REPLICAWorkingSet

Description: Working Set is the current size, in bytes, of the Working Set of this process. the Working Set is the set of memory pages touched recently by the threads in the process. If free memory in the computer is above a threshold, pages are left in the Working Set of a process even if they are not in use. When free memory falls below a threshold, pages are trimmed from Working Sets. If they are needed they will then be soft-faulted back into the Working Set before leaving main memory.

Metric SpecName: WORKINGSET

Metric Field Name: Working Set

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20000000

Policy: MSBS_REPLICAWorkingSet

Message text: The value of the counter 'Working Set' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: REPLICAPageFaultsPerSec

Description: Page Faults/sec is the average number of pages faulted per second. It is measured in number of pages faulted per second because only one page is faulted in each fault operation, hence this is also equal to the number of page fault operations. This counter includes both hard faults (those that require disk access) and soft faults (where the faulted page is found elsewhere in physical memory.) Most processors can handle large numbers of soft faults without significant consequence. However, hard faults, which require disk access, can cause significant delays.

Metric SpecName: PAGEFAULTS

Metric Field Name: Page FaultsPersec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 100

Policy: MSBS_REPLICAPageFaultsPerSec

Message text: The value of the counter 'Page Faults/sec' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: REPLICAPrivateBytes

Description: Private Bytes is the current size, in bytes, of memory that this process has allocated that cannot be shared with other processes.

Metric SpecName: PRIVATEBYTES

Metric Field Name: Private Bytes

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20000000

Policy: MSBS_REPLICAPrivateBytes

Message text: The value of the counter 'Private Bytes' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: REPLICAThreadCount

Description: the number of threads currently active in this process. An instruction is the basic unit of execution in a processor, and a thread is the object that executes instructions. Every running process has at least one thread.

Metric SpecName: THREADCOUNT

Metric Field Name: Thread Count

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 150

Policy: MSBS_REPLICAThreadCount

Message text: The value of the counter 'Thread Count' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Collect_Edge_DataProxy_Server_Connections

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / LSDATAPROXY

Source / Collection Definition: PERFMON / LS:DATAPROXY - Server Connections(*)

Metric: EdgeDataProxyInstance

Description: instance of perfmon object LS:DATAPROXY - Server Connections

Metric SpecName: DPINSTANAME

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: EdgeDataProxyServerConnActive

Description: Current number of active connections to Web Conferencing Server

Metric SpecName: SRVACTIVECONN

Metric Field Name: DATAPROXY - Server Connections Currently Active

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 2, Major / 5

Policy: MSBS_EdgeDataProxyServerConnActive

Message text: The value of DATAPROXY - Server Connections Currently Active for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Web Conferencing Server has malfunctioned and is not running in a healthy state

Potential Impact: NA

Suggested Action(s): Make sure that the Web Conferencing Server is in a healthy state

Metric: EdgeDataProxyInstance

Description: instance of perfmon object LS:DATAPROXY - 00 - Server Connections(_Total)

Metric SpecName: DPINSTANAME

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: DataPrxySrvrconndisconduetothrotlng

> **Description**: The total number of server connections disconnected due to throttling
>
> **Metric SpecName**: SRVCONNDISCONDTHROTLNG
>
> **Metric Field Name**: DATAPROXY - 035 - Server connections disconnected due to throttling
>
> **Data type**: UINT32
>
> **Alarm**: TRUE
>
> **Category** : MSSkype
>
> **Severity / Threshold** : Major / 100
>
> **Policy**: MSBS_DataPrxySrvrconndisconduetothrotlng
>
> **Message text**: The value of the counter 'Server connections disconnected due to throttling' value <VALUE> has crossed the threshold of <THRESHOLD> .
>
> **Instructional Text**:
>
> **Probable Cause(s)**: NA
>
> **Potential Impact**: NA
>
> **Suggested Action(s)**: NA

Metric: EdgeDataProxySystemisthrottling

Description: system wide throttling is on

Metric SpecName: SYSTEMISTHROTLNG

Metric Field Name: DATAPROXY - 041 - System is throttling

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20

Policy: MSBS_EdgeDataProxySystemisthrottling

Message text: The value of the counter 'System is throttling' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: WebEdgeDataProxySystemisthrottling

Description: system wide throttling.

Metric SpecName: SYSTEMISTHROTLNG

Metric Field Name: DATAPROXY - 041 - System is throttling

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 2

Policy: MSBS_WebEdgeDataProxySystemisthrottling

Message text: The value of the counter 'WebEdge DataProxy System is throttling' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: DataPrxyCurrcountofsrvrconnthrottled

Description: The number of throttled server connections

Metric SpecName: CURRENTSRVCONNTHROTLD

Metric Field Name: DATAPROXY - 034 - Current count of server connections that are throttled

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 2

Policy: MSBS_DataPrxyCurrcountofsrvrconnthrottled

Message text: The value of the counter 'Current count of server connections that are throttled' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

SimplePortWatcher5262

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / Port5262

Source / Collection Definition: PORTCOL / PORTCHECKER

Metric: SimpleWatcherPort5262

Description: Used For XMPP fereration

Metric SpecName: SimpleWatcherPort5262

Metric Field Name: SimpleWatcherPort5262

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort5262

Message text: The Port No:5262 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

Metric: SimpleWatcherPort5262

Description: Used For XMPP fereration

Metric SpecName: SimpleWatcherPort5262

Metric Field Name: SimpleWatcherPort5262

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort5262

Message text: The Port No:5262 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

SimplePortWatcher5073

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / Port5073

Source / Collection Definition: PORTCOL / PORTCHECKER

Metric: SimpleWatcherPort5073

Description: Used for incoming SIP requests for the Lync Server Conferencing Announcement service (that is, for dial-in conferencing).

Metric SpecName: SimpleWatcherPort5073

Metric Field Name: SimpleWatcherPort5073

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort5073

Message text: The Port No:5073 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

Metric: SimpleWatcherPort5073

Description: Used for incoming SIP requests for the Lync Server Conferencing Announcement service (that is, for dial-in conferencing).

Metric SpecName: SimpleWatcherPort5073

Metric Field Name: SimpleWatcherPort5073

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort5073

Message text: The Port No:5073 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

SimplePortWatcher443

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / Port443

Source / Collection Definition: PORTCOL / PORTCHECKER

Metric: SimpleWatcherPort443

Description: Used for communication from Front End Servers to the web farm FQDNs (the URLs used by IIS web components).

Metric SpecName: SimpleWatcherPort443

Metric Field Name: SimpleWatcherPort443

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_SimpleWatcherPort443

Message text: The Port No:443 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

Metric: SimpleWatcherPort443

Description: Used for communication from Front End Servers to the web farm FQDNs (the URLs used by IIS web components).

Metric SpecName: SimpleWatcherPort443

Metric Field Name: SimpleWatcherPort443

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_SimpleWatcherPort443

Message text: The Port No:443 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

Collect_FrontEnd_Web_Distribution_List_Expansion

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / LSWEBDISTRLISTEXP

Source / Collection Definition: PERFMON / LS:WEB - Distribution List Expansion(*)

Metric: DistrListExpansionInstance

Description: instance of perfmon object LS:WEB - Distribution List Expansion

Metric SpecName: FEDISTRLSTEXPANSION

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: SuccessfulRequestProcTime

Description: Average processing time for a successful request to be completed

Metric SpecName: SUCREQPROCTIME

Metric Field Name: WEB - Successful Request Processing Time

Data type: UINT32

Alarm: FALSE

Metric: SOAPExceptions

Description: the per-second rate of Soap Exceptions

Metric SpecName: FESOAPEXCEPT

Metric Field Name: WEB - Soap exceptions/sec

Data type: UINT32

Alarm: FALSE

Metric: DistrListExpansionInstance

Description: instance of perfmon object LS:WEB - 00 - Distribution List Expansion

Metric SpecName: FEDISTRLSTEXPANSION

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: SuccessfulRequestProcTime

Description: Average processing time for a successful request to be completed

Metric SpecName: SUCREQPROCTIME

Metric Field Name: WEB - Successful Request Processing Time

Data type: UINT32

Alarm: FALSE

Metric: SOAPExceptions

Description: The number of SOAP exceptions per second during address book list expansion

Metric SpecName: FESOAPEXCEPT

Metric Field Name: WEB - 015 - Soap exceptions/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 50, Major / 100

Policy: MSBS_SOAPExceptions

Message text: The value of the counter ' Soap exceptions/sec' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: Averagememberpropertiesfetchtimeinmilliseconds

Description: average fetch time of member properties in milliseconds

Metric SpecName: AVGFETCHTIME

Metric Field Name: WEB - 008 - Average member properties fetch time in milliseconds

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 1000, Major / 3000

Policy: MSBS_Averagememberpropertiesfetchtimeinmilliseconds

Message text: The value of the counter ' Average member properties fetch time in milliseconds' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: PendingActiveDirectoryRequests

Description: number of request waiting currently for Active Directory responses

Metric SpecName: PENDINGADREQUESTS

Metric Field Name: WEB - 004 - Pending Active Directory Requests

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 50, Major / 100

Policy: MSBS_PendingActiveDirectoryRequests

Message text: The value of the counter ' Pending Active Directory Requests' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

ChkFrontEndConferencingAttendentServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SERVSTAT

Source / Collection Definition: SERVICECHECK / RTCCAA

Metric: FERTCCAAServName

Description: Name of the Service

Metric SpecName: SERVNAME

Metric Field Name: Service_Name

Data type: TEXT

Alarm: FALSE

Metric: FERTCCAAServDisplayName

Description: Display Name of the Service

Metric SpecName: SRVDISPNAME

Metric Field Name: Service_Displayname

Data type: TEXT

Alarm: FALSE

Metric: FERTCCAAServStatus

Description: Status of the Service

Metric SpecName: SERVSTATUS

Metric Field Name: Service_Status

Data type: TEXT

Alarm: FALSE

Metric: FERTCCAAServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_FERTCCAAServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): Lync Server Conferencing Attendant' Windows Service is stopped.

Potential Impact: NA

Suggested Action(s): Lync Server Conferencing Attendant' Windows Service is stopped. Please restart the service.

AuthenticCredential

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: SKYPE / AUTHENTICCREDENTIAL

Source / Collection Definition: PERFMON / LS:A/V Auth - Requests(*)

Metric: CredentialsIssuedAuth

Description: This metric captures the Credentials Issued by Skype Audio/Video Authentication Server

Metric SpecName: CredentialsIssueAuth

Metric Field Name: CredentialsIssuedAuth

Data type: TEXT

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Critical / 1, Major / 1

Policy: MSBS_CredentialsIssuedAuth

Message text: The value of Credentials Issued Authentication is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): The Audio-Video Conferencing Server cannot communicate with A/V Authentication Service.

Potential Impact: Check the A/V Authentication Service is alive and that network connectivity exists.

Suggested Action(s): Users face issue In Conecting to Audio-Video Conferencing Server

Metric: AuthCredentialsIssuedPS

Description: This metric captures Credentials Issued per second by Skype Audio/Video Authentication Server

Metric SpecName: CredentialsIssuedPS

Metric Field Name: AuthCredentialsIssuedPS

Data type: TEXT

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Critical / 9999, Major / 5

Policy: MSBS_AuthCredentialsIssuedPS

Message text: The value of Credentials Issued Per Second is <VALUE>

Instructional Text:

Probable Cause(s): The Audio-Video Conferencing Server cannot communicate with A/V Authentication Service.

Potential Impact: heck the A/V Authentication Service is alive and that network connectivity exists.

Suggested Action(s): Users face issue In COnnecting to Audio-Video Conferencing Server

Metric: CurrentRequestsServiced

Description: This metric captures Current requests serviced by Skype Audio/Video Authentication Server

Metric SpecName: CurrentRequestsSev

Metric Field Name: CurrentRequestsServiced

Data type: TEXT

Alarm: FALSE

Metric: CredentialsIssuedAuth

Description: This metric captures the Credentials Issued by Skype Audio/Video Authentication Server

Metric SpecName: CredentialsIssueAuth

Metric Field Name: - Credentials Issued

Data type: TEXT

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Critical / 1, Major / 1

Policy: MSBS_CredentialsIssuedAuth

Message text: The value of Credentials Issued Authentication is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): The Audio-Video Conferencing Server cannot communicate with A/V Authentication Service.

Potential Impact: Check the A/V Authentication Service is alive and that network connectivity exists.

Suggested Action(s): Users face issue In Conecting to Audio-Video Conferencing Server

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: AuthCredentialsIssuedPS

Description: This metric captures Credentials Issued per second by Skype Audio/Video Authentication Server

Metric SpecName: CredentialsIssuedPS

Metric Field Name: - Credentials Issued/sec

Data type: TEXT

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Critical / 9999, Major / 5

Policy: MSBS_AuthCredentialsIssuedPS

Message text: The value of Credentials Issued Per Second is <VALUE>

Instructional Text:

Probable Cause(s): The Audio-Video Conferencing Server cannot communicate with A/V Authentication Service.

Potential Impact: heck the A/V Authentication Service is alive and that network connectivity exists.

Suggested Action(s): Users face issue In COnnecting to Audio-Video Conferencing Server

Metric: CurrentRequestsServiced

Description: This metric captures Current requests serviced by Skype Audio/Video Authentication Server

Metric SpecName: CurrentRequestsSev

Metric Field Name: - Current requests serviced

Data type: TEXT

Alarm: FALSE

Collect_FrontEnd_UsrvDBSTORE

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / LSUSRVDBSTORE

Source / Collection Definition: PERFMON / LS:USrv - DBStore(*)

Metric: USRVDBStoreInstance

> **Description**: instance of perfmon object LS:USrv - DBStore
>
> **Metric SpecName**: USRVDBSTOREINSTANCE
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: UsrvQueueDepth

> **Description**: the average number of database requests waiting to be executed.
>
> **Metric SpecName**: QUEUEDEPTH
>
> **Metric Field Name**: USrv - Queue Depth
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Metric: UsrvQueueLatency

> **Description**: the average time (in milliseconds) a request is held in the database queue.
>
> **Metric SpecName**: FEQUEUELATENCY
>
> **Metric Field Name**: USrv - Queue Latency (msec)
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Metric: UsrvSprocLatency

Description: the average time (in milliseconds) it takes to process a RtcAuthorizeDelegate sproc call.

Metric SpecName: FESPROCLATENCY

Metric Field Name: USrv - Sproc Latency (msec)

Data type: UINT32

Alarm: FALSE

Metric: USRVDBStoreInstance

Description: instance of perfmon object LS:USrv - 01 - DBStore

Metric SpecName: USRVDBSTOREINSTANCE

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: UsrvQueueDepth

Description: the average number of database requests waiting to be executed.

Metric SpecName: QUEUEDEPTH

Metric Field Name: USrv - Queue Depth

Data type: UINT32

Alarm: FALSE

Metric: UsrvQueueLatency

Description: This counter represents the time each requests spent in queue to the backed database

Metric SpecName: FEQUEUELATENCY

Metric Field Name: USrv - 002 - Queue Latency (msec)

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 6000

Policy: MSBS_UsrvQueueLatency

Message text: The value of the counter 'Sproc Latency (msec)' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: UsrvSprocLatency

Description: Time taken for the backend database to process the request from server

Metric SpecName: FESPROCLATENCY

Metric Field Name: USrv - 004 - Sproc Latency (msec)

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 6000

Policy: MSBS_UsrvSprocLatency

Message text: The value of the counter 'Sproc Latency (msec)' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: BlockedClientThreads

Description: The average number of client threads that are blocked in the queue, waiting for the queue depth to decrease

Metric SpecName: BLKCLTTHRDS

Metric Field Name: USrv - 011 - Blocked Client Threads

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 4000, Major / 6000

Policy: MSBS_BlockedClientThreads

Message text: The value of the counter 'Blocked Client Threads' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

SimplePortWatcher8057

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / Port8057

Source / Collection Definition: PORTCOL / PORTCHECKER

Metric: SimpleWatcherPort8057

Description: Used to listen for Persistent Shared Object Model (PSOM) connections from client.

Metric SpecName: SimpleWatcherPort8057

Metric Field Name: SimpleWatcherPort8057

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort8057

Message text: The Port No:8057 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

> **Description**: This is the key for metric
>
> **Metric SpecName**: HOSTNAME
>
> **Metric Field Name**: HOSTNAME
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: SimpleWatcherPort8057

Description: Used to listen for Persistent Shared Object Model (PSOM) connections from client.

Metric SpecName: SimpleWatcherPort8057

Metric Field Name: SimpleWatcherPort8057

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort8057

Message text: The Port No:8057 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

SimplePortWatcher5041

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / Port5041

Source / Collection Definition: PORTCOL / PORTCHECKER

Metric: SimpleWatcherPort5041

Description: Used for internal communications between servers and for client connections.

Metric SpecName: SimpleWatcherPort5041

Metric Field Name: SimpleWatcherPort5041

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_SimpleWatcherPort5041

Message text: The Port No:5041 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

SprocCallsPerSecUser

This policy maintains the information about the status for the different services

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_SubscribedUser_Conf

Aspect: Skype Subscribed User

CIT: Front End Server

Data source / Data class: LYNC / SPROCCALLSPERSECUSR

Source / Collection Definition: PERFMON / LS:USrv - UpdateEndpoint sproc(*)

Metric: SprocCallsPerSecUser

> **Description**: This metric captures Sproc Calls Per Sec
>
> **Metric SpecName**: SprocCallsPerSecUser
>
> **Metric Field Name**: USrv - Sproc Calls/Sec
>
> **Data type**: REAL64
>
> **Alarm**: FALSE

Metric: Instance_Name

> **Description**: This is the key for metric
>
> **Metric SpecName**: Instance_Name
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Collect_Director_Process_ReplicaReplicatorAgent

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / CS_PROCESS

Source / Collection Definition: PERFMON / Process(ReplicaReplicatorAgent)

Metric: DirREPLICAInstance

> **Description**: instance of ReplicaReplicatorAgent process
>
> **Metric SpecName**: INSTANCENAME
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: DirREPLICAPercentprocessorTime

> **Description**: Percentage Processor Time is the percentage of elapsed time that all of process threads used the processor to execution instructions.
>
> **Metric SpecName**: PCTPROCESSORTIME
>
> **Metric Field Name**: % Processor Time
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Metric: DirREPLICAWorkingSet

Description: Working Set is the current size, in bytes, of the Working Set of this process. the Working Set is the set of memory pages touched recently by the threads in the process. If free memory in the computer is above a threshold, pages are left in the Working Set of a process even if they are not in use. When free memory falls below a threshold, pages are trimmed from Working Sets. If they are needed they will then be soft-faulted back into the Working Set before leaving main memory.

Metric SpecName: WORKINGSET

Metric Field Name: Working Set

Data type: UINT32

Alarm: FALSE

Metric: DirREPLICAPageFaultsPerSec

Description: Page Faults/sec is the average number of pages faulted per second. It is measured in number of pages faulted per second because only one page is faulted in each fault operation, hence this is also equal to the number of page fault operations. This counter includes both hard faults (those that require disk access) and soft faults (where the faulted page is found elsewhere in physical memory.) Most processors can handle large numbers of soft faults without significant consequence. However, hard faults, which require disk access, can cause significant delays.

Metric SpecName: PAGEFAULTS

Metric Field Name: Page Faults/sec

Data type: UINT32

Alarm: FALSE

Metric: DirREPLICAPrivateBytes

Description: Private Bytes is the current size, in bytes, of memory that this process has allocated that cannot be shared with other processes.

Metric SpecName: PRIVATEBYTES

Metric Field Name: Private Bytes

Data type: UINT32

Alarm: FALSE

Metric: DirREPLICAThreadCount

> **Description**: the number of threads currently active in this process. An instruction is the basic unit of execution in a processor, and a thread is the object that executes instructions. Every running process has at least one thread.
>
> **Metric SpecName**: THREADCOUNT
>
> **Metric Field Name**: Thread Count
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

FileTransferFailurePercentage

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / FILETRANSFERFAILURE

Source / Collection Definition: SQLDB / select isnull(cast(100.0 * cast((SUM(CASE WHEN SD.ResponseCode != 200 THEN 1 ELSE 0 END)) as float) / cast((SUM(CASE WHEN SD.ResponseCode is NOT NULL THEN 1 ELSE 0 END)) as float) as decimal(4, 1)),0) as FileTransferFailurePercentage,SERVERPROPERTY('MACHINENAME') AS 'ServerName' from [LcsCDR].[dbo].SessionDetails SD RIGHT OUTER JOIN [LcsCDR].[dbo].[FileTransfersView] FT ON SD.SessionIdTime = FT.SessionIdTime WHERE SD.SessionIdTime >= dateadd (MINUTE,@Duration,GETUTCDATE())

Metric: FileTransferFailurePercentage

Description: This metric captures call failures periodically from the CDR database and raises an alert whenever call failures exceed the specified "threshold" percentage value. When an File Transfer Session fails, this failure is reported to the Monitoring Server database (Call Detail Records database).

Metric SpecName: FileTransferFailPer

Metric Field Name: FileTransferFailurePercentage

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 40, Major / 70, Warning / 40, Major / 70

Policy: MSBS_FileTransferFailurePercentage

Message text: The current value of Percentage File Transfer Failure is <VALUE> which exceeds the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): The reason for a Failed File transfer may be because of session time expiration, conference deletion ,policy violation by message , request timeout, unsupported message type, large file size etc

Potential Impact: Users face issue in transferring some types of files

Suggested Action(s): Defining appropriate file content, configuring server for timeouts, sending file of size as defined in policy etc

Metric: ServerName

Description: This is the key for metric

Metric SpecName: ServerName

Metric Field Name: ServerName

Data type: TEXT

Alarm: FALSE

Metric: FileTransferFailurePercentage

Description: This metric captures call failures periodically from the CDR database and raises an alert whenever call failures exceed the specified "threshold" percentage value. When an File Transfer Session fails, this failure is reported to the Monitoring Server database (Call Detail Records database).

Metric SpecName: FileTransferFailPer

Metric Field Name: FileTransferFailurePercentage

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 40, Major / 70, Warning / 40, Major / 70

Policy: MSBS_FileTransferFailurePercentage

Message text: The current value of Percentage File Transfer Failure is <VALUE> which exceeds the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): The reason for a Failed File transfer may be because of session time expiration, conference deletion ,policy violation by message , request timeout, unsupported message type, large file size etc

Potential Impact: Users face issue in transferring some types of files

Suggested Action(s): Defining appropriate file content, configuring server for timeouts, sending file of size as defined in policy etc

Metric: ServerName

Description: This is the key for metric

Metric SpecName: ServerName

Metric Field Name: ServerName

Data type: TEXT

Alarm: FALSE

ChkPersistentChatComplianceServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SERVSTAT

Source / Collection Definition: SERVICECHECK / RTCCHATCOMPL

Metric: PersistentChatRTCCHATCOMPLServName

> **Description**: Name of the Service
>
> **Metric SpecName**: SERVNAME
>
> **Metric Field Name**: Service_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: PersistentChatRTCCHATCOMPLServDisplayName

> **Description**: Display Name of the Service
>
> **Metric SpecName**: SRVDISPNAME
>
> **Metric Field Name**: Service_Displayname
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: PersistentChatRTCCHATCOMPLServStatus

Description: Status of the Service

Metric SpecName: SERVSTATUS

Metric Field Name: Service_Status

Data type: TEXT

Alarm: FALSE

Metric: PersistentChatRTCCHATCOMPLServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_PersistentChatRTCCHATCOMPLServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): Lync Server Persistent Chat Compliance' Windows Service is stopped.

Potential Impact: NA

Suggested Action(s): Lync Server Persistent Chat Compliance' Windows Service is stopped. Please restart the service.

ChkFrontEndOnlinePushNotificationServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SERVSTAT

Source / Collection Definition: SERVICECHECK / PnchService

Metric: FEPnchServiceServName

> **Description**: Name of the Service
>
> **Metric SpecName**: SERVNAME
>
> **Metric Field Name**: Service_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FEPnchServiceServDisplayName

> **Description**: Display Name of the Service
>
> **Metric SpecName**: SRVDISPNAME
>
> **Metric Field Name**: Service_Displayname
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FEPnchServiceServStatus

> **Description**: Status of the Service
>
> **Metric SpecName**: SERVSTATUS
>
> **Metric Field Name**: Service_Status
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FEPnchServiceServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_FEPnchServiceServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): Lync Online Push Notification Service' Windows Service is stopped.

Potential Impact: NA

Suggested Action(s): Lync Online Push Notification Service' Windows Service is stopped. Please restart the service.

SimplePortWatcher5063

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / Port5063

Source / Collection Definition: PORTCOL / PORTCHECKER

Metric: SimpleWatcherPort5063

Description: Used for incoming SIP requests for audio/video (A/V) conferencing.

Metric SpecName: SimpleWatcherPort5063

Metric Field Name: SimpleWatcherPort5063

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort5063

Message text: The Port No:5063 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

Metric: SimpleWatcherPort5063

Description: Used for incoming SIP requests for audio/video (A/V) conferencing.

Metric SpecName: SimpleWatcherPort5063

Metric Field Name: SimpleWatcherPort5063

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort5063

Message text: The Port No:5063 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

Operations

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / KHIOPERATIONS

Source / Collection Definition: PERFMON / LS:CAA - 00 - Operations(*)

Metric: Incompletecallspersec

Description: This policy monitors the per second rate of incomplete calls to Conferencing Attendant. This includes calls disconnected by the user and by the system due to invalid conference id, passcode, etc.

Metric SpecName: Incompcallspersec

Metric Field Name: CAA - 000 - Incomplete calls per sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Minor / 20, Minor / 20

Policy: MSBS_Incompletecallspersec

Message text: The current value of Incompletecallspersec is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): Conferencing Attendant could not get primary application end point.

Potential Impact: Check if Conferencing Attendant contact object exists in management store and in Active Directory.

Suggested Action(s): Incomplete PSTN calls to the Conferencing Auto Attendant.

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: Incompletecallspersec

Description: This policy monitors the per second rate of incomplete calls to Conferencing Attendant. This includes calls disconnected by the user and by the system due to invalid conference id, passcode, etc.

Metric SpecName: Incompcallspersec

Metric Field Name: CAA - Incomplete calls per sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Minor / 20, Minor / 20

Policy: MSBS_Incompletecallspersec

Message text: The current value of Incompletecallspersec is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): Conferencing Attendant could not get primary application end point.

Potential Impact: Check if Conferencing Attendant contact object exists in management store and in Active Directory.

Suggested Action(s): Incomplete PSTN calls to the Conferencing Auto Attendant.

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Collect_FrontEnd_Processor

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / LSPROCESSOR

Source / Collection Definition: PERFMON / Processor(_Total)

Metric: ProcesserInstance

> **Description**: instance of perfmon object Processor Total
>
> **Metric SpecName**: PROCESSORINST
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: SystemPercentProcessorTime

> **Description**: Percentage Processor Time is the percentage of elapsed time that all of process
> threads used the processor to execution instructions.
>
> **Metric SpecName**: SYSPCTPROCESSORTIME
>
> **Metric Field Name**: % Processor Time
>
> **Data type**: UINT32
>
> **Alarm**: TRUE
>
> **Category** : MSSkype
>
> **Severity / Threshold** : Warning / 50, Major / 70
>
> **Policy**: MSBS_SystemPercentProcessorTime
>
> **Message text**: The value of % Processor Time for instance <OPTION(InstanceName)> is
> <VALUE> and has crossed the threshold of <THRESHOLD>
>
> **Instructional Text**:
>
> **Probable Cause(s)**: Check CPU usage in task manager.
>
> **Potential Impact**: NA
>
> **Suggested Action(s)**: If the machine is under heavy load, please consider adding more
> machine into the pool to increase load balancing.

SimpleURLWatcherMeet

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / URLWATCHMEET

Source / Collection Definition: POWERSHELL / Invoke-WebRequest -Uri meet.{SIPDOMAIN} - UseDefaultCredentials

Metric: URLWatcherMeet

Description: This metric check HTTP response of a Meet URL

Metric SpecName: URLWatcherMeet

Metric Field Name: StatusCode

Data type: TEXT

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Minor / 1

Policy: MSBS_URLWatcherMeet

Message text: The Meeting in URL to access Meeting conferences is down

Instructional Text:

Probable Cause(s): The page is unreachable. If behind a proxy, check if the proxy settings are correct. Unexpected API call failures. Multiple reasons could cause this, for instance a memory allocation error. The site or URL is not accessible or is down.

Potential Impact: URL cannot be accessed

Suggested Action(s): Try to access the same URL from an internet browser like Internet Explorer.

Metric: ServerName

Description: This metric check HTTP response of a Meet URL

Metric SpecName: ServerName

Metric Field Name: ServerName

Data type: TEXT

Alarm: FALSE

Collect_FrontEnd_Process_MasterReplicatorAgent

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / CS_PROCESS

Source / Collection Definition: PERFMON / Process(MasterReplicatorAgent)

Metric: FEMRAInstance

> **Description**: instance of perfmon object Process(MasterReplicatorAgent)
>
> **Metric SpecName**: INSTANCENAME
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FEMRAPageFaultsPersec

> **Description**: Page Faults/sec counter available in the CS Server Master Replicator Agent service .
>
> **Metric SpecName**: PAGEFAULTPERSEC
>
> **Metric Field Name**: Page Faults/sec
>
> **Data type**: UINT32
>
> **Alarm**: TRUE
>
> **Category** : MSSkype
>
> **Severity / Threshold** : Major / 100
>
> **Policy**: MSBS_FEMRAPageFaultsPersec
>
> **Message text**: The value of the counter 'Page Faults/sec' value <VALUE> has crossed the threshold of <THRESHOLD> .
>
> **Instructional Text**:
>
> **Probable Cause(s)**: NA
>
> **Potential Impact**: NA
>
> **Suggested Action(s)**: NA

Metric: FEMRAPrivateBytes

Description: Private Bytes counter available in the CS Server Master Replicator Agent service.

Metric SpecName: PRIVATEBYTES

Metric Field Name: Private Bytes

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20000000

Policy: MSBS_FEMRAPrivateBytes

Message text: The value of the counter 'Private Bytes' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: FEMRAPercentprocessorTime

Description: % Processor Time counter available in the CS Server Master Replicator Agent service.

Metric SpecName: PROCESSORTIME

Metric Field Name: % Processor Time

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 90

Policy: MSBS_FEMRAPercentprocessorTime

Message text: The value of the counter '% Processor Time' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: FEMRAThreadCount

Description: Thread Count counter available in the CS Server Master Replicator Agent service.

Metric SpecName: THREADCOUNT

Metric Field Name: Thread Count

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 150

Policy: MSBS_FEMRAThreadCount

Message text: The value of the counter 'Thread Count' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: FEMRAWorkingSet

Description: Working Set counter available in the CS Server Master Replicator Agent service.

Metric SpecName: WORKINGSET

Metric Field Name: Working Set

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20000000

Policy: MSBS_FEMRAWorkingSet

Message text: The value of the counter 'Working Set' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Collect_FrontEnd_SIP_Response

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / CS_FRONTEND

Source / Collection Definition: PERFMON / LS:SIP - 04 - Responses(*)

Metric: SIPResponseInstance

Description: instance of perfmon object LS:SIP - 04 - Responses

Metric SpecName: SIPRESPINSTANCE

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: SIPLocal503ResponsePerSec

Description: number of 503 responses received in a second. Code 503 means that the server is unavailable.

Metric SpecName: SIPLOCAL503RESPONSES

Metric Field Name: SIP - 055 - Local 503 Responses/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 5

Policy: MSBS_SIPLocal503ResponsePerSec

Message text: The value of the counter 'Local 503 Responses/sec' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: SIPLocal504ResponsePerSec

Description: number of 504 responses received in a second. Code 504 implies that there are problems connecting to other servers.

Metric SpecName: SIPLOCAL504RESPONSES

Metric Field Name: SIP - 057 - Local 504 Responses/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 5

Policy: MSBS_SIPLocal504ResponsePerSec

Message text: The value of the counter 'Local 504 Responses/sec' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Protocol

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / KHIPROTOCOL

Source / Collection Definition: PERFMON / LS:SIP - 02 - Protocol(*)

Metric: AverageIncomingMessageProcessingTime

Description: This policy monitors the average time (in seconds) it takes to process an incoming message

Metric SpecName: AvgIncmMessProTim

Metric Field Name: SIP - 021 - Average Incoming Message Processing Time

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_AverageIncomingMessageProcessingTime

Message text: The current value of AverageIncomingMessageProcessingTime is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): This server is too busy and is unable to process user requests in timely fashion.

Potential Impact: Please ensure that hardware and software requirements at the destination and network bandwidth allocation meet the user usage characteristics.

Suggested Action(s): Slow SIP message transmissions

Metric: IncomingRequestsDropped

Description: This policy monitors the per-second rate of incoming requests dropped because they could not be processed (due to bad headers, insufficient routing information, server resource allocation failure).

Metric SpecName: IncomReqDrop

Metric Field Name: SIP - 005 - Incoming Requests Dropped/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_IncomingRequestsDropped

Message text: The current value of IncomingRequestsDropped is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): This server is too busy and is unable to process user requests in timely fashion.

Potential Impact: Please ensure that hardware and software requirements at the destination and network bandwidth allocation meet the user usage characteristics.

Suggested Action(s): Slow SIP message transmissions

Metric: IncomingResponsesDropped

Description: This policy monitors the per-second rate of incoming responses dropped because they could not be processed (due to bad headers, insufficient routing information, server resource allocation failure).

Metric SpecName: IncomRespDrop

Metric Field Name: SIP - 009 - Incoming Responses Dropped/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_IncomingResponsesDropped

Message text: The current value of IncomingResponsesDropped is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): This server is too busy and is unable to process user requests in timely fashion.

Potential Impact: Please ensure that hardware and software requirements at the destination and network bandwidth allocation meet the user usage characteristics.

Suggested Action(s): Slow SIP message transmissions

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: AverageIncomingMessageProcessingTime

Description: This policy monitors the average time (in seconds) it takes to process an incoming message.

Metric SpecName: AvgIncmMessProTim

Metric Field Name: SIP - Average Incoming Message Processing Time

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_AverageIncomingMessageProcessingTime

Message text: The current value of AverageIncomingMessageProcessingTime is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): This server is too busy and is unable to process user requests in timely fashion.

Potential Impact: Please ensure that hardware and software requirements at the destination and network bandwidth allocation meet the user usage characteristics.

Suggested Action(s): Slow SIP message transmissions

Metric: IncomingRequestsDropped

Description: This policy monitors the per-second rate of incoming requests dropped because they could not be processed (due to bad headers, insufficient routing information, server resource allocation failure).

Metric SpecName: IncomReqDrop

Metric Field Name: SIP - Incoming Requests Dropped/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_IncomingRequestsDropped

Message text: The current value of IncomingRequestsDropped is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): This server is too busy and is unable to process user requests in timely fashion.

Potential Impact: Please ensure that hardware and software requirements at the destination and network bandwidth allocation meet the user usage characteristics.

Suggested Action(s): Slow SIP message transmissions

Metric: IncomingResponsesDropped

Description: This policy monitors the per-second rate of incoming responses dropped because they could not be processed (due to bad headers, insufficient routing information, server resource allocation failure).

Metric SpecName: IncomRespDrop

Metric Field Name: SIP - Incoming Responses Dropped/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_IncomingResponsesDropped

Message text: The current value of IncomingResponsesDropped is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): This server is too busy and is unable to process user requests in timely fashion.

Potential Impact: Please ensure that hardware and software requirements at the destination and network bandwidth allocation meet the user usage characteristics.

Suggested Action(s): Slow SIP message transmissions

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

ChkFrontEndOnlineTelephonyConferencingServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SERVSTAT

Source / Collection Definition: SERVICECHECK / RTCACPMCU

Metric: FERTCACPMCUServName

> **Description**: Name of the Service
>
> **Metric SpecName**: SERVNAME
>
> **Metric Field Name**: Service_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FERTCACPMCUServDisplayName

> **Description**: Display Name of the Service
>
> **Metric SpecName**: SRVDISPNAME
>
> **Metric Field Name**: Service_Displayname
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FERTCACPMCUServStatus

> **Description**: Status of the Service
>
> **Metric SpecName**: SERVSTATUS
>
> **Metric Field Name**: Service_Status
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FERTCACPMCUServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_FERTCACPMCUServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): Lync Online Telephony Conferencing' Windows Service is stopped.

Potential Impact: NA

Suggested Action(s): Lync Online Telephony Conferencing' Windows Service is stopped. Please restart the service.

ChkMediationReplicaReplicatorAgentServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SERVSTAT

Source / Collection Definition: SERVICECHECK / REPLICA

Metric: MediationREPLICAServName

Description: Name of the Service

Metric SpecName: SERVNAME

Metric Field Name: Service_Name

Data type: TEXT

Alarm: FALSE

Metric: MediationREPLICAServDisplayName

Description: Display Name of the Service

Metric SpecName: SRVDISPNAME

Metric Field Name: Service_Displayname

Data type: TEXT

Alarm: FALSE

Metric: MediationREPLICAServStatus

Description: Status of the Service

Metric SpecName: SERVSTATUS

Metric Field Name: Service_Status

Data type: TEXT

Alarm: FALSE

Metric: MediationREPLICAServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_MediationREPLICAServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): Lync Server Replica Replicator Agent' Windows Service is stopped.

Potential Impact: NA

Suggested Action(s): Lync Server Replica Replicator Agent' Windows Service is stopped. Please restart the service.

RGSServiceHosting

This policy maintains the information about the status for the different services

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_ConferenceProcPerform_2010_Conf

Aspect: Skype Conference Processing Performance

CIT: Mediation Server, Front End Server, Edge Server

Data source / Data class: SKYPE / TTLNUMINCLDCLMTMAKFA

Source / Collection Definition: PERFMON / LS:RGS - 00 - Response Group Service Hosting(*)

Metric: TotalNumOfIncomingCallsWereDeclineBecauseOfAMatchMakingFail

Description: This metric captures Total Number Of Incoming Calls Declined Because Of A Match Making Failure

Metric SpecName: TtlNumInClDclMtMakFa

Metric Field Name: RGS - 000 - Total number of incoming calls that were declined because of a Match Making failure

Data type: UINT32

Alarm: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: TotalNumOfIncomingCallsWereDeclineBecauseOfAMatchMakingFail

Description: This metric captures Total Number Of Incoming Calls Declined Because Of A Match Making Failure

Metric SpecName: TtlNumInClDclMtMakFa

Metric Field Name: RGS - Total Number Of Incoming Calls That Were Declined Because Of A Match Making Failure

Data type: UINT32

Alarm: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Collect_FrontEnd_DBStoreLogging

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / CS_FEDBSTORE

Source / Collection Definition: PERFMON / LS:USrv - DBStore(*)

Metric: FELoggingInstanceName

> **Description**: instance of perfmon object LS:USrv - DBStore
>
> **Metric SpecName**: DBSTOREINSTNAME
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: UsrvDBStoreQueueLatencyLogging

> **Description**: the average time (in milliseconds) a request is held in the database queue.
>
> **Metric SpecName**: QUEUELATENCY
>
> **Metric Field Name**: USrv - Queue Latency (msec)
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Metric: UsrvDBStoreSprocLatencyLogging

> **Description**: the average time (in milliseconds) it takes to process a RtcAuthorizeDelegate sproc call.
>
> **Metric SpecName**: SPROCLATENCY
>
> **Metric Field Name**: USrv - Sproc Latency (msec)
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

VideoPacketLossPoorCallsPercentage

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / VIDEOPACKETLOSSCALLS

Source / Collection Definition: SQLDB / select isnull(cast(100.0 * cast((SUM(CASE WHEN [VideoPacketLossRate] > [VideoPacketLossRateOptimal] THEN 1 ELSE 0 END)) as float) / cast ((SUM(CASE WHEN MediaLineLabel is NOT NULL THEN 1 ELSE 0 END)) as float) as decimal(4, 1)),0) as VideoPacketLossPoorCallsPercentage,SERVERPROPERTY('MACHINENAME') AS 'ServerName' from [QoEMetrics].[dbo].[QoEReportsCallDetailView] Where MediaLineLabel IN (1,2) AND ConferenceDateTime >= dateadd(MINUTE,@Duration,GETUTCDATE())

Metric: VideoPacketLossPoorCallsPercentage

Description: This metric captures Poor Video that have Packet Loss more than a set threshold value and calculates percentage of poor calls for a given interval At the end of each call, parameters that determine Quality of a call that include network, audio and video parameters are logged into QoE database of Lync Server. Each call is categorized as having Acceptable quality or Poor quality based on the same.

Metric SpecName: VidPacktLosPoorCall

Metric Field Name: VideoPacketLossPoorCallsPercentage

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 40, Major / 70, Warning / 40, Major / 70

Policy: MSBS_VideoPacketLossPoorCallsPercentage

Message text: The current value of Percentage Video Packet Loss Poor Calls is <VALUE> which exceeds the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): As Lync leverages UDP for video , the Lync client doesn't ask for retransmission of lost packets. If packets arrive out of sequence, Lync just ignores them. Lack of bandwidth and overloaded server could be probable causes

Potential Impact: Distorted video Call drops

Suggested Action(s): UDP does not provide recovery for packet loss, but increasing network bandwidth could be a workaround

Metric: ServerName

Description: This is the key for metric

Metric SpecName: ServerName

Metric Field Name: ServerName

Data type: TEXT

Alarm: FALSE

Metric: VideoPacketLossPoorCallsPercentage

Description: This metric captures Poor Video that have Packet Loss more than a set threshold value and calculates percentage of poor calls for a given interval At the end of each call, parameters that determine Quality of a call that include network, audio and video parameters are logged into QoE database of Lync Server. Each call is categorized as having Acceptable quality or Poor quality based on the same.

Metric SpecName: VidPacktLosPoorCall

Metric Field Name: VideoPacketLossPoorCallsPercentage

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 40, Major / 70, Warning / 40, Major / 70

Policy: MSBS_VideoPacketLossPoorCallsPercentage

Message text: The current value of Percentage Video Packet Loss Poor Calls is <VALUE> which exceeds the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): As Lync leverages UDP for video , the Lync client doesn't ask for retransmission of lost packets. If packets arrive out of sequence, Lync just ignores them. Lack of bandwidth and overloaded server could be probable causes

Potential Impact: Distorted video Call drops

Suggested Action(s): UDP does not provide recovery for packet loss, but increasing network bandwidth could be a workaround

Metric: ServerName

Description: This is the key for metric

Metric SpecName: ServerName

Metric Field Name: ServerName

Data type: TEXT

Alarm: FALSE

MCUFactoryRequest

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HALFHOURLY

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: SKYPE / MCUFACTORYREQUEST

Source / Collection Definition: PERFMON / LS:MCUF - 00 - MCU Factory(*)

Metric: GetMCURequestsReceivedPerSec

> **Description**: This metric captures Get MCU Request sReceived Per Sec
>
> **Metric SpecName**: GetMCURequestsRecPS
>
> **Metric Field Name**: MCUF - 003 - GetMCU Requests Received/sec
>
> **Data type**: REAL64
>
> **Alarm**: FALSE

Metric: Instance_Name

> **Description**: This is the key for metric
>
> **Metric SpecName**: Instance_Name
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: HealthNotificationsReceivedPerSec

Description: This metric captures Health Notification sReceived Per Sec

Metric SpecName: HealthNotificaRecPS

Metric Field Name: MCUF - 006 - Health Notifications Received/sec

Data type: REAL64

Alarm: FALSE

Metric: TotalDrainRequestsReceived

Description: This metric captures Total Drain Requests Received

Metric SpecName: TotalDrainReqRec

Metric Field Name: MCUF - 007 - Total Drain Requests Received

Data type: UINT32

Alarm: FALSE

Metric: TotalEmptyGetMCUResponses

Description: This metric captures Total Empty Get MCU Responses

Metric SpecName: TotalEmptyGetMCURes

Metric Field Name: MCUF - 002 - Total empty GetMCU Responses

Data type: UINT32

Alarm: FALSE

Metric: TotalGetMCURequestsFailed

Description: This metric captures Total Get MCU Requests Failed

Metric SpecName: TotalGetMCUReqFail

Metric Field Name: MCUF - 001 - Total GetMCU Requests Failed

Data type: UINT32

Alarm: FALSE

Metric: TotalGetMCURequestsReceived

Description: This metric captures Total Get MCU Requests Received

Metric SpecName: TotalGetMCUReqRec

Metric Field Name: MCUF - 000 - Total GetMCU Requests Received

Data type: UINT32

Alarm: FALSE

Metric: TotalHealthNotificationsFailed

Description: This metric captures Total Health Notifications Failed

Metric SpecName: TotalHealthNotiFail

Metric Field Name: MCUF - 005 - Total Health Notifications Failed

Data type: UINT32

Alarm: FALSE

Metric: TotalHealthNotificationsReceived

Description: This metric captures Total Health Notifications Received

Metric SpecName: TtlHealthNotificRec

Metric Field Name: MCUF - 004 - Total Health Notifications Received

Data type: UINT32

Alarm: FALSE

Metric: GetMCURequestsReceivedPerSec

Description: This metric captures Get MCU Request sReceived Per Sec

Metric SpecName: GetMCURequestsRecPS

Metric Field Name: MCUF - GetMCU Requests Received/Sec

Data type: REAL64

Alarm: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: HealthNotificationsReceivedPerSec

Description: This metric captures Health Notification sReceived Per Sec

Metric SpecName: HealthNotificaRecPS

Metric Field Name: MCUF - Health Notifications Received/Sec

Data type: REAL64

Alarm: FALSE

Metric: TotalDrainRequestsReceived

Description: This metric captures Total Drain Requests Received

Metric SpecName: TotalDrainReqRec

Metric Field Name: MCUF - Total Drain Requests Received

Data type: UINT32

Alarm: FALSE

Metric: TotalEmptyGetMCUResponses

Description: This metric captures Total Empty Get MCU Responses

Metric SpecName: TotalEmptyGetMCURes

Metric Field Name: MCUF - Total Empty GetMCU Responses

Data type: UINT32

Alarm: FALSE

Metric: TotalGetMCURequestsFailed

Description: This metric captures Total Get MCU Requests Failed

Metric SpecName: TotalGetMCUReqFail

Metric Field Name: MCUF - Total GetMCU Requests Failed

Data type: UINT32

Alarm: FALSE

Metric: TotalGetMCURequestsReceived

Description: This metric captures Total Get MCU Requests Received

Metric SpecName: TotalGetMCUReqRec

Metric Field Name: MCUF - Total GetMCU Requests Received

Data type: UINT32

Alarm: FALSE

Metric: TotalHealthNotificationsFailed

Description: This metric captures Total Health Notifications Failed

Metric SpecName: TotalHealthNotiFail

Metric Field Name: MCUF - Total Health Notifications Failed

Data type: UINT32

Alarm: FALSE

Metric: TotalHealthNotificationsReceived

Description: This metric captures Total Health Notifications Received

Metric SpecName: TtlHealthNotificRec

Metric Field Name: MCUF - Total Health Notifications Received

Data type: UINT32

Alarm: FALSE

Collect_REGDBStore

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / CS_FRONTEND

Source / Collection Definition: PERFMON / LS:USrv - 00 - REGDBStore(*)

Metric: RegDBStrInstance

> **Description**: instance of perfmon object LS:USrv - 00 - REGDBStore
>
> **Metric SpecName**: REGDBSTINST
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: RegDBSTQueueLatency

Description: average wait time in database queue by registrar module

Metric SpecName: REGDBSTQLTNC

Metric Field Name: USrv - 002 - Queue Latency (msec)

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 4000, Major / 6000

Policy: MSBS_RegDBSTQueueLatency

Message text: The value of the counter 'Queue Latency (msec)' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: RegDBStrSprocLatencyLogging

Description: Time taken for the regDB Store to process the request from server

Metric SpecName: REGDBSTSPROCLTNCLOGGING

Metric Field Name: Usrv - 004 - Sproc Latency (msec)

Data type: UINT32

Alarm: FALSE

Metric: RegistrarQueueDepth

Description: average number of database requests to execute.

Metric SpecName: QDEPTH

Metric Field Name: USrv - 000 - Queue Depth

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20

Policy: MSBS_RegistrarQueueDepth

Message text: The value of the counter 'USrv - 000 - Queue Depth' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: RegistrarThrottledrequestsPersec

Description: number of requests rejected in a second with a message to retry later because of the high database latency.

Metric SpecName: THROTLDRQSTPERSEC

Metric Field Name: USrv - 020 - Throttled requests/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20

Policy: MSBS_RegistrarThrottledrequestsPersec

Message text: The value of the counter 'USrv - 020 - Throttled requests/sec' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: RegistrarTotalDeadlockFailures

Description: number of deadlock failures occurred since the server was started.

Metric SpecName: TOTDEADLOCKFAILRS

Metric Field Name: USrv - 015 - Total Deadlock Failures

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20

Policy: MSBS_RegistrarTotalDeadlockFailures

Message text: The value of the counter 'USrv - 015 - Total Deadlock Failures' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: RegistrarTotalDeadlocks

Description: number of deadlocks occurred since the server was started.

Metric SpecName: TOTDEADLOCKS

Metric Field Name: USrv - 013 - Total Deadlocks

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20

Policy: MSBS_RegistrarTotalDeadlocks

Message text: The value of the counter 'USrv - 013 - Total Deadlocks' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: RegistrarTotalDroppedRequests

Description: number of requests dropped by the database layer as they will time out.

Metric SpecName: TOTDROPPEDRQSTS

Metric Field Name: USrv - 014 - Total Dropped Requests

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20

Policy: MSBS_RegistrarTotalDroppedRequests

Message text: The value of the counter 'USrv - 014 - Total Dropped Requests' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: RegistrarTotalfatalSQLerrors

Description: number of fatal SQL errors occurred since the server started.

Metric SpecName: TOTFATALSQLERRORS

Metric Field Name: USrv - 019 - Total fatal SQL errors

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20

Policy: MSBS_RegistrarTotalfatalSQLerrors

Message text: The value of the counter 'USrv - 019 - Total fatal SQL errors' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: RegistrarTotalODBCTimeoutFailures

Description: number of ODBC timeout failures occurred since the server was started.

Metric SpecName: TOTODBCTIMEOUTFAILURES

Metric Field Name: USrv - 017 - Total ODBC Timeout Failures

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20

Policy: MSBS_RegistrarTotalODBCTimeoutFailures

Message text: The value of the counter 'USrv - 017 - Total ODBC Timeout Failures' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: RegistrarTotalsevereSQLerrors

Description: number of severe SQL errors occurred since the server started.

Metric SpecName: TOTSEVERESQLERRORS

Metric Field Name: USrv - 018 - Total severe SQL errors

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20

Policy: MSBS_RegistrarTotalsevereSQLerrors

Message text: The value of the counter 'USrv - 018 - Total severe SQL errors' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: RegistrarTotalthrottledrequests

Description: number of requests rejected with a message to retry after some time because of high database queue latency.

Metric SpecName: TOTTHROTLDREQSTS

Metric Field Name: USrv - 021 - Total throttled requests

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20

Policy: MSBS_RegistrarTotalthrottledrequests

Message text: The value of the counter 'USrv - 021 - Total throttled requests' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

RegistrationLatency

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_LOW

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SYNREGISTRATIONLAT

Source / Collection Definition: POWERSHELL / TestCsRegistration TargetFQDN ${fqdn}

Metric: RegistrationLatency

Description: This metric will capture the latency in registration of the user to the group.

Metric SpecName: RegistrationLatency

Metric Field Name: RegistrationLatency

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1000, Major / 1000

Policy: MSBS_RegistrationLatency

Message text: The value of Registration Latency (ms) is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): 1. User configuration not done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: Users would not be able to avail peer to peer services

Suggested Action(s): 1. Configuration : Most common issues are invalid or expired Test user password, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availability: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution error or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responds to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Metric: UserRegistration

Description: This test allows you to monitor the operation of log on registration to a Lync pool. The successful registration of a test user is followed immediately by a disconnection with no impact on any real users.

Metric SpecName: UserRegistration

Metric Field Name: UserRegistration

Data type: TEXT

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_UserRegistration

Message text: The User Registration is down

Instructional Text:

Probable Cause(s): 1. User configuration must not have done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: New users cannot be registered

Suggested Action(s): 1. Configuration errors: Most common issues are: Test user password is invalid or expired, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availability: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution errors or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responded to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Metric: TargetFqdn

Description: This is the key for metric

Metric SpecName: TargetFqdn

Metric Field Name: TargetFqdn

Data type: TEXT

Alarm: FALSE

Metric: RegistrationLatency

Description: This metric will capture the latency in registration of the user to the group.

Metric SpecName: RegistrationLatency

Metric Field Name: RegistrationLatency

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1000, Major / 1000

Policy: MSBS_RegistrationLatency

Message text: The value of Registration Latency (ms) is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): 1. User configuration not done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: Users would not be able to avail peer to peer services

Suggested Action(s): 1. Configuration : Most common issues are invalid or expired Test user password, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availability: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution error or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responds to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Metric: UserRegistration

Description: This test allows you to monitor the operation of log on registration to a Lync pool. The successful registration of a test user is followed immediately by a disconnection with no impact on any real users.

Metric SpecName: UserRegistration

Metric Field Name: UserRegistration

Data type: TEXT

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_UserRegistration

Message text: The User Registration is down

Instructional Text:

Probable Cause(s): 1. User configuration must not have done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: New users cannot be registered

Suggested Action(s): 1. Configuration errors: Most common issues are: Test user password is invalid or expired, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availability: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution errors or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responded to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Metric: TargetFqdn

> **Description**: This is the key for metric
>
> **Metric SpecName**: TargetFqdn
>
> **Metric Field Name**: TargetFqdn
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

AVEdgeConnectivity

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_LOW

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SYNNPDAVEGCONN

Source / Collection Definition: POWERSHELL / TestCsAVEdgeConnectivity TargetFQDN ${fqdn}

Metric: AVEdgeConnectivity

Description: This metric gathers the information which confirms that the A/V Edge servers are able to accept connections for peertopeer calls and conference calls.

Metric SpecName: AVEdgeConn

Metric Field Name: AVEdgeConnectivity

Data type: TEXT

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Minor / 1

Policy: MSBS_AVEdgeConnectivity

Message text: The AVEdge Connectivity is down

Instructional Text:

Probable Cause(s): 1. User configuration must not have done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: New users cannot be registered

Suggested Action(s): 1. Configuration errors: Most common issues are: Test user password is invalid or expired, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availability: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution errors or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responded to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Metric: TargetFqdn

Description: This is the key for metric

Metric SpecName: TargetFqdn

Metric Field Name: TargetFqdn

Data type: TEXT

Alarm: FALSE

Metric: AVEdgeConnectivityLatency

Description: This metric will capture latency in receipt of confirmation that the A/V Edge servers are able to accept connections for peertopeer calls and conference calls.

Metric SpecName: AVEdgeConnLat

Metric Field Name: AVEdgeConnectivityLatency

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Minor / 1000

Policy: MSBS_AVEdgeConnectivityLatency

Message text: The value of AVEdge Connectivity Latency is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): 1. User configuration must not have done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: New users cannot be registered

Suggested Action(s): 1. Configuration errors: Most common issues are: Test user password is invalid or expired, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availibility: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution errors or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responded to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

AVMCUHealthState

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: SKYPE / AVMCUHEALTHSTATE

Source / Collection Definition: PERFMON / LS:AVMCU - 04 - MCU Health And Performance(*)

Metric: MCUHealthStateAva

> **Description**: This metric captures current health of the MCU. 0 = Normal. 1 = Loaded. 2 = Full. 3 = Unavailable
>
> **Metric SpecName**: MCUHealthStateAva
>
> **Metric Field Name**: AVMCU - 005 - MCU Health State
>
> **Data type**: UINT32
>
> **Alarm**: TRUE
>
> **Category** : MSSkype
>
> **Severity / Threshold** : Warning / 1, Warning / 2, Warning / 3, Warning / 1, Warning / 2, Warning / 3
>
> **Policy**: MSBS_MCUHealthStateAva
>
> **Message text**: The value of MCU Health State is Unavailable
>
> **Instructional Text**:
>
> **Probable Cause(s)**: MCU is overloaded
>
> **Potential Impact**: Check if too many conferences are assigned to this MCU
>
> **Suggested Action(s)**: MCU may be unavailable

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: MCUHealthStateChangedCount

Description: This metric captures MCU Health State Changed Count

Metric SpecName: MCUHealthStateChange

Metric Field Name: AVMCU - 007 - MCU Health State Changed Count

Data type: UINT32

Alarm: FALSE

Metric: MCUHealthStateAva

Description: This metric captures current health of the MCU. 0 = Normal. 1 = Loaded. 2 = Full.
3 = Unavailable

Metric SpecName: MCUHealthStateAva

Metric Field Name: AVMCU - MCU Health State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 1, Warning / 2, Warning / 3, Warning / 1, Warning / 2, Warning
/ 3

Policy: MSBS_MCUHealthStateAva

Message text: The value of MCU Health State is Unavailable

Instructional Text:

Probable Cause(s): MCU is overloaded

Potential Impact: Check if too many conferences are assigned to this MCU

Suggested Action(s): MCU may be unavailable

Metric: Instance_Name

> **Description**: This is the key for metric
>
> **Metric SpecName**: Instance_Name
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: MCUHealthStateChangedCount

> **Description**: This metric captures MCU Health State Changed Count
>
> **Metric SpecName**: MCUHealthStateChange
>
> **Metric Field Name**: AVMCU - MCU Health State Changed Count
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

SIPPeersQueue

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: SKYPE / SIPPEERSQUEUE

Source / Collection Definition: PERFMON / LS:SIP - 01 - Peers(*)

Metric: AverageOutgoingQueueDelay

Description: This metric captures Average Outgoing Queue Delay

Metric SpecName: AvgOutgoingQuDelay

Metric Field Name: SIP - 020 - Average Outgoing Queue Delay

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Critical / 100, Major / 100

Policy: MSBS_AverageOutgoingQueueDelay

Message text: The value of Average Out going message Queue Delay is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): A large number here might indicate that a peer server is overloaded, or that network bandwidth to a peer server is insufficient.

Potential Impact: This might be a temporary condition. If the problem persists, please ensure that hardware and software requirements at the destination and network bandwidth allocation meet the user usage characteristics.

Suggested Action(s): The messages may not be recieved.

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: FlowControlledConnections

Description: The number of connections that are currently being flow-controlled (no socket receives are posted).

Metric SpecName: FlowControlledConn

Metric Field Name: SIP - 023 - Flow-controlled Connections

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Critical / 100, Major / 100

Policy: MSBS_FlowControlledConnections

Message text: The number of Flow Controlled Connections is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): This server or another server to which this server proxies user requests is too busy and is unable to process user requests in timely fashion.

Potential Impact: This might be a temporary condition. If the problem persists, please ensure that hardware and software requirements for this server and servers it proxies user requests to as well as network bandwidth allocation for inter-server traffic meet the user usage characteristics

Suggested Action(s): The connections that are being flow-controlled cannot be established

Metric: FlowControlledConnectionsDropped

Description: The total number of connections dropped because of excessive flow-control.

Metric SpecName: FlowControllConDrop

Metric Field Name: SIP - 024 - Flow-controlled Connections Dropped

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Critical / 100, Major / 100

Policy: MSBS_FlowControlledConnectionsDropped

Message text: The number of Flow Controlled Connections Dropped is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): This server or another server to which this server proxies user requests is too busy and is unable to process user requests in timely fashion.

Potential Impact: This might be a temporary condition. If the problem persists, please ensure that hardware and software requirements for this server and servers it proxies user requests to as well as network bandwidth allocation for inter-server traffic meet the user usage characteristics

Suggested Action(s): The connections that are being flow-controlled cannot be established

Metric: NonBlockingSends

Description: This metric captures Non Blocking messages sent

Metric SpecName: NonBlockingSends

Metric Field Name: SIP - 013 - Non-blocking Sends

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Critical / 100, Major / 100

Policy: MSBS_NonBlockingSends

Message text: The value of Non Blocking message sent is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): A small number here might indicate that a peer server is overloaded, or that network bandwidth to a peer server is insufficient.

Potential Impact: This might be a temporary condition. If the problem persists, please ensure that hardware and software requirements at the destination and network bandwidth allocation meet the user usage characteristics.

Suggested Action(s): The messages may not be recieved.

Metric: NonBlockingSendsPerSec

Description: This metric captures Non Blocking messages sent per second

Metric SpecName: NonBlockingSendsPS

Metric Field Name: SIP - 014 - Non-blocking Sends/sec

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Critical / 100, Major / 100

Policy: MSBS_NonBlockingSendsPerSec

Message text: The value of Non Blocking Sent Per Second is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): A small number here might indicate that a peer server is overloaded, or that network bandwidth to a peer server is insufficient.

Potential Impact: This might be a temporary condition. If the problem persists, please ensure that hardware and software requirements at the destination and network bandwidth allocation meet the user usage characteristics.

Suggested Action(s): The messages may not be recieved.

Metric: ReceivedBytes

Description: This metric captures the number of bytes received by the server

Metric SpecName: ReceivedBytes

Metric Field Name: SIP - 007 - Received Bytes

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Critical / 100, Major / 100

Policy: MSBS_ReceivedBytes

Message text: The value of Received Bytes is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): This server is too busy and is unable to process user requests in timely fashion.

Potential Impact: This might be a temporary condition. If the problem persists, please ensure that hardware and software requirements for this server meet the user usage characteristics

Suggested Action(s): The user may expereince delay in reciept of messages.

Metric: ReceivedBytesPerSec

Description: This metric captures the number of bytes received per second by the server

Metric SpecName: ReceivedBytesPerSec

Metric Field Name: SIP - 008 - Received Bytes/sec

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Critical / 100, Major / 100

Policy: MSBS_ReceivedBytesPerSec

Message text: The value of Received Bytes Per Second is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): This server is too busy and is unable to process user requests in timely fashion

Potential Impact: This might be at emporary condition. If the problem persists Please ensure that hardware and software requirements for this server meet the user usage characteristics.

Suggested Action(s): The user may expereince delay in reciept of messages

Metric: SendsOutstanding

Description: The number of messages that are currently present in the outgoing (send) queues.

Metric SpecName: SendsOutstanding

Metric Field Name: SIP - 017 - Sends Outstanding

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Critical / 100, Major / 100

Policy: MSBS_SendsOutstanding

Message text: The number of messages on Outgoing Queue is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): A large number here might indicate that a peer server is overloaded or that network bandwidth to a peer server is insufficient

Potential Impact: This might be a temporary condition. If the problem persists please ensure that hardware and software requirements at the destination and network bandwidth allocation meet the user usage characteristics.

Suggested Action(s): The messages may not be recieved

Metric: SentBytes

Description: This metric captures Sent Bytes by the Server.

Metric SpecName: SentBytes

Metric Field Name: SIP - 009 - Sent Bytes

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Critical / 100, Major / 100

Policy: MSBS_SentBytes

Message text: The value of Sent Bytes is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): This server is too busy and is unable to process user requests in timely fashion

Potential Impact: This might be a temporary condition. If the problem persists please ensure that hardware and software requirements for this server meet the user usage characteristics

Suggested Action(s): The user may expereince delay in reciept of messages

Metric: SentBytesPerSec

Description: This metric captures Bytes sent per second by the server

Metric SpecName: SentBytesPerSec

Metric Field Name: SIP - 010 - Sent Bytes/sec

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Critical / 100, Major / 100

Policy: MSBS_SentBytesPerSec

Message text: The value of Sent Bytes Per Second is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): This server is too busy and is unable to process user requests in timely fashion

Potential Impact: This might be a temporary condition. If the problem persists please ensure that hardware and software requirements for this server meet the user usage characteristics

Suggested Action(s): The user may expereince delay in reciept of messages

Metric: AverageOutgoingQueueDelay

Description: This metric captures Average Outgoing Queue Delay

Metric SpecName: AvgOutgoingQuDelay

Metric Field Name: SIP - Average Outgoing Queue Delay

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Critical / 100, Major / 100

Policy: MSBS_AverageOutgoingQueueDelay

Message text: The value of Average Out going message Queue Delay is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): A large number here might indicate that a peer server is overloaded, or that network bandwidth to a peer server is insufficient.

Potential Impact: This might be a temporary condition. If the problem persists, please ensure that hardware and software requirements at the destination and network bandwidth allocation meet the user usage characteristics.

Suggested Action(s): The messages may not be recieved.

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: FlowControlledConnections

Description: The number of connections that are currently being flow-controlled (no socket receives are posted).

Metric SpecName: FlowControlledConn

Metric Field Name: SIP - Flow-Controlled Connections

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Critical / 100, Major / 100

Policy: MSBS_FlowControlledConnections

Message text: The number of Flow Controlled Connections is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): This server or another server to which this server proxies user requests is too busy and is unable to process user requests in timely fashion.

Potential Impact: This might be a temporary condition. If the problem persists, please ensure that hardware and software requirements for this server and servers it proxies user requests to as well as network bandwidth allocation for inter-server traffic meet the user usage characteristics

Suggested Action(s): The connections that are being flow-controlled cannot be established

Metric: FlowControlledConnectionsDropped

Description: The total number of connections dropped because of excessive flow-control.

Metric SpecName: FlowControlConDrop

Metric Field Name: SIP - Flow-Controlled Connections Dropped

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Critical / 100, Major / 100

Policy: MSBS_FlowControlledConnectionsDropped

Message text: The number of Flow Controlled Connections Dropped is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): This server or another server to which this server proxies user requests is too busy and is unable to process user requests in timely fashion.

Potential Impact: This might be a temporary condition. If the problem persists, please ensure that hardware and software requirements for this server and servers it proxies user requests to as well as network bandwidth allocation for inter-server traffic meet the user usage characteristics

Suggested Action(s): The connections that are being flow-controlled cannot be established

Metric: NonBlockingSends

Description: This metric captures Non Blocking messages sent

Metric SpecName: NonBlockingSends

Metric Field Name: SIP - Non-Blocking Sends

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Critical / 100, Major / 100

Policy: MSBS_NonBlockingSends

Message text: The value of Non Blocking message sent is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): A small number here might indicate that a peer server is overloaded, or that network bandwidth to a peer server is insufficient.

Potential Impact: This might be a temporary condition. If the problem persists, please ensure that hardware and software requirements at the destination and network bandwidth allocation meet the user usage characteristics.

Suggested Action(s): The messages may not be recieved.

Metric: NonBlockingSendsPerSec

Description: This metric captures Non Blocking messages sent per second

Metric SpecName: NonBlockingSendsPS

Metric Field Name: SIP - Non-Blocking Sends/Sec

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Critical / 100, Major / 100

Policy: MSBS_NonBlockingSendsPerSec

Message text: The value of Non Blocking Sent Per Second is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): A small number here might indicate that a peer server is overloaded, or that network bandwidth to a peer server is insufficient.

Potential Impact: This might be a temporary condition. If the problem persists, please ensure that hardware and software requirements at the destination and network bandwidth allocation meet the user usage characteristics.

Suggested Action(s): The messages may not be recieved.

Metric: ReceivedBytes

Description: This metric captures the number of bytes received by the server

Metric SpecName: ReceivedBytes

Metric Field Name: SIP - Received Bytes

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Critical / 100, Major / 100

Policy: MSBS_ReceivedBytes

Message text: The value of Received Bytes is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): This server is too busy and is unable to process user requests in timely fashion.

Potential Impact: This might be a temporary condition. If the problem persists, please ensure that hardware and software requirements for this server meet the user usage characteristics

Suggested Action(s): The user may expereince delay in reciept of messages.

Metric: ReceivedBytesPerSec

Description: This metric captures the number of bytes received per second by the server

Metric SpecName: ReceivedBytesPerSec

Metric Field Name: SIP - Received Bytes/Sec

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Critical / 100, Major / 100

Policy: MSBS_ReceivedBytesPerSec

Message text: The value of Received Bytes Per Second is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): This server is too busy and is unable to process user requests in timely fashion

Potential Impact: This might be at emporary condition. If the problem persists Please ensure that hardware and software requirements for this server meet the user usage characteristics.

Suggested Action(s): The user may expereince delay in reciept of messages

Metric: SendsOutstanding

Description: The number of messages that are currently present in the outgoing (send) queues.

Metric SpecName: SendsOutstanding

Metric Field Name: SIP - Sends Outstanding

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Critical / 100, Major / 100

Policy: MSBS_SendsOutstanding

Message text: The number of messages on Outgoing Queue is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): A large number here might indicate that a peer server is overloaded or that network bandwidth to a peer server is insufficient

Potential Impact: This might be a temporary condition. If the problem persists please ensure that hardware and software requirements at the destination and network bandwidth allocation meet the user usage characteristics.

Suggested Action(s): The messages may not be recieved

Metric: SentBytes

Description: This metric captures Sent Bytes by the Server.

Metric SpecName: SentBytes

Metric Field Name: SIP - Sent Bytes

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Critical / 100, Major / 100

Policy: MSBS_SentBytes

Message text: The value of Sent Bytes is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): This server is too busy and is unable to process user requests in timely fashion

Potential Impact: This might be a temporary condition. If the problem persists please ensure that hardware and software requirements for this server meet the user usage characteristics

Suggested Action(s): The user may expereince delay in reciept of messages

Metric: SentBytesPerSec

Description: This metric captures Bytes sent per second by the server

Metric SpecName: SentBytesPerSec

Metric Field Name: SIP - Sent Bytes/Sec

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Critical / 100, Major / 100

Policy: MSBS_SentBytesPerSec

Message text: The value of Sent Bytes Per Second is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): This server is too busy and is unable to process user requests in timely fashion

Potential Impact: This might be a temporary condition. If the problem persists please ensure that hardware and software requirements for this server meet the user usage characteristics

Suggested Action(s): The user may expereince delay in reciept of messages

ChkFrontEndCallParkServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SERVSTAT

Source / Collection Definition: SERVICECHECK / RTCCPS

Metric: FERTCCPSServName

Description: Name of the Service

Metric SpecName: SERVNAME

Metric Field Name: Service_Name

Data type: TEXT

Alarm: FALSE

Metric: FERTCCPSServDisplayName

Description: Display Name of the Service

Metric SpecName: SRVDISPNAME

Metric Field Name: Service_Displayname

Data type: TEXT

Alarm: FALSE

Metric: FERTCCPSServStatus

Description: Status of the Service

Metric SpecName: SERVSTATUS

Metric Field Name: Service_Status

Data type: TEXT

Alarm: FALSE

Metric: FERTCCPSServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_FERTCCPSServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): Lync Server Call Park' Windows Service is stopped.

Potential Impact: NA

Suggested Action(s): Lync Server Call Park' Windows Service is stopped. Please restart the service.

ChkFrontEndWebConfCompatibilityServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / SERVSTAT

Source / Collection Definition: SERVICECHECK / RTCMEETINGMCU

Metric: FERTCMEETINGMCUServName

Description: Name of the Service

Metric SpecName: SERVNAME

Metric Field Name: Service_Name

Data type: TEXT

Alarm: FALSE

Metric: FERTCMEETINGMCUDisplayName

Description: Display Name of the Service

Metric SpecName: SRVDISPNAME

Metric Field Name: Service_Displayname

Data type: TEXT

Alarm: FALSE

Metric: FERTCMEETINGMCUServStatus

Description: Status of the Service

Metric SpecName: SERVSTATUS

Metric Field Name: Service_Status

Data type: TEXT

Alarm: FALSE

Metric: FERTCMEETINGMCUServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_FERTCMEETINGMCUServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

SimplePortWatcher8061

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / Port8061

Source / Collection Definition: PORTCOL / PORTCHECKER

Metric: SimpleWatcherPort8061

Description: Used to listen for Persistent Shared Object Model (PSOM) connections from the Live Meeting client and previous versions of Lync Server.

Metric SpecName: SimpleWatcherPort8061

Metric Field Name: SimpleWatcherPort8061

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_SimpleWatcherPort8061

Message text: The Port No:8061 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

Metric: SimpleWatcherPort8061

Description: Used to listen for Persistent Shared Object Model (PSOM) connections from the Live Meeting client and previous versions of Lync Server.

Metric SpecName: SimpleWatcherPort8061

Metric Field Name: SimpleWatcherPort8061

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_SimpleWatcherPort8061

Message text: The Port No:8061 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

JoinLauncherScheduledMeetings

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_LOW

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SYNJOINLAUNCHMEETS

Source / Collection Definition: POWERSHELL / Test-CsGroupIM –TestJoinLauncher true - TargetFQDN {fqdn}

Metric: JoinLauncherScheduledMeetings

Description: This metric gathers the information which confirms that users are able to create and join scheduled meetings via a web address link. The following functions are tested: • Sign on to the Lync Server • creation and joining scheduled meeting • Message/Data exchange • Session termination •Log out

Metric SpecName: JoinLaunchSchdlMeets

Metric Field Name: JoinLauncherScheduledMeetings

Data type: TEXT

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_JoinLauncherScheduledMeetings

Message text: The Join Launcher Scheduled Meetings is down

Instructional Text:

Probable Cause(s): 1. User configuration not done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: Users would not be able to avail peer to peer services

Suggested Action(s): 1. Configuration : Most common issues are invalid or expired Test user password, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availability: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution error or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responds to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Metric: ServerName

Description: This is the key for metric

Metric SpecName: ServerName

Metric Field Name: ServerName

Data type: TEXT

Alarm: FALSE

Metric: JoinLauncherLatency

Description: This metric will capture latency in receipt of confirmation that users are able to create and join scheduled meetings via a web address link

Metric SpecName: JoinLaunchLat

Metric Field Name: JoinLauncherLatency

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1000

Policy: MSBS_JoinLauncherLatency

Message text: The value of Join Launcher Latency is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): 1. User configuration must not have done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: New users cannot be registered

Suggested Action(s): 1. Configuration errors: Most common issues are: Test user password is invalid or expired, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availibility: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution errors or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responded to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Collect_Edge_AddressBook_Web_Query

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / EDGLSWEBADDRBKWEBQRY

Source / Collection Definition: PERFMON / LS:WEB - Address Book Web Query(*)

Metric: EdgeAddressBookWebQueryInstance

> **Description**: instance of perfmon object LS:WEB - Address Book Web Query
>
> **Metric SpecName**: EDGADDRBKWEBQRYINST
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: EdgeFailedSearchRequests

Description: the per-second rate of failed address book search requests

Metric SpecName: EDGFAILEDSEARCHREQ

Metric Field Name: WEB - Failed search requests/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 4, Major / 20

Policy: MSBS_EdgeFailedSearchRequests

Message text: The value of WEB - Failed search requests/sec for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Issues with backend database connectivity

Potential Impact: NA

Suggested Action(s): Verify backend database is running and accessible.

Metric: EdgeAvgProcessingTimeForSearchRequests

Description: the average processing time for a address book search request in milliseconds

Metric SpecName: EDGAVGPROCTIME

Metric Field Name: WEB - Average processing time for a search request in milliseconds

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 500, Major / 1000

Policy: MSBS_EdgeAvgProcessingTimeForSearchRequests

Message text: The value of WEB - Average processing time for a search request in milliseconds for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Issues with backend database connectivity

Potential Impact: NA

Suggested Action(s): Verify CPU load on backend database machine.

Collect_FrontEnd_Process_DataMCUSvc

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / CS_PROCESS

Source / Collection Definition: PERFMON / Process(DataMCUSvc)

Metric: FERTCDATAMCUInstance

Description: instance of DATAMCUSvc process

Metric SpecName: INSTANCENAME

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: FERTCDATAMCUPercentprocessorTime

Description: Percentage Processor Time is the percentage of elapsed time that all of process threads used the processor to execution instructions.

Metric SpecName: PCTPROCESSORTIME

Metric Field Name: % Processor Time

Data type: UINT32

Alarm: FALSE

Metric: FERTCDATAMCUWorkingSet

Description: Working Set is the current size, in bytes, of the Working Set of this process. the Working Set is the set of memory pages touched recently by the threads in the process. If free memory in the computer is above a threshold, pages are left in the Working Set of a process even if they are not in use. When free memory falls below a threshold, pages are trimmed from Working Sets. If they are needed they will then be soft-faulted back into the Working Set before leaving main memory.

Metric SpecName: WORKINGSET

Metric Field Name: Working Set

Data type: UINT32

Alarm: FALSE

Metric: FERTCDATAMCUPageFaultsPerSec

Description: Page Faults/sec is the average number of pages faulted per second. It is measured in number of pages faulted per second because only one page is faulted in each fault operation, hence this is also equal to the number of page fault operations. This counter includes both hard faults (those that require disk access) and soft faults (where the faulted page is found elsewhere in physical memory.) Most processors can handle large numbers of soft faults without significant consequence. However, hard faults, which require disk access, can cause significant delays.

Metric SpecName: PAGEFAULTS

Metric Field Name: Page Faults/sec

Data type: UINT32

Alarm: FALSE

Metric: FERTCDATAMCUPrivateBytes

Description: Private Bytes is the current size, in bytes, of memory that this process has allocated that cannot be shared with other processes.

Metric SpecName: PRIVATEBYTES

Metric Field Name: Private Bytes

Data type: UINT32

Alarm: FALSE

Metric: FERTCDATAMCUThreadCount

Description: the number of threads currently active in this process. An instruction is the basic unit of execution in a processor, and a thread is the object that executes instructions. Every running process has at least one thread.

Metric SpecName: THREADCOUNT

Metric Field Name: Thread Count

Data type: UINT32

Alarm: FALSE

Metric: FERTCDATAMCUInstance

Description: instance of DATAMCUSvc process

Metric SpecName: INSTANCENAME

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: FERTCDATAMCUPercentprocessorTime

Description: Percentage Processor Time is the percentage of elapsed time that all of process threads used the processor to execution instructions.

Metric SpecName: PCTPROCESSORTIME

Metric Field Name: % Processor Time

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 90

Policy: MSBS_FERTCDATAMCUPercentprocessorTime

Message text: The value of the counter '% Processor Time' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: FERTCDATAMCUWorkingSet

Description: Working Set is the current size, in bytes, of the Working Set of this process. the Working Set is the set of memory pages touched recently by the threads in the process. If free memory in the computer is above a threshold, pages are left in the Working Set of a process even if they are not in use. When free memory falls below a threshold, pages are trimmed from Working Sets. If they are needed they will then be soft-faulted back into the Working Set before leaving main memory.

Metric SpecName: WORKINGSET

Metric Field Name: Working Set

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20000000

Policy: MSBS_FERTCDATAMCUWorkingSet

Message text: The value of the counter 'Working Set' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: FERTCDATAMCUPageFaultsPerSec

Description: Page Faults/sec is the average number of pages faulted per second. It is measured in number of pages faulted per second because only one page is faulted in each fault operation, hence this is also equal to the number of page fault operations. This counter includes both hard faults (those that require disk access) and soft faults (where the faulted page is found elsewhere in physical memory.) Most processors can handle large numbers of soft faults without significant consequence. However, hard faults, which require disk access, can cause significant delays.

Metric SpecName: PAGEFAULTS

Metric Field Name: Page Faults/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 100

Policy: MSBS_FERTCDATAMCUPageFaultsPerSec

Message text: The value of the counter 'Page Faults/sec' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: FERTCDATAMCUPrivateBytes

Description: Private Bytes is the current size, in bytes, of memory that this process has allocated that cannot be shared with other processes.

Metric SpecName: PRIVATEBYTES

Metric Field Name: Private Bytes

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20000000

Policy: MSBS_FERTCDATAMCUPrivateBytes

Message text: The value of the counter 'Private Bytes' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: FERTCDATAMCUThreadCount

Description: the number of threads currently active in this process. An instruction is the basic unit of execution in a processor, and a thread is the object that executes instructions. Every running process has at least one thread.

Metric SpecName: THREADCOUNT

Metric Field Name: Thread Count

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 150

Policy: MSBS_FERTCDATAMCUThreadCount

Message text: The value of the counter 'Thread Count' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

AudioVideoConferencing

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_LOW

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SYNAVCONFERENCING

Source / Collection Definition: POWERSHELL / Test-CsAVConference -TargetFQDN ${fqdn}

Metric: AudioVideoConferencing

Description: This metric gathers the information which confirms that users are able to create and participate in an audio/video conference. It will monitor the operation of audio/video conferencing between two test users in a Lync pool. The following functions are tested: • Sign on to the Lync Server • Invitation and acceptance to conduct an audio/video call • Conference creation and joining • Exchange of Audio/Video • Conference termination •Log out

Metric SpecName: AudVidConfer

Metric Field Name: AudioVideoConferencing

Data type: TEXT

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_AudioVideoConferencing

Message text: The Audio Video Conferencing is down

Instructional Text:

Probable Cause(s): 1. User configuration not done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: Users would not be able to avail peer to peer services

Suggested Action(s): 1. Configuration : Most common issues are invalid or expired Test user password, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availability: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution error or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responds to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Metric: ServerName

Description: This is the key for metric

Metric SpecName: ServerName

Metric Field Name: ServerName

Data type: TEXT

Alarm: FALSE

Metric: AudioVideoConferenceLatency

Description: This metric will capture latency in group audio/video conference transaction

Metric SpecName: AudVidConferenceLat

Metric Field Name: AudioVideoConferenceLatency

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1000, Major / 1000

Policy: MSBS_AudioVideoConferenceLatency

Message text: The value of Audio Video Conference Latency(ms) is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): 1. User configuration not done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: Users would not be able to avail peer to peer services

Suggested Action(s): 1. Configuration : Most common issues are invalid or expired Test user password, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availability: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution error or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responds to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Metric: AudioVideoConferencing

Description: This metric gathers the information which confirms that users are able to create and participate in an audio/video conference. It will monitor the operation of audio/video conferencing between two test users in a Lync pool. The following functions are tested: • Sign on to the Lync Server • Invitation and acceptance to conduct an audio/video call • Conference creation and joining • Exchange of Audio/Video • Conference termination •Log out

Metric SpecName: AudVidConfer

Metric Field Name: AudioVideoConferencing

Data type: TEXT

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_AudioVideoConferencing

Message text: The Audio Video Conferencing is down

Instructional Text:

Probable Cause(s): 1. User configuration not done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: Users would not be able to avail peer to peer services

Suggested Action(s): 1. Configuration : Most common issues are invalid or expired Test user password, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availability: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution error or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responds to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Metric: ServerName

Description: This is the key for metric

Metric SpecName: ServerName

Metric Field Name: ServerName

Data type: TEXT

Alarm: FALSE

Metric: AudioVideoConferenceLatency

Description: This metric will capture latency in group audio/video conference transaction

Metric SpecName: AudVidConferenceLat

Metric Field Name: AudioVideoConferenceLatency

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1000, Major / 1000

Policy: MSBS_AudioVideoConferenceLatency

Message text: The value of Audio Video Conference Latency(ms) is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): 1. User configuration not done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: Users would not be able to avail peer to peer services

Suggested Action(s): 1. Configuration : Most common issues are invalid or expired Test user password, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availability: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution error or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responds to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Collect_FrontEnd_StoreWebHandle

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / LSSTOREWEBHANDLER

Source / Collection Definition: PERFMON / LS:StoreWeb - Store Web Handler(*)

Metric: StoreWebHandlerInstance

> **Description**: instance of perfmon object LS:StoreWeb - Store Web Handler
>
> **Metric SpecName**: STOREWEBINSTANCE
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FailedToPerformNotificationOperation

Description: Total number of failed notification calls to Storage Service

Metric SpecName: FAILEDNOTIFOPR

Metric Field Name: STOREWEB - Failed to perform Notification operation

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 2, Major / 20

Policy: MSBS_FailedToPerformNotificationOperation

Message text: The value of STOREWEB - Failed to perform Notification operation for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Runtime or configuration problems with Storage Service or Exchange Server.

Potential Impact: NA

Suggested Action(s): Check error details for this event and also trace logs for Storage Service to identify the problem. Check that Storage Service is running properly.

Metric: RequestsForWhichResponseStatusIsNotSuccess

Description: Total number of requests for which response status is not Success

Metric SpecName: WHUNSUCRESSTATUS

Metric Field Name: STOREWEB - Requests for which Response Status is not Success

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 2, Major / 20

Policy: MSBS_RequestsForWhichResponseStatusIsNotSuccess

Message text: The value of STOREWEB - Requests for which Response Status is not Success for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Bad requests coming from the client, possible code bug or malicious attempt. Or Store Web not able to connect to Storage service.

Potential Impact: NA

Suggested Action(s): Check logs to detect malicious attempts, perform IIS reset to reset the state of Store Web. Check that Storage service is up and running.

Metric: FailedCallsToStorageService

Description: Total number of failed calls to Storage Service

Metric SpecName: FAILEDCALLTOSTGSVC

Metric Field Name: STOREWEB - Failed calls to the Storage Service

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 2, Major / 20

Policy: MSBS_FailedCallsToStorageService

Message text: The value of STOREWEB - Failed calls to the Storage Service for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Unable to open a connection to Storage Service.

Potential Impact: NA

Suggested Action(s): Check error details for this event and also trace logs for Storage Service to identify the problem. Check that Storage Service is running properly.

Collect_LogicalDisk_PersistentChat

This Policy monitors the logical disk feature of Microsoft Skype Business Server

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Logical_Disk_Conf

Aspect: Skype Logical Disk

CIT: Edge Server, Director Server, Mediation Server, Front End Server, Persistent Chat Server

Data source / Data class: LYNC / LOGICALDISK

Source / Collection Definition: PERFMON / LogicalDisk(*)

Metric: PCLogicalDiskInstance

Description: instance of perfmon object LogicalDisk

Metric SpecName: LGDISKINSTNAME

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: PCPercentageFreeSpace

Description: % Free Space is the percentage of total usable space on the selected logical disk drive that was free.

Metric SpecName: FREESPACE

Metric Field Name: % Free Space

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 70, Major / 90

Policy: MSBS_PCPercentageFreeSpace

Message text: The value of % Free Space for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Database size grows indefinitely.

Potential Impact: NA

Suggested Action(s): Please check each disk drive and clean up unnecessary files.

Collect_AVEdge_UDP_Logging

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / CS_AVEDGEUDP

Source / Collection Definition: PERFMON / LS:A/V Edge - UDP Counters(*)

Metric: AVEdgeInstanceNameLogging

> **Description**: instance of perfmon object LS:A/V Edge - UDP Counters
>
> **Metric SpecName**: CSUDPINSTANAME
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: AVEdgeUDPAuthFailurPerSecLogging

> **Description**: Authentication Failures/sec over TCP
>
> **Metric SpecName**: UDPAUTHFAILURES
>
> **Metric Field Name**: A/V Edge - Authentication Failures/sec
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

ChkFrontEndOnlineBIDataCollectorServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SERVSTAT

Source / Collection Definition: SERVICECHECK / RtcBIDataCollector

Metric: FERtcBIDataCollectorServName

Description: Name of the Service

Metric SpecName: SERVNAME

Metric Field Name: Service_Name

Data type: TEXT

Alarm: FALSE

Metric: FERtcBIDataCollectorServDisplayName

Description: Display Name of the Service

Metric SpecName: SRVDISPNAME

Metric Field Name: Service_Displayname

Data type: TEXT

Alarm: FALSE

Metric: FERtcBIDataCollectorServStatus

Description: Status of the Service

Metric SpecName: SERVSTATUS

Metric Field Name: Service_Status

Data type: TEXT

Alarm: FALSE

Metric: FERtcBIDataCollectorServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_FERtcBIDataCollectorServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): Lync Online BI Data Collector Service' Windows Service is stopped.

Potential Impact: NA

Suggested Action(s): Lync Online BI Data Collector Service' Windows Service is stopped.
Please restart the service.

SimplePortWatcher448

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect
metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / Port448

Source / Collection Definition: PORTCOL / PORTCHECKER

Metric: SimpleWatcherPort448

Description: Used for call admission control by the Lync Server Bandwidth Policy Service.

Metric SpecName: SimpleWatcherPort448

Metric Field Name: SimpleWatcherPort448

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_SimpleWatcherPort448

Message text: The Port No:448 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

Metric: SimpleWatcherPort448

Description: Used for call admission control by the Lync Server Bandwidth Policy Service.

Metric SpecName: SimpleWatcherPort448

Metric Field Name: SimpleWatcherPort448

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_SimpleWatcherPort448

Message text: The Port No:448 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

SimplePortWatcher8058

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / Port8058

Source / Collection Definition: PORTCOL / PORTCHECKER

Metric: SimpleWatcherPort8058

Description: Used to listen for Persistent Shared Object Model (PSOM) connections from the Live Meeting client and previous versions of Lync Server.

Metric SpecName: SimpleWatcherPort8058

Metric Field Name: SimpleWatcherPort8058

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort8058

Message text: The Port No:8058 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

> **Description**: This is the key for metric
>
> **Metric SpecName**: HOSTNAME
>
> **Metric Field Name**: HOSTNAME
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: SimpleWatcherPort8058

Description: Used to listen for Persistent Shared Object Model (PSOM) connections from the Live Meeting client and previous versions of Lync Server.

Metric SpecName: SimpleWatcherPort8058

Metric Field Name: SimpleWatcherPort8058

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort8058

Message text: The Port No:8058 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

ChkMediationServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SERVSTAT

Source / Collection Definition: SERVICECHECK / RTCMEDSRV

Metric: MediationRTCMEDSRVServName

Description: Name of the Service

Metric SpecName: SERVNAME

Metric Field Name: Service_Name

Data type: TEXT

Alarm: FALSE

Metric: MediationRTCMEDSRVServDisplayName

Description: Display Name of the Service

Metric SpecName: SRVDISPNAME

Metric Field Name: Service_Displayname

Data type: TEXT

Alarm: FALSE

Metric: MediationRTCMEDSRVServStatus

Description: Status of the Service

Metric SpecName: SERVSTATUS

Metric Field Name: Service_Status

Data type: TEXT

Alarm: FALSE

Metric: MediationRTCMEDSRVServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_MediationRTCMEDSRVServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): Lync Server Mediation' Windows Service is stopped.

Potential Impact: NA

Suggested Action(s): Lync Server Mediation' Windows Service is stopped. Please restart the service.

WEBAddressWeb

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: SKYPE / WEBADDRESSWEB

Source / Collection Definition: PERFMON / LS:WEB - 02 - Address Book Web Query(*)

Metric: AvgProcessingTimeForAAddressBookDatabaseQueryInMilliseconds

> **Description**: This metric captures Average Processing Time For A Address Book Database Query In Milliseconds
>
> **Metric SpecName**: AvgPrcTAddBkDBQryMS
>
> **Metric Field Name**: WEB - 009 - Average processing time for a address book database query in milliseconds
>
> **Data type**: REAL64
>
> **Alarm**: FALSE

Metric: Instance_Name

> **Description**: This is the key for metric
>
> **Metric SpecName**: Instance_Name
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FailSearchRequest

Description: This metric captures Failed Search Requests

Metric SpecName: FailedSearchRequest

Metric Field Name: WEB - 004 - Failed search requests

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Critical / 5, Major / 5

Policy: MSBS_FailSearchRequest

Message text: The number of Failed Search Requests is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): 1.Watcher Node Configuration issues 2.Server/Component is down for maintenance. 3.Network/connectivity issues between. Watcher node (where the ST executes) and the Front-end Pool.

Potential Impact: 1. Test user password is invalid or expired test users have not been configured correctly for this Pool. 2. Ensure that Synthetic Transactions is in maintenance mode before performing server/pool maintenance

Suggested Action(s): Synthetic transactions may not be able to monitor Address Book Web Query.

Metric: SearchRequests

Description: This metric captures Search Requests

Metric SpecName: SearchRequests

Metric Field Name: WEB - 000 - Search requests

Data type: REAL64

Alarm: FALSE

Metric: SuccessfulSearchRequests

Description: This metric captures Successful Search Requests

Metric SpecName: SuccessfulSearchReq

Metric Field Name: WEB - 002 - Successful search requests

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Critical / 20

Policy: MSBS_SuccessfulSearchRequests

Message text: The value of Successful Search Requests is <VALUE>

Instructional Text:

Probable Cause(s): 1.Watcher Node Configuration issues 2.Server/Component is down for maintenance. 3.Network/connectivity issues between Watcher node (where the ST executes) and the Front-end Pool.

Potential Impact: 1. Test user password is invalid or expired test users have not been configured correctly for this Pool. 2. Ensure that Synthetic Transactions is in maintenance mode before performing server/pool maintenance. 3. Check Alert Context tab for more details on the exact connectivity error such as DNS resolution errors or Connection Timeout

Suggested Action(s): Synthetic transactions may not be able to monitor Address Book Web Query.

Metric: SuccessfulSearchRequestsPerSec

Description: This metric captures Successful Search Requests Per Sec

Metric SpecName: SuccessfulSercReqPS

Metric Field Name: WEB - 003 - Successful search requests/sec

Data type: REAL64

Alarm: FALSE

Metric: AvgProcessingTimeForAAddressBookDatabaseQueryInMilliseconds

Description: This metric captures Average Processing Time For A Address Book Database Query In Milliseconds

Metric SpecName: AvgPrcTAddBkDBQryMS

Metric Field Name: WEB - Average processing time for a address book database query in milliseconds

Data type: REAL64

Alarm: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: FailSearchRequest

Description: This metric captures Failed Search Requests

Metric SpecName: FailedSearchRequest

Metric Field Name: WEB - Failed Search Requests

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Critical / 5, Major / 5

Policy: MSBS_FailSearchRequest

Message text: The number of Failed Search Requests is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): 1.Watcher Node Configuration issues 2.Server/Component is down for maintenance. 3.Network/connectivity issues between. Watcher node (where the ST executes) and the Front-end Pool.

Potential Impact: 1. Test user password is invalid or expired test users have not been configured correctly for this Pool. 2. Ensure that Synthetic Transactions is in maintenance mode before performing server/pool maintenance

Suggested Action(s): Synthetic transactions may not be able to monitor Address Book Web Query.

Metric: SearchRequests

Description: This metric captures Search Requests

Metric SpecName: SearchRequests

Metric Field Name: WEB - Search Requests

Data type: REAL64

Alarm: FALSE

Metric: SuccessfulSearchRequests

> **Description**: This metric captures Successful Search Requests
>
> **Metric SpecName**: SuccessfulSearchReq
>
> **Metric Field Name**: WEB - Successful Search Requests
>
> **Data type**: REAL64
>
> **Alarm**: FALSE

Metric: SuccessfulSearchRequestsPerSec

> **Description**: This metric captures Successful Search Requests Per Sec
>
> **Metric SpecName**: SuccessfulSercReqPS
>
> **Metric Field Name**: WEB - Successful Search Requests/Sec
>
> **Data type**: REAL64
>
> **Alarm**: FALSE

Collect_FrontEnd_LYSS

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / LSLYSS

Source / Collection Definition: PERFMON / LS:LYSS - Storage Service API(*)

Metric: LYSSInstance

Description: instance of perfmon object LS:LYSS - Storage Service API

Metric SpecName: LYSSINSTANCE

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: LYSSCurrentNumberofStorageServiceStaleQueueItems

Description: Current number of Storage Service queue items which are not owned and last attempted a long time ago.

Metric SpecName: NUMSTRGSVCSTLQUE

Metric Field Name: LYSS - Current number of Storage Service stale queue items

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 1, Major / 25

Policy: MSBS_LYSSCurrentNumberofStorageServiceStaleQueueItems

Message text: The value of Current number of Storage Service stale queue items for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Data deleted on primary but the deletion failed to be replicated to the secondary or the deletion failed on the secondary

Potential Impact: NA

Suggested Action(s): Use the Storage Service resource kit to search for and delete stale queue item data

Metric: LYSSTotalNumberOfEWSSubscriptionsFailed

Description: Total number of EWS Subscriptions failed

Metric SpecName: TOTNUMEWSSUBFAILED

Metric Field Name: LYSS - Total number of EWS Subscriptions failed

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 1, Major / 25

Policy: MSBS_LYSSTotalNumberOfEWSSubscriptionsFailed

Message text: The value of Total number of EWS Subscriptions failed for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): There was a failure to create or remove a subscription.

Potential Impact: NA

Suggested Action(s): Verify that EWS endpoint is reachable and healthy. If the problem persists, notify your organization's support team with the event detail.

Metric: LYSSTotalNoofStorageAdptAsyncTskStopOprFailure

Description: Total number of storage adaptor asynchronous task stop operation failures

Metric SpecName: STGADAPTASYNOPRFAIL

Metric Field Name: LYSS - Total number of storage adaptor asynchronous task stop operation failures

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 1, Major / 25

Policy: MSBS_LYSSTotalNoofStorageAdptAsyncTskStopOprFailure

Message text: The value of Total number of storage adaptor asynchronous task stop operation failures <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): The Storage Adaptor has failed to stop the task. Either the Asynchronous Task is hung .

Potential Impact: NA

Suggested Action(s): This condition should not be left unattended as data loss can occur. If the problem persists, notify your organization's support team with the event detail.

Metric: LYSSTotNoOfStorageAdptorAsyncTskStopUnhandExcept

Description: Total number of storage adaptor asynchronous task unhandled exceptions

Metric SpecName: STGADAPTASYNUNEXCEP

Metric Field Name: LYSS - Total number of storage adaptor asynchronous task unhandled exceptions

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 1, Major / 25

Policy: MSBS_LYSSTotNoOfStorageAdptorAsyncTskStopUnhandExcept

Message text: The value of Total number of storage adaptor asynchronous task unhandled exceptions for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Failed to initialize a storage adaptor asynchronous task.

Potential Impact: NA

Suggested Action(s): Check the error details in event log. If problem persists, notify your organization's support team with the event detail.

Metric: LYSSTotalNumberofDeleteBlobOprFailed

Description: the total number of delete blob operations failed to be executed by Storage Service.

Metric SpecName: TOTNUMDELBLOPFAILED

Metric Field Name: LYSS - Total number of DELETE blob operations failed

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 1, Major / 25

Policy: MSBS_LYSSTotalNumberofDeleteBlobOprFailed

Message text: The value of Total number of DELETE blob operations failed for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Authorization failure, bad input parameters, fabric errors, timeouts.

Potential Impact: NA

Suggested Action(s): Check error details in event log. If problem persists, notify your organization's support team with the event detail.

Metric: LYSSTotalNumberofQueueMessagesFailure

Description: the total number of queue messages requests failed to be executed by Storage Service

Metric SpecName: TOTNUMQUEMSGFAIL

Metric Field Name: LYSS - Total number of queue messages failures

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 1, Major / 25

Policy: MSBS_LYSSTotalNumberofQueueMessagesFailure

Message text: The value of Total number of queue messages failures for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Authorization failure, bad input parameters, fabric errors, timeouts.

Potential Impact: NA

Suggested Action(s): Check error details in event log. If problem persists, notify your organization's support team with the event detail.

Metric: LYSSTotalNumberofExecuteCommandFailure

Description: the total number of execute command requests failed to be executed by Storage Service

Metric SpecName: TOTNUMEXECCMDFAIL

Metric Field Name: LYSS - Total number of execute command failure

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 1, Major / 25

Policy: MSBS_LYSSTotalNumberofExecuteCommandFailure

Message text: The value of Total number of execute command failure for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Authorization failure, bad input parameters, timeouts, other errors.

Potential Impact: NA

Suggested Action(s): Check error details in event log. If problem persists, notify your organization's support team with the event detail.

Metric: LYSSTotalNumberofGetBlobOprFailed

Description: the total number of get blob operations failed to be executed by Storage Service

Metric SpecName: TOTNUMGETBLOBFAIL

Metric Field Name: LYSS - Total number of GET blob operations failed

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 1, Major / 25

Policy: MSBS_LYSSTotalNumberofGetBlobOprFailed

Message text: The value of Total number of GET blob operations failed for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Authorization failure, bad input parameters, fabric errors, timeouts, other errors.

Potential Impact: NA

Suggested Action(s): Check error details in event log. If problem persists, notify your organization's support team with the event detail.

Metric: LYSSTotalNumberofDatabaseOprFailures

Description: Total number of times that LYSS database operations failed to execute

Metric SpecName: TOTNUMDBOPRFAIL

Metric Field Name: LYSS - Total number of LYSS database operation failures

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 1, Major / 25

Policy: MSBS_LYSSTotalNumberofDatabaseOprFailures

Message text: The value ofTotal number of LYSS database operation failures for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Cannot perform a LYSS DB operation.

Potential Impact: NA

Suggested Action(s): Verify that the data is valid and that the LYSS database is available.

Metric: LYSSTotNumofStorageServiceEWSAutoDiscoveryErrors

Description: Total number of Storage Service EWS Autodiscovery errors

Metric SpecName: STGSVCDISCERRORS

Metric Field Name: LYSS - Total number of Storage Service EWS Autodiscovery errors

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 1, Major / 25

Policy: MSBS_LYSSTotNumofStorageServiceEWSAutoDiscoveryErrors

Message text: The value of Total number of Storage Service EWS Autodiscovery errors for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Autodiscovery Uri was not correctly configured or unreachable, that there is a problem with the Proxy, or other errors.

Potential Impact: NA

Suggested Action(s): Check error details in event log. If problem persists, notify your organization's support team with the event detail.

Metric: LYSSTotNumofStgServiceFabricServiceUnhandExcep

Description: Total number of Storage Service Fabric Service unhandled exceptions

Metric SpecName: STGSVCFSUNHANDEXCEP

Metric Field Name: LYSS - Total number of Storage Service Fabric Service unhandled exceptions

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 1, Major / 25

Policy: MSBS_LYSSTotNumofStgServiceFabricServiceUnhandExcep

Message text: The value of Total number of Storage Service Fabric Service unhandled exceptions for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Cannot perform a fabric operation such as replication, or connection errors.

Potential Impact: NA

Suggested Action(s): Check that the fabric is configured and working properly. If problem persists, notify your organization's support team with the event detail.

Metric: LYSSTotalNumberofStorageServiceOAuthFailures

Description: Total number of Storage Service OAuth authentication failures

Metric SpecName: OAUTHFAILURES

Metric Field Name: LYSS - Total number of Storage Service OAuth authentication failures

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 1, Major / 25

Policy: MSBS_LYSSTotalNumberofStorageServiceOAuthFailures

Message text: The value of Total number of Storage Service OAuth authentication failures for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Bad input data or configuration error.

Potential Impact: NA

Suggested Action(s): Check error details in event log. If problem persists, notify your organization's support team with the event detail.

Metric: LYSSTotalNumberofUnexpectedExceptions

Description: Total number of unexpected exceptions from sources such as storage adaptors, custom commands, and controller

Metric SpecName: TOTNUMUNEXCEPT

Metric Field Name: LYSS - Total number of unexpected exceptions

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 1, Major / 25

Policy: MSBS_LYSSTotalNumberofUnexpectedExceptions

Message text: The value of Total number of unexpected exceptions for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Failure to initialize the adaptors from loading DLL, or runtime unhandled exceptions in the adaptor.

Potential Impact: NA

Suggested Action(s): Check the error details in event log. If problem persists, notify your organization's support team with the event detail.

Metric: LYSSTotalNumberofNotificationFailure

Description: the total number of notification requests failed to be executed by Storage Service

Metric SpecName: TOTNUMNOTIFFAIL

Metric Field Name: LYSS - Total number of notification failure

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 1, Major / 25

Policy: MSBS_LYSSTotalNumberofNotificationFailure

Message text: The value of Total number of notification failure for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Bad inputs to the API, serialization error, or other errors.

Potential Impact: NA

Suggested Action(s): Check error details in event log. If problem persists, notify your organization's support team with the event detail.

Metric: LYSSTotNumofStorageServiceOAuthSTSRequestFailure

Description: Total number of Storage Service OAuth STS request failures

Metric SpecName: OAUTHSTSREQFAILURE

Metric Field Name: LYSS - Total number of Storage Service OAuth STS request failures

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 1, Major / 25

Policy: MSBS_LYSSTotNumofStorageServiceOAuthSTSRequestFailure

Message text: The value of Total number of Storage Service OAuth STS request failures for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Improper configuration of STS used by Storage Service, or STS server was unavailable.

Potential Impact: NA

Suggested Action(s): Not sure what to put.

Metric: LYSSTotalNumberofPUTBlobOprFailed

Description: the total number of put blob operations failed to be executed by Storage Service

Metric SpecName: PUTBLOBFAILED

Metric Field Name: LYSS - Total number of PUT blob operations failed

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 1, Major / 25

Policy: MSBS_LYSSTotalNumberofPUTBlobOprFailed

Message text: The value of Total number of PUT blob operations failed for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Authorization failure, bad input parameters, fabric errors, timeouts, other errors.

Potential Impact: NA

Suggested Action(s): Check error details in event log. If problem persists, notify your organization's support team with the event detail.

Metric: LYSSTotalNumberofFailedStoredProcedureTimeouts

Description: Total number of failed stored procedure time outs

Metric SpecName: STRPROCTIMEOUT

Metric Field Name: LYSS - Total number of failed stored procedure time outs

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 1, Major / 10

Policy: MSBS_LYSSTotalNumberofFailedStoredProcedureTimeouts

Message text: The value of Total number of failed stored procedure time outs for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Locking and contention, or high load can cause time outs for stored procedure execution

Potential Impact: NA

Suggested Action(s): Check the database and event logs for errors. If the problem persists, notify your organization's support team.

Metric: LYSSTotalNumberofFailedGetItemListCalls

Description: the total number of failed GetImItemList calls while processing ucs contact notifications

Metric SpecName: FAILEDGETITEMLIST

Metric Field Name: LYSS - Total number of failed GetImItemList calls while processing ucs contact notifications

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 5, Major / 20

Policy: MSBS_LYSSTotalNumberofFailedGetItemListCalls

Message text: The value ofTotal number of failed GetImItemList calls while processing ucs contact notifications for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): The failure can be caused by a number of reasons including exchange configuration errors, connectivity issues.

Potential Impact: NA

Suggested Action(s): This condition should not be left unattended as this can result in perceived data loss. If the problem persists, notify your organization's support team.

Metric: LYSSTotNumofStorageAdaptReportedinUnhealthState

Description: Total number of storage adaptors reported in unhealthy state

Metric SpecName: STGADPUNHEALTHSTATE

Metric Field Name: LYSS - Total number of storage adaptors reported in unhealthy state

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 1, Major / 10

Policy: MSBS_LYSSTotNumofStorageAdaptReportedinUnhealthState

Message text: The value of Total number of storage adaptors reported in unhealthy state for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): This happens when a registered adaptor reports it is unhealthy, possibly from having timed out and hung.

Potential Impact: NA

Suggested Action(s): This condition should not be left unattended as data loss can occur. If the problem persists, notify your organization's support team with the event detail.

Collect_AccessEdge_EdgeLogging

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / CS_ACCESSEDGE

Source / Collection Definition: PERFMON / LS:SIP - Protocol(*)

Metric: SIPProtocolInstance

Description: instance of perfmon object LS:SIP - Protocol

Metric SpecName: SIPPROTOINSTANCE

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: SIPAvgIncomMsgeProcessingTimeLogging

Description: the average time (in seconds) it takes to process an incoming message.

Metric SpecName: AVINCMSGPROCTIME

Metric Field Name: SIP - Average Incoming Message Processing Time

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 3, Major / 9

Policy: MSBS_SIPAvgIncomMsgeProcessingTimeLogging

Message text: The value of SIP - Average Incoming Message Processing Time (sec) for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): This server is too busy and is unable to process user requests.

Potential Impact: NA

Suggested Action(s): This might be a temporary condition. If the problem persists, please ensure that hardware and software requirements for this server meet the user usage characteristics.

Metric: SIPProtocolInstance

Description: instance of perfmon object LS:SIP - 02 - Protocol

Metric SpecName: SIPPROTOINSTANCE

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: SIPAvgIncomMsgeProcessingTime

Description: average processing time of an incoming message in seconds.

Metric SpecName: AVINCMSGPROCTIME

Metric Field Name: SIP - 021 - Average Incoming Message Processing Time

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 5

Policy: MSBS_SIPAvgIncomMsgeProcessingTime

Message text: The value of the counter 'Average Incoming Message Processing Time' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: SIPIncomingReqtsDropdpersec

Description: rate at which the incoming requests are dropped, as they could not be processed due to bad headers, insufficient routing information, and severe resource allocation failure.

Metric SpecName: INCMGRQSTSDROPDPERSEC

Metric Field Name: SIP - 005 - Incoming Requests Dropped/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 10

Policy: MSBS_SIPIncomingReqtsDropdpersec

Message text: The value of the counter ' Incoming Requests Dropped/sec' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: SIPIncomingResponsesDropdpersec

Description: rate at which the incoming responses are dropped per second as they could not be processed.

Metric SpecName: INCMGRSPNSEDROPDPERSEC

Metric Field Name: SIP - 009 - Incoming Responses Dropped/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 10

Policy: MSBS_SIPIncomingResponsesDropdpersec

Message text: The value of the counter ' Incoming Responses Dropped/sec' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: SIPMessagesInServer

Description: number of messages currently being processed by the server.

Metric SpecName: MSGINSERVER

Metric Field Name: SIP - 012 - Messages In Server

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 2500, Major / 5000

Policy: MSBS_SIPMessagesInServer

Message text: The value of the counter 'Messages In Server' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: SIPMsgsPersecDropdDueToCertiMismatch

Description: rate at which the messages are dropped per second as they did not have an FQDN that matched the remote peer's certificate.

Metric SpecName: MSGPERSECDRPDDUETOCERTMISMATCH

Metric Field Name: SIP - 011 - Messages/sec Dropped Due To Certificate Mismatch

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 100

Policy: MSBS_SIPMsgsPersecDropdDueToCertiMismatch

Message text: The value of the counter 'Messages/sec Dropped Due To Certificate Mismatch' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Collect_Monitoring_Process_QmsSvc

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / CS_PROCESS

Source / Collection Definition: PERFMON / Process(QmsSvc)

Metric: MonitoringQmsSvcInstance

Description: instance of perfmon object Process(QmsSvc)

Metric SpecName: INSTANCENAME

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: MonitoringQmsSvcPageFaultsPersec

Description: Page Faults/sec counter available in the QoE Monitoring service.

Metric SpecName: PAGEFAULTS

Metric Field Name: Page Faults/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 100

Policy: MSBS_MonitoringQmsSvcPageFaultsPersec

Message text: The value of the counter 'Page Faults/sec' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: MonitoringQmsSvcPrivateBytes

Description: Private Bytes counter available in the QoE Monitoring service.

Metric SpecName: PRIVATEBYTES

Metric Field Name: Private Bytes

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20000000

Policy: MSBS_MonitoringQmsSvcPrivateBytes

Message text: The value of the counter 'Private Bytes' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: MonitoringQmsSvcProcessorTime

Description: the % Processor Time counter available in the QoE Monitoring service.

Metric SpecName: PROCESSORTIME

Metric Field Name: % Processor Time

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 90

Policy: MSBS_MonitoringQmsSvcProcessorTime

Message text: The value of the counter '% Processor Time' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: MonitoringQmsSvcThreadCount

Description: Thread Count counter available in the QoE Monitoring service.

Metric SpecName: THREADCOUNT

Metric Field Name: Thread Count

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 150

Policy: MSBS_MonitoringQmsSvcThreadCount

Message text: The value of the counter 'Thread Count' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: MonitoringQmsSvcWorkingSet

Description: Working Set Counter available in the QoE Monitoring service.

Metric SpecName: WORKINGSET

Metric Field Name: Working Set

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20000000

Policy: MSBS_MonitoringQmsSvcWorkingSet

Message text: The value of the counter 'Working Set' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

ReplicationDBQueueDepth

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / REPLICATDBQUEUEDEPTH

Source / Collection Definition: PERFMON / LS:USrv - ReplicationDBStore(*)

Metric: ReplicationDBQueueDepth

> **Description**: This metric captures the average number of database requests waiting to be executed for Replication Db Store
>
> **Metric SpecName**: ReplicationDBQueueDepth
>
> **Metric Field Name**: USrv - Queue Depth
>
> **Data type**: REAL64
>
> **Alarm**: FALSE

Metric: Instance_Name

> **Description**: This is the key for metric
>
> **Metric SpecName**: Instance_Name
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

ArchivingMessage

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: SKYPE / ARCHIVINGMESSAGE

Source / Collection Definition: PERFMON / LS:Arch Agent - 00 - MSMQ(*)

Metric: ArchivingMessageBytesPerSec

Description: This metric captures messages archived in bytes per second by the Server

Metric SpecName: ArchivingMsgBytesPS

Metric Field Name: Arch Agent - 003 - Archiving Message bytes/sec

Data type: REAL64

Alarm: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: ArchivingMessagesPerSec

Description: This metric captures messages archived in messages per second by the Server

Metric SpecName: ArchivingMsgPerSec

Metric Field Name: Arch Agent - 001 - Archiving Messages/sec

Data type: TEXT

Alarm: FALSE

Metric: CallDetailsRecordingMessageBytesPerSec

Description: This metric captures Call Details Recording Message in bytes per second by the Server

Metric SpecName: CallDtlsRecdMsgBtPS

Metric Field Name: Arch Agent - 007 - Call Details Recording Message bytes/sec

Data type: REAL64

Alarm: FALSE

Metric: CallDetailsRecordingMessagesPerSec

Description: This metric captures Call Details Recording Message in messages per second by the Server

Metric SpecName: CALDTLRECORDINGMSGPS

Metric Field Name: Arch Agent - 005 - Call Details Recording Messages/sec

Data type: TEXT

Alarm: FALSE

Metric: ArchivingMessageBytesPerSec

Description: This metric captures messages archived in bytes per second by the Server

Metric SpecName: ArchivingMsgBytesPS

Metric Field Name: Arch Agent - Archiving Message Bytes/Sec

Data type: REAL64

Alarm: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: ArchivingMessagesPerSec

Description: This metric captures messages archived in messages per second by the Server

Metric SpecName: ArchivingMsgPerSec

Metric Field Name: Arch Agent - Archiving Messages/Sec

Data type: TEXT

Alarm: FALSE

Metric: CallDetailsRecordingMessageBytesPerSec

> **Description**: This metric captures Call Details Recording Message in bytes per second by the Server
>
> **Metric SpecName**: CallDtlsRecdMsgBtPS
>
> **Metric Field Name**: Arch Agent - Call Details Recording Message Bytes/Sec
>
> **Data type**: REAL64
>
> **Alarm**: FALSE

Metric: CallDetailsRecordingMessagesPerSec

> **Description**: This metric captures Call Details Recording Message in messages per second by the Server
>
> **Metric SpecName**: CALDTLRECORDINGMSGPS
>
> **Metric Field Name**: Arch Agent - Call Details Recording Messages/Sec
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

ChkArchivingRTCLOGServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / NA

Source / Collection Definition: SERVICECHECK / RTCLOG

Metric: ArchivingRTCLOGServName

Description: Name of the Service

Metric SpecName: SERVNAME

Metric Field Name: Service_Name

Data type: TEXT

Alarm: FALSE

Metric: ArchivingRTCLOGDisplayName

Description: Display Name of the Service

Metric SpecName: SRVDISPNAME

Metric Field Name: Service_Displayname

Data type: TEXT

Alarm: FALSE

Metric: ArchivingRTCLOGServStatus

Description: Status of the Service

Metric SpecName: SERVSTATUS

Metric Field Name: Service_Status

Data type: TEXT

Alarm: FALSE

Metric: ArchivingRTCLOGServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_ArchivingRTCLOGServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Collect_FrontEnd_SIPPeers_Logging

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / CS_FESIPPEERS

Source / Collection Definition: PERFMON / LS:SIP - Peers(*)

Metric: SIPPeersInstance

Description: instance of perfmon object LS:SIP - Peers

Metric SpecName: SIPPEERINSTANCE

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: SIPPeersSendsOutstandingLogging

Description: the number of messages that are currently present in the outgoing (send) queues.

Metric SpecName: SENDSOUTSTANDING

Metric Field Name: SIP - Sends Outstanding

Data type: UINT32

Alarm: FALSE

Metric: SIPPeersInstance

Description: instance of perfmon object LS:SIP - 01 - Peers

Metric SpecName: SIPPEERINSTANCE

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: SIPPeersSendsOutstandingLogging

Description: The number of outstanding send requests waiting to be processed

Metric SpecName: SENDSOUTSTANDING

Metric Field Name: SIP - 017 - Sends Outstanding

Data type: UINT32

Alarm: FALSE

CallParkService

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: SKYPE / CALLPARKSERVICE

Source / Collection Definition: PERFMON / LS:CPS - 01 - Call Park Service Planning(*)

Metric: TotalParkRequestsFailedBecauseUnavailableOrbit.

> **Description**: This metric captures Total Park Requests Failed Because Unavailable Orbit
>
> **Metric SpecName**: TotlPrkReqFailUnavOr
>
> **Metric Field Name**: CPS - 013 - Total park requests failed because unavailable orbit.
>
> **Data type**: REAL64
>
> **Alarm**: FALSE

Metric: Instance_Name

> **Description**: This is the key for metric
>
> **Metric SpecName**: Instance_Name
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: TotalParkRequestsThatFailed.

Description: This metric captures Total Park Requests That Failed

Metric SpecName: TotalParkReqFail

Metric Field Name: CPS - 012 - Total park requests that failed.

Data type: REAL64

Alarm: FALSE

Metric: TotalParkRequestsFailedBecauseUnavailableOrbit.

Description: This metric captures Total Park Requests Failed Because Unavailable Orbit

Metric SpecName: TotlPrkReqFailUnavOr

Metric Field Name: CPS - Total Park Requests Failed Because Unavailable Orbit.

Data type: REAL64

Alarm: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: TotalParkRequestsThatFailed.

Description: This metric captures Total Park Requests That Failed

Metric SpecName: TotalParkReqFail

Metric Field Name: CPS - Total Park Requests That Failed.

Data type: REAL64

Alarm: FALSE

Collect_Edge_Process_DataProxy

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / CS_PROCESS

Source / Collection Definition: PERFMON / Process(DataProxy)

Metric: EdgeDataProxyWorkingSet

> **Description**: Working Set counter available in the Web Conferencing Edge service.
>
> **Metric SpecName**: WORKINGSET
>
> **Metric Field Name**: Working Set
>
> **Data type**: UINT32
>
> **Alarm**: TRUE
>
> **Category** : MSSkype
>
> **Severity / Threshold** : Major / 20000000
>
> **Policy**: MSBS_EdgeDataProxyWorkingSet
>
> **Message text**: The value of the counter 'Working Set' value <VALUE> has crossed the threshold of <THRESHOLD> .
>
> **Instructional Text**:
>
> **Probable Cause(s)**: NA
>
> **Potential Impact**: NA
>
> **Suggested Action(s)**: NA

Metric: EdgeDataProxyThreadCount

Description: Thread Count counter available in the Web Conferencing Edge service.

Metric SpecName: THREADCOUNT

Metric Field Name: Thread Count

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 150

Policy: MSBS_EdgeDataProxyThreadCount

Message text: The value of the counter 'Thread Count' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: EdgeDataProxyProcessorTime

Description: the % Processor Time counter available in the Web Conferencing Edge service.

Metric SpecName: PROCESSORTIME

Metric Field Name: % Processor Time

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 90

Policy: MSBS_EdgeDataProxyProcessorTime

Message text: The value of the counter '% Processor Time' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: EdgeDataProxyPrivateBytes

Description: Private Bytes counter available in the Web Conferencing Edge service.

Metric SpecName: PRIVATEBYTES

Metric Field Name: Private Bytes

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20000000

Policy: MSBS_EdgeDataProxyPrivateBytes

Message text: The value of the counter 'Private Bytes' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: EdgeDataProxyPageFaultsPersec

Description: Page Faults/sec counter available in the Web Conferencing Edge service.

Metric SpecName: PAGEFAULTPERSEC

Metric Field Name: Page Faults/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 100

Policy: MSBS_EdgeDataProxyPageFaultsPersec

Message text: The value of the counter 'Page Faults/sec' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: EdgeDataProxyInstance

Description: instance of perfmon object Process(DataProxy)

Metric SpecName: DATAPROXYINSTANCE

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Collect_FrontEnd_IMMCU_Confernces

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / LSIMMCUCONF

Source / Collection Definition: PERFMON / LS:ImMcu - IMMcu Conferences(*)

Metric: IMMCUINstanceName

> **Description**: instance of perfmon object LS:ImMcu - IMMcu Conferences
>
> **Metric SpecName**: IMMCUINSTANCE
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: ThrottledSIPConnection

> **Description**: the number of throttled Sip connections
>
> **Metric SpecName**: THROTLEDSIPCONN
>
> **Metric Field Name**: IMMCU - Throttled Sip Connections
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Collect_Monitoring_Process_RtcCdr

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / CS_PROCESS

Source / Collection Definition: PERFMON / Process(RtcCdr)

Metric: MonitoringRtcCdrInstance

Description: instance of perfmon object Process(RtcCdr)

Metric SpecName: INSTANCENAME

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: MonitoringRtcCdrPageFaultsPersec

Description: Page Faults/sec counter available Lync Server Call Detail Recording service.

Metric SpecName: PAGEFAULTS

Metric Field Name: Page Faults/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 100

Policy: MSBS_MonitoringRtcCdrPageFaultsPersec

Message text: The value of the counter 'Page Faults/sec' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: MonitoringRtcCdrPrivateBytes

Description: Private Bytes counter available in the Lync Server Call Detail Recording service.

Metric SpecName: PRIVATEBYTES

Metric Field Name: Private Bytes

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20000000

Policy: MSBS_MonitoringRtcCdrPrivateBytes

Message text: The value of the counter 'Private Bytes' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: MonitoringRtcCdrProcessorTime

Description: the % Processor Time counter available in Lync Server Call Detail Recording service.

Metric SpecName: PROCESSORTIME

Metric Field Name: % Processor Time

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 90

Policy: MSBS_MonitoringRtcCdrProcessorTime

Message text: The value of the counter '% Processor Time' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: MonitoringRtcCdrThreadCount

Description: Thread Count counter available Lync Server Call Detail Recording service.

Metric SpecName: THREADCOUNT

Metric Field Name: Thread Count

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 150

Policy: MSBS_MonitoringRtcCdrThreadCount

Message text: The value of the counter 'Thread Count' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: MonitoringRtcCdrWorkingSet

Description: Working Set Counter available in the Lync Server Call Detail Recording service.

Metric SpecName: WORKINGSET

Metric Field Name: Working Set

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20000000

Policy: MSBS_MonitoringRtcCdrWorkingSet

Message text: The value of the counter 'Working Set' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

ChkEdgeAVAuthenticationServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SERVSTAT

Source / Collection Definition: SERVICECHECK / RTCMRAUTH

Metric: EdgeRTCMRAUTHServName

Description: Name of the Service

Metric SpecName: SERVNAME

Metric Field Name: Service_Name

Data type: TEXT

Alarm: FALSE

Metric: EdgeRTCMRAUTHServDisplayName

Description: Display Name of the Service

Metric SpecName: SRVDISPNAME

Metric Field Name: Service_Displayname

Data type: TEXT

Alarm: FALSE

Metric: EdgeRTCMRAUTHServStatus

Description: Status of the Service

Metric SpecName: SERVSTATUS

Metric Field Name: Service_Status

Data type: TEXT

Alarm: FALSE

Metric: EdgeRTCMRAUTHServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_EdgeRTCMRAUTHServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): Lync Server Audio/Video Authentication' Windows Service is stopped.

Potential Impact: NA

Suggested Action(s): Lync Server Audio/Video Authentication' Windows Service is stopped. Please restart the service.

SimplePortWatcher5087

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / Port5087

Source / Collection Definition: PORTCOL / PORTCHECKER

Metric: SimpleWatcherPort5087

Description: SIP port used by Mobility Services internal processes

Metric SpecName: SimpleWatcherPort5087

Metric Field Name: SimpleWatcherPort5087

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_SimpleWatcherPort5087

Message text: The Port No:5087 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

SimplePortWatcher5067

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / Port5067

Source / Collection Definition: PORTCOL / PORTCHECKER

Metric: SimpleWatcherPort5067

Description: Used for incoming SIP requests from the PSTN gateway.

Metric SpecName: SimpleWatcherPort5067

Metric Field Name: SimpleWatcherPort5067

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort5067

Message text: The Port No:5067 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

Metric: SimpleWatcherPort5067

Description: Used for incoming SIP requests from the PSTN gateway.

Metric SpecName: SimpleWatcherPort5067

Metric Field Name: SimpleWatcherPort5067

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort5067

Message text: The Port No:5067 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

ChkFrontEndOnlineLegalInterceptServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SERVSTAT

Source / Collection Definition: SERVICECHECK / RTCLISVC

Metric: FERTCLISVCServName

Description: Name of the Service

Metric SpecName: SERVNAME

Metric Field Name: Service_Name

Data type: TEXT

Alarm: FALSE

Metric: FERTCLISVCServDisplayName

Description: Display Name of the Service

Metric SpecName: SRVDISPNAME

Metric Field Name: Service_Displayname

Data type: TEXT

Alarm: FALSE

Metric: FERTCLISVCServStatus

Description: Status of the Service

Metric SpecName: SERVSTATUS

Metric Field Name: Service_Status

Data type: TEXT

Alarm: FALSE

Metric: FERTCLISVCServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_FERTCLISVCServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): Lync Online Legal Intercept Service' Windows Service is stopped.

Potential Impact: NA

Suggested Action(s): Lync Online Legal Intercept Service' Windows Service is stopped.
Please restart the service.

Collect_Director_AddressBook_WebQuery

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / DIRLSWEBADDRBKWEBQRY

Source / Collection Definition: PERFMON / LS:WEB - Address Book Web Query(*)

Metric: DirectorAddressBookWebQueryInstance

> **Description**: instance of perfmon object LS:WEB - Address Book Web Query
>
> **Metric SpecName**: DIRADDRBKWEBQRYINST
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: DirectorFailedSearchRequests

Description: the per-second rate of failed address book search requests

Metric SpecName: DIRFAILEDSEARCHREQ

Metric Field Name: WEB - Failed search requests/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 4, Major / 20

Policy: MSBS_DirectorFailedSearchRequests

Message text: The value of WEB - Failed search requests/sec for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Issues with backend database connectivity

Potential Impact: NA

Suggested Action(s): Verify backend database is running and accessible.

Metric: DirectorAvgProcessingTimeForSearchReq

Description: the average processing time for a address book search request in milliseconds

Metric SpecName: DIRAVGPROCTIME

Metric Field Name: WEB - Average processing time for a search request in milliseconds

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 500, Major / 1000

Policy: MSBS_DirectorAvgProcessingTimeForSearchReq

Message text: The value of WEB - Average processing time for a search request in milliseconds for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Issues with backend database connectivity

Potential Impact: NA

Suggested Action(s): Verify CPU load on backend database machine.

Collect_FrontEnd_UCStore

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / LSUSRVUCS

Source / Collection Definition: PERFMON / LS:USrv - Unified Contact Store(*)

Metric: UCSInstance

Description: instance of perfmon object LS:USrv - Unified Contact Store

Metric SpecName: UCSINSTANCE

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: NumberofFailedContactSubscriptionToExchange

Description: the total number of failed contact subscriptions to Exchange

Metric SpecName: FAILEDCONTACTSUBSCR

Metric Field Name: USrv - Number of failed contact subscriptions to Exchange

Data type: UINT32

Alarm: FALSE

Metric: NoFailedUsrMigrToUnifiedContactStore

Description: the total number of failed user migrations to Unified Contact Store due to malformed AddNewImContactToGroupResponses from Exchange

Metric SpecName: FAILEDUSRMIGRTOUCS

Metric Field Name: USrv - Number of failed user migrations to Unified Contact Store due to malformed AddNewImContactToGroupResponses from Exchange

Data type: UINT32

Alarm: FALSE

DistributionListExpansion

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / KHIDISTLISEXPAN

Source / Collection Definition: PERFMON / LS:WEB - 00 - Distribution List Expansion(*)

Metric: TimedoutActiveDirecRequests

> **Description**: This policy monitors the per-second rate of timed out Active Directory requests
>
> **Metric SpecName**: TimoutActDirReq
>
> **Metric Field Name**: WEB - 011 - Timed out Active Directory Requests/sec
>
> **Data type**: UINT32
>
> **Alarm**: TRUE
>
> **Category** : MSSkype
>
> **Severity / Threshold** : Minor / 5, Minor / 5
>
> **Policy**: MSBS_TimedoutActiveDirecRequests
>
> **Message text**: The current value of Timedout Active Directory Requests is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:
>
> **Instructional Text**:
>
> **Probable Cause(s)**: Too many pending DLX requests. That can be validated by checking the "WEB – Pending Active Directory Requests" Performance Counter. Problems with the Domain Controllers within the AD site of the Lync Server 2013 Servers.
>
> **Potential Impact**: Check if AD is up and running
>
> **Suggested Action(s)**: Unable to expand Distribution List

Metric: Instance_Name

> **Description**: This is the key for metric
>
> **Metric SpecName**: Instance_Name
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: TimedoutActiveDirecRequests

Description: This policy monitors the per-second rate of timed out Active Directory requests

Metric SpecName: TimoutActDirReq

Metric Field Name: WEB - Timed out Active Directory Requests/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Minor / 5, Minor / 5

Policy: MSBS_TimedoutActiveDirecRequests

Message text: The current value of Timedout Active Directory Requests is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): Too many pending DLX requests. That can be validated by checking the "WEB – Pending Active Directory Requests" Performance Counter. Problems with the Domain Controllers within the AD site of the Lync Server 2013 Servers.

Potential Impact: Check if AD is up and running

Suggested Action(s): Unable to expand Distribution List

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

ChkFrontEndFileTransferAgentServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SERVSTAT

Source / Collection Definition: SERVICECHECK / FTA

Metric: FEFTAServName

> **Description**: Name of the Service
>
> **Metric SpecName**: SERVNAME
>
> **Metric Field Name**: Service_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FEFTAServDisplayName

> **Description**: Display Name of the Service
>
> **Metric SpecName**: SRVDISPNAME
>
> **Metric Field Name**: Service_Displayname
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FEFTAServStatus

> **Description**: Status of the Service
>
> **Metric SpecName**: SERVSTATUS
>
> **Metric Field Name**: Service_Status
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FEFTAServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_FEFTAServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): Lync Server File Transfer Agent' Windows Service is stopped.

Potential Impact: NA

Suggested Action(s): Lync Server File Transfer Agent' Windows Service is stopped. Please restart the service.

Collect_FrontEnd_DataCollection_QoE_Adapter

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / LSDCQOEADAPT

Source / Collection Definition: PERFMON / LS:DATACOLLECTION - QoE Adaptor(*)

Metric: UDCNumberofQoERptDroppedDuetoDBInsertionFailure

Description: This counter represents the total number of reports dropped due to database insertion failure.

Metric SpecName: NUMQOERPTDROPPEDIN

Metric Field Name: UDC - Number of QoE reports dropped due to database insertion failure

Data type: UINT32

Alarm: FALSE

Metric: UDCNumberofQoERptFailedDuetoUnexpServerProcErrors

Description: This counter represents the total number of reports failed due to unexpected server processing errors.

Metric SpecName: NUMQOERPTFAILED

Metric Field Name: UDC - Number of QoE reports failed due to unexpected server processing errors

Data type: UINT32

Alarm: FALSE

Collect_Registrar_USrv_Register

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / NA

Source / Collection Definition: PERFMON / LS:USrv - 12 - Register(*)

Metric: RegistrarUsrvRegisterInstance

Description: instance of perfmon object LS:USrv - 12 - Register

Metric SpecName: REGISTERINSTANCE

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: RegistrarEndpointsDisconnected

Description: number of endpoints that are disconnected because of missed keep-alives.

Metric SpecName: ENDPTSDISCONNTD

Metric Field Name: USrv - 011 - Endpoints Disconnected

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20

Policy: MSBS_RegistrarEndpointsDisconnected

Message text: The value of the counter 'USrv - 011 - Endpoints Disconnected' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: RegIndirectlyConndEndpointsDisconntd

Description: number of indirect endpoints that are disconnected because of error responses.

Metric SpecName: INDCONNTDENDPTDISCONNTD

Metric Field Name: USrv - 012 - Indirectly Connected Endpoints Disconnected

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20

Policy: MSBS_RegIndirectlyConndEndpointsDisconntd

Message text: The value of the counter 'USrv - 012 - Indirectly Connected Endpoints Disconnected' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: RegistrarLegacyREGISTERsrejected

Description: number of legacy registers that are rejected because of the publisher is in rich mode.

Metric SpecName: LEGACYREGSREJCTD

Metric Field Name: USrv - 005 - Legacy REGISTERs rejected (421 Response)

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20

Policy: MSBS_RegistrarLegacyREGISTERsrejected

Message text: The value of the counter 'USrv - 005 - Legacy REGISTERs rejected' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: RegistrarRegistrationNotificationsSent

Description: number of deregistered notifications that are sent to the contacts.These notifications are sent when the server decides that the contacts are invalid.

Metric SpecName: REGNOTIFCTNSENT

Metric Field Name: USrv - 006 - Registration Notifications Sent

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20

Policy: MSBS_RegistrarRegistrationNotificationsSent

Message text: The value of the counter 'USrv - 006 - Registration Notifications Sent' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

ChkEdgeWebConferencingServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SERVSTAT

Source / Collection Definition: SERVICECHECK / RTCDATAPROXY

Metric: EdgeRTCDATAPROXYServName

Description: Name of the Service

Metric SpecName: SERVNAME

Metric Field Name: Service_Name

Data type: TEXT

Alarm: FALSE

Metric: EdgeRTCDATAPROXYServDisplayName

Description: Display Name of the Service

Metric SpecName: SRVDISPNAME

Metric Field Name: Service_Displayname

Data type: TEXT

Alarm: FALSE

Metric: EdgeRTCDATAPROXYServStatus

Description: Status of the Service

Metric SpecName: SERVSTATUS

Metric Field Name: Service_Status

Data type: TEXT

Alarm: FALSE

Metric: EdgeRTCDATAPROXYServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_EdgeRTCDATAPROXYServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): Lync Server Web Conferencing Edge' Windows Service is stopped.

Potential Impact: NA

Suggested Action(s): Lync Server Web Conferencing Edge' Windows Service is stopped. Please restart the service.

StorageServiceAPI

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / STORAGESERVICEAPI

Source / Collection Definition: PERFMON / LS:LYSS - Storage Service API(*)

Metric: TotalNumberOfDELETEBlobOperationsFailed.

Description: This metric captures Total Number Of DELETE blob Operations Failed.

Metric SpecName: TotlNumDELblOpeFail

Metric Field Name: LYSS - Total Number Of DELETE Blob Operations Failed.

Data type: UINT32

Alarm: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: TotalNumberOfGETBlobOperationsFailed.

Description: This metric captures Total Number Of GET Blob Operations Failed.

Metric SpecName: TotlNumGTblOpeFailed

Metric Field Name: LYSS - Total Number Of GET Blob Operations Failed.

Data type: UINT32

Alarm: FALSE

Metric: TotalNumberOfPUTBlobOperationsFailed.

Description: This metric captures Total Number Of PUT Blob Operations Failed

Metric SpecName: TotlNumPUTBlOpeFail

Metric Field Name: LYSS - Total Number Of PUT Blob Operations Failed.

Data type: UINT32

Alarm: FALSE

Metric: TotalNumberOfStorageServiceEWSAutodiscoveryErrors.

Description: This metric captures Total Number Of Storage Service EWS Auto discovery Errors.

Metric SpecName: TotlNumStSrvEWSAutoE

Metric Field Name: LYSS - Total Number Of Storage Service EWS Autodiscovery Errors.

Data type: UINT32

Alarm: FALSE

Metric: TotalNumberOfStorageServiceFabricServiceUnhandledExceptions.

Description: This metric captures Total Number Of Storage Service Fabric Service Unhandled Exceptions.

Metric SpecName: TtlNumStSrvFabSrvExc

Metric Field Name: LYSS - Total Number Of Storage Service Fabric Service Unhandled Exceptions.

Data type: UINT32

Alarm: FALSE

Metric: TotalNumberOfStorageServiceOAuthAuthenticationFailures.

Description: This metric captures Total Number Of Storage Service OAuth Authentication Failures.

Metric SpecName: TtlNumStSrvAuthFail

Metric Field Name: LYSS - Total Number Of Storage Service OAuth Authentication Failures.

Data type: UINT32

Alarm: FALSE

Metric: TotalNumberOfStorageServiceOAuthSTSRequestFailures.

Description: This metric captures Total Number Of Storage Service Oauth STS Request Failures.

Metric SpecName: TtlNumStSrvAuthReqFa

Metric Field Name: LYSS - Total Number Of Storage Service OAuth STS Request Failures.

Data type: UINT32

Alarm: FALSE

ClusterManager

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / KHICLUSMANAGER

Source / Collection Definition: PERFMON / LS:Usrv - Cluster Manager

Metric: NumoffailureofreplicationoperatsenttootherReplicaspersecond

Description: This policy monitors the per-second rate of replication operation failures

Metric SpecName: NoFailRepSeToRepl

Metric Field Name: Usrv - Number of failures of replication operations sent to other Replicas per second

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Minor / 0

Policy: MSBS_NumoffailureofreplicationoperatsenttootherReplicaspersecond

Message text: The current value of NumoffailureofreplicationoperatsenttootherReplicaspersecond is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): This server or local database is overloaded.

Potential Impact: Please ensure that servers are not running out of disk space.

Suggested Action(s): indicates the number of failures in checking with the CMS on if the Lync Server has the latest copy of the environments configuration data.

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

SIPNetworking

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HALFHOURLY

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SIPNETWORKING

Source / Collection Definition: PERFMON / LS:SIP - Networking(*)

Metric: ConnectionsRefusedDueToServerOverloadPerSec

> **Description**: This metric captures Connections Refused Due To Server Overload Per Sec
>
> **Metric SpecName**: ConRefuSrvOverlodPS
>
> **Metric Field Name**: SIP - Connections Refused Due To Server Overload/Sec
>
> **Data type**: REAL64
>
> **Alarm**: FALSE

Metric: Instance_Name

> **Description**: This is the key for metric
>
> **Metric SpecName**: Instance_Name
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

MediationMedia

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: SKYPE / MEDIATIONMEDIA

Source / Collection Definition: PERFMON / LS:MediationServer - Media Relay(*)

Metric: MediaConnectivityCheckFailure

> **Description**: This metric captures Number of media connectivity check failures.
>
> **Metric SpecName**: MediaConnChkFail
>
> **Metric Field Name**: - Media Connectivity Check Failure
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Metric: Instance_Name

> **Description**: This is the key for metric
>
> **Metric SpecName**: Instance_Name
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: MediaConnectivityCheckFailure

> **Description**: This metric captures Number of media connectivity check failures.
>
> **Metric SpecName**: MediaConnChkFail
>
> **Metric Field Name**: - Media Connectivity Check Failure
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Metric: Instance_Name

> **Description**: This is the key for metric
>
> **Metric SpecName**: Instance_Name
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

SimplePortWatcher5075

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / Port5075

Source / Collection Definition: PORTCOL / PORTCHECKER

Metric: SimpleWatcherPort5075

Description: Used for incoming SIP requests for the Call Park application.

Metric SpecName: SimpleWatcherPort5075

Metric Field Name: SimpleWatcherPort5075

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort5075

Message text: The Port No:5075 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

Metric: SimpleWatcherPort5075

Description: Used for incoming SIP requests for the Call Park application.

Metric SpecName: SimpleWatcherPort5075

Metric Field Name: SimpleWatcherPort5075

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort5075

Message text: The Port No:5075 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

ChkEdgeXMPPTranslatingGatewayProxyServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SERVSTAT

Source / Collection Definition: SERVICECHECK / RTCXMPPTGWPX

Metric: EdgeRTCXMPPTGWPXServName

> **Description**: Name of the Service
>
> **Metric SpecName**: SERVNAME
>
> **Metric Field Name**: Service_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: EdgeRTCXMPPTGWPXServDisplayName

Description: Display Name of the Service

Metric SpecName: SRVDISPNAME

Metric Field Name: Service_Displayname

Data type: TEXT

Alarm: FALSE

Metric: EdgeRTCXMPPTGWPXServStatus

Description: Status of the Service

Metric SpecName: SERVSTATUS

Metric Field Name: Service_Status

Data type: TEXT

Alarm: FALSE

Metric: EdgeRTCXMPPTGWPXServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_EdgeRTCXMPPTGWPXServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): Lync Server XMPP Translating Gateway Proxy' Windows Service is stopped.

Potential Impact: NA

Suggested Action(s): Lync Server XMPP Translating Gateway Proxy' Windows Service is stopped. Please restart the service.

Collect_LogicalDisk_Edge

This Policy monitors the logical disk feature of Microsoft Skype Business Server

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Logical_Disk_Conf

Aspect: Skype Logical Disk

CIT: Edge Server, Director Server, Mediation Server, Front End Server, Persistent Chat Server

Data source / Data class: LYNC / LOGICALDISK

Source / Collection Definition: PERFMON / LogicalDisk(*)

Metric: EdgeLogicalDiskInstance

> **Description**: instance of perfmon object LogicalDisk
>
> **Metric SpecName**: LGDISKINSTNAME
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: EdgePercentageFreeSpace

Description: % Free Space is the percentage of total usable space on the selected logical disk drive that was free.

Metric SpecName: FREESPACE

Metric Field Name: % Free Space

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 70, Major / 90

Policy: MSBS_EdgePercentageFreeSpace

Message text: The value of % Free Space for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Database size grows indefinitely.

Potential Impact: NA

Suggested Action(s): Please check each disk drive and clean up unnecessary files.

PresenceLatency

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_LOW

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SYNPRESENCELAT

Source / Collection Definition: POWERSHELL / TestCsPresence TargetFQDN ${fqdn}

Metric: PresenceLatency

Description: This metric will capture latency in the notification of presence of the user

Metric SpecName: PresenceLatency

Metric Field Name: PresenceLatency

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1000, Major / 1000

Policy: MSBS_PresenceLatency

Message text: The value of Presence Latency (ms) is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): 1. User configuration not done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: Users would not be able to avail peer to peer services

Suggested Action(s): 1. Configuration : Most common issues are invalid or expired Test user password, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availability: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution error or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responds to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Metric: Presence

Description: This metric gathers the information which confirms that users are able contact. It monitor the exchange of presence information between two test users in a Lync pool. The following functions are tested • Sign on to the Lync Server • Request for presence information • Publishing of presence information • Receipt of presence information •Log out

Metric SpecName: Presence

Metric Field Name: Presence

Data type: TEXT

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_Presence

Message text: The Presence is down

Instructional Text:

Probable Cause(s): 1. User configuration must not have done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: New users cannot be registered

Suggested Action(s): 1. Configuration errors: Most common issues are: Test user password is invalid or expired, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availability: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution errors or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responded to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Metric: TargetFqdn

Description: This is the key for metric

Metric SpecName: TargetFqdn

Metric Field Name: TargetFqdn

Data type: TEXT

Alarm: FALSE

Metric: PresenceLatency

Description: This metric will capture latency in the notification of presence of the user

Metric SpecName: PresenceLatency

Metric Field Name: PresenceLatency

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1000, Major / 1000

Policy: MSBS_PresenceLatency

Message text: The value of Presence Latency (ms) is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): 1. User configuration not done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: Users would not be able to avail peer to peer services

Suggested Action(s): 1. Configuration : Most common issues are invalid or expired Test user password, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availability: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution error or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responds to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Metric: Presence

Description: This metric gathers the information which confirms that users are able contact. It monitor the exchange of presence information between two test users in a Lync pool. The following functions are tested • Sign on to the Lync Server • Request for presence information • Publishing of presence information • Receipt of presence information •Log out

Metric SpecName: Presence

Metric Field Name: Presence

Data type: TEXT

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_Presence

Message text: The Presence is down

Instructional Text:

Probable Cause(s): 1. User configuration must not have done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: New users cannot be registered

Suggested Action(s): 1. Configuration errors: Most common issues are: Test user password is invalid or expired, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availability: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution errors or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responded to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Metric: TargetFqdn

Description: This is the key for metric

Metric SpecName: TargetFqdn

Metric Field Name: TargetFqdn

Data type: TEXT

Alarm: FALSE

SimplePortWatcher5064

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / Port5064

Source / Collection Definition: PORTCOL / PORTCHECKER

Metric: SimpleWatcherPort5064

Description: Used for incoming SIP requests for dial-in conferencing.

Metric SpecName: SimpleWatcherPort5064

Metric Field Name: SimpleWatcherPort5064

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort5064

Message text: The Port No:5064 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

Metric: SimpleWatcherPort5064

Description: Used for incoming SIP requests for dial-in conferencing.

Metric SpecName: SimpleWatcherPort5064

Metric Field Name: SimpleWatcherPort5064

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort5064

Message text: The Port No:5064 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

Collect_FrontEnd_Process_IMMCUSvc

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / CS_PROCESS

Source / Collection Definition: PERFMON / Process(IMMCUSvc)

Metric: FERTCIMMCUInstance

Description: instance of IMMCUSvc process

Metric SpecName: INSTANCENAME

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: FERTCIMMCUPercentprocessorTime

Description: Percentage Processor Time is the percentage of elapsed time that all of process threads used the processor to execution instructions.

Metric SpecName: PCTPROCESSORTIME

Metric Field Name: % Processor Time

Data type: UINT32

Alarm: FALSE

Metric: FERTCIMMCUWorkingSet

Description: Working Set is the current size, in bytes, of the Working Set of this process. the Working Set is the set of memory pages touched recently by the threads in the process. If free memory in the computer is above a threshold, pages are left in the Working Set of a process even if they are not in use. When free memory falls below a threshold, pages are trimmed from Working Sets. If they are needed they will then be soft-faulted back into the Working Set before leaving main memory.

Metric SpecName: WORKINGSET

Metric Field Name: Working Set

Data type: UINT32

Alarm: FALSE

Metric: FERTCIMMCUPageFaultsPerSec

Description: Page Faults/sec is the average number of pages faulted per second. It is measured in number of pages faulted per second because only one page is faulted in each fault operation, hence this is also equal to the number of page fault operations. This counter includes both hard faults (those that require disk access) and soft faults (where the faulted page is found elsewhere in physical memory.) Most processors can handle large numbers of soft faults without significant consequence. However, hard faults, which require disk access, can cause significant delays.

Metric SpecName: PAGEFAULTS

Metric Field Name: Page Faults/sec

Data type: UINT32

Alarm: FALSE

Metric: FERTCIMMCUPrivateBytes

Description: Private Bytes is the current size, in bytes, of memory that this process has allocated that cannot be shared with other processes.

Metric SpecName: PRIVATEBYTES

Metric Field Name: Private Bytes

Data type: UINT32

Alarm: FALSE

Metric: FERTCIMMCUThreadCount

Description: the number of threads currently active in this process. An instruction is the basic unit of execution in a processor, and a thread is the object that executes instructions. Every running process has at least one thread.

Metric SpecName: THREADCOUNT

Metric Field Name: Thread Count

Data type: UINT32

Alarm: FALSE

Metric: FERTCIMMCUInstance

Description: instance of IMMCUSvc process

Metric SpecName: INSTANCENAME

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: FERTCIMMCUPercentprocessorTime

Description: Percentage Processor Time is the percentage of elapsed time that all of process threads used the processor to execution instructions.

Metric SpecName: PCTPROCESSORTIME

Metric Field Name: % Processor Time

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 90

Policy: MSBS_FERTCIMMCUPercentprocessorTime

Message text: The value of the counter '% Processor Time' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: FERTCIMMCUWorkingSet

Description: Working Set is the current size, in bytes, of the Working Set of this process. the Working Set is the set of memory pages touched recently by the threads in the process. If free memory in the computer is above a threshold, pages are left in the Working Set of a process even if they are not in use. When free memory falls below a threshold, pages are trimmed from Working Sets. If they are needed they will then be soft-faulted back into the Working Set before leaving main memory.

Metric SpecName: WORKINGSET

Metric Field Name: Working Set

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20000000

Policy: MSBS_FERTCIMMCUWorkingSet

Message text: The value of the counter 'Working Set' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: FERTCIMMCUPageFaultsPerSec

Description: Page Faults/sec is the average number of pages faulted per second. It is measured in number of pages faulted per second because only one page is faulted in each fault operation, hence this is also equal to the number of page fault operations. This counter includes both hard faults (those that require disk access) and soft faults (where the faulted page is found elsewhere in physical memory.) Most processors can handle large numbers of soft faults without significant consequence. However, hard faults, which require disk access, can cause significant delays.

Metric SpecName: PAGEFAULTS

Metric Field Name: Page Faults/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 100

Policy: MSBS_FERTCIMMCUPageFaultsPerSec

Message text: The value of the counter 'Page Faults/sec' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: FERTCIMMCUPrivateBytes

Description: Private Bytes is the current size, in bytes, of memory that this process has allocated that cannot be shared with other processes.

Metric SpecName: PRIVATEBYTES

Metric Field Name: Private Bytes

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20000000

Policy: MSBS_FERTCIMMCUPrivateBytes

Message text: The value of the counter 'Private Bytes' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: FERTCIMMCUThreadCount

Description: the number of threads currently active in this process. An instruction is the basic unit of execution in a processor, and a thread is the object that executes instructions. Every running process has at least one thread.

Metric SpecName: THREADCOUNT

Metric Field Name: Thread Count

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 150

Policy: MSBS_FERTCIMMCUThreadCount

Message text: The value of the counter 'Thread Count' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

SimplePortWatcher8080

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / Port8080

Source / Collection Definition: PORTCOL / PORTCHECKER

Metric: SimpleWatcherPort8080

Description: Used by web components for external access.

Metric SpecName: SimpleWatcherPort8080

Metric Field Name: SimpleWatcherPort8080

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort8080

Message text: The Port No:8080 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

Metric: SimpleWatcherPort8080

Description: Used by web components for external access.

Metric SpecName: SimpleWatcherPort8080

Metric Field Name: SimpleWatcherPort8080

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort8080

Message text: The Port No:8080 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

MediationInbound

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: SKYPE / MEDIATIONINBOUND

Source / Collection Definition: PERFMON / LS:MediationServer - Inbound Calls(*)

Metric: InboundCurrent

Description: This metric captures Current Inbound Calls

Metric SpecName: InboundCurrent

Metric Field Name: - Current

Data type: UINT32

Alarm: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: TotalAttemptsInbound

Description: This metric captures Total Attempts at in bound calls

Metric SpecName: TotalAttemptsInbound

Metric Field Name: - Total Attempts

Data type: UINT32

Alarm: FALSE

Metric: TotalEstablished

Description: This metric captures Total Established Inbound Calls

Metric SpecName: TotalEstablished

Metric Field Name: - Total Established

Data type: UINT32

Alarm: FALSE

Metric: TotalRejectedDueToLoadIn

Description: This metric captures Total Inbound Calls Rejected Due To Load

Metric SpecName: TotlRejecteDueLoadIn

Metric Field Name: - Total Rejected Due To Load

Data type: UINT32

Alarm: FALSE

Metric: InboundCurrent

Description: This metric captures Current Inbound Calls

Metric SpecName: InboundCurrent

Metric Field Name: - 000 - Current

Data type: UINT32

Alarm: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: TotalAttemptsInbound

Description: This metric captures Total Attempts at in bound calls

Metric SpecName: TotalAttemptsInbound

Metric Field Name: - 002 - Total attempts

Data type: UINT32

Alarm: FALSE

Metric: TotalEstablished

Description: This metric captures Total Established Inbound Calls

Metric SpecName: TotalEstablished

Metric Field Name: - 001 - Total established

Data type: UINT32

Alarm: FALSE

Metric: TotalRejectedDueToLoadIn

Description: This metric captures Total Inbound Calls Rejected Due To Load

Metric SpecName: TotlRejecteDueLoadIn

Metric Field Name: - 003 - Total rejected due to load

Data type: UINT32

Alarm: FALSE

Metric: InboundCurrent

Description: This metric captures Current Inbound Calls

Metric SpecName: InboundCurrent

Metric Field Name: - Current

Data type: UINT32

Alarm: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: TotalAttemptsInbound

Description: This metric captures Total Attempts at in bound calls

Metric SpecName: TotalAttemptsInbound

Metric Field Name: - Total Attempts

Data type: UINT32

Alarm: FALSE

Metric: TotalEstablished

> **Description**: This metric captures Total Established Inbound Calls
>
> **Metric SpecName**: TotalEstablished
>
> **Metric Field Name**: - Total Established
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Metric: TotalRejectedDueToLoadIn

> **Description**: This metric captures Total Inbound Calls Rejected Due To Load
>
> **Metric SpecName**: TotlRejecteDueLoadIn
>
> **Metric Field Name**: - Total Rejected Due To Load
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

ExchangeUnifiedMessageConnectivityVoiceMail

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_LOW

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SYNNPDEXCUNIMSGCON

Source / Collection Definition: POWERSHELL / Test-CsExUMConnectivity -TargetFQDN {fqdn}

Metric: ExchangeUnifiedMessageConnectivityVoiceMail

Description: This metric gathers the information which confirms that a user can connect to Exchange Unified Messaging (UM).

Metric SpecName: ExchanUniMessConn

Metric Field Name: ExchangeUnifiedMessageConnectivityVoiceMail

Data type: TEXT

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Minor / 1

Policy: MSBS_ExchangeUnifiedMessageConnectivityVoiceMail

Message text: The Exchange Unified Message Connectivity VoiceMail is down

Instructional Text:

Probable Cause(s): 1. User configuration must not have done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: New users cannot be registered

Suggested Action(s): 1. Configuration errors: Most common issues are: Test user password is invalid or expired, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availability: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution errors or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responded to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Metric: TargetFqdn

Description: This is the key for metric

Metric SpecName: TargetFqdn

Metric Field Name: TargetFqdn

Data type: TEXT

Alarm: FALSE

Metric: ExchangeUnifiedMessageConnectivityVoiceMailLatency

Description: This metric will capture latency in receipt of confirmation that a user can connect to Exchange Unified Messaging (UM).

Metric SpecName: ExcUniMesConnLat

Metric Field Name: ExchangeUnifiedMessageConnectivityVoiceMailLatency

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Minor / 1000

Policy: MSBS_ExchangeUnifiedMessageConnectivityVoiceMailLatency

Message text: The value of Exchange Unified Message Connectivity VoiceMail Latency is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): 1. User configuration must not have done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: New users cannot be registered

Suggested Action(s): 1. Configuration errors: Most common issues are: Test user password is invalid or expired, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availibility: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution errors or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responded to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Collect_Edge_SIP_Load_Management

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / CS_FELOADMGMT

Source / Collection Definition: PERFMON / LS:SIP - Load Management(*)

Metric: EdgeSIPLoaManagementInstance

> **Description**: instance of perfmon object LS:SIP - Load Management
>
> **Metric SpecName**: SIPLOADMGMTINST
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: EdgeSIPLoadMgmtAvgHoldTimeForInMsgLogging

Description: the average time that the server held the incoming messages currently being processed.

Metric SpecName: HOLDINGTIMEFORINCMSG

Metric Field Name: SIP - Average Holding Time For Incoming Messages

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 3, Major / 9

Policy: MSBS_EdgeSIPLoadMgmtAvgHoldTimeForInMsgLogging

Message text: The value of SIP - Average Holding Time For Incoming Messages for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): This server is too busy and is unable to process user requests.

Potential Impact: NA

Suggested Action(s): This might be a temporary condition. If the problem persists, please ensure that hardware and software requirements for this server meet the user usage characteristics.

Metric: EdgeSIPIncomingMessagesTimedOut

Description: the number of incoming messages currently being held by the server for processing for more than the maximum tracking interval.

Metric SpecName: INCOMGMSGTIMEOUT

Metric Field Name: SIP - Incoming Messages Timed out

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 200, Major / 250

Policy: MSBS_EdgeSIPIncomingMessagesTimedOut

Message text: The value of SIP - Incoming Messages Timed out for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): This server is too busy and is unable to process user requests.

Potential Impact: NA

Suggested Action(s): This might be a temporary condition. If the problem persists, please ensure that hardware and software requirements for this server meet the user usage characteristics.

Metric: EdgeSIPLoaManagementInstance

Description: instance of perfmon object LS:SIP - Load Management

Metric SpecName: SIPLOADMGMTINST

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: EdgeSIPAddressspaceusage

Description: percentage of available address space currently in use by the server process.

Metric SpecName: ADDRSSPACEUSAGE

Metric Field Name: SIP - 009 - Address space usage

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 65, Major / 75

Policy: MSBS_EdgeSIPAddressspaceusage

Message text: The value of the counter 'Address space usage' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: IncomngMesgsAbovOvrloadWatermark

Description: number of incoming messages which are currently held by the server for processing for more than the overload watermark time threshold.

Metric SpecName: INCOMGMSGABVOVERLD

Metric Field Name: SIP - 005 - Incoming Messages Held Above Overload Watermark

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 40

Policy: MSBS_IncomngMesgsAbovOvrloadWatermark

Message text: The value of the counter 'Incoming Messages Held Above Overload Watermark' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

AudioRoundTripPoorCallsPercentage

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / ROUNDTRIPPOORCALLS

Source / Collection Definition: SQLDB / select isnull(cast(100.0 * cast((SUM(CASE WHEN [AudioRoundTrip]>[RoundTripOptimal] THEN 1 ELSE 0 END)) as float) / cast((SUM(CASE WHEN MediaLineLabel is NOT NULL THEN 1 ELSE 0 END)) as float) as decimal(4, 1)),0) as AudioRoundTripPoorCallsPercentage, SERVERPROPERTY('MACHINENAME') AS 'ServerName'

from [QoEMetrics].[dbo].[QoEReportsCallDetailView] Where MediaLineLabel = 0 AND ConferenceDateTime >= dateadd(MINUTE,@Duration,GETUTCDATE())

Metric: AudioRoundTripPoorCallsPercentage

> **Description**: This metric captures Poor Audio that have Network Packet Roundtrip Time more than a set threshold value and calculates percentage of poor calls for a given interval At the end of each call, parameters that determine Quality of a call that include network, audio and video parameters are logged into QoE database of Lync Server. Each call is categorized as having Acceptable quality or Poor quality based on the same.
>
> **Metric SpecName**: AudRoundTripPoorCall
>
> **Metric Field Name**: AudioRoundTripPoorCallsPercentage
>
> **Data type**: REAL64
>
> **Alarm**: TRUE
>
> **Category** : MSSkype
>
> **Severity / Threshold** : Warning / 40, Major / 70, Warning / 40, Major / 70
>
> **Policy**: MSBS_AudioRoundTripPoorCallsPercentage
>
> **Message text**: The current value of Percentage Audio Round Trip Poor Calls is <VALUE> which exceeds the threshold of <THRESHOLD>
>
> **Instructional Text**:
>
> **Probable Cause(s)**: High round-trip values can be caused by a routing misconfiguration, a long distance call or an overloaded media server.
>
> **Potential Impact**: -Poor Voice quality -Echo -Audio Latency
>
> **Suggested Action(s)**: Network upgrade Reconfigure routing rules

Metric: ServerName

> **Description**: This is the key for metric
>
> **Metric SpecName**: ServerName
>
> **Metric Field Name**: ServerName
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: AudioRoundTripPoorCallsPercentage

Description: This metric captures Poor Audio that have Network Packet Roundtrip Time more than a set threshold value and calculates percentage of poor calls for a given interval At the end of each call, parameters that determine Quality of a call that include network, audio and video parameters are logged into QoE database of Lync Server. Each call is categorized as having Acceptable quality or Poor quality based on the same.

Metric SpecName: AudRoundTripPoorCall

Metric Field Name: AudioRoundTripPoorCallsPercentage

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 40, Major / 70, Warning / 40, Major / 70

Policy: MSBS_AudioRoundTripPoorCallsPercentage

Message text: The current value of Percentage Audio Round Trip Poor Calls is <VALUE> which exceeds the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): High round-trip values can be caused by a routing misconfiguration, a long distance call or an overloaded media server.

Potential Impact: -Poor Voice quality -Echo -Audio Latency

Suggested Action(s): Network upgrade Reconfigure routing rules

Metric: ServerName

Description: This is the key for metric

Metric SpecName: ServerName

Metric Field Name: ServerName

Data type: TEXT

Alarm: FALSE

Collect_FrontEnd_DataMCU_HealthAndPerformance

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / NA

Source / Collection Definition: PERFMON / LS:DATAMCU - 04 - MCU Health And Performance(*)

Metric: MCUHealthStateInstance

> **Description**: instance of perfmon object LS:DATAMCU - 04 - MCU Health And Performance
>
> **Metric SpecName**: HEALTHSTATEINSTANCE
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: MCUHealthState

Description: DATAMCU's current health. The value od 0 signifies normal , 1 signifies loaded , 2 signifies full and 3 signifies unavailable of MCU

Metric SpecName: MCUHEALTHSTATE

Metric Field Name: DATAMCU - 005 - MCU Health State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 1, Major / 2

Policy: MSBS_MCUHealthState

Message text: The value of the counter 'DATAMCU - 005 - MCU Health State' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Collect_FrontEnd_Process_FileTransferAgent

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / CS_PROCESS

Source / Collection Definition: PERFMON / Process(FileTransferAgent)

Metric: FEFTAInstance

Description: instance of FileTransferAgent process

Metric SpecName: INSTANCENAME

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: FEFTAPercentprocessorTime

Description: Percentage Processor Time is the percentage of elapsed time that all of process threads used the processor to execution instructions.

Metric SpecName: PCTPROCESSORTIME

Metric Field Name: % Processor Time

Data type: UINT32

Alarm: FALSE

Metric: FEFTAWorkingSet

Description: Working Set is the current size, in bytes, of the Working Set of this process. the Working Set is the set of memory pages touched recently by the threads in the process. If free memory in the computer is above a threshold, pages are left in the Working Set of a process even if they are not in use. When free memory falls below a threshold, pages are trimmed from Working Sets. If they are needed they will then be soft-faulted back into the Working Set before leaving main memory.

Metric SpecName: WORKINGSET

Metric Field Name: Working Set

Data type: UINT32

Alarm: FALSE

Metric: FEFTAPageFaultsPerSec

Description: Page Faults/sec is the average number of pages faulted per second. It is measured in number of pages faulted per second because only one page is faulted in each fault operation, hence this is also equal to the number of page fault operations. This counter includes both hard faults (those that require disk access) and soft faults (where the faulted page is found elsewhere in physical memory.) Most processors can handle large numbers of soft faults without significant consequence. However, hard faults, which require disk access, can cause significant delays.

Metric SpecName: PAGEFAULTS

Metric Field Name: Page Faults/sec

Data type: UINT32

Alarm: FALSE

Metric: FEFTAPrivateBytes

Description: Private Bytes is the current size, in bytes, of memory that this process has allocated that cannot be shared with other processes.

Metric SpecName: PRIVATEBYTES

Metric Field Name: Private Bytes

Data type: UINT32

Alarm: FALSE

Metric: FEFTAThreadCount

Description: the number of threads currently active in this process. An instruction is the basic unit of execution in a processor, and a thread is the object that executes instructions. Every running process has at least one thread.

Metric SpecName: THREADCOUNT

Metric Field Name: Thread Count

Data type: UINT32

Alarm: FALSE

Metric: FEFTAInstance

Description: instance of FileTransferAgent process

Metric SpecName: INSTANCENAME

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: FEFTAPercentprocessorTime

Description: Percentage Processor Time is the percentage of elapsed time that all of process threads used the processor to execution instructions.

Metric SpecName: PCTPROCESSORTIME

Metric Field Name: % Processor Time

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 90

Policy: MSBS_FEFTAPercentprocessorTime

Message text: The value of the counter '% Processor Time' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: FEFTAWorkingSet

Description: Working Set is the current size, in bytes, of the Working Set of this process. the Working Set is the set of memory pages touched recently by the threads in the process. If free memory in the computer is above a threshold, pages are left in the Working Set of a process even if they are not in use. When free memory falls below a threshold, pages are trimmed from Working Sets. If they are needed they will then be soft-faulted back into the Working Set before leaving main memory.

Metric SpecName: WORKINGSET

Metric Field Name: Working Set

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20000000

Policy: MSBS_FEFTAWorkingSet

Message text: The value of the counter 'Working Set' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: FEFTAPageFaultsPerSec

Description: Page Faults/sec is the average number of pages faulted per second. It is measured in number of pages faulted per second because only one page is faulted in each fault operation, hence this is also equal to the number of page fault operations. This counter includes both hard faults (those that require disk access) and soft faults (where the faulted page is found elsewhere in physical memory.) Most processors can handle large numbers of soft faults without significant consequence. However, hard faults, which require disk access, can cause significant delays.

Metric SpecName: PAGEFAULTS

Metric Field Name: Page Faults/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 100

Policy: MSBS_FEFTAPageFaultsPerSec

Message text: The value of the counter 'Page Faults/sec' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: FEFTAPrivateBytes

Description: Private Bytes is the current size, in bytes, of memory that this process has allocated that cannot be shared with other processes.

Metric SpecName: PRIVATEBYTES

Metric Field Name: Private Bytes

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20000000

Policy: MSBS_FEFTAPrivateBytes

Message text: The value of the counter 'Private Bytes' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: FEFTAThreadCount

Description: the number of threads currently active in this process. An instruction is the basic unit of execution in a processor, and a thread is the object that executes instructions. Every running process has at least one thread.

Metric SpecName: THREADCOUNT

Metric Field Name: Thread Count

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 150

Policy: MSBS_FEFTAThreadCount

Message text: The value of the counter 'Thread Count' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

WEBDeviceUpdate

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: SKYPE / WEBDEVICEUPDATE

Source / Collection Definition: PERFMON / LS:WEB - 07 - Device Update(*)

Metric: TotalLogUploadAttempts

Description: This metric captures Total Log Upload Attempts

Metric SpecName: TtlLogUploadAttempts

Metric Field Name: WEB - 003 - Total Log Upload Attempts

Data type: UINT32

Alarm: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: TotalUpdateRequests

Description: This metric captures Total Update Requests

Metric SpecName: TotalUpdateRequests

Metric Field Name: WEB - 001 - Total Update Requests

Data type: UINT32

Alarm: FALSE

Metric: TotalLogUploadAttempts

Description: This metric captures Total Log Upload Attempts

Metric SpecName: TtlLogUploadAttempts

Metric Field Name: WEB - Total Log Upload Attempts

Data type: UINT32

Alarm: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: TotalRequestsReceived

Description: This metric captures Total Requests Received

Metric SpecName: TotalRequestsReceive

Metric Field Name: WEB - Total Requests Received

Data type: UINT32

Alarm: FALSE

Metric: TotalUpdateRequests

Description: This metric captures Total Update Requests

Metric SpecName: TotalUpdateRequests

Metric Field Name: WEB - Total Update Requests

Data type: UINT32

Alarm: FALSE

Memory

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / KHIMEMORY

Source / Collection Definition: PERFMON / Memory(*)

Metric: Memory

> **Description**: This policy monitors displays the bytes of physical memory available to processes running on the computer.
>
> **Metric SpecName**: Memory
>
> **Metric Field Name**: Available Mbytes
>
> **Data type**: UINT32
>
> **Alarm**: TRUE
>
> **Category** : MSSkype
>
> **Severity / Threshold** : Major / 2.5, Major / 2.5
>
> **Policy**: MSBS_Memory
>
> **Message text**: The current value of Memory is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:
>
> **Instructional Text**:
>
> **Probable Cause(s)**: Low available physical memory can be because of the following reasons: Too many applications are running simultaneously on the computer. An application may be leaking memory over time.
>
> **Potential Impact**: To address a low physical memory condition an administrator may chose one or more of the following options: Close or stop one or more applications, services, processes. Add additional Physical Memory to the computer. Move applications to one or more additional servers.
>
> **Suggested Action(s)**: Memory starvation by processes which can lead to deadlocks and slow processing.

Metric: Instance_Name

> **Description**: This is the key for metric
>
> **Metric SpecName**: Instance_Name
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: Memory

Description: This policy monitors displays the bytes of physical memory available to processes running on the computer.

Metric SpecName: Memory

Metric Field Name: Available Mbytes

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 2.5, Major / 2.5

Policy: MSBS_Memory

Message text: The current value of Memory is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): Low available physical memory can be because of the following reasons: Too many applications are running simultaneously on the computer. An application may be leaking memory over time.

Potential Impact: To address a low physical memory condition an administrator may chose one or more of the following options: Close or stop one or more applications, services, processes. Add additional Physical Memory to the computer. Move applications to one or more additional servers.

Suggested Action(s): Memory starvation by processes which can lead to deadlocks and slow processing.

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

DATAMCUConference

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: SKYPE / DATAMCUCOFERENCE

Source / Collection Definition: PERFMON / LS:DATAMCU - 00 - DataMCU Conferences(*)

Metric: ActiveConferences

> **Description**: This metric captures Active Conferences
>
> **Metric SpecName**: ActiveConferences
>
> **Metric Field Name**: DATAMCU - 003 - Active Conferences
>
> **Data type**: REAL64
>
> **Alarm**: FALSE

Metric: Instance_Name

> **Description**: This is the key for metric
>
> **Metric SpecName**: Instance_Name
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: AverageTimeQueuedInDataMcuForLDMMessages

Description: This metric captures Average Time Queued In Data Mcu For LDM Messages

Metric SpecName: AvgTimeQuDtMcuLDMMsg

Metric Field Name: DATAMCU - 014 - Average time queued in data Mcu for LDM messages

Data type: REAL64

Alarm: FALSE

Metric: BlockedFiles

Description: This metric captures Blocked Files

Metric SpecName: BlockedFiles

Metric Field Name: DATAMCU - 000 - Blocked files

Data type: REAL64

Alarm: FALSE

Metric: BlockedFilesPerSec

Description: This metric captures Blocked Files Per Sec

Metric SpecName: BlockedFilesPerSec

Metric Field Name: DATAMCU - 001 - Blocked files/sec

Data type: REAL64

Alarm: FALSE

Metric: ConferenceWorkitemsLoad

Description: This metric captures Conference Work items Load

Metric SpecName: ConfWorkitemsLoad

Metric Field Name: DATAMCU - 007 - Conference workitems load

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 1, Critical / 2, Warning / 1, Major / 2

Policy: MSBS_ConferenceWorkitemsLoad

Message text: The value of Estimated conference workitems load is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Failure to do an app sharing event may be because of policy violation, processing error, network overload, server overload etc

Potential Impact: Defining appropriate policy, troubleshoote network etc

Suggested Action(s): Users face issue in sharing desktop or other applications

Metric: NumberOfUnhandledApplicationException

Description: This metric captures Number Of Unhandled Application Exception

Metric SpecName: NumOfUnhandledAppExc

Metric Field Name: DATAMCU - 005 - Number of Unhandled Application Exception

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Critical / 10, Major / 10

Policy: MSBS_NumberOfUnhandledApplicationException

Message text: The number of Unhandled Application Exception is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Failure to do an app sharing event may be because of policy violation, processing error, network overload, server overload etc

Potential Impact: Defining appropriate policy, troubleshoote network etc

Suggested Action(s): Users face issue in sharing desktop or other applications

Metric: TotalDataArchivingEventsRecorded.

Description: This metric captures Total Data Archiving Events Recorded.

Metric SpecName: TotlDtArchEvRecorded

Metric Field Name: DATAMCU - 020 - Total data archiving events recorded.

Data type: REAL64

Alarm: FALSE

Metric: ActiveConferences

Description: This metric captures Active Conferences

Metric SpecName: ActiveConferences

Metric Field Name: DATAMCU - Active Conferences

Data type: REAL64

Alarm: FALSE

Metric: Instance_Name

> **Description**: This is the key for metric
>
> **Metric SpecName**: Instance_Name
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: AverageTimeQueuedInDataMcuForLDMMessages

> **Description**: This metric captures Average Time Queued In Data Mcu For LDM Messages
>
> **Metric SpecName**: AvgTimeQuDtMcuLDMMsg
>
> **Metric Field Name**: DATAMCU - Average Time Queued In Data Mcu For LDM Messages
>
> **Data type**: REAL64
>
> **Alarm**: FALSE

Metric: BlockedFiles

> **Description**: This metric captures Blocked Files
>
> **Metric SpecName**: BlockedFiles
>
> **Metric Field Name**: DATAMCU - Blocked Files
>
> **Data type**: REAL64
>
> **Alarm**: FALSE

Metric: BlockedFilesPerSec

> **Description**: This metric captures Blocked Files Per Sec
>
> **Metric SpecName**: BlockedFilesPerSec
>
> **Metric Field Name**: DATAMCU - Blocked Files/Sec
>
> **Data type**: REAL64
>
> **Alarm**: FALSE

Metric: ConferenceWorkitemsLoad

Description: This metric captures Conference Work items Load

Metric SpecName: ConfWorkitemsLoad

Metric Field Name: DATAMCU - Conference Workitems Load

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 1, Critical / 2, Warning / 1, Major / 2

Policy: MSBS_ConferenceWorkitemsLoad

Message text: The value of Estimated conference workitems load is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Failure to do an app sharing event may be because of policy violation, processing error, network overload, server overload etc

Potential Impact: Defining appropriate policy, troubleshoote network etc

Suggested Action(s): Users face issue in sharing desktop or other applications

Metric: NumberOfUnhandledApplicationException

Description: This metric captures Number Of Unhandled Application Exception

Metric SpecName: NumOfUnhandledAppExc

Metric Field Name: DATAMCU - Number Of Unhandled Application Exception

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Critical / 10, Major / 10

Policy: MSBS_NumberOfUnhandledApplicationException

Message text: The number of Unhandled Application Exception is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Failure to do an app sharing event may be because of policy violation, processing error, network overload, server overload etc

Potential Impact: Defining appropriate policy, troubleshoote network etc

Suggested Action(s): Users face issue in sharing desktop or other applications

Metric: TotalDataArchivingEventsRecorded.

Description: This metric captures Total Data Archiving Events Recorded.

Metric SpecName: TotlDtArchEvRecorded

Metric Field Name: DATAMCU - Total Data Archiving Events Recorded.

Data type: REAL64

Alarm: FALSE

XMPPInstantMessagingFederation

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_LOW

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SYNNPDXMPPINSMSGFED

Source / Collection Definition: POWERSHELL / Test-CsXmppIM -TargetFQDN {fqdn} -Receiver {receiveremail}

Metric: XMPPInstantMessagingFederation

Description: This metric gathers the information which confirms that an instant message can be sent across the XMPP (Extensible Messaging and Presence Protocol) gateway.

Metric SpecName: XMPPIMFed

Metric Field Name: XMPPInstantMessagingFederation

Data type: TEXT

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Minor / 1

Policy: MSBS_XMPPInstantMessagingFederation

Message text: The XMPP Instant Messaging Federation is down

Instructional Text:

Probable Cause(s): 1. User configuration must not have done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: New users cannot be registered

Suggested Action(s): 1. Configuration errors: Most common issues are: Test user password is invalid or expired, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availability: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution errors or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responded to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Metric: TargetFqdn

Description: This is the key for metric

Metric SpecName: TargetFqdn

Metric Field Name: TargetFqdn

Data type: TEXT

Alarm: FALSE

Metric: XMPPInstantMessagingFederationLatency

Description: This metric will capture latency in receipt of confirmation that an instant message can be sent across the XMPP (Extensible Messaging and Presence Protocol) gateway.

Metric SpecName: XMPPIMFedLat

Metric Field Name: XMPPInstantMessagingFederationLatency

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Minor / 1000

Policy: MSBS_XMPPInstantMessagingFederationLatency

Message text: The value of XMPP Instant Messaging Federation Latency is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): 1. User configuration must not have done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: New users cannot be registered

Suggested Action(s): 1. Configuration errors: Most common issues are: Test user password is invalid or expired, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availibility: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution errors or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responded to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Collect_Mediation_Global Per Gateway Counters

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / NA

Source / Collection Definition: PERFMON / LS:MediationServer - 05 - Global Per Gateway Counters(*)

Metric: MedGlobalPerGateWayCountersInstance

> **Description**: instance of perfmon object LS:MediationServer - 05 - Global Per Gateway Counters
>
> **Metric SpecName**: GLOBLGATEWAYINSTANCE
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: TotFaildCallsCausdbyUnexpctdIntefrmGateway

Description: number of call failures due to unexpected interaction with proxy

Metric SpecName: TOTFAILDCALLSBYUNEXPTDINTERCTNFGATEWAY

Metric Field Name: Total failed calls caused by unexpected interaction from a gateway

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 5, Major / 10

Policy: MSBS_TotFaildCallsCausdbyUnexpctdIntefrmGateway

Message text: The value of the counter 'Total failed calls caused by unexpected interaction from a gateway' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

VideoRoundTripPoorCallsPercentage

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / VIDEOROUNDTRIPCALLS

Source / Collection Definition: SQLDB / select isnull(cast(100.0 * cast((SUM(CASE WHEN [VideoRoundTrip] > [RoundTripOptimal] THEN 1 ELSE 0 END)) as float) / cast((SUM(CASE WHEN MediaLineLabel is NOT NULL THEN 1 ELSE 0 END)) as float) as decimal(4, 1)),0) as VideoRoundTripPoorCallsPercentage,SERVERPROPERTY('MACHINENAME') AS 'ServerName'

from [QoEMetrics].[dbo].[QoEReportsCallDetailView] Where MediaLineLabel IN (1,2) AND ConferenceDateTime >= dateadd(MINUTE,@Duration,GETUTCDATE())

Metric: VideoRoundTripPoorCallsPercentage

> **Description**: This metric captures Poor Video that have Network Packet Roundtrip Time more than a set threshold value and calculates percentage of poor calls for a given interval At the end of each call, parameters that determine Quality of a call that include network, audio and video parameters are logged into QoE database of Lync Server. Each call is categorized as having Acceptable quality or Poor quality based on the same.
>
> **Metric SpecName**: VidRoundTripPoorCall
>
> **Metric Field Name**: VideoRoundTripPoorCallsPercentage
>
> **Data type**: REAL64
>
> **Alarm**: TRUE
>
> **Category** : MSSkype
>
> **Severity / Threshold** : Warning / 40, Major / 70, Warning / 40, Major / 70
>
> **Policy**: MSBS_VideoRoundTripPoorCallsPercentage
>
> **Message text**: The current value of Percentage Video Round Trip Poor Calls is <VALUE> which exceeds the threshold of <THRESHOLD>
>
> **Instructional Text**:
>
> **Probable Cause(s)**: High round-trip values can be caused by a routing misconfiguration, a long distance call or an overloaded media server.
>
> **Potential Impact**: -Poor Voice quality - Distorted Video rendering
>
> **Suggested Action(s)**: Network upgrade -Reconfigure routing rules

Metric: ServerName

> **Description**: This is the key for metric
>
> **Metric SpecName**: ServerName
>
> **Metric Field Name**: ServerName
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: VideoRoundTripPoorCallsPercentage

Description: This metric captures Poor Video that have Network Packet Roundtrip Time more than a set threshold value and calculates percentage of poor calls for a given interval At the end of each call, parameters that determine Quality of a call that include network, audio and video parameters are logged into QoE database of Lync Server. Each call is categorized as having Acceptable quality or Poor quality based on the same.

Metric SpecName: VidRoundTripPoorCall

Metric Field Name: VideoRoundTripPoorCallsPercentage

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 40, Major / 70, Warning / 40, Major / 70

Policy: MSBS_VideoRoundTripPoorCallsPercentage

Message text: The current value of Percentage Video Round Trip Poor Calls is <VALUE> which exceeds the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): High round-trip values can be caused by a routing misconfiguration, a long distance call or an overloaded media server.

Potential Impact: -Poor Voice quality - Distorted Video rendering

Suggested Action(s): Network upgrade -Reconfigure routing rules

Metric: ServerName

Description: This is the key for metric

Metric SpecName: ServerName

Metric Field Name: ServerName

Data type: TEXT

Alarm: FALSE

Collect_Archiving_ArchService_WRITE

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / NA

Source / Collection Definition: PERFMON / LS:Arch Service - 02 - WRITE(*)

Metric: ArchServiceWriteInstance

> **Description**: instance of perfmon object LS:Arch Service - 02 - WRITE
>
> **Metric SpecName**: ARCHSERVCEWRITEINSTANCE
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: ArchServiceMessagesfailedtobewrittentoDB

Description: rate of failure in numbers when the messages are written in to SQL database

Metric SpecName: MSGFAILDWRITNTODB

Metric Field Name: Arch Service - 002 - Messages failed to be written to DB

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 0, Major / 1

Policy: MSBS_ArchServiceMessagesfailedtobewrittentoDB

Message text: The value of the counter 'Arch Service - 002 - Messages failed to be written to DB' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

SIPAuthentication

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: SKYPE / SIPAUTHENTICATION

Source / Collection Definition: PERFMON / LS:SIP - 06 - Authentication(*)

Metric: AuthenticationSystemErrorsPerSec

Description: This metric captures per-second rate of authentication failures caused by system errors

Metric SpecName: AuthSysErrorsPS

Metric Field Name: SIP - 031 - Authentication System Errors/sec

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Critical / 0, Major / 0

Policy: MSBS_AuthenticationSystemErrorsPerSec

Message text: The value of Authentication System Errors Per Second is <VALUE>

Instructional Text:

Probable Cause(s): This server may be experiencing problems when using Windows Authentication subsystem.

Potential Impact: Check that this server can reach its domain controller.

Suggested Action(s): Messages may not be received

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: IncomingMessagesNotAuthenticatedPerSec

Description: This metric captures per-second rate of incoming messages that could not be authenticated

Metric SpecName: IncomMsgNotAuthPS

Metric Field Name: SIP - 017 - Incoming Messages Not Authenticated/sec

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Critical / 0, Major / 0

Policy: MSBS_IncomingMessagesNotAuthenticatedPerSec

Message text: The value of Incoming Messages Not Authenticated Per Second is <VALUE>

Instructional Text:

Probable Cause(s): This server and users connecting to it may have mismatched authentication configuration.

Potential Impact: Check that users supply credentials that match this server authentication configuration.

Suggested Action(s): Messages may not be received

Metric: IncomingMessagesNotAuthorizedPerSec

Description: This metric captures per-second rate of incoming messages that could not be authorized.

Metric SpecName: IncomMsgNotAthrPS

Metric Field Name: SIP - 019 - Incoming Messages Not Authorized/sec

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Critical / 0, Major / 0

Policy: MSBS_IncomingMessagesNotAuthorizedPerSec

Message text: The value of Incoming Messages Not Authorized Per Second is <VALUE>

Instructional Text:

Probable Cause(s): This server and users connecting to it may have mismatched authentication configuration.

Potential Impact: Check that users supply credentials that match this server authentication configuration.

Suggested Action(s): Messages may not be received

Metric: AuthenticationSystemErrorsPerSec

Description: This metric captures per-second rate of authentication failures caused by system errors

Metric SpecName: AuthSysErrorsPS

Metric Field Name: SIP - Authentication System Errors/Sec

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Critical / 0, Major / 0

Policy: MSBS_AuthenticationSystemErrorsPerSec

Message text: The value of Authentication System Errors Per Second is <VALUE>

Instructional Text:

Probable Cause(s): This server may be experiencing problems when using Windows Authentication subsystem.

Potential Impact: Check that this server can reach its domain controller.

Suggested Action(s): Messages may not be received

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: IncomingMessagesNotAuthenticatedPerSec

Description: This metric captures per-second rate of incoming messages that could not be authenticated

Metric SpecName: IncomMsgNotAuthPS

Metric Field Name: SIP - Incoming Messages Not Authenticated/Sec

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Critical / 0, Major / 0

Policy: MSBS_IncomingMessagesNotAuthenticatedPerSec

Message text: The value of Incoming Messages Not Authenticated Per Second is <VALUE>

Instructional Text:

Probable Cause(s): This server and users connecting to it may have mismatched authentication configuration.

Potential Impact: Check that users supply credentials that match this server authentication configuration.

Suggested Action(s): Messages may not be received

Metric: IncomingMessagesNotAuthorizedPerSec

Description: This metric captures per-second rate of incoming messages that could not be authorized.

Metric SpecName: IncomMsgNotAthrPS

Metric Field Name: SIP - Incoming Messages Not Authorized/Sec

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Critical / 0, Major / 0

Policy: MSBS_IncomingMessagesNotAuthorizedPerSec

Message text: The value of Incoming Messages Not Authorized Per Second is <VALUE>

Instructional Text:

Probable Cause(s): This server and users connecting to it may have mismatched authentication configuration.

Potential Impact: Check that users supply credentials that match this server authentication configuration.

Suggested Action(s): Messages may not be received

Collect_FrontEnd_RichPresenceSubscribeSQLCalls

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / LSUSRVRICHPRSUBSCR

Source / Collection Definition: PERFMON / LS:USrv - Rich presence subscribe SQL calls(*)

Metric: RichpresenceSubscribeSQLCallInstance

Description: instance of perfmon object LS:USrv - Rich presence subscribe SQL calls

Metric SpecName: SUBSCSQLCALLINST

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: PollingSubscribeReqThrottledByDBStoreThrottle

Description: Per-second rate of polling subscribe requests throttled by the database store throttling mechanism.

Metric SpecName: REQTHROTBYDBSTORE

Metric Field Name: USrv - Polling subscribe requests throttled by database store throttle/Sec

Data type: UINT32

Alarm: FALSE

Metric: PollingSubscribeRequestsThrottledByQueueThrottle

Description: Per-second rate of polling subscribe requests throttled by the polling subscribe queue throttling mechanism.

Metric SpecName: REQTHROTBYPOLSUBSCR

Metric Field Name: USrv - Polling subscribe requests throttled by polling subscribe queue throttle/Sec

Data type: UINT32

Alarm: FALSE

Collect_Edge_AV_UDP_Counters

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / AVEDGEUDPCOUNTERS

Source / Collection Definition: PERFMON / LS:A/V Edge - UDP Counters(*)

Metric: AVEdgeUDPCounterInstance

> **Description**: instance of perfmon object LS:A/V Edge - UDP Counters
>
> **Metric SpecName**: AVUDPINSTANAME
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: AVEdgeUDPAllocateReqExceedPortLimit

> **Description**: Allocate Requests Exceeding Port Limit/sec over TCP
>
> **Metric SpecName**: REQEXCEEDPORTLIMIT
>
> **Metric Field Name**: A/V Edge - Allocate Requests Exceeding Port Limit/sec
>
> **Data type**: UINT32
>
> **Alarm**: TRUE
>
> **Category** : MSSkype
>
> **Severity / Threshold** : Warning / 10, Major / 20
>
> **Policy**: MSBS_AVEdgeUDPAllocateReqExceedPortLimit
>
> **Message text**: The value of A/V Edge - Allocate Requests Exceeding Port Limit/sec for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>
>
> **Instructional Text**:
>
> **Probable Cause(s)**: This error occurs when there is an unexpectedly high rate of requests over TCP for ports associated with the same user ID. .
>
> **Potential Impact**: NA
>
> **Suggested Action(s)**: Check that the profile of network traffic to the A/V Edge Server is in line with expected usage. A network level trace can be used to determine if there is unusual amount of traffic originating from a single source.

Metric: AVEdgeUDPAuthFailurePerSec

Description: Authentication Failures/sec over TCP

Metric SpecName: UDPAUTHFAILURE

Metric Field Name: A/V Edge - Authentication Failures/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 10, Major / 20

Policy: MSBS_AVEdgeUDPAuthFailurePerSec

Message text: The value of A/V Edge - Authentication Failures/sec for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): This error occurs when there is unexpectedly high rate of message authentication failures over TCP. This could be the result of a configuration error.

Potential Impact: NA

Suggested Action(s): If the A/V Edge Server is deployed in a load balanced array verify that the same authentication certificate is deployed on each machine. Check that the profile of network traffic to the A/V Edge Server is in line with expected usage.

Metric: AVEdgeUDPPacketsDroppedPerSec

Description: Packets Dropped/sec over TCP

Metric SpecName: UDPPACKETDROPPED

Metric Field Name: A/V Edge - Packets Dropped/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 300, Major / 400

Policy: MSBS_AVEdgeUDPPacketsDroppedPerSec

Message text: The value of A/V Edge - Packets Dropped/sec for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): This error occurs when an unexpectedly high rate of TCP packets is received at the A/V Edge Server causing some packets to be discarded.

Potential Impact: NA

Suggested Action(s): Check that the profile of network traffic to the A/V Edge Server is in line with expected usage.

Metric: AVEdgeUDPActSessionsExcceedingAvgBWLmt

Description: Active Sessions Exceeding Average Bandwidth Limit over TCP

Metric SpecName: UDPSESEXCEEDAVGBW

Metric Field Name: A/V Edge - Active Sessions Exceeding Avg Bandwidth Limit

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 10, Major / 20

Policy: MSBS_AVEdgeUDPActSessionsExcceedingAvgBWLmt

Message text: The value of A/V Edge - Active Sessions Exceeding Avg Bandwidth Limit for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): This error occurs when there is an unexpectedly high rate of traffic sent through the A/V Edge Server within a UDP session. These sessions will be throttled by the A/V Edge Server.

Potential Impact: NA

Suggested Action(s): Check that the profile of network traffic to the A/V Edge Server is in line with expected usage.

Metric: AVEdgeUDPActSessionsExcceedingPeakBWLmt

Description: Active Sessions Exceeding Peak Bandwidth Limit over TCP

Metric SpecName: UDPSESEXCEEDPKBW

Metric Field Name: A/V Edge - Active Sessions Exceeding Peak Bandwidth Limit

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 10, Major / 20

Policy: MSBS_AVEdgeUDPActSessionsExcceedingPeakBWLmt

Message text: The value of A/V Edge - Active Sessions Exceeding Peak Bandwidth Limit for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): This error occurs when there is an unexpectedly high rate of traffic sent through the A/V Edge Server within a UDP session. These sessions will be throttled by the A/V Edge Server.

Potential Impact: NA

Suggested Action(s): Check that the profile of network traffic to the A/V Edge Server is in line with expected usage.

Metric: AVEdgeUDPClientRequestErrorsPersecLogg

Description: The number of UDP client requests error's

Metric SpecName: CLIENTREQERRORPERSEC

Metric Field Name: A/V Edge - 014 - Client Request Errors/sec (4xx Responses/sec)

Data type: UINT32

Alarm: FALSE

Metric: AVEdgeUDPClientSendRequestErrorsLogg

> **Description**: The number of client request errors during a UDP session
>
> **Metric SpecName**: CLIENTSENDREQERROR
>
> **Metric Field Name**: A/V Edge - 017 - Client Send Request Errors/sec
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Metric: AVEdgeUDPSessionIdleTimeoutsPersecLogg

> **Description**: The number of UDP session time out per second
>
> **Metric SpecName**: SESSIONIDLETIMEOUT
>
> **Metric Field Name**: A/V Edge - 020 - Session Idle Timeouts/sec
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Peer2PeerMobileIM

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_LOW

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SYNP2PMOBILEIM

Source / Collection Definition: POWERSHELL / Test-CsMcxP2PIM -TargetFQDN {fqdn} -Authentication {Authentication} -SenderSipAddress {SenderSipAddress} -ReceiverSipAddress {receiversip}

Metric: Peer2PeerMobileIM

Description: This metric gathers the information which confirms that mobile device users are able to register and send instant messages. It will monitor the operation of instant messaging conferencing between two test mobile device users in a Lync pool. The following functions are tested: • Sign on to the Lync Server • Conference initiation • Conference invitation and joining • Message exchange through the conference • Conference disconnect and termination • Log out

Metric SpecName: Peer2PeerMobileIM

Metric Field Name: Peer2PeerMobileIM

Data type: TEXT

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_Peer2PeerMobileIM

Message text: The Peer To Peer Mobile IM is down

Instructional Text:

Probable Cause(s): 1. User configuration not done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: Users would not be able to avail peer to peer services

Suggested Action(s): 1. Configuration : Most common issues are invalid or expired Test user password, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availability: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution error or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responds to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Metric: ServerName

Description: This is the key for metric

Metric SpecName: ServerName

Metric Field Name: ServerName

Data type: TEXT

Alarm: FALSE

Metric: Peer2PeerMobileIMLatency

Description: This metric will capture the latency peer to peer Mobile IM.

Metric SpecName: P2PMobIMLat

Metric Field Name: Peer2PeerMobileIMLatency

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1000

Policy: MSBS_Peer2PeerMobileIMLatency

Message text: The value of Peer 2 Peer Mobile IM Latency is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): 1. User configuration must not have done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: New users cannot be registered

Suggested Action(s): 1. Configuration errors: Most common issues are: Test user password is invalid or expired, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availibility: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution errors or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responded to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

MRASRealTime

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: SKYPE / MRASREALTIME

Source / Collection Definition: PERFMON / LS:AVMCU - 02 - Informational(*)

Metric: TotalMRASRealTimeExceptions

> **Description**: This metric captures the number of MRAS Real Time Exceptions encountered by A/V Conferencing Server.
>
> **Metric SpecName**: TotalMRASRealTimeExc
>
> **Metric Field Name**: AVMCU - 017 - Total MRAS Real Time Exceptions
>
> **Data type**: REAL64
>
> **Alarm**: FALSE

Metric: Instance_Name

> **Description**: This is the key for metric
>
> **Metric SpecName**: Instance_Name
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: TotalMRASRealTimeExceptions

> **Description**: This metric captures the number of MRAS Real Time Exceptions encountered by A/V Conferencing Server.
>
> **Metric SpecName**: TotalMRASRealTimeExc
>
> **Metric Field Name**: AVMCU - Total MRAS Real Time Exceptions
>
> **Data type**: REAL64
>
> **Alarm**: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Collect_AvConf_Process_AVMCUSvc

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / CS_PROCESS

Source / Collection Definition: PERFMON / Process(AVMCUSvc)

Metric: AvConfAVMCUSvcInstance

Description: instance of perfmon object Process(AVMCUSvc)

Metric SpecName: INSTANCENAME

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: AvConfAVMCUSvcPageFaultsPersec

Description: Page Faults/sec counter available in the Lync Server Replica Replicator Agent service.

Metric SpecName: PAGEFAULTS

Metric Field Name: Page Faults/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 100

Policy: MSBS_AvConfAVMCUSvcPageFaultsPersec

Message text: The value of the counter 'Page Faults/sec' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: AvConfAVMCUSvcPrivateBytes

Description: Private Bytes counter available in the Lync Server Replica Replicator Agent service.

Metric SpecName: PRIVATEBYTES

Metric Field Name: Private Bytes

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20000000

Policy: MSBS_AvConfAVMCUSvcPrivateBytes

Message text: The value of the counter 'Private Bytes' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: AvConfAVMCUSvcProcessorTime

Description: the % Processor Time counter available in the Lync Server Replica Replicator Agent service.

Metric SpecName: PROCESSORTIME

Metric Field Name: % Processor Time

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 90

Policy: MSBS_AvConfAVMCUSvcProcessorTime

Message text: The value of the counter '% Processor Time' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: AvConfAVMCUSvcThreadCount

Description: Thread Count counter available Lync Server Replica Replicator Agent service

Metric SpecName: THREADCOUNT

Metric Field Name: Thread Count

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 150

Policy: MSBS_AvConfAVMCUSvcThreadCount

Message text: The value of the counter 'Thread Count' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: AvConfAVMCUSvcWorkingSet

Description: Working Set Counter available in the Lync Server Replica Replicator Agent service.

Metric SpecName: WORKINGSET

Metric Field Name: Working Set

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20000000

Policy: MSBS_AvConfAVMCUSvcWorkingSet

Message text: The value of the counter 'Working Set' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

InstantMessagingFailurePercentage

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / INSTANTMESSAGING

Source / Collection Definition: SQLDB / select isnull(cast(100.0 * cast((SUM(CASE WHEN SD.ResponseCode != 200 THEN 1 ELSE 0 END)) as float) / cast((SUM(CASE WHEN SD.ResponseCode is NOT NULL THEN 1 ELSE 0 END)) as float) as decimal(4, 1)),0) as InstantMessagingFailurePercentage,SERVERPROPERTY('MACHINENAME') AS 'ServerName'

from [LcsCDR].[dbo].SessionDetails SD LEFT OUTER JOIN [LcsCDR].[dbo].Media M ON SD.SessionIdTime = M.SessionIdTime LEFT OUTER JOIN [LcsCDR].[dbo].MediaList ML ON M.MediaId = ML.MediaId Where ML.MediaId = 1 AND SD.SessionIdTime >= dateadd (MINUTE,@Duration,GETUTCDATE())

Metric: InstantMessagingFailurePercentage

Description: This metric captures call failures periodically from the CDR database and raises an alert whenever call failures exceed the specified "threshold" percentage value. When an Instant Messaging session fails, this failure is reported to the Monitoring Server database (Call Detail Records database).

Metric SpecName: IMFailPer

Metric Field Name: InstantMessagingFailurePercentage

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 40, Major / 70, Warning / 40, Major / 70

Policy: MSBS_InstantMessagingFailurePercentage

Message text: The current value of Percentage Instant Messaging Failure is <VALUE> which exceeds the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): An IM Session may fail because of session time expiration, conference deletion ,policy violation by message , request timeout, unsupported message type etc

Potential Impact: Users face issue in connecting an IM or sending some types of message content

Suggested Action(s): Defining appropriate message content, configuring server for timeouts etc

Metric: ServerName

Description: This is the key for metric

Metric SpecName: ServerName

Metric Field Name: ServerName

Data type: TEXT

Alarm: FALSE

SimplePortWatcher135

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / Port135

Source / Collection Definition: PORTCOL / PORTCHECKER

Metric: SimpleWatcherPort135

Description: Used for DCOM based operations such as Moving Users, User Replicator Synchronization, and Address Book Synchronization.

Metric SpecName: SimpleWatcherPort135

Metric Field Name: SimpleWatcherPort135

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_SimpleWatcherPort135

Message text: The Port No:135 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

Metric: SimpleWatcherPort135

Description: Used for DCOM based operations such as Moving Users, User Replicator Synchronization, and Address Book Synchronization.

Metric SpecName: SimpleWatcherPort135

Metric Field Name: SimpleWatcherPort135

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_SimpleWatcherPort135

Message text: The Port No:135 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

> **Description**: This is the key for metric
>
> **Metric SpecName**: HOSTNAME
>
> **Metric Field Name**: HOSTNAME
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

SimplePortWatcher5081

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / Port5081

Source / Collection Definition: PORTCOL / PORTCHECKER

Metric: SimpleWatcherPort5081

Description: Used for outgoing SIP requests from the Mediation Server to the PSTN gateway.

Metric SpecName: SimpleWatcherPort5081

Metric Field Name: SimpleWatcherPort5081

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort5081

Message text: The Port No:5081 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

LoadCallFailureIndex

This policy maintains the information about the status for the different services

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_ConferenceProcPerform_2010_Conf

Aspect: Skype Conference Processing Performance

CIT: Mediation Server, Front End Server, Edge Server

Data source / Data class: SKYPE / LOADCALLFAILINDEX

Source / Collection Definition: PERFMON / LS:MediationServer - Health Indices(*)

Metric: LoadCallFailureIndex

Description: This metric captures Load Call Failure Index

Metric SpecName: LoadCallFailIndex

Metric Field Name: - Load Call Failure Index

Data type: REAL64

Alarm: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: LoadCallFailureIndex

> **Description**: This metric captures Load Call Failure Index
>
> **Metric SpecName**: LoadCallFailIndex
>
> **Metric Field Name**: - Load Call Failure Index
>
> **Data type**: REAL64
>
> **Alarm**: FALSE

Metric: Instance_Name

> **Description**: This is the key for metric
>
> **Metric SpecName**: Instance_Name
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

AVMCUConferences

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: SKYPE / AVMCUCONFERENCES

Source / Collection Definition: PERFMON / LS:AVMCU - 00 - Operations(*)

Metric: NumberOfConferences

Description: This metric captures the number of active conferences on the A/V Conferencing Server.

Metric SpecName: NumberOfConferences

Metric Field Name: AVMCU - 000 - Number of Conferences

Data type: UINT32

Alarm: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: NumberOfTrustedUsers

Description: This metric captures current count of active trusted users in A/V Conferencing Server.

Metric SpecName: NumberOfTrustedUsrs

Metric Field Name: AVMCU - 002 - Number of Trusted Users

Data type: UINT32

Alarm: FALSE

Metric: NumberOfUsers

Description: This metric captures Counter provides current count of active users in A/V Conferencing Server.

Metric SpecName: NumberOfUsers

Metric Field Name: AVMCU - 001 - Number of Users

Data type: UINT32

Alarm: FALSE

Metric: NumberOfConferences

Description: This metric captures the number of active conferences on the A/V Conferencing Server.

Metric SpecName: NumberOfConferences

Metric Field Name: IMMCU - Active Conferences

Data type: UINT32

Alarm: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: NumberOfTrustedUsers

Description: This metric captures current count of active trusted users in A/V Conferencing Server.

Metric SpecName: NumberOfTrustedUsrs

Metric Field Name: IMMCU - Connected Users

Data type: UINT32

Alarm: FALSE

Metric: NumberOfUsers

Description: This metric captures Counter provides current count of active users in A/V Conferencing Server.

Metric SpecName: NumberOfUsers

Metric Field Name: IMMCU - MCU Health State Changed Count

Data type: UINT32

Alarm: FALSE

MSSQL

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / KHIMSSQL

Source / Collection Definition: PERFMON / MSSQL$RTCLOCAL:Buffer Manager(*)

Metric: RtclocalPagelifeexpectancy

Description: This policy monitors how many seconds SQL Server expects a data page to stay in cache.

Metric SpecName: RtcloPagelifeexp

Metric Field Name: Page life expectancy

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 300

Policy: MSBS_RtclocalPagelifeexpectancy

Message text: The current value of RtclocalPagelifeexpectancy is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): Too small memory on the system Too small memory configured for SQL Server's use Poor index design

Potential Impact: Check I/O system to verify how it handles the load, if values of Avg. Disk sec/Read and Avg. Disk sec/Write counters for object PhysicalDisk are high (usually higher than 10 msec.), it means your system may overloaded or opportunities exist for query and index improvement.Buffer Pool can be overloaded because SQL Server works with high amount of tables simultaneously, or full scanning is used in place of search by criteria. Check SQL Server:Access Methods:Full Scans/sec counter to verify the problem.You may use SQL Server Profiler and browse Showplan Statistics in the Performance category to find an application that cause full scanning.

Suggested Action(s): Low cache data may lead to delayed data requests

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: LynclocalPagelifeexpectancy

Description: This policy monitors how many seconds SQL Server expects a data page to stay in cache.

Metric SpecName: LyncloPagelifeexp

Metric Field Name: Page life expectancy

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 300

Policy: MSBS_LynclocalPagelifeexpectancy

Message text: The current value of LynclocalPagelifeexpectancy is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): Too small memory on the system Too small memory configured for SQL Server's use Poor index design

Potential Impact: Check I/O system to verify how it handles the load, if values of Avg. Disk sec/Read and Avg. Disk sec/Write counters for object PhysicalDisk are high (usually higher than 10 msec.), it means your system may overloaded or opportunities exist for query and index improvement.Buffer Pool can be overloaded because SQL Server works with high amount of tables simultaneously, or full scanning is used in place of search by criteria. Check SQL Server:Access Methods:Full Scans/sec counter to verify the problem.You may use SQL Server Profiler and browse Showplan Statistics in the Performance category to find an application that cause full scanning.

Suggested Action(s): Low cache data may lead to delayed data requests

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Collect_EdgeAddressBook_File_Download

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / EDGLSWEBADDRBKDNL

Source / Collection Definition: PERFMON / LS:WEB - Address Book File Download(*)

Metric: EdgeAddressBookDownloadInstance

> **Description**: instance of perfmon object LS:WEB - Address Book File Download
>
> **Metric SpecName**: ADEDWEBINSTANCE
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: EdgeFailedRequestsperSecond

Description: the per-second rate of failed Address Book file requests

Metric SpecName: EDGFAILEDREQUESTS

Metric Field Name: WEB - Failed File Requests/Second

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 3, Major / 6

Policy: MSBS_EdgeFailedRequestsperSecond

Message text: The value of Failed File Requests/Second for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Caused by authentication issues or network connectivity issues

Potential Impact: NA

Suggested Action(s): Check Lync Server event log for failure causes and correct

Peer2PeerAudioVideo

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_LOW

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SYNP2PAV

Source / Collection Definition: POWERSHELL / Test-CsP2PAV -TargetFQDN ${fqdn}

Metric: Peer2PeerAudioVideo

Description: This metric gathers the information which confirms that users are able to place peer-to-peer audio calls (signaling only). It will monitor the operation of peer-to-peer audio/video conversation between two test users in a Lync pool. The following functions are tested: • Sign on to the Lync Server • Invitation and acceptance to conduct an audio/video call • Connection test • Call termination •Log out

Metric SpecName: Peer2PeerAudioVideo

Metric Field Name: Peer2PeerAudioVideo

Data type: TEXT

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_Peer2PeerAudioVideo

Message text: The Peer To Peer Audio Video is down

Instructional Text:

Probable Cause(s): 1. User configuration not done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: Users would not be able to avail peer to peer services

Suggested Action(s): 1. Configuration : Most common issues are invalid or expired Test user password, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availability: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution error or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responds to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Metric: ServerName

Description: This is the key for metric

Metric SpecName: ServerName

Metric Field Name: ServerName

Data type: TEXT

Alarm: FALSE

Metric: PeerToPeerAudioVideoLatency

Description: This metric will capture the latency peer to peer audio/video transaction

Metric SpecName: PeerToPeer AudVidLat

Metric Field Name: PeerToPeerAudioVideoLatency

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1000, Major / 1000

Policy: MSBS_PeerToPeerAudioVideoLatency

Message text: The value of Peer To Peer Audio Video Latency(ms) is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): 1. User configuration not done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: Users would not be able to avail peer to peer services

Suggested Action(s): 1. Configuration : Most common issues are invalid or expired Test user password, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availability: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution error or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responds to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Metric: Peer2PeerAudioVideo

Description: This metric gathers the information which confirms that users are able to place peer-to-peer audio calls (signaling only). It will monitor the operation of peer-to-peer audio/video conversation between two test users in a Lync pool. The following functions are tested: • Sign on to the Lync Server • Invitation and acceptance to conduct an audio/video call • Connection test • Call termination •Log out

Metric SpecName: Peer2PeerAudioVideo

Metric Field Name: Peer2PeerAudioVideo

Data type: TEXT

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_Peer2PeerAudioVideo

Message text: The Peer To Peer Audio Video is down

Instructional Text:

Probable Cause(s): 1. User configuration not done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: Users would not be able to avail peer to peer services

Suggested Action(s): 1. Configuration : Most common issues are invalid or expired Test user password, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availability: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution error or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responds to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Metric: ServerName

Description: This is the key for metric

Metric SpecName: ServerName

Metric Field Name: ServerName

Data type: TEXT

Alarm: FALSE

Metric: PeerToPeerAudioVideoLatency

Description: This metric will capture the latency peer to peer audio/video transaction

Metric SpecName: PeerToPeer AudVidLat

Metric Field Name: PeerToPeerAudioVideoLatency

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1000, Major / 1000

Policy: MSBS_PeerToPeerAudioVideoLatency

Message text: The value of Peer To Peer Audio Video Latency(ms) is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): 1. User configuration not done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: Users would not be able to avail peer to peer services

Suggested Action(s): 1. Configuration : Most common issues are invalid or expired Test user password, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availability: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution error or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responds to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

ChkFrontEndXMPPTranslatingGatewayServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SERVSTAT

Source / Collection Definition: SERVICECHECK / RTCXMPPTGW

Metric: FERTCXMPPTGWServName

> **Description**: Name of the Service
>
> **Metric SpecName**: SERVNAME
>
> **Metric Field Name**: Service_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FERTCXMPPTGWServDisplayName

> **Description**: Display Name of the Service
>
> **Metric SpecName**: SRVDISPNAME
>
> **Metric Field Name**: Service_Displayname
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FERTCXMPPTGWServStatus

> **Description**: Status of the Service
>
> **Metric SpecName**: SERVSTATUS
>
> **Metric Field Name**: Service_Status
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FERTCXMPPTGWServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_FERTCXMPPTGWServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): Lync Server XMPP Translating Gateway' Windows Service is stopped.

Potential Impact: NA

Suggested Action(s): Lync Server XMPP Translating Gateway' Windows Service is stopped. Please restart the service.

MWINOTIFYsReceivedPerSec

This policy maintains the information about the status for the different services

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_SubscribedUser_Conf

Aspect: Skype Subscribed User

CIT: Front End Server

Data source / Data class: LYNC / MWINOTIFYSRECEIVEPS

Source / Collection Definition: PERFMON / LS:USrv - Service(*)

Metric: MWINOTIFYsReceivedPerSec

Description: This metric captures MWI NOTIFYs Received Per Sec

Metric SpecName: MWINOTIFYsReceivePS

Metric Field Name: USrv - MWI NOTIFYs Received/Sec

Data type: REAL64

Alarm: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

SIPDNSConnection

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SIPDNSCONNECTION

Source / Collection Definition: PERFMON / LS:SipEps - SipEps Connections(*)

Metric: NumberOfDNSResolutionFailures

Description: This metric captures Number Of DNS Resolution Failures

Metric SpecName: NumOfDNSResolFail

Metric Field Name: SipEps - NumberOfDNSResolutionFailures

Data type: UINT32

Alarm: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: NumberOfDNSResolutionFailuresPerSecond

Description: This metric captures Number Of DNS Resolution Failures Per Second

Metric SpecName: NumOfDNSResolFailPS

Metric Field Name: SipEps - NumberOfDNSResolutionFailuresPerSecond

Data type: REAL64

Alarm: FALSE

PoorStreamsBtwnMediationAndGatewayPercentage

The policy contains the metric definition xml which will get used by Microsoft Collector to collect metrics.

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / STRBTWNMEDANDGATE

Source / Collection Definition: SQLDB / select (SELECT SERVERPROPERTY ('MACHINENAME')) AS 'ServerName', isnull((100 * (select SUM(case when (PacketLossRate > .01 OR PacketLossRateMax > .05) THEN 1 ELSE null END) as 'PoorCalls' FROM [Session] s WITH (NOLOCK) INNER JOIN [MediaLine] AS m WITH (NOLOCK) ON m.ConferenceDateTime = s.ConferenceDateTime AND m.SessionSeq = s.SessionSeq INNER JOIN [AudioStream] AS a WITH (NOLOCK) ON a.MediaLineLabel = m.MediaLineLabel and a.ConferenceDateTime = m.ConferenceDateTime and a.SessionSeq = m.SessionSeq INNER JOIN [UserAgent] AS CallerUA WITH (NOLOCK) ON CallerUA.UserAgentKey = s.CallerUserAgent INNER JOIN [UserAgent] AS CalleeUA WITH (NOLOCK) ON CalleeUA.UserAgentKey = s.CalleeUserAgent WHERE m.CallerInside = 1 AND m.CalleeInside = 1 and s.StartTime >= (dateadd (MINUTE,@Duration,GETUTCDATE())) AND s.StartTime < (dateadd(MINUTE,0,GETUTCDATE())) and ((CallerUA.UAType in (1) and CalleeUA.UAType in (32769)) or (CallerUA.UAType in (32769) and CalleeUA.UAType in (1))))) / ((select SUM(CASE WHEN s.ConferenceDateTime is not null THEN 1 ELSE null END) FROM [Session] s WITH (NOLOCK) INNER JOIN [MediaLine] AS m WITH (NOLOCK) ON m.ConferenceDateTime = s.ConferenceDateTime AND m.SessionSeq = s.SessionSeq INNER JOIN [AudioStream] AS a WITH (NOLOCK) ON a.MediaLineLabel = m.MediaLineLabel and a.ConferenceDateTime = m.ConferenceDateTime and a.SessionSeq = m.SessionSeq INNER JOIN [UserAgent] AS CallerUA WITH (NOLOCK) ON CallerUA.UserAgentKey = s.CallerUserAgent INNER JOIN [UserAgent] AS CalleeUA WITH (NOLOCK) ON CalleeUA.UserAgentKey = s.CalleeUserAgent WHERE m.CallerInside = 1 AND m.CalleeInside = 1 and s.StartTime >= (dateadd(MINUTE,@Duration,GETUTCDATE())) AND s.StartTime (dateadd(MINUTE,0,GETUTCDATE())) and ((CallerUA.UAType in (1) and CalleeUA.UAType in (32769)) or (CallerUA.UAType in (32769) and CalleeUA.UAType in (1)))),0) as 'PoorStreamsBtwnMediationAndGatewayPercentage'

Metric: PoorStreamsBtwnMediationAndGatewayPercentage

Description: This metric captures Poor Streams between Mediation and Gateway Server and calculates percentage for a given interval At the end of each call, parameters that determine Quality of a call that include network, audio and video parameters are logged into QoE database of Lync Server. Each call is categorized as having Acceptable quality or Poor quality based on the same.

Metric SpecName: PoorStrBtwMedAndGate

Metric Field Name: PoorStreamsBtwnMediationAndGatewayPercentage

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 40, Major / 70, Warning / 40, Major / 70

Policy: MSBS_PoorStreamsBtwnMediationAndGatewayPercentage

Message text: The Percentage of Poor Video that have Relative Network One Way Average Time is <VALUE> which exceeds the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): The reason would be an overloaded server.

Potential Impact: Poor Streams between Mediation and Gateway Server

Suggested Action(s): Ramp up server

Metric: ServerName

Description: This is the key for metric

Metric SpecName: ServerName

Metric Field Name: ServerName

Data type: TEXT

Alarm: FALSE

Metric: PoorStreamsBtwnMediationAndGatewayPercentage

Description: This metric captures Poor Streams between Mediation and Gateway Server and calculates percentage for a given interval At the end of each call, parameters that determine Quality of a call that include network, audio and video parameters are logged into QoE database of Lync Server. Each call is categorized as having Acceptable quality or Poor quality based on the same.

Metric SpecName: PoorStrBtwMedAndGate

Metric Field Name: PoorStreamsBtwnMediationAndGatewayPercentage

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 40, Major / 70, Warning / 40, Major / 70

Policy: MSBS_PoorStreamsBtwnMediationAndGatewayPercentage

Message text: The Percentage of Poor Video that have Relative Network One Way Average Time is <VALUE> which exceeds the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): The reason would be an overloaded server.

Potential Impact: Poor Streams between Mediation and Gateway Server

Suggested Action(s): Ramp up server

Metric: ServerName

Description: This is the key for metric

Metric SpecName: ServerName

Metric Field Name: ServerName

Data type: TEXT

Alarm: FALSE

AsMcuConferences

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: SKYPE / ASMCUCONFERENCES

Source / Collection Definition: PERFMON / LS:AsMcu - 00 - AsMcu Conferences(*)

Metric: ActiveAjaxViewers

> **Description**: This metric captures ASMCU - Active Ajax Viewers
>
> **Metric SpecName**: ActiveAjaxViewers
>
> **Metric Field Name**: ASMCU - 006 - Active Ajax Viewers
>
> **Data type**: REAL64
>
> **Alarm**: FALSE

Metric: Instance_Name

> **Description**: This is the key for metric
>
> **Metric SpecName**: Instance_Name
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: ActiveConferences

> **Description**: This metric captures ASMCU - Active Conferences
>
> **Metric SpecName**: ActiveConferencesAS
>
> **Metric Field Name**: ASMCU - 000 - Active Conferences
>
> **Data type**: REAL64
>
> **Alarm**: FALSE

Metric: ActiveDataChannels

Description: This metric captures ASMCU - Active Data Channels

Metric SpecName: ActiveDataChannels

Metric Field Name: ASMCU - 002 - Active Data Channels

Data type: REAL64

Alarm: FALSE

Metric: ActiveTranscoders

Description: This metric captures ASMCU - Active Transcoders

Metric SpecName: ActiveTranscoders

Metric Field Name: ASMCU - 001 - Active Transcoders

Data type: REAL64

Alarm: FALSE

Metric: ConnectedUsersASMCU

Description: This metric captures ASMCU - Connected Users

Metric SpecName: ConnectedUsersASMCU

Metric Field Name: ASMCU - 003 - Connected Users

Data type: REAL64

Alarm: FALSE

Metric: MediaTimeoutFailures

Description: This metric captures ASMCU - Media Timeout Failures

Metric SpecName: MediaTimeoutFailures

Metric Field Name: ASMCU - 029 - Media Timeout Failures

Data type: REAL64

Alarm: FALSE

Metric: PacketLossFailure

Description: This metric captures ASMCU - Packet Loss Failure

Metric SpecName: PacketLossFailure

Metric Field Name: ASMCU - 030 - Packet Loss Failure

Data type: REAL64

Alarm: FALSE

Metric: RdpConnectionTimeoutFailures

Description: This metric captures ASMCU - Rdp Connection Timeout Failures

Metric SpecName: RdpConnTimeoutFail

Metric Field Name: ASMCU - 032 - Rdp Connection Timeout Failures

Data type: REAL64

Alarm: FALSE

Metric: SipDialogFailures

Description: This metric captures ASMCU - Sip Dialog Failures

Metric SpecName: SipDialogFailures

Metric Field Name: ASMCU - 031 - Sip Dialog Failures

Data type: REAL64

Alarm: FALSE

Metric: ActiveAjaxTranscoders

Description: This metric captures Active Ajax Transcoders

Metric SpecName: ActiveAjaxTranscod

Metric Field Name: ASMCU - Active Ajax Transcoders

Data type: REAL64

Alarm: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: ActiveAjaxViewers

Description: This metric captures ASMCU - Active Ajax Viewers

Metric SpecName: ActiveAjaxViewers

Metric Field Name: ASMCU - Active Ajax Viewers

Data type: REAL64

Alarm: FALSE

Metric: ActiveConferences

Description: This metric captures ASMCU - Active Conferences

Metric SpecName: ActiveConferencesAS

Metric Field Name: ASMCU - Active Conferences

Data type: REAL64

Alarm: FALSE

Metric: ActiveDataChannels

Description: This metric captures ASMCU - Active Data Channels

Metric SpecName: ActiveDataChannels

Metric Field Name: ASMCU - Active Data Channels

Data type: REAL64

Alarm: FALSE

Metric: ActiveTranscoders

Description: This metric captures ASMCU - Active Transcoders

Metric SpecName: ActiveTranscoders

Metric Field Name: ASMCU - Active Transcoders

Data type: REAL64

Alarm: FALSE

Metric: ConnectedUsersASMCU

Description: This metric captures ASMCU - Connected Users

Metric SpecName: ConnectedUsersASMCU

Metric Field Name: ASMCU - Connected Users

Data type: REAL64

Alarm: FALSE

Metric: MediaTimeoutFailures

Description: This metric captures ASMCU - Media Timeout Failures

Metric SpecName: MediaTimeoutFailures

Metric Field Name: ASMCU - Media Timeout Failures

Data type: REAL64

Alarm: FALSE

Metric: PacketLossFailure

Description: This metric captures ASMCU - Packet Loss Failure

Metric SpecName: PacketLossFailure

Metric Field Name: ASMCU - Packet Loss Failure

Data type: REAL64

Alarm: FALSE

Metric: RdpConnectionTimeoutFailures

Description: This metric captures ASMCU - Rdp Connection Timeout Failures

Metric SpecName: RdpConnTimeoutFail

Metric Field Name: ASMCU - Rdp Connection Timeout Failures

Data type: REAL64

Alarm: FALSE

Metric: SipDialogFailures

Description: This metric captures ASMCU - Sip Dialog Failures

Metric SpecName: SipDialogFailures

Metric Field Name: ASMCU - Sip Dialog Failures

Data type: REAL64

Alarm: FALSE

InstantMessageConferencing

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_LOW

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SYNIMCONFERENCING

Source / Collection Definition: POWERSHELL / Test-CsGroupIm -TargetFQDN ${fqdn}

Metric: InstantMessageConferencing

Description: This metric gathers the information which confirms that users are able to send instant messages in conferences and participate in instant message conversations with three or more people. It will monitor the operation of instant messaging between two test users in a Lync pool. The following functions are tested: • Sign on to the Lync Server • Conference creation and joining • Message exchange • Session termination •Log out

Metric SpecName: IMConfer

Metric Field Name: InstantMessageConferencing

Data type: TEXT

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_InstantMessageConferencing

Message text: The Instant Message Conferencing is down

Instructional Text:

Probable Cause(s): 1. User configuration not done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: Users would not be able to avail peer to peer services

Suggested Action(s): 1. Configuration : Most common issues are invalid or expired Test user password, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availability: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution error or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responds to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Metric: ServerName

Description: This is the key for metric

Metric SpecName: ServerName

Metric Field Name: ServerName

Data type: TEXT

Alarm: FALSE

Metric: GroupInstantMessagingLatency

Description: This metric will capture the latency in reciept of instant messages in group instant messaging

Metric SpecName: GroupIMLat

Metric Field Name: GroupInstantMessagingLatency

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1000, Major / 1000

Policy: MSBS_GroupInstantMessagingLatency

Message text: The value of Group Instant Messaging Latency(ms) is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): 1. User configuration not done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: Users would not be able to avail peer to peer services

Suggested Action(s): 1. Configuration : Most common issues are invalid or expired Test user password, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availability: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution error or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responds to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Metric: InstantMessageConferencing

Description: This metric gathers the information which confirms that users are able to send instant messages in conferences and participate in instant message conversations with three or more people. It will monitor the operation of instant messaging between two test users in a Lync pool. The following functions are tested: • Sign on to the Lync Server • Conference creation and joining • Message exchange • Session termination •Log out

Metric SpecName: IMConfer

Metric Field Name: InstantMessageConferencing

Data type: TEXT

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_InstantMessageConferencing

Message text: The Instant Message Conferencing is down

Instructional Text:

Probable Cause(s): 1. User configuration not done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: Users would not be able to avail peer to peer services

Suggested Action(s): 1. Configuration : Most common issues are invalid or expired Test user password, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availability: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution error or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responds to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Metric: ServerName

Description: This is the key for metric

Metric SpecName: ServerName

Metric Field Name: ServerName

Data type: TEXT

Alarm: FALSE

Metric: GroupInstantMessagingLatency

Description: This metric will capture the latency in reciept of instant messages in group instant messaging

Metric SpecName: GroupIMLat

Metric Field Name: GroupInstantMessagingLatency

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1000, Major / 1000

Policy: MSBS_GroupInstantMessagingLatency

Message text: The value of Group Instant Messaging Latency(ms) is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): 1. User configuration not done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: Users would not be able to avail peer to peer services

Suggested Action(s): 1. Configuration : Most common issues are invalid or expired Test user password, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availability: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution error or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responds to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

MediaRelay

This policy maintains the monitoring of Mediation Server Health

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_MEDIATIONSERVER_Conf

Aspect: Skype Mediation Server Key Health

CIT: Mediation Server

Data source / Data class: LYNC / KHIMEDRELAY

Source / Collection Definition: PERFMON / LS:MediationServer - Media Relay

Metric: CandidatesMissing

> **Description**: This policy monitors the number of times Media stack does not have Media relay candidates.
>
> **Metric SpecName**: CandidatesMiss
>
> **Metric Field Name**: - Candidates Missing
>
> **Data type**: UINT32
>
> **Alarm**: TRUE
>
> **Category** : MSSkype
>
> **Severity / Threshold** : Minor / 0
>
> **Policy**: MSBS_CandidatesMissing
>
> **Message text**: The current value of CandidatesMissing is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:
>
> **Instructional Text**:
>
> **Probable Cause(s)**: Mediation Server cannot reach the Media Relay.
>
> **Potential Impact**: Make sure that Media Relay is running and is accessible by Mediation Server.
>
> **Suggested Action(s)**: Media cannot be transmitted

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

SimplePortWatcher5062

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / Port5062

Source / Collection Definition: PORTCOL / PORTCHECKER

Metric: SimpleWatcherPort5062

Description: Used for incoming SIP requests for instant messaging (IM) conferencing.

Metric SpecName: SimpleWatcherPort5062

Metric Field Name: SimpleWatcherPort5062

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort5062

Message text: The Port No:5062 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

Metric: SimpleWatcherPort5062

Description: Used for incoming SIP requests for instant messaging (IM) conferencing.

Metric SpecName: SimpleWatcherPort5062

Metric Field Name: SimpleWatcherPort5062

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort5062

Message text: The Port No:5062 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

Collect_Edge_AV_Auth_Requests

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / LSAVAUTH

Source / Collection Definition: PERFMON / LS:A/V Auth - Requests(*)

Metric: EdgeAVAuthInstance

Description: instance of perfmon object LS:A/V Auth - Requests

Metric SpecName: AVAITHINSYANCE

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: EdgeBadRequestsReceived

Description: Bad Requests Received per second

Metric SpecName: BADREQRECEIVED

Metric Field Name: - Bad Requests Received/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 20, Major / 30

Policy: MSBS_EdgeBadRequestsReceived

Message text: The value of Bad Requests Received/sec for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): This error occurs when an unexpectedly high rate of invalid requests is received by the A/V Authentication Service. Authentication Service.

Potential Impact: NA

Suggested Action(s): If the situation persists then enable Microsoft Lync Server 2013 logging for SIP messages to the A/V Authentication Service to identify the source of the invalid requests.

ChkFrontEndCentralizedLoggingAgentServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SERVSTAT

Source / Collection Definition: SERVICECHECK / RTCCLSAGT

Metric: FERTCCLSAGTServName

Description: Name of the Service

Metric SpecName: SERVNAME

Metric Field Name: Service_Name

Data type: TEXT

Alarm: FALSE

Metric: FERTCCLSAGTServDisplayName

Description: Display Name of the Service

Metric SpecName: SRVDISPNAME

Metric Field Name: Service_Displayname

Data type: TEXT

Alarm: FALSE

Metric: FERTCCLSAGTServStatus

Description: Status of the Service

Metric SpecName: SERVSTATUS

Metric Field Name: Service_Status

Data type: TEXT

Alarm: FALSE

Metric: FERTCCLSAGTServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_FERTCCLSAGTServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): Lync Server Centralized Logging Service Agent' Windows Service is stopped.

Potential Impact: NA

Suggested Action(s): Lync Server Centralized Logging Service Agent' Windows Service is stopped. Please restart the service.

Collect_Archiving_ArchService_DBArch

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / NA

Source / Collection Definition: PERFMON / LS:Arch Service - 00 - DBArch(*)

Metric: ArchServiceDBArchInstance

Description: instance of perfmon object LS:Arch Service - 00 - DBArch

Metric SpecName: ARCHSERVCEDBARCHINSTANCE

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: ArchServiceBlockedClientThreads

Description: average number of client threads that are blocked and waiting for the decrease in the queue depth

Metric SpecName: BLKDCLIENTTHRDS

Metric Field Name: Arch Service - 011 - Blocked Client Threads

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 0, Major / 100

Policy: MSBS_ArchServiceBlockedClientThreads

Message text: The value of the counter 'Arch Service - 011 - Blocked Client Threads' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: ArchServiceQueueLatency

Description: average time (in milliseconds) spent by a request in the database queue before it is processed

Metric SpecName: QLATENCY

Metric Field Name: Arch Service - 002 - Queue Latency (msec)

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 0, Major / 100

Policy: MSBS_ArchServiceQueueLatency

Message text: The value of the counter 'Arch Service - 002 - Queue Latency (msec)' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Streams

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / KHISTREAMS

Source / Collection Definition: PERFMON / LS:XmppFederationProxy - Streams

Metric: Failedinboundstreamestablishespersec

Description: This policy monitors the per-second number of inbound stream establishment failures.

Metric SpecName: Failinboustreestab

Metric Field Name: XmppFederationProxy - Failed inbound stream establishes/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Minor / 0

Policy: MSBS_Failedinboundstreamestablishespersec

Message text: The current value of Failedinboundstreamestablishespersec is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): The most common root cause is not selecting the correct Connection Type when establishing XMPP federation.

Potential Impact: Validate that the appropriate firewall ports opened.

Suggested Action(s): This would impact the ability for Lync users to contact XMPP federated partners

Metric: Failedoutboundstreamestablishespersec

Description: This policy monitors the per-second number of outbound stream establishment failures.

Metric SpecName: Failouboustreestab

Metric Field Name: XmppFederationProxy - Failed outbound stream establishes/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Minor / 0

Policy: MSBS_Failedoutboundstreamestablishespersec

Message text: The current value of Failedoutboundstreamestablishespersec is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): The most common root cause is not selecting the correct Connection Type when establishing XMPP federation.

Potential Impact: Validate that the appropriate firewall ports opened.

Suggested Action(s): This would impact the ability for Lync users to contact XMPP federated partners

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Collect_AvConf_AVMCU_Operations

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / NA

Source / Collection Definition: PERFMON / LS:AVMCU - 00 - Operations

Metric: AvConfAVMCUOperationsInstance

> **Description**: instance of perfmon object LS:AVMCU - 00 - Operations
>
> **Metric SpecName**: AVCONFOPERATIONSINSTANCE
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: AvConfNumberofConferences

> **Description**: In A/V conferencing server , the number of conferences that are currently active
>
> **Metric SpecName**: NOFCONFS
>
> **Metric Field Name**: AVMCU - 000 - Number of Conferences
>
> **Data type**: UINT32
>
> **Alarm**: TRUE
>
> **Category** : MSSkype
>
> **Severity / Threshold** : Warning / 4000, Major / 5000
>
> **Policy**: MSBS_AvConfNumberofConferences
>
> **Message text**: The value of the counter 'AVMCU - 000 - Number of Conferences' value <VALUE> has crossed the threshold of <THRESHOLD> .
>
> **Instructional Text**:
>
> **Probable Cause(s)**: NA
>
> **Potential Impact**: NA
>
> **Suggested Action(s)**: NA

Collect_FrontEnd_SipEps

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / LSSIPEPSCON

Source / Collection Definition: PERFMON / LS:SipEps - SipEps Connections(*)

Metric: SIPEPSInstance

> **Description**: instance of perfmon object LS:SipEps - SipEps Connections
>
> **Metric SpecName**: SIPEPSINSTANCE
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: NumberofDNSReolutionFailures

> **Description**: the total number of DNS resolution failures
>
> **Metric SpecName**: NUMDNSRESFAILURE
>
> **Metric Field Name**: SipEps - NumberOfDNSResolutionFailures
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

DBStore

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / KHIDBSTORE

Source / Collection Definition: PERFMON / LS:Usrv - 01 - DBStore(*)

Metric: DBStoreThrottledrequests

> **Description**: This policy monitors the number of requests that were rejected with a retry since the database queue latency was high.
>
> **Metric SpecName**: DBStThrottledreq
>
> **Metric Field Name**: Usrv - 020 - Throttled requests/sec
>
> **Data type**: UINT32
>
> **Alarm**: TRUE
>
> **Category** : MSSkype
>
> **Severity / Threshold** : Major / 0, Major / 0
>
> **Policy**: MSBS_DBStoreThrottledrequests
>
> **Message text**: The current value of DBStoreThrottledrequests is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:
>
> **Instructional Text**:
>
> **Probable Cause(s)**: The backend might be busy and is unable to respond to requests quickly.
>
> **Potential Impact**: Please ensure that the hardware and software requirements meet the user usage characteristics.
>
> **Suggested Action(s)**: The number of requests rejected by a database would be high

Metric: Instance_Name

> **Description**: This is the key for metric
>
> **Metric SpecName**: Instance_Name
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: DBStoreThrottledrequests

> **Description**: This policy monitors the number of requests that were rejected with a retry since the database queue latency was high.
>
> **Metric SpecName**: DBStThrottledreq
>
> **Metric Field Name**: Usrv - Throttled requests/sec
>
> **Data type**: UINT32
>
> **Alarm**: TRUE
>
> **Category** : MSSkype
>
> **Severity / Threshold** : Major / 0, Major / 0
>
> **Policy**: MSBS_DBStoreThrottledrequests
>
> **Message text**: The current value of DBStoreThrottledrequests is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:
>
> **Instructional Text**:
>
> **Probable Cause(s)**: The backend might be busy and is unable to respond to requests quickly.
>
> **Potential Impact**: Please ensure that the hardware and software requirements meet the user usage characteristics.
>
> **Suggested Action(s)**: The number of requests rejected by a database would be high

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Collect_Director_Auth_Delegate_Sproc

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / NA

Source / Collection Definition: PERFMON / LS:USrv - 31 - Authorize delegate sproc(*)

Metric: DirAuthDelegateSprocInstance

Description: instance of perfmon object LS:USrv - 31 - Authorize delegate sproc

Metric SpecName: DIRAUTHDELGTSPROCINSTANCE

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: DirSprocLatency

> **Description**: average time taken in processing a RTCAuthorizeDelegate sproc call
>
> **Metric SpecName**: SPROCLATENCY
>
> **Metric Field Name**: USrv - 001 - Sproc Latency (msec)
>
> **Data type**: UINT32
>
> **Alarm**: TRUE
>
> **Category** : MSSkype
>
> **Severity / Threshold** : Major / 20
>
> **Policy**: MSBS_DirSprocLatency
>
> **Message text**: The value of the counter ' Sproc Latency (msec)' value <VALUE> has crossed the threshold of <THRESHOLD> .
>
> **Instructional Text**:
>
> **Probable Cause(s)**: NA
>
> **Potential Impact**: NA
>
> **Suggested Action(s)**: NA

SimplePortWatcher4443

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / Port4443

Source / Collection Definition: PORTCOL / PORTCHECKER

Metric: SimpleWatcherPort4443

Description: Used for internal communications between servers and for client connections.

Metric SpecName: SimpleWatcherPort4443

Metric Field Name: SimpleWatcherPort4443

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort4443

Message text: The Port No:4443 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

Metric: SimpleWatcherPort4443

Description: Used for internal communications between servers and for client connections.

Metric SpecName: SimpleWatcherPort4443

Metric Field Name: SimpleWatcherPort4443

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort4443

Message text: The Port No:4443 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

ChkFrontEndIMConferencingServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SERVSTAT

Source / Collection Definition: SERVICECHECK / RTCIMMCU

Metric: FERTCIMMCUServName

Description: Name of the Service

Metric SpecName: SERVNAME

Metric Field Name: Service_Name

Data type: TEXT

Alarm: FALSE

Metric: FERTCIMMCUServDisplayName

Description: Display Name of the Service

Metric SpecName: SRVDISPNAME

Metric Field Name: Service_Displayname

Data type: TEXT

Alarm: FALSE

Metric: FERTCIMMCUServStatus

Description: Status of the Service

Metric SpecName: SERVSTATUS

Metric Field Name: Service_Status

Data type: TEXT

Alarm: FALSE

Metric: FERTCIMMCUServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_FERTCIMMCUServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): Lync Server IM Conferencing' Windows Service is stopped.

Potential Impact: NA

Suggested Action(s): Lync Server IM Conferencing' Windows Service is stopped. Please restart the service.

Collect_Edge_SipEps_Connections

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / NA

Source / Collection Definition: PERFMON / LS:SipEps - 02 - SipEps Connections(_Total)

Metric: EdgeSipEpsNumberOfDNSResolutionFailures

> **Description**: The total number of DNS resolution failures
>
> **Metric SpecName**: NOFDNSRESFAIL
>
> **Metric Field Name**: SipEps - 010 - NumberOfDNSResolutionFailures
>
> **Data type**: UINT32
>
> **Alarm**: TRUE
>
> **Category** : MSSkype
>
> **Severity / Threshold** : Warning / 50, Major / 100
>
> **Policy**: MSBS_EdgeSipEpsNumberOfDNSResolutionFailures
>
> **Message text**: The value of the counter 'NumberOfDNSResolutionFailures' value <VALUE> has crossed the threshold of <THRESHOLD> .
>
> **Instructional Text**:
>
> **Probable Cause(s)**: NA
>
> **Potential Impact**: NA
>
> **Suggested Action(s)**: NA

Metric: EdgeSipEpsConnectionInstance

> **Description**: instance of perfmon object LS:SipEps - 02 - SipEps Connections(_Total)
>
> **Metric SpecName**: INSTANCENAME
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

ProcessorInformation

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / KHIPROCINFO

Source / Collection Definition: PERFMON / Processor(_Total)

Metric: ProcessorInformation

Description: This policy monitors CPU Utilization; this event indicates that an application is consuming excessive processor resources

Metric SpecName: ProcessorInform

Metric Field Name: % Processor Time

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 80, Major / 80

Policy: MSBS_ProcessorInformation

Message text: The current value of ProcessorInformation is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): This may be caused by an application consuming excessive processor resources.

Potential Impact: In order to resolve this issue try one of the following resolutions: Identify processes that are running when the processor time is at the highest.Stop or kill any unnecessary identified processes. Add more processor cores to the system.

Suggested Action(s): Processes may starve processor cycles and lead to an unresponsive system

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: ProcessorInformation

Description: This policy monitors CPU Utilization; this event indicates that an application is consuming excessive processor resources

Metric SpecName: ProcessorInform

Metric Field Name: % Processor Time

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 80, Major / 80

Policy: MSBS_ProcessorInformation

Message text: The current value of ProcessorInformation is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): This may be caused by an application consuming excessive processor resources.

Potential Impact: In order to resolve this issue try one of the following resolutions: Identify processes that are running when the processor time is at the highest.Stop or kill any unnecessary identified processes. Add more processor cores to the system.

Suggested Action(s): Processes may starve processor cycles and lead to an unresponsive system

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

VOIPFailurePercentage

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / VOIPFAILURE

Source / Collection Definition: SQLDB / select isnull(cast(100.0 * cast((SUM(CASE WHEN SD.ResponseCode != 200 THEN 1 ELSE 0 END)) as float) / cast((SUM(CASE WHEN SD.ResponseCode is NOT NULL THEN 1 ELSE 0 END)) as float) as decimal(4, 1)),0) as VOIPFailurePercentage,SERVERPROPERTY('MACHINENAME') AS 'ServerName' from [LcsCDR]. [dbo].SessionDetails SD right OUTER JOIN [LcsCDR].[dbo].VoipDetailsView VP ON SD.SessionIdTime = VP.SessionIdTime where VP.SessionIdTime >= dateadd (MINUTE,@Duration,GETUTCDATE())

Metric: VOIPFailurePercentage

Description: This metric captures call failures periodically from the CDR database and raises an alert whenever call failures exceed the specified "threshold" percentage value. When a VOIP call fails, this failure is reported to the Monitoring Server database (Call Detail Records database).

Metric SpecName: VOIPFailPer

Metric Field Name: VOIPFailurePercentage

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 40, Major / 70, Warning / 40, Major / 70

Policy: MSBS_VOIPFailurePercentage

Message text: The current value of Percentage VOIP Failure is <VALUE> which exceeds the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Possible causes are connectivity issues between the Mediation Server and the ACP partners.

Potential Impact: Users face issue in connecting a VOIP-PSTN call or establishing a conference

Suggested Action(s): Check and make sure that there are no connectivity issues with the partner network(s) for the partner(s).Also, check to see that the ACP partner(s) are not out of service. Check previous events from ACP MCU component for more details on the failures.

Metric: ServerName

Description: This is the key for metric

Metric SpecName: ServerName

Metric Field Name: ServerName

Data type: TEXT

Alarm: FALSE

Metric: VOIPFailurePercentage

Description: This metric captures call failures periodically from the CDR database and raises an alert whenever call failures exceed the specified "threshold" percentage value. When a VOIP call fails, this failure is reported to the Monitoring Server database (Call Detail Records database).

Metric SpecName: VOIPFailPer

Metric Field Name: VOIPFailurePercentage

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 40, Major / 70, Warning / 40, Major / 70

Policy: MSBS_VOIPFailurePercentage

Message text: The current value of Percentage VOIP Failure is <VALUE> which exceeds the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Possible causes are connectivity issues between the Mediation Server and the ACP partners.

Potential Impact: Users face issue in connecting a VOIP-PSTN call or establishing a conference

Suggested Action(s): Check and make sure that there are no connectivity issues with the partner network(s) for the partner(s).Also, check to see that the ACP partner(s) are not out of service. Check previous events from ACP MCU component for more details on the failures.

Metric: ServerName

Description: This is the key for metric

Metric SpecName: ServerName

Metric Field Name: ServerName

Data type: TEXT

Alarm: FALSE

AddressSpaceUsage

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / ADDRESSSPACEUSAGE

Source / Collection Definition: PERFMON / LS:SIP - Load Management(*)

Metric: AddressSpaceUsage

> **Description**: This metric captures the percentage of available address space currently in use by the server process.
>
> **Metric SpecName**: AddressSpaceUsage
>
> **Metric Field Name**: SIP - Address Space Usage
>
> **Data type**: REAL64
>
> **Alarm**: FALSE

Metric: Instance_Name

> **Description**: This is the key for metric
>
> **Metric SpecName**: Instance_Name
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Collect_Edge_SipEps_Transactions

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / NA

Source / Collection Definition: PERFMON / LS:SipEps - 01 - SipEps Transactions(*)

Metric: EdgeTransactionsTimedOutPersec

> **Description**: The total number of Transactions Timed Out
>
> **Metric SpecName**: TRANSTIMEOUT
>
> **Metric Field Name**: SipEps - 008 - Transactions Timed Out/sec
>
> **Data type**: UINT32
>
> **Alarm**: TRUE
>
> **Category** : MSSkype
>
> **Severity / Threshold** : Major / 20
>
> **Policy**: MSBS_EdgeTransactionsTimedOutPersec
>
> **Message text**: The value of the counter 'Transactions Timed Out/sec' value <VALUE> has crossed the threshold of <THRESHOLD> .
>
> **Instructional Text**:
>
> **Probable Cause(s)**: NA
>
> **Potential Impact**: NA
>
> **Suggested Action(s)**: NA

Metric: EdgeSipEpsTransactionInstance

Description: instance of perfmon object LS:SipEps - 01 - SipEps Transactions

Metric SpecName: INSTANCENAME

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

AVMCUInformation

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: SKYPE / AVMCUINFORMATION

Source / Collection Definition: PERFMON / LS:AVMCU - 02 - Informational(*)

Metric: TotalMRASFailureResponseExceptions

Description: This metric captures Total MRAS Failure Response Exceptions

Metric SpecName: TotalMRASFailResExc

Metric Field Name: AVMCU - 016 - Total MRAS Failure Response Exceptions

Data type: REAL64

Alarm: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: TotalMRASGenericExceptions

Description: This metric captures Total MRAS Generic Exceptions

Metric SpecName: TotalMRASGenericExc

Metric Field Name: AVMCU - 018 - Total MRAS Generic Exceptions

Data type: REAL64

Alarm: FALSE

Metric: TotalMRASRequest

Description: This metric captures Total MRAS Request

Metric SpecName: TotalMRASRequest

Metric Field Name: AVMCU - 011 - Total MRAS Request

Data type: REAL64

Alarm: FALSE

Metric: TotalMRASRequestError

Description: This metric captures Total MRAS Request Error

Metric SpecName: TotalMRASRequestEr

Metric Field Name: AVMCU - 012 - Total MRAS Request error

Data type: REAL64

Alarm: FALSE

Metric: TotalMRASRequestsRejected

Description: This metric captures Total MRAS Requests Rejected

Metric SpecName: TotalMRASReqRej

Metric Field Name: AVMCU - 014 - Total MRAS Requests Rejected

Data type: REAL64

Alarm: FALSE

Metric: TotalMRASFailureResponseExceptions

Description: This metric captures Total MRAS Failure Response Exceptions

Metric SpecName: TotalMRASFailResExc

Metric Field Name: AVMCU - Total MRAS Failure Response Exceptions

Data type: REAL64

Alarm: FALSE

Metric: TotalMRASGenericExceptions

Description: This metric captures Total MRAS Generic Exceptions

Metric SpecName: TotalMRASGenericExc

Metric Field Name: AVMCU - Total MRAS Generic Exceptions

Data type: REAL64

Alarm: FALSE

Metric: TotalMRASRequest

Description: This metric captures Total MRAS Request

Metric SpecName: TotalMRASRequest

Metric Field Name: AVMCU - Total MRAS Request

Data type: REAL64

Alarm: FALSE

Metric: TotalMRASRequestError

Description: This metric captures Total MRAS Request Error

Metric SpecName: TotalMRASRequestEr

Metric Field Name: AVMCU - Total MRAS Request error

Data type: REAL64

Alarm: FALSE

Metric: TotalMRASRequestsRejected

Description: This metric captures Total MRAS Requests Rejected

Metric SpecName: TotalMRASReqRej

Metric Field Name: AVMCU - Total MRAS Requests Rejected

Data type: REAL64

Alarm: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: TotalMRASTimeoutExceptions

Description: This metric captures Total MRAS Timeout Exceptions

Metric SpecName: TotalMRASTimeoutExc

Metric Field Name: AVMCU - Total MRAS Timeout Exceptions

Data type: REAL64

Alarm: FALSE

Collect_FrontEnd_Process_OcsAppServerHost

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / CS_PROCESS

Source / Collection Definition: PERFMON / Process(OcsAppServerHost*)

Metric: FERTCPDPAUTHInstance

> **Description**: instance of OCSAppServerHost
>
> **Metric SpecName**: INSTANCENAME
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FERTCPDPAUTHPercentprocessorTime

> **Description**: Percentage Processor Time is the percentage of elapsed time that all of process threads used the processor to execution instructions.
>
> **Metric SpecName**: PCTPROCESSORTIME
>
> **Metric Field Name**: % Processor Time
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Metric: FERTCPDPAUTHWorkingSet

Description: Working Set is the current size, in bytes, of the Working Set of this process. the Working Set is the set of memory pages touched recently by the threads in the process. If free memory in the computer is above a threshold, pages are left in the Working Set of a process even if they are not in use. When free memory falls below a threshold, pages are trimmed from Working Sets. If they are needed they will then be soft-faulted back into the Working Set before leaving main memory.

Metric SpecName: WORKINGSET

Metric Field Name: Working Set

Data type: UINT32

Alarm: FALSE

Metric: FERTCPDPAUTHPageFaultsPerSec

Description: Page Faults/sec is the average number of pages faulted per second. It is measured in number of pages faulted per second because only one page is faulted in each fault operation, hence this is also equal to the number of page fault operations. This counter includes both hard faults (those that require disk access) and soft faults (where the faulted page is found elsewhere in physical memory.) Most processors can handle large numbers of soft faults without significant consequence. However, hard faults, which require disk access, can cause significant delays.

Metric SpecName: PAGEFAULTS

Metric Field Name: Page Faults/sec

Data type: UINT32

Alarm: FALSE

Metric: FERTCPDPAUTHPrivateBytes

Description: Private Bytes is the current size, in bytes, of memory that this process has allocated that cannot be shared with other processes.

Metric SpecName: PRIVATEBYTES

Metric Field Name: Private Bytes

Data type: UINT32

Alarm: FALSE

Metric: FERTCPDPAUTHThreadCount

> **Description**: the number of threads currently active in this process. An instruction is the basic unit of execution in a processor, and a thread is the object that executes instructions. Every running process has at least one thread.
>
> **Metric SpecName**: THREADCOUNT
>
> **Metric Field Name**: Thread Count
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Collect_FrontEnd_Process_ASMCUSvc

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / CS_PROCESS

Source / Collection Definition: PERFMON / Process(ASMCUSvc)

Metric: FERTCASMCUInstance

> **Description**: instance of perfmon object Process(ASMCUSvc)
>
> **Metric SpecName**: INSTANCENAME
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FERTCASMCUPercentprocessorTime

Description: Percentage Processor Time is the percentage of elapsed time that all of process threads used the processor to execution instructions.

Metric SpecName: PCTPROCESSORTIME

Metric Field Name: % Processor Time

Data type: UINT32

Alarm: FALSE

Metric: FERTCASMCUWorkingSet

Description: Working Set is the current size, in bytes, of the Working Set of this process. the Working Set is the set of memory pages touched recently by the threads in the process. If free memory in the computer is above a threshold, pages are left in the Working Set of a process even if they are not in use. When free memory falls below a threshold, pages are trimmed from Working Sets. If they are needed they will then be soft-faulted back into the Working Set before leaving main memory.

Metric SpecName: WORKINGSET

Metric Field Name: Working Set

Data type: UINT32

Alarm: FALSE

Metric: FERTCASMCUPageFaultsPerSec

Description: Page Faults/sec is the average number of pages faulted per second. It is measured in number of pages faulted per second because only one page is faulted in each fault operation, hence this is also equal to the number of page fault operations. This counter includes both hard faults (those that require disk access) and soft faults (where the faulted page is found elsewhere in physical memory.) Most processors can handle large numbers of soft faults without significant consequence. However, hard faults, which require disk access, can cause significant delays.

Metric SpecName: PAGEFAULTS

Metric Field Name: Page Faults/sec

Data type: UINT32

Alarm: FALSE

Metric: FERTCASMCUPrivateBytes

Description: Private Bytes is the current size, in bytes, of memory that this process has allocated that cannot be shared with other processes.

Metric SpecName: PRIVATEBYTES

Metric Field Name: Private Bytes

Data type: UINT32

Alarm: FALSE

Metric: FERTCASMCUThreadCount

Description: the number of threads currently active in this process. An instruction is the basic unit of execution in a processor, and a thread is the object that executes instructions. Every running process has at least one thread.

Metric SpecName: THREADCOUNT

Metric Field Name: Thread Count

Data type: UINT32

Alarm: FALSE

Metric: FERTCASMCUInstance

Description: instance of ASMCUSvc process

Metric SpecName: INSTANCENAME

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: FERTCASMCUPercentprocessorTime

Description: Percentage Processor Time is the percentage of elapsed time that all of process threads used the processor to execution instructions.

Metric SpecName: PCTPROCESSORTIME

Metric Field Name: % Processor Time

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 90

Policy: MSBS_FERTCASMCUPercentprocessorTime

Message text: The value of the counter '% Processor Time' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: FERTCASMCUWorkingSet

Description: Working Set is the current size, in bytes, of the Working Set of this process. the Working Set is the set of memory pages touched recently by the threads in the process. If free memory in the computer is above a threshold, pages are left in the Working Set of a process even if they are not in use. When free memory falls below a threshold, pages are trimmed from Working Sets. If they are needed they will then be soft-faulted back into the Working Set before leaving main memory.

Metric SpecName: WORKINGSET

Metric Field Name: Working Set

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20000000

Policy: MSBS_FERTCASMCUWorkingSet

Message text: The value of the counter 'Working Set' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: FERTCASMCUPageFaultsPerSec

Description: Page Faults/sec is the average number of pages faulted per second. It is measured in number of pages faulted per second because only one page is faulted in each fault operation, hence this is also equal to the number of page fault operations. This counter includes both hard faults (those that require disk access) and soft faults (where the faulted page is found elsewhere in physical memory.) Most processors can handle large numbers of soft faults without significant consequence. However, hard faults, which require disk access, can cause significant delays.

Metric SpecName: PAGEFAULTS

Metric Field Name: Page Faults/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 100

Policy: MSBS_FERTCASMCUPageFaultsPerSec

Message text: The value of the counter 'Page Faults/sec' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: FERTCASMCUPrivateBytes

Description: Private Bytes is the current size, in bytes, of memory that this process has allocated that cannot be shared with other processes.

Metric SpecName: PRIVATEBYTES

Metric Field Name: Private Bytes

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20000000

Policy: MSBS_FERTCASMCUPrivateBytes

Message text: The value of the counter 'Private Bytes' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: FERTCASMCUThreadCount

Description: the number of threads currently active in this process. An instruction is the basic unit of execution in a processor, and a thread is the object that executes instructions. Every running process has at least one thread.

Metric SpecName: THREADCOUNT

Metric Field Name: Thread Count

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 150

Policy: MSBS_FERTCASMCUThreadCount

Message text: The value of the counter 'Thread Count' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

SimpleURLWatcherAdmin

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / URLWATCHADMIN

Source / Collection Definition: POWERSHELL / Invoke-WebRequest -Uri admin.{SIPDOMAIN} -UseDefaultCredentials

Metric: URLWatcherAdmin

Description: This metric check HTTP response of a Admin URL

Metric SpecName: URLWatcherAdmin

Metric Field Name: StatusCode

Data type: TEXT

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Minor / 1

Policy: MSBS_URLWatcherAdmin

Message text: The Admin URL to access Lync Server Control Panel is down

Instructional Text:

Probable Cause(s): The page is unreachable. If behind a proxy, check if the proxy settings are correct. Unexpected API call failures. Multiple reasons could cause this, for instance a memory allocation error. The site or URL is not accessible or is down.

Potential Impact: URL cannot be accessed

Suggested Action(s): Try to access the same URL from an internet browser like Internet Explorer.

Metric: ServerName

Description: This metric check HTTP response of a Admin URL

Metric SpecName: ServerName

Metric Field Name: ServerName

Data type: TEXT

Alarm: FALSE

AudioPacketLossPoorCallsPercentage

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / AUDIOPACKETLOSSCALLS

Source / Collection Definition: SQLDB / select isnull(cast(100.0 * cast((SUM(CASE WHEN [AudioPacketLossRate] > [PacketLossRateOptimal] THEN 1 ELSE 0 END)) as float) / cast((SUM (CASE WHEN MediaLineLabel is NOT NULL THEN 1 ELSE 0 END)) as float) as decimal(4, 1)),0) as AudioPacketLossPoorCallsPercentage, SERVERPROPERTY('MACHINENAME') AS 'ServerName' from [QoEMetrics].[dbo].[QoEReportsCallDetailView] Where MediaLineLabel = 0 AND ConferenceDateTime >= dateadd(MINUTE,@Duration,GETUTCDATE())

Metric: AudioPacketLossPoorCallsPercentage

Description: This metric captures Poor Audio that have Packet Loss more than a set threshold value and calculates percentage of poor calls for a given interval. At the end of each call, parameters that determine Quality of a call that include network, audio and video parameters are logged into QoE database of Lync Server. Each call is categorized as having Acceptable quality or Poor quality based on the same.

Metric SpecName: AudPacktLosPoorCall

Metric Field Name: AudioPacketLossPoorCallsPercentage

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 40, Major / 70, Warning / 40, Major / 70

Policy: MSBS_AudioPacketLossPoorCallsPercentage

Message text: The current value of Percentage Audio Packet Loss Poor Calls is <VALUE> which exceeds the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): As Lync leverages UDP for audio , the Lync client doesn't ask for retransmission of lost packets. If packets arrive out of sequence, Lync just ignores them. Lack of bandwidth and overloaded server could be probable causes.

Potential Impact: Distorted audio and call drops

Suggested Action(s): UDP does not provide recovery for packet loss, but increasing network bandwidth could be a workaround

Metric: ServerName

Description: This is the key for metric

Metric SpecName: ServerName

Metric Field Name: ServerName

Data type: TEXT

Alarm: FALSE

Metric: AudioPacketLossPoorCallsPercentage

Description: This metric captures Poor Audio that have Packet Loss more than a set threshold value and calculates percentage of poor calls for a given interval. At the end of each call, parameters that determine Quality of a call that include network, audio and video parameters are logged into QoE database of Lync Server. Each call is categorized as having Acceptable quality or Poor quality based on the same.

Metric SpecName: AudPacktLosPoorCall

Metric Field Name: AudioPacketLossPoorCallsPercentage

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 40, Major / 70, Warning / 40, Major / 70

Policy: MSBS_AudioPacketLossPoorCallsPercentage

Message text: The current value of Percentage Audio Packet Loss Poor Calls is <VALUE> which exceeds the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): As Lync leverages UDP for audio , the Lync client doesn't ask for retransmission of lost packets. If packets arrive out of sequence, Lync just ignores them. Lack of bandwidth and overloaded server could be probable causes.

Potential Impact: Distorted audio and call drops

Suggested Action(s): UDP does not provide recovery for packet loss, but increasing network bandwidth could be a workaround

Metric: ServerName

Description: This is the key for metric

Metric SpecName: ServerName

Metric Field Name: ServerName

Data type: TEXT

Alarm: FALSE

Collect_FrontEnd_RGS

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / LSRGSRESPGRPMATMKG

Source / Collection Definition: PERFMON / LS:RGS - Response Group Service Match Making(*)

Metric: RGSInstance

> **Description**: instance of perfmon object LS:RGS - Response Group Service Match Making
>
> **Metric SpecName**: RGSINSTANCE
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: RGSCurrentNumberofCalls

> **Description**: the number of calls that are currently being handled.
>
> **Metric SpecName**: CURRENTCALLS
>
> **Metric Field Name**: RGS - Current number of calls
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Collect_Edge_Distribution_List_Expansion

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / EDGLSWEBDISTRLISTEXP

Source / Collection Definition: PERFMON / LS:WEB - Distribution List Expansion(*)

Metric: EdgeDistributionListExpansionInstance

> **Description**: instance of perfmon object LS:WEB - Distribution List Expansion
>
> **Metric SpecName**: EDGDISTRLSTEXPANSION
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: EdgeSuccessRequestProcTime

Description: Average processing time for a successful request to be completed

Metric SpecName: EDGSUCREQPROCTIME

Metric Field Name: WEB - Successful Request Processing Time

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 3000, Major / 5000

Policy: MSBS_EdgeSuccessRequestProcTime

Message text: The value of WEB - Successful Request Processing Time for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Issues with Active Directory performance

Potential Impact: NA

Suggested Action(s): Verify CPU load on active directory machines.

Metric: EdgeSoapExceptionPerSecond

Description: the per-second rate of Soap Exceptions

Metric SpecName: SOAPEXCEPT

Metric Field Name: WEB - Soap exceptions/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 3, Major / 6

Policy: MSBS_EdgeSoapExceptionPerSecond

Message text: The value of WEB - Average processing time for a search request in milliseconds for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Soap Exceptions.

Potential Impact: NA

Suggested Action(s): This is an internal error.

AudioVideoCallFailurePercentage

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / AUDIOVIDEOFAILURE

Source / Collection Definition: SQLDB / select isnull(cast(100.0 * cast((SUM(CASE WHEN SD.ResponseCode != 200 THEN 1 ELSE 0 END)) as float) / cast((SUM(CASE WHEN SD.ResponseCode is NOT NULL THEN 1 ELSE 0 END)) as float) as decimal(4, 1)),0) as AudioVideoCallFailurePercentage,SERVERPROPERTY('MACHINENAME') AS 'ServerName' from

[LcsCDR].[dbo].SessionDetails SD LEFT OUTER JOIN [LcsCDR].[dbo].Media M ON
SD.SessionIdTime = M.SessionIdTime LEFT OUTER JOIN [LcsCDR].[dbo].MediaList ML ON
M.MediaId = ML.MediaId Where ML.MediaId = 6 AND SD.SessionIdTime >= dateadd
(MINUTE,@Duration,GETUTCDATE())

Metric: AudioVideoCallFailurePercentage

> **Description**: This metric captures call failures periodically from the CDR database and raises
> an alert whenever call failures exceed the specified "threshold" percentage value. When an
> Audio-Video call fails, this failure is reported to the Monitoring Server database (Call Detail
> Records database).
>
> **Metric SpecName**: AudVidCallFailPer
>
> **Metric Field Name**: AudioVideoCallFailurePercentage
>
> **Data type**: REAL64
>
> **Alarm**: TRUE
>
> **Category** : MSSkype
>
> **Severity / Threshold** : Warning / 40, Major / 70, Warning / 40, Major / 70
>
> **Policy**: MSBS_AudioVideoCallFailurePercentage
>
> **Message text**: The current value of Percentage Audio Video Call Failure is <VALUE> which
> exceeds the threshold of <THRESHOLD>
>
> **Instructional Text**:
>
> **Probable Cause(s)**: The causes are related to server errors which point out to source of error
> like Mediatation, Front-end etc Probable causes include server overload, unknown MIME
> type,timeout, policy violation, protocol errors etc
>
> **Potential Impact**: Users face issue in connecting a P2P calls or establishing a conference
>
> **Suggested Action(s)**: Ramping up server resources, checking health of servers and network,
> modifying policy Refer Response codes MS Diagnostic codes

Metric: ServerName

Description: This is the key for metric

Metric SpecName: ServerName

Metric Field Name: ServerName

Data type: TEXT

Alarm: FALSE

AuthBadRequests

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / AUTHBADREQUESTS

Source / Collection Definition: PERFMON / LS:PDP Auth - Requests(*)

Metric: BadRequestsReceivedPerSec

Description: This metric captures The number of bad requests received per second

Metric SpecName: BadRequstReceivedPS

Metric Field Name: - Bad requests Received/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 30

Policy: MSBS_BadRequestsReceivedPerSec

Message text: The value of Bad Requests Received Per Second is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): This error occurs when an unexpectedly high rate of invalid requests is received by the A/V Authentication Service. This could be the result of an attempt to misuse the A/V Authentication Service.

Potential Impact: If the situation persists then enable Skype for Business Server 2015 logging for SIP messages to the A/V Authentication Service to identify the source of the invalid requests.

Suggested Action(s): High rate of invalid requests is received by the A/V Authentication Service

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

CallsThatFailedDueToCriticalServerErrors

This policy maintains the information about the status for the different services

Schedule Task Policy: MSBS_SCH_HALFHOURLY

ConfigFile Policy: MSBS_ConferenceProcPerform_2010_Conf

Aspect: Skype Conference Processing Performance

CIT: Mediation Server, Front End Server, Edge Server

Data source / Data class: SKYPE / CALFAILCRITSRVER

Source / Collection Definition: PERFMON / LS:RGS - 03 - Response Group Service Workflow(*)

Metric: CallsThatFailedDueToCriticalServerErrors

> **Description**: This metric captures Calls That Failed Due To Critical Server Errors
>
> **Metric SpecName**: CalFailCritSrvEr
>
> **Metric Field Name**: RGS - 011 - Calls that failed due to critical server errors
>
> **Data type**: REAL64
>
> **Alarm**: FALSE

Metric: Instance_Name

> **Description**: This is the key for metric
>
> **Metric SpecName**: Instance_Name
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: CallsThatFailedDueToCriticalServerErrors

> **Description**: This metric captures Calls That Failed Due To Critical Server Errors
>
> **Metric SpecName**: CalFailCritSrvEr
>
> **Metric Field Name**: RGS - Calls That Failed Due To Critical Server Errors
>
> **Data type**: REAL64
>
> **Alarm**: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Collect_FrontEnd_MediaPlanning

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / LSMEDIA

Source / Collection Definition: PERFMON / LS:MEDIA - Planning(*)

Metric: MediaPlanningInstance

Description: NA

Metric SpecName: MEDIAPLANINSTANCE

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: MEDIADelayedProcessing

Description: Number of occasions conference processing is delayed

Metric SpecName: DELAYEDCONFPROC

Metric Field Name: MEDIA - Number of occasions conference processing is delayed significantly

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 15, Major / 30

Policy: MSBS_MEDIADelayedProcessing

Message text: The Number of occasions conference processing delayed for instance <OPTION(InstanceName)> is <VALUE> and crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): This issue may occur if the Audio Video Conferencing server is overloaded, or is not getting enough CPU resources to process audio.

Potential Impact: NA

Suggested Action(s): To resolve this issue, please check the affected machine for overall CPU consumption and remove any unnecessary competing processes.

Collect_FrontEnd_SIP_Response_Logging

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / CS_FESIPRESPONSE

Source / Collection Definition: PERFMON / LS:SIP - Responses(*)

Metric: SIPResponseInstance

Description: instance of perfmon object LS:SIP - Responses

Metric SpecName: SIPRESPINSTANCE

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: SIPLocal503ResponsePerSecLogging

Description: the per-second rate of 503 responses generated by the server.

Metric SpecName: LOCAL503RESPONSES

Metric Field Name: SIP - Local 503 Responses/sec

Data type: UINT32

Alarm: FALSE

Metric: SIPLocal504ResponsePerSecLogging

Description: the per-second rate of 504 responses generated by the server.

Metric SpecName: LOCAL504RESPONSES

Metric Field Name: SIP - Local 504 Responses/sec

Data type: UINT32

Alarm: FALSE

Peer2PeerInstantMessaging

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_LOW

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SYNP2PIM

Source / Collection Definition: POWERSHELL / Test-CsIm -TargetFQDN {fqdn}

Metric: Peer2PeerInstantMessaging

> **Description**: This metric gathers the information which confirms that users are able to send peer-to-peer instant messages. It will monitor the operation of instant messaging conferencing between two test users in a Lync pool. The following functions are tested: • Sign on to the Lync Server • Conference initiation • Conference invitation and joining • Message exchange through the conference • Conference disconnect and termination • Log out
>
> **Metric SpecName**: Peer2PeerIM
>
> **Metric Field Name**: Peer2PeerInstantMessaging
>
> **Data type**: TEXT
>
> **Alarm**: TRUE
>
> **Category** : MSSkype
>
> **Severity / Threshold** : Major / 1, Major / 1
>
> **Policy**: MSBS_Peer2PeerInstantMessaging
>
> **Message text**: The Peer To Peer Instant Messaging is down
>
> **Instructional Text**:
>
> **Probable Cause(s)**: 1. User configuration not done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors
>
> **Potential Impact**: Users would not be able to avail peer to peer services
>
> **Suggested Action(s)**: 1. Configuration : Most common issues are invalid or expired Test user password, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availability: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution error or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responds to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Metric: ServerName

Description: This is the key for metric

Metric SpecName: ServerName

Metric Field Name: ServerName

Data type: TEXT

Alarm: FALSE

Metric: InstantMessagingLatency

Description: This metric will capture the instant messaging latency

Metric SpecName: IMLatency

Metric Field Name: InstantMessagingLatency

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Minor / 1000, Minor / 1000

Policy: MSBS_InstantMessagingLatency

Message text: The value of Instant Messaging Latency(ms) is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): 1. User configuration must not have done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: New users cannot be registered

Suggested Action(s): 1. Configuration errors: Most common issues are: Test user password is invalid or expired, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availibility: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution errors or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responded to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Metric: Peer2PeerInstantMessaging

Description: This metric gathers the information which confirms that users are able to send peer-to-peer instant messages. It will monitor the operation of instant messaging conferencing between two test users in a Lync pool. The following functions are tested: • Sign on to the Lync Server • Conference initiation • Conference invitation and joining • Message exchange through the conference • Conference disconnect and termination • Log out

Metric SpecName: Peer2PeerIM

Metric Field Name: Peer2PeerInstantMessaging

Data type: TEXT

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_Peer2PeerInstantMessaging

Message text: The Peer To Peer Instant Messaging is down

Instructional Text:

Probable Cause(s): 1. User configuration not done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: Users would not be able to avail peer to peer services

Suggested Action(s): 1. Configuration : Most common issues are invalid or expired Test user password, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availability: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution error or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responds to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Metric: ServerName

> **Description**: This is the key for metric
>
> **Metric SpecName**: ServerName
>
> **Metric Field Name**: ServerName
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: InstantMessagingLatency

Description: This metric will capture the instant messaging latency

Metric SpecName: IMLatency

Metric Field Name: InstantMessagingLatency

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Minor / 1000, Minor / 1000

Policy: MSBS_InstantMessagingLatency

Message text: The value of Instant Messaging Latency(ms) is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): 1. User configuration must not have done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: New users cannot be registered

Suggested Action(s): 1. Configuration errors: Most common issues are: Test user password is invalid or expired, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availibility: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution errors or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responded to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

SimplePortWatcher8404

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / Port8404

Source / Collection Definition: PORTCOL / PORTCHECKER

Metric: SimpleWatcherPort8404

Description: Used for incoming SIP requests for the Response Group application.

Metric SpecName: SimpleWatcherPort8404

Metric Field Name: SimpleWatcherPort8404

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort8404

Message text: The Port No:8404 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

Metric: SimpleWatcherPort8404

Description: Used for incoming SIP requests for the Response Group application.

Metric SpecName: SimpleWatcherPort8404

Metric Field Name: SimpleWatcherPort8404

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort8404

Message text: The Port No:8404 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

> **Description**: This is the key for metric
>
> **Metric SpecName**: HOSTNAME
>
> **Metric Field Name**: HOSTNAME
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Collect_FrontEnd_DataMCUConferences

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / LSDATAMACU

Source / Collection Definition: PERFMON / LS:DATAMCU - DataMCU Conferences(*)

Metric: DataMCUInstance

> **Description**: Instance of perfmon object DataMCU Conferences
>
> **Metric SpecName**: DATAMCUINSTANCE
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: SessionQueuesState

Description: Estimated conference workitems load in milliseconds

Metric SpecName: SESSIONQUESTATE

Metric Field Name: DATAMCU - Session queues state

Data type: UINT32

Alarm: FALSE

Metric: DataMCUInstance

Description: instance of perfmon object LS:DATAMCU - 00 - DataMCU Conferences

Metric SpecName: DATAMCUINSTANCE

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: SessionQueuesState

Description: State of session queue of DATAMCU performance counter

Metric SpecName: SESSIONQUESTATE

Metric Field Name: DATAMCU - 008 - Session queues state

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 1, Major / 2

Policy: MSBS_SessionQueuesState

Message text: The value of the counter 'DATAMCU - 008 - Session queues state' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: No.ofUnhandledApplicationException

Description: Number of unhavdled excepitons in Data MCU conferences

Metric SpecName: UNHANDLDEXCEPTIONS

Metric Field Name: DATAMCU - 005 - Number of Unhandled Application Exception

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 5, Major / 10

Policy: MSBS_No.ofUnhandledApplicationException

Message text: The value of the counter 'DATAMCU - 005 - Number of Unhandled Application Exception' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Collect_Persistent_Chat_Protocol

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / CHATPROTOCOL

Source / Collection Definition: PERFMON / LS:CHAT - Persistent Chat Protocol(*)

Metric: PersistentChatProtocolInstance

Description: instance of perfmon object LS:CHAT - Persistent Chat Protocol

Metric SpecName: CHATPROTOINSTANCE

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: ChatInboundQueueSize

Description: the current size of the inbound message processing queue.

Metric SpecName: CHATINBOUNDQUE

Metric Field Name: CHAT - Inbound Queue Size

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 50, Major / 100

Policy: MSBS_ChatInboundQueueSize

Message text: The value of chat inbound queue size for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): The server is overloaded with incoming requests.

Potential Impact: NA

Suggested Action(s): Check the event logs for details. Ensure that all active Persistent Chat servers are active and able to connect with the Lync services Front End.

Metric: ChatLastMessageWaitTime

Description: the wait time in milliseconds for the last XCCOS message processed.

Metric SpecName: CHATLSTMSGWAITTIME

Metric Field Name: CHAT - Last Msg Wait Time

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 30000, Major / 60000

Policy: MSBS_ChatLastMessageWaitTime

Message text: The value of chat message wait time for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): A large wait time can be caused by one of several conditions such as poor network connectivity between the Persistent Chat components.

Potential Impact: NA

Suggested Action(s): Confirm that you have expected network connectivity between components, there are no hardware related errors in the event logs, that CPU utilization is not consistently at 100%.

Metric: ChatMessagesInUCMAQueue

Description: Pending Outbound Messages to Clients

Metric SpecName: CHATMSGINUCMAQUE

Metric Field Name: CHAT - Messages in UCMA queue

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 5000, Major / 10000

Policy: MSBS_ChatMessagesInUCMAQueue

Message text: The value of chat message in UCMA queue for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Outbound connections from the Persistent Chat server to the Lync Front End server or to Lync client computers are failing.

Potential Impact: NA

Suggested Action(s): Check Front End event logs for details. Ensure that network connectivity between the Lync Front End servers and the Lync client computers are functioning.

Collect_PersistentChat_Mediation_Process_ ReplicaReplicatorAgent

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / CS_PROCESS

Source / Collection Definition: PERFMON / Process(ReplicaReplicatorAgent)

Metric: PerChatREPLICAInstance

> **Description**: instance of ReplicaReplicatorAgent process
>
> **Metric SpecName**: INSTANCENAME
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: PerChatREPLICAPercentprocessorTime

> **Description**: Percentage Processor Time is the percentage of elapsed time that all of process threads used the processor to execution instructions.
>
> **Metric SpecName**: PCTPROCESSORTIME
>
> **Metric Field Name**: % Processor Time
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Metric: PerChatREPLICAWorkingSet

> **Description**: Working Set is the current size, in bytes, of the Working Set of this process. the Working Set is the set of memory pages touched recently by the threads in the process. If free memory in the computer is above a threshold, pages are left in the Working Set of a process even if they are not in use. When free memory falls below a threshold, pages are trimmed from Working Sets. If they are needed they will then be soft-faulted back into the Working Set before leaving main memory.
>
> **Metric SpecName**: WORKINGSET
>
> **Metric Field Name**: Working Set
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Metric: PerChatREPLICAPageFaultsPerSec

Description: Page Faults/sec is the average number of pages faulted per second. It is measured in number of pages faulted per second because only one page is faulted in each fault operation, hence this is also equal to the number of page fault operations. This counter includes both hard faults (those that require disk access) and soft faults (where the faulted page is found elsewhere in physical memory.) Most processors can handle large numbers of soft faults without significant consequence. However, hard faults, which require disk access, can cause significant delays.

Metric SpecName: PAGEFAULTS

Metric Field Name: Page Faults/sec

Data type: UINT32

Alarm: FALSE

Metric: PerChatREPLICAPrivateBytes

Description: Private Bytes is the current size, in bytes, of memory that this process has allocated that cannot be shared with other processes.

Metric SpecName: PRIVATEBYTES

Metric Field Name: Private Bytes

Data type: UINT32

Alarm: FALSE

Metric: PerChatREPLICAThreadCount

Description: the number of threads currently active in this process. An instruction is the basic unit of execution in a processor, and a thread is the object that executes instructions. Every running process has at least one thread.

Metric SpecName: THREADCOUNT

Metric Field Name: Thread Count

Data type: UINT32

Alarm: FALSE

ChkDirectorFrontEndServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / NA

Source / Collection Definition: SERVICECHECK / RTCSrv

Metric: DirectorRTCSrvServName

> **Description**: Name of the Service
>
> **Metric SpecName**: SERVNAME
>
> **Metric Field Name**: Service_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: DirectorRTCSrvServDisplayName

> **Description**: Display Name of the Service
>
> **Metric SpecName**: SRVDISPNAME
>
> **Metric Field Name**: Service_Displayname
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: DirectorRTCSrvServStatus

> **Description**: Status of the Service
>
> **Metric SpecName**: SERVSTATUS
>
> **Metric Field Name**: Service_Status
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: DirectorRTCSrvServState

> **Description**: State of the Service
>
> **Metric SpecName**: SERVSTATE
>
> **Metric Field Name**: Service_State
>
> **Data type**: UINT32
>
> **Alarm**: TRUE
>
> **Category** : MSSkype
>
> **Severity / Threshold** : Major / 1
>
> **Policy**: MSBS_DirectorRTCSrvServState
>
> **Message text**: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>
>
> **Instructional Text**:
>
> **Probable Cause(s)**: NA
>
> **Potential Impact**: NA
>
> **Suggested Action(s)**: NA

ChkDirectorReplicaReplicatorAgentServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SERVSTAT

Source / Collection Definition: SERVICECHECK / REPLICA

Metric: DirectorREPLICAServName

> **Description**: Name of the Service
>
> **Metric SpecName**: SERVNAME
>
> **Metric Field Name**: Service_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: DirectorREPLICAServDisplayName

> **Description**: Display Name of the Service
>
> **Metric SpecName**: SRVDISPNAME
>
> **Metric Field Name**: Service_Displayname
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: DirectorREPLICAServStatus

> **Description**: Status of the Service
>
> **Metric SpecName**: SERVSTATUS
>
> **Metric Field Name**: Service_Status
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: DirectorREPLICAServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_DirectorREPLICAServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): Lync Server Replica Replicator Agent' Windows Service is stopped.

Potential Impact: NA

Suggested Action(s): Lync Server Replica Replicator Agent' Windows Service is stopped. Please restart the service.

WebRelayDataCollab

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: SKYPE / WEBRELAYDATACOLLAB

Source / Collection Definition: PERFMON / LS:WebRelay - 00 - Reach Web Relay Server(*)

Metric: ActiveAppShareConnections

Description: This metric captures Active App Share Connections

Metric SpecName: ActiveAppShareConn

Metric Field Name: WEBRELAY - 016 - Active AppShare Connections

Data type: REAL64

Alarm: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: ActiveSipConnections

Description: This metric captures Active Sip Connections

Metric SpecName: ActiveSipConn

Metric Field Name: WEBRELAY - 000 - Active Sip Connections

Data type: REAL64

Alarm: FALSE

Metric: NumOfDataCollaborationClientConnClosedDueToThrottlingPerSec

Description: This metric captures Number Of Data Collaboration Client Connections Closed Due To Throttling Per Second.

Metric SpecName: NumDtColClntConClsPS

Metric Field Name: WEBRELAY - 023 - Number of Data Collaboration client connections closed due to throttling per second.

Data type: REAL64

Alarm: FALSE

Metric: NumOfDataCollaborationConnFailWithDataCollaborationServers

Description: This metric captures Number Of Data Collaboration Connection Failures With Data Collaboration Servers.

Metric SpecName: NumDtColConFlDtClSrv

Metric Field Name: WEBRELAY - 031 - Number of Data Collaboration connection failures with Data Collaboration servers.

Data type: REAL64

Alarm: FALSE

Metric: NumOfFailedDataCollaborationAuthenticationRequestPerSecond

Description: This metric captures Number Of Failed Data Collaboration Authentication Request Per Second.

Metric SpecName: NumFailDTClAuthReqPS

Metric Field Name: WEBRELAY - 025 - Number of failed Data Collaboration authentication request per second.

Data type: REAL64

Alarm: FALSE

Metric: SipConnectionFailures

Description: This metric captures Sip Connection Failures

Metric SpecName: SipConnectionFailure

Metric Field Name: WEBRELAY - 006 - Sip Connection Failures

Data type: REAL64

Alarm: FALSE

Metric: SipConnectionFailuresPerSecond

Description: This metric captures Sip Connection Failures Per Second

Metric SpecName: SipConnectionFailPS

Metric Field Name: WEBRELAY - 007 - Sip Connection Failures per second.

Data type: REAL64

Alarm: FALSE

Metric: TotalNumOfQueuedBytesForDataCollaborationServerConnections

Description: This metric captures Total Number Of Queued Bytes For Data Collaboration Server Connections.

Metric SpecName: TotlNmQuBtDtClSrvCon

Metric Field Name: WEBRELAY - 035 - Total number of queued bytes for Data Collaboration Server Connections.

Data type: REAL64

Alarm: FALSE

Metric: ActiveAppShareConnections

Description: This metric captures Active App Share Connections

Metric SpecName: ActiveAppShareConn

Metric Field Name: WEBRELAY - Active AppShare Connections

Data type: REAL64

Alarm: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: ActiveSipConnections

Description: This metric captures Active Sip Connections

Metric SpecName: ActiveSipConn

Metric Field Name: WEBRELAY - Active Sip Connections

Data type: REAL64

Alarm: FALSE

Metric: NumOfDataCollaborationClientConnClosedDueToThrottlingPerSec

Description: This metric captures Number Of Data Collaboration Client Connections Closed Due To Throttling Per Second.

Metric SpecName: NumDtColClntConClsPS

Metric Field Name: WEBRELAY - Number of Data Collaboration client connections closed due to throttling per second.

Data type: REAL64

Alarm: FALSE

Metric: NumOfDataCollaborationConnFailWithDataCollaborationServers

Description: This metric captures Number Of Data Collaboration Connection Failures With Data Collaboration Servers.

Metric SpecName: NumDtColConFlDtClSrv

Metric Field Name: WEBRELAY - Number of Data Collaboration connection failures with Data Collaboration servers.

Data type: REAL64

Alarm: FALSE

Metric: NumOfFailedDataCollaborationAuthenticationRequestPerSecond

Description: This metric captures Number Of Failed Data Collaboration Authentication Request Per Second.

Metric SpecName: NumFailDTClAuthReqPS

Metric Field Name: WEBRELAY - Number of failed Data Collaboration authentication request per second.

Data type: REAL64

Alarm: FALSE

Metric: SipConnectionFailures

Description: This metric captures Sip Connection Failures

Metric SpecName: SipConnectionFailure

Metric Field Name: WEBRELAY - Sip Connection Failures

Data type: REAL64

Alarm: FALSE

Metric: SipConnectionFailuresPerSecond

Description: This metric captures Sip Connection Failures Per Second

Metric SpecName: SipConnectionFailPS

Metric Field Name: WEBRELAY - Sip Connection Failures per Second.

Data type: REAL64

Alarm: FALSE

Metric: TotalNumOfQueuedBytesForDataCollaborationServerConnections

Description: This metric captures Total Number Of Queued Bytes For Data Collaboration Server Connections.

Metric SpecName: TotlNmQuBtDtClSrvCon

Metric Field Name: WEBRELAY - Total number of queued bytes for Data Collaboration Server Connections.

Data type: REAL64

Alarm: FALSE

JoinLauncherRequests

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / JOINLAUNCHERREQUESTS

Source / Collection Definition: PERFMON / LS:JoinLauncher - Join Launcher Service incoming Requests(*)

Metric: IncomingJoinRequests

> **Description**: This metric captures Incoming Join Requests
>
> **Metric SpecName**: IncomingJoinRequests
>
> **Metric Field Name**: JOINLAUNCHER - Incoming Join Requests
>
> **Data type**: REAL64
>
> **Alarm**: FALSE

Metric: Instance_Name

> **Description**: This is the key for metric
>
> **Metric SpecName**: Instance_Name
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: IncomingJoinRequestsFromARMDevices

> **Description**: This metric captures Incoming Join Requests From ARM Devices
>
> **Metric SpecName**: IncomJoinReqFrmARMDv
>
> **Metric Field Name**: JOINLAUNCHER - Incoming Join Requests From ARM Devices
>
> **Data type**: REAL64
>
> **Alarm**: FALSE

ChkFrontEndBandwidthPolicyServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SERVSTAT

Source / Collection Definition: SERVICECHECK / RTCPDPCORE

Metric: FERTCPDPCOREServName

> **Description**: Name of the Service
>
> **Metric SpecName**: SERVNAME
>
> **Metric Field Name**: Service_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FERTCPDPCOREServDisplayName

> **Description**: Display Name of the Service
>
> **Metric SpecName**: SRVDISPNAME
>
> **Metric Field Name**: Service_Displayname
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FERTCPDPCOREServStatus

> **Description**: Status of the Service
>
> **Metric SpecName**: SERVSTATUS
>
> **Metric Field Name**: Service_Status
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FERTCPDPCOREServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_FERTCPDPCOREServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): Lync Server Bandwidth Policy Service' Windows Service is stopped.

Potential Impact: NA

Suggested Action(s): Lync Server Bandwidth Policy Service' Windows Service is stopped. Please restart the service.

LoadManagement

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / KHILOADMANG

Source / Collection Definition: PERFMON / LS:SIP - 07 - Load Management(*)

Metric: IncomingMessagesTimedout

Description: This policy monitors the number of incoming messages currently being held by the server for processing for more than the maximum tracking interval.

Metric SpecName: IncomMessTimou

Metric Field Name: SIP - 006 - Incoming Messages Timed out

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Minor / 2, Minor / 2

Policy: MSBS_IncomingMessagesTimedout

Message text: The current value of IncomingMessagesTimedout is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): This server is too busy and is unable to process user requests in timely fashion.

Potential Impact: Please ensure that the hardware and software requirements meet the user usage characteristics.

Suggested Action(s): Slow SIP message transmissions

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: IncomingMessagesTimedout

Description: This policy monitors the number of incoming messages currently being held by the server for processing for more than the maximum tracking interval.

Metric SpecName: IncomMessTimou

Metric Field Name: SIP - Incoming Messages Timed out

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Minor / 2, Minor / 2

Policy: MSBS_IncomingMessagesTimedout

Message text: The current value of IncomingMessagesTimedout is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): This server is too busy and is unable to process user requests in timely fashion.

Potential Impact: Please ensure that the hardware and software requirements meet the user usage characteristics.

Suggested Action(s): Slow SIP message transmissions

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

AuthProviderrelatedcalls

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / KHIAUTHPROCALL

Source / Collection Definition: PERFMON / LS:WEB - 06 - Auth Provider related calls(*)

Metric: Failedvalidcertcallstocertauthprovider

> **Description**: This policy monitors the number of failed validate cert calls to the cert auth provider
>
> **Metric SpecName**: Failvalicercalceau
>
> **Metric Field Name**: WEB - 006 - Failed validate cert calls to the cert auth provider
>
> **Data type**: UINT32
>
> **Alarm**: TRUE
>
> **Category** : MSSkype
>
> **Severity / Threshold** : Minor / 0, Minor / 0
>
> **Policy**: MSBS_Failedvalidcertcallstocertauthprovider
>
> **Message text**: The current value of Failedvalidcertcallstocertauthprovider is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:
>
> **Instructional Text**:
>
> **Probable Cause(s)**: AD encounters this state when one or more authentication providers fail to load. This is more common to occur on custom authentication providers used for multi-factor authentication.
>
> **Potential Impact**: In most cases be remediated by ensuring those servers can access the CRL on the internet over port 80. To validate further, check the Microsoft-Windows-CAPI2 event logs.
>
> **Suggested Action(s)**: Certificate authetication failure.

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: Failedvalidcertcallstocertauthprovider

Description: This policy monitors the number of failed validate cert calls to the cert auth provider

Metric SpecName: Failvalicercalceau

Metric Field Name: WEB - Failed validate cert calls to the cert auth provider

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Minor / 0, Minor / 0

Policy: MSBS_Failedvalidcertcallstocertauthprovider

Message text: The current value of Failedvalidcertcallstocertauthprovider is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): AD encounters this state when one or more authentication providers fail to load. This is more common to occur on custom authentication providers used for multi-factor authentication.

Potential Impact: In most cases be remediated by ensuring those servers can access the CRL on the internet over port 80. To validate further, check the Microsoft-Windows-CAPI2 event logs.

Suggested Action(s): Certificate authetication failure.

Metric: Instance_Name

> **Description**: This is the key for metric
>
> **Metric SpecName**: Instance_Name
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Collect_FrontEnd_Web_Throttling_Authentication

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / LSWEBTHROTLAUTH

Source / Collection Definition: PERFMON / LS:WEB - Throttling and Authentication(*)

Metric: ThrottlingAndAuthInstance

> **Description**: instance of perfmon object LS:WEB - Throttling and Authentication
>
> **Metric SpecName**: THROTANDAUTHINST
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FailedHTTPProxyRequests

Description: the number of HTTP proxy requests that failed.

Metric SpecName: FAILEDHTTPPROXYREQ

Metric Field Name: WEB - Failed HTTP Proxy Requests

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 10, Major / 30

Policy: MSBS_FailedHTTPProxyRequests

Message text: The value of Failed HTTP Proxy Requests for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Attempts to forward an HTTP request to another server have failed.

Potential Impact: NA

Suggested Action(s): Check the Event log for reports of problems with specific servers and determine if those servers are functioning and reachable from this server.

Metric: NumberofProxyRequestsAwaitingCompletion

Description: Number of proxy requests awaiting completion.

Metric SpecName: PROXYREQAWAITCOMPL

Metric Field Name: WEB - Number of proxy requests awaiting completion

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 2000, Major / 2499

Policy: MSBS_NumberofProxyRequestsAwaitingCompletion

Message text: The value of Number of proxy requests awaiting completion for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): This value may grow if an application is overloaded because of a large number of requests.

Potential Impact: NA

Suggested Action(s): If the traffic volume is overloading the server, reduce traffic by adding additional servers to the pool.

Metric: RequestsExceededPerAppLimit

Description: the number of requests that were rejected because per-application queue limit was exceeded

Metric SpecName: REQEXCEEDPERAPPLMT

Metric Field Name: WEB - Requests Exceeded Per-App Limit

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 1, Major / 3

Policy: MSBS_RequestsExceededPerAppLimit

Message text: The value of Requests Exceeded Per-App Limit for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): This value may grow if an application is overloaded because of a large number of requests.

Potential Impact: NA

Suggested Action(s): If the traffic volume is overloading the server, reduce traffic by adding additional servers to the pool.

Metric: TotalRequestsInProcessing

Description: the total number of requests currently being processed by application.

Metric SpecName: TOTREQINPROC

Metric Field Name: WEB - Total Requests In Processing

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 2000, Major / 2499

Policy: MSBS_TotalRequestsInProcessing

Message text: The value of Total Requests In Processing for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): This value may grow if an application is overloaded because of a large number of requests.

Potential Impact: NA

Suggested Action(s): If the traffic volume is overloading the server, reduce traffic by adding additional servers to the pool.

Metric: UnAuthenticatedRequestInProcessing

Description: the number of requests currently in processing by application that have not yet been authenticated or are processed anonymously.

Metric SpecName: UNAUTHREQINPROC

Metric Field Name: WEB - Unauthenticated Requests In Processing

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 2000, Major / 2499

Policy: MSBS_UnAuthenticatedRequestInProcessing

Message text: The value of Unauthenticated Requests In Processing for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): This value may grow if an application is overloaded because of a large number of requests.

Potential Impact: NA

Suggested Action(s): If the traffic volume is overloading the server, reduce traffic by adding additional servers to the pool.

AudioNetworkMOSPoorCallsPercentage

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / AUDIONETWORKMOSCALLS

Source / Collection Definition: SQLDB / select isnull(cast(100.0 * cast((SUM(CASE WHEN [AudioOverallAvgNetworkMOS] > 0.50 THEN 1 ELSE 0 END)) as float) / cast((SUM(CASE WHEN

MediaLineLabel is NOT NULL THEN 1 ELSE 0 END)) as float) as decimal(4, 1)),0) as AudioNetworkMOSPoorCallsPercentage,SERVERPROPERTY('MACHINENAME') AS 'ServerName' from [QoEMetrics].[dbo].[QoEReportsCallDetailView] Where MediaLineLabel = 0 AND ConferenceDateTime >= dateadd(MINUTE,@Duration,GETUTCDATE())

Metric: AudioNetworkMOSPoorCallsPercentage

> **Description**: This metric captures Poor Audio that a Network Degradation Mean Opinion Score more than a set threshold value and calculates percentage of poor calls for a given interval. At the end of each call, parameters that determine Quality of a call that include network, audio and video parameters are logged into QoE database of Lync Server. Each call is categorized as having Acceptable quality or Poor quality based on the same. Network Degradation Mean Opinion Score(MOS) is a prediction of the wideband Listening Quality Mean Opinion Score (MOS-LQ) of audio that is played to the user. This value takes into consideration only network factors such as codec used, packet loss, packet reorder, packet errors and jitter.It is on a scale of 1 to 5
>
> **Metric SpecName**: AudNetwMOSPoorCall
>
> **Metric Field Name**: AudioNetworkMOSPoorCallsPercentage
>
> **Data type**: REAL64
>
> **Alarm**: TRUE
>
> **Category** : MSSkype
>
> **Severity / Threshold** : Warning / 40, Major / 70, Warning / 40, Major / 70
>
> **Policy**: MSBS_AudioNetworkMOSPoorCallsPercentage
>
> **Message text**: The current value of Percentage Audio Network MOS Poor Calls is <VALUE> which exceeds the threshold of <THRESHOLD>
>
> **Instructional Text**:
>
> **Probable Cause(s)**: This is a derived value by taking network factors such as audio codec , packet loss, packet reordering, packet level errors and jitter into consideration
>
> **Potential Impact**: -Poor Voice quality -Echo -Audio Latency -Call drops -Noise
>
> **Suggested Action(s)**: Network upgrade Reconfigure routing rules

Metric: ServerName

Description: This is the key for metric

Metric SpecName: ServerName

Metric Field Name: ServerName

Data type: TEXT

Alarm: FALSE

Metric: AudioNetworkMOSPoorCallsPercentage

Description: This metric captures Poor Audio that a Network Degradation Mean Opinion Score more than a set threshold value and calculates percentage of poor calls for a given interval. At the end of each call, parameters that determine Quality of a call that include network, audio and video parameters are logged into QoE database of Lync Server. Each call is categorized as having Acceptable quality or Poor quality based on the same. Network Degradation Mean Opinion Score(MOS) is a prediction of the wideband Listening Quality Mean Opinion Score (MOS-LQ) of audio that is played to the user. This value takes into consideration only network factors such as codec used, packet loss, packet reorder, packet errors and jitter.It is on a scale of 1 to 5

Metric SpecName: AudNetwMOSPoorCall

Metric Field Name: AudioNetworkMOSPoorCallsPercentage

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 40, Major / 70, Warning / 40, Major / 70

Policy: MSBS_AudioNetworkMOSPoorCallsPercentage

Message text: The current value of Percentage Audio Network MOS Poor Calls is <VALUE> which exceeds the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): This is a derived value by taking network factors such as audio codec , packet loss, packet reordering, packet level errors and jitter into consideration

Potential Impact: -Poor Voice quality -Echo -Audio Latency -Call drops -Noise

Suggested Action(s): Network upgrade Reconfigure routing rules

Metric: ServerName

> **Description**: This is the key for metric
>
> **Metric SpecName**: ServerName
>
> **Metric Field Name**: ServerName
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Collect_Mediation_Process_MediationServerSvc

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / CS_PROCESS

Source / Collection Definition: PERFMON / Process(MediationServerSvc)

Metric: MedREPLICAInstance

> **Description**: instance of mediationServerSvc
>
> **Metric SpecName**: INSTANCENAME
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: MedREPLICAPercentprocessorTime

Description: Percentage Processor Time is the percentage of elapsed time that all of process threads used the processor to execution instructions.

Metric SpecName: PCTPROCESSORTIME

Metric Field Name: % Processor Time

Data type: UINT32

Alarm: FALSE

Metric: MedREPLICAWorkingSet

Description: Working Set is the current size, in bytes, of the Working Set of this process. the Working Set is the set of memory pages touched recently by the threads in the process. If free memory in the computer is above a threshold, pages are left in the Working Set of a process even if they are not in use. When free memory falls below a threshold, pages are trimmed from Working Sets. If they are needed they will then be soft-faulted back into the Working Set before leaving main memory.

Metric SpecName: WORKINGSET

Metric Field Name: Working Set

Data type: UINT32

Alarm: FALSE

Metric: MedREPLICAPageFaultsPerSec

Description: Page Faults/sec is the average number of pages faulted per second. It is measured in number of pages faulted per second because only one page is faulted in each fault operation, hence this is also equal to the number of page fault operations. This counter includes both hard faults (those that require disk access) and soft faults (where the faulted page is found elsewhere in physical memory.) Most processors can handle large numbers of soft faults without significant consequence. However, hard faults, which require disk access, can cause significant delays.

Metric SpecName: PAGEFAULTS

Metric Field Name: Page Faults/sec

Data type: UINT32

Alarm: FALSE

Metric: MedREPLICAPrivateBytes

Description: Private Bytes is the current size, in bytes, of memory that this process has allocated that cannot be shared with other processes.

Metric SpecName: PRIVATEBYTES

Metric Field Name: Private Bytes

Data type: UINT32

Alarm: FALSE

Metric: MedREPLICAThreadCount

Description: the number of threads currently active in this process. An instruction is the basic unit of execution in a processor, and a thread is the object that executes instructions. Every running process has at least one thread.

Metric SpecName: THREADCOUNT

Metric Field Name: Thread Count

Data type: UINT32

Alarm: FALSE

Metric: MedMediationServerSvcInstance

Description: instance of mediationServerSvc

Metric SpecName: INSTANCENAME

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: MedMediationServerSvcPercentprocessorTime

Description: Percentage Processor Time is the percentage of elapsed time that all of process threads used the processor to execution instructions.

Metric SpecName: PCTPROCESSORTIME

Metric Field Name: % Processor Time

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 90

Policy: MSBS_MedMediationServerSvcPercentprocessorTime

Message text: The value of the counter '% Processor Time' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: MedMediationServerSvcWorkingSet

Description: Working Set is the current size, in bytes, of the Working Set of this process. the Working Set is the set of memory pages touched recently by the threads in the process. If free memory in the computer is above a threshold, pages are left in the Working Set of a process even if they are not in use. When free memory falls below a threshold, pages are trimmed from Working Sets. If they are needed they will then be soft-faulted back into the Working Set before leaving main memory.

Metric SpecName: WORKINGSET

Metric Field Name: Working Set

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20000000

Policy: MSBS_MedMediationServerSvcWorkingSet

Message text: The value of the counter 'Working Set' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: MedMediationServerSvcPageFaultsPerSec

Description: Page Faults/sec is the average number of pages faulted per second. It is measured in number of pages faulted per second because only one page is faulted in each fault operation, hence this is also equal to the number of page fault operations. This counter includes both hard faults (those that require disk access) and soft faults (where the faulted page is found elsewhere in physical memory.) Most processors can handle large numbers of soft faults without significant consequence. However, hard faults, which require disk access, can cause significant delays.

Metric SpecName: PAGEFAULTS

Metric Field Name: Page Faults/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 100

Policy: MSBS_MedMediationServerSvcPageFaultsPerSec

Message text: The value of the counter 'Page Faults/sec' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: MedMediationServerSvcPrivateBytes

Description: Private Bytes is the current size, in bytes, of memory that this process has allocated that cannot be shared with other processes.

Metric SpecName: PRIVATEBYTES

Metric Field Name: Private Bytes

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20000000

Policy: MSBS_MedMediationServerSvcPrivateBytes

Message text: The value of the counter 'Private Bytes' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: MedMediationServerSvcThreadCount

Description: the number of threads currently active in this process. An instruction is the basic unit of execution in a processor, and a thread is the object that executes instructions. Every running process has at least one thread.

Metric SpecName: THREADCOUNT

Metric Field Name: Thread Count

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 150

Policy: MSBS_MedMediationServerSvcThreadCount

Message text: The value of the counter 'Thread Count' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Collect_Director_WebRelay_Data_Collab

This polcy gives us the information for the collaboration of Skype Business Server

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collaboration_Service_Conf

Aspect: Skype Collaboration Service

CIT: Edge Server, Director Server, Front End Server

Data source / Data class: LYNC / LSWEBRELAY

Source / Collection Definition: PERFMON / LS:WebRelay - Data Collab Web Relay Server(*)

Metric: DirectorWebRelayDataCollabInstance

Description: instance of perfmon object LS:WebRelay - Data Collab Web Relay Server

Metric SpecName: WEBRELAYINSTANCE

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: DirNofDCClientConnClosedDuetoThrottlingPerSecond

Description: the number of Data Collaboration client connections closed due to throttling per second.

Metric SpecName: DCCLNTCONNCLOSED

Metric Field Name: WEBRELAY - Number of Data Collaboration client connections closed due to throttling per second

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 25, Major / 50

Policy: MSBS_DirNofDCClientConnClosedDuetoThrottlingPerSecond

Message text: The value of WEBRELAY - Number of Data Collaboration client connections closed due to throttling per second for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Client Data Collaboration was closed because client failed to read data in a timely manner. This may indicate a network failure.

Potential Impact: NA

Suggested Action(s): Check client network connectivity to Lync Web App.

Metric: DirectorNoDCConnFailureWithServers

Description: the number of Data Collaboration connection failures with Data Collaboration servers.

Metric SpecName: DCCONFAILURE

Metric Field Name: WEBRELAY - Number of Data Collaboration connection failures with Data Collaboration servers

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 5, Major / 10

Policy: MSBS_DirectorNoDCConnFailureWithServers

Message text: The value of WEBRELAY - Number of Data Collaboration connection failures with Data Collaboration servers for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Connection closed by local party or remote party or network issues.

Potential Impact: NA

Suggested Action(s): Check availability of Web Conferencing Server servers.

Metric: DirectorNoFailedDCAuthRequestsPerSecond

Description: the number of failed Data Collaboration authentication request per second.

Metric SpecName: DATACOLLABAUTHREQ

Metric Field Name: WEBRELAY - Number of failed Data Collaboration authentication request per second

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 10, Major / 20

Policy: MSBS_DirectorNoFailedDCAuthRequestsPerSecond

Message text: The value of WEBRELAY - Number of failed Data Collaboration authentication request per second for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Attempts to authenticate incoming client connections for data collaboration failed.

Potential Impact: NA

Suggested Action(s): Perform

Metric: DirectorNoQueuedBytesForDCServerConnections

Description: the total number of queued bytes for Data Collaboration Server Connections.

Metric SpecName: DATACOLLABSRVCONQ

Metric Field Name: WEBRELAY - Total number of queued bytes for Data Collaboration Server Connections

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 536870912, Major / 1073741824

Policy: MSBS_DirectorNoQueuedBytesForDCServerConnections

Message text: The value of WEBRELAY - Total number of queued bytes for Data Collaboration Server Connections for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Failure to read outgoing date by Web Conferencing Server servers.

Potential Impact: NA

Suggested Action(s): Check availability of Web Conferencing Server servers. Also check network connectivity.

Metric: DirectorSIPConnectionFailuresPerSecond

Description: the number of Sip connection failures per second.

Metric SpecName: SIPCONNFAILURE

Metric Field Name: WEBRELAY - Sip Connection Failures per second

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 25, Major / 50

Policy: MSBS_DirectorSIPConnectionFailuresPerSecond

Message text: The value of WEBRELAY - Sip Connection Failures per second for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Sip connection is terminated unexpectedly due to network issues or unavailability of remote servers.

Potential Impact: NA

Suggested Action(s): Check network and SIP server availability.

PSTNPeer2PeerCall

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_LOW

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SYNNPDPSTNP2PCALL

Source / Collection Definition: POWERSHELL / Test-CsPstnPeerToPeerCall -TargetFQDN {fqdn}

Metric: PSTNPeer2PeerCall

Description: This metric gathers the information which confirms that users are able to place and receive calls with people outside of the enterprise (PSTN numbers).

Metric SpecName: PSTNP2PCall

Metric Field Name: PSTNPeer2PeerCall

Data type: TEXT

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Minor / 1, Minor / 1

Policy: MSBS_PSTNPeer2PeerCall

Message text: The PSTN Peer 2 Peer Call is down

Instructional Text:

Probable Cause(s): 1. User configuration must not have done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: New users cannot be registered

Suggested Action(s): 1. Configuration errors: Most common issues are: Test user password is invalid or expired, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availability: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution errors or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responded to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Metric: TargetFqdn

Description: This is the key for metric

Metric SpecName: TargetFqdn

Metric Field Name: TargetFqdn

Data type: TEXT

Alarm: FALSE

Metric: PSTNPeer2PeerCallLatency

Description: This metric will capture latency in receipt of confirmation that users are able to place and receive calls with people outside of the enterprise (PSTN numbers).

Metric SpecName: PSTNP2PCallLat

Metric Field Name: PSTNPeer2PeerCallLatency

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Minor / 1000, Minor / 1000

Policy: MSBS_PSTNPeer2PeerCallLatency

Message text: The value of PSTN Peer 2 Peer Call Latency is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): 1. User configuration must not have done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: New users cannot be registered

Suggested Action(s): 1. Configuration errors: Most common issues are: Test user password is invalid or expired, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availibility: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution errors or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responded to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Metric: PSTNPeer2PeerCall

Description: This metric gathers the information which confirms that users are able to place and receive calls with people outside of the enterprise (PSTN numbers).

Metric SpecName: PSTNP2PCall

Metric Field Name: PSTNPeer2PeerCall

Data type: TEXT

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Minor / 1, Minor / 1

Policy: MSBS_PSTNPeer2PeerCall

Message text: The PSTN Peer 2 Peer Call is down

Instructional Text:

Probable Cause(s): 1. User configuration must not have done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: New users cannot be registered

Suggested Action(s): 1. Configuration errors: Most common issues are: Test user password is invalid or expired, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availability: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution errors or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responded to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Metric: TargetFqdn

Description: This is the key for metric

Metric SpecName: TargetFqdn

Metric Field Name: TargetFqdn

Data type: TEXT

Alarm: FALSE

Metric: PSTNPeer2PeerCallLatency

Description: This metric will capture latency in receipt of confirmation that users are able to place and receive calls with people outside of the enterprise (PSTN numbers).

Metric SpecName: PSTNP2PCallLat

Metric Field Name: PSTNPeer2PeerCallLatency

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Minor / 1000, Minor / 1000

Policy: MSBS_PSTNPeer2PeerCallLatency

Message text: The value of PSTN Peer 2 Peer Call Latency is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): 1. User configuration must not have done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: New users cannot be registered

Suggested Action(s): 1. Configuration errors: Most common issues are: Test user password is invalid or expired, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availibility: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution errors or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responded to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

SharedDBStore

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / KHISHDBSTORE

Source / Collection Definition: PERFMON / LS:Usrv - SharedDBStore

Metric: SHAREDDBStoreQueueLatency

Description: This policy monitors the average time a request is held in the request queue to RTCShared database

Metric SpecName: ShDBStQueueLatency

Metric Field Name: Usrv - Queue Latency (msec)

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 100

Policy: MSBS_SHAREDDBStoreQueueLatency

Message text: The current value of SHAREDDBStoreQueueLatency is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): The backend might be busy and is unable to respond to requests quickly.

Potential Impact: Please ensure that the hardware and software requirements meet the user usage characteristics.

Suggested Action(s): The average time a request is held in the request queue to RTCShared database would be high and would lead to a delayed response.

Metric: SHAREDDBStoreSprocLatency

Description: This policy monitors the average time it takes to execute a sproc call against RTCShared database.

Metric SpecName: ShDBStSprocLatency

Metric Field Name: Usrv - Sproc Latency (msec)

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 100

Policy: MSBS_SHAREDDBStoreSprocLatency

Message text: The current value of SHAREDDBStoreSprocLatency is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): The backend might be busy and is unable to respond to requests quickly.

Potential Impact: Please ensure that the hardware and software requirements meet the user usage characteristics.

Suggested Action(s): The average time it takes to execute a sproc call against RTCShared database.

Metric: SHAREDDBStoreThrottledrequests

Description: This policy monitors the number of requests that were rejected with a retry since the database queue latency was high.

Metric SpecName: ShDBStThrottledreq

Metric Field Name: Usrv - Throttled requests/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 0

Policy: MSBS_SHAREDDBStoreThrottledrequests

Message text: The current value of SHAREDDBStoreThrottledrequests is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): The backend might be busy and is unable to respond to requests quickly.

Potential Impact: Please ensure that the hardware and software requirements meet the user usage characteristics.

Suggested Action(s): The number of requests that were rejected with a retry since the database queue latency was high.

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Collect_FrontEnd_IMMCU_Health_And_Performance

This policy gives us the information about the Server Health

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Server_Health_Conf

Aspect: Skype Server Health

CIT: Mediation Server, AV Conferencing Server, Front End Server

Data source / Data class: LYNC / LSIMMCUHLTPERF

Source / Collection Definition: PERFMON / LS:ImMcu - MCU Health And Performance(*)

Metric: MCUHealthInstance

> **Description**: instance of perfmon object LS:ImMcu - MCU Health And Performance
>
> **Metric SpecName**: IMMCUHEALTHINST
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: MCUHealthState

> **Description**: the current health of the MCU. 0 = Normal. 1 = Loaded. 2 = Full. 3 = Unavailable.
>
> **Metric SpecName**: IMMCUHEALTHSTATE
>
> **Metric Field Name**: IMMCU - MCU Health State
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

ChkPersistentChatReplicaReplicatorAgentServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SERVSTAT

Source / Collection Definition: SERVICECHECK / REPLICA

Metric: PersistentChatREPLICAServName

> **Description**: Name of the Service
>
> **Metric SpecName**: SERVNAME
>
> **Metric Field Name**: Service_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: PersistentChatREPLICAServDisplayName

> **Description**: Display Name of the Service
>
> **Metric SpecName**: SRVDISPNAME
>
> **Metric Field Name**: Service_Displayname
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: PersistentChatREPLICAServStatus

> **Description**: Status of the Service
>
> **Metric SpecName**: SERVSTATUS
>
> **Metric Field Name**: Service_Status
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: PersistentChatREPLICAServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_PersistentChatREPLICAServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): Lync Server Replica Replicator Agent' Windows Service is stopped.

Potential Impact: NA

Suggested Action(s): Lync Server Replica Replicator Agent' Windows Service is stopped. Please restart the service.

SimplePortWatcher5061

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / Port5061

Source / Collection Definition: PORTCOL / PORTCHECKER

Metric: SimpleWatcherPort5061

Description: Used by Standard Edition servers and Front End pools for all internal SIP communications between servers (MTLS), for SIP communications between Server and Client (TLS) and for SIP communications between Front End Servers and Mediation Servers (MTLS). Also used for communications with Monitoring Server.

Metric SpecName: SimpleWatcherPort5061

Metric Field Name: SimpleWatcherPort5061

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort5061

Message text: The Port No:5061 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

Metric: SimpleWatcherPort5061

Description: Used by Standard Edition servers and Front End pools for all internal SIP communications between servers (MTLS), for SIP communications between Server and Client (TLS) and for SIP communications between Front End Servers and Mediation Servers (MTLS). Also used for communications with Monitoring Server.

Metric SpecName: SimpleWatcherPort5061

Metric Field Name: SimpleWatcherPort5061

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort5061

Message text: The Port No:5061 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

> **Description**: This is the key for metric
>
> **Metric SpecName**: HOSTNAME
>
> **Metric Field Name**: HOSTNAME
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Collect_FrontEnd_Web_AddressBook_File_Downlaod

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / FELSWEBADDRBKDNL

Source / Collection Definition: PERFMON / LS:WEB - Address Book File Download(*)

Metric: WEBAddrBookFileDnlInstance

> **Description**: instance of perfmon object LS:WEB - Address Book File Download
>
> **Metric SpecName**: ADFEWEBINSTANCE
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FailedFileRequests

Description: the per-second rate of failed Address Book file requests

Metric SpecName: FEFAILEDREQUESTS

Metric Field Name: WEB - Failed File Requests/Second

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 4, Major / 20

Policy: MSBS_FailedFileRequests

Message text: The value of Address Book File Download Failed File Requests/Second for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Caused by authentication issues or network connectivity issues

Potential Impact: NA

Suggested Action(s): Check Lync Server event log for failure causes and correct

PDPAuthRequests

This policy maintains the information about the status for the different services

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_ConferenceProcPerform_2010_Conf

Aspect: Skype Conference Processing Performance

CIT: Mediation Server, Front End Server, Edge Server

Data source / Data class: SKYPE / PDPAUTHREQUESTS

Source / Collection Definition: PERFMON / LS:PDP Auth - Requests(*)

Metric: CredentialsIssued

Description: This metric captures Credentials Issued

Metric SpecName: CredentialsIssued

Metric Field Name: CredentialsIssued

Data type: REAL64

Alarm: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: CurrentRequestsServiced

Description: This metric captures Current Requests Serviced

Metric SpecName: CurrentRequestsSrv

Metric Field Name: CurrentRequestsServiced

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 30, Warning / 30

Policy: MSBS_CurrentRequestsServiced

Message text: The value of Current Requests Serviced is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Edge server is not properly configured

Potential Impact: Select an existing A/V Authentication Service. Install an A/V Authentication Service if you do not have one.

Suggested Action(s): Connections that require firewall traversal may not be successful

Metric: CredentialsIssued

> **Description**: This metric captures Credentials Issued
>
> **Metric SpecName**: CredentialsIssued
>
> **Metric Field Name**: - Credentials Issued
>
> **Data type**: REAL64
>
> **Alarm**: FALSE

Metric: Instance_Name

> **Description**: This is the key for metric
>
> **Metric SpecName**: Instance_Name
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: CredentialsIssuedPerSec

Description: This metric captures Credentials Issued Per Sec

Metric SpecName: CredentialsIssuedPS

Metric Field Name: - Credentials Issued/sec

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 30

Policy: MSBS_CredentialsIssuedPerSec

Message text: The number of Credentials Issued Per Second is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): The Audio-Video Conferencing Server cannot communicate with A/V Authentication Service.

Potential Impact: Check the A/V Authentication Service is alive and that network connectivity exists.

Suggested Action(s): Users face issue In Connecting to Audio-Video Conferencing Server

Metric: CurrentRequestsServiced

Description: This metric captures Current Requests Serviced

Metric SpecName: CurrentRequestsSrv

Metric Field Name: - Current requests serviced

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 30, Warning / 30

Policy: MSBS_CurrentRequestsServiced

Message text: The value of Current Requests Serviced is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Edge server is not properly configured

Potential Impact: Select an existing A/V Authentication Service. Install an A/V Authentication Service if you do not have one.

Suggested Action(s): Connections that require firewall traversal may not be successful

NumberOfAggregationRequestsPerSecond

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / NUMBEROFAGGREREQPS

Source / Collection Definition: PERFMON / LS:USrv - Server Aggregation(*)

Metric: NumberOfAggregationRequestsPerSecond

> **Description**: This metric captures Number Of Aggregation Requests Per Second
>
> **Metric SpecName**: NumberOfAggreReqPS
>
> **Metric Field Name**: USrv - Number Of Aggregation Requests/Second
>
> **Data type**: REAL64
>
> **Alarm**: FALSE

Metric: Instance_Name

> **Description**: This is the key for metric
>
> **Metric SpecName**: Instance_Name
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Collect_FrontEnd_Process_MeetingMCUSvc

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / CS_PROCESS

Source / Collection Definition: PERFMON / Process(MeetingMCUSvc)

Metric: FEMeetingMCUSvcInstance

Description: instance of perfmon object Process(MeetingMCUSvc)

Metric SpecName: INSTANCENAME

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: FEMeetingMCUPageFaultsPersec

Description: The Page Faults / sec of Web Conference compatibility proces

Metric SpecName: PCMMCUPAGEFAULTPERSEC

Metric Field Name: Page Faults/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 100

Policy: MSBS_FEMeetingMCUPageFaultsPersec

Message text: The value of the counter 'Page Faults/sec' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: FEMeetingMCUPrivateBytes

Description: Private bytes of Web conference compatibility process

Metric SpecName: PCMMCUPRIVATEBYTES

Metric Field Name: Private Bytes

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20000000

Policy: MSBS_FEMeetingMCUPrivateBytes

Message text: The value of the counter 'Private Bytes' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: FEMeetingMCUPercentProcessorTime

Description: % processor time of web conference compatibility process

Metric SpecName: PCMMCUPROCESSORTIME

Metric Field Name: % Processor Time

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 90

Policy: MSBS_FEMeetingMCUPercentProcessorTime

Message text: The value of the counter '% Processor Time' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: FEMeetingMCUThreadCount

Description: The thread count of web conference compatibility process

Metric SpecName: PCMMCUTHREADCOUNT

Metric Field Name: Thread Count

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 150

Policy: MSBS_FEMeetingMCUThreadCount

Message text: The value of the counter 'Thread Count' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: FEMeetingMCUWorkingSet

Description: The Working Set bytes of web conference compatibility process

Metric SpecName: PCMMCUWORKINGSET

Metric Field Name: Working Set

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20000000

Policy: MSBS_FEMeetingMCUWorkingSet

Message text: The value of the counter 'Working Set' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

SIPInstantMessaging

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / KHISIPINSMESS

Source / Collection Definition: PERFMON / LS:XMPPFederation - SIP Instant Messaging

Metric: FailureIMDNssent

Description: This policy monitors the Failure IMDNs sent/sec

Metric SpecName: FailureIMDNssent

Metric Field Name: XMPPFederation - Failure IMDNs sent/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Minor / 0

Policy: MSBS_FailureIMDNssent

Message text: The current value of FailureIMDNssent is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): XMPP Gateway not configured properly

Potential Impact: Review Configure XMPP Gateway on Lync Server 2013. Use Test-CsXmppIM to verify whether or not an instant message can be sent across an XMPP gateway.

Suggested Action(s): Failure to send XMPP messages

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

SimplePortWatcher5068

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / Port5068

Source / Collection Definition: PORTCOL / PORTCHECKER

Metric: SimpleWatcherPort5068

Description: Used for incoming SIP requests from the PSTN gateway.

Metric SpecName: SimpleWatcherPort5068

Metric Field Name: SimpleWatcherPort5068

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort5068

Message text: The Port No:5068 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

Metric: SimpleWatcherPort5068

Description: Used for incoming SIP requests from the PSTN gateway.

Metric SpecName: SimpleWatcherPort5068

Metric Field Name: SimpleWatcherPort5068

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort5068

Message text: The Port No:5068 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

> **Description**: This is the key for metric
>
> **Metric SpecName**: HOSTNAME
>
> **Metric Field Name**: HOSTNAME
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Collect_Director_AddressBook_FileDownload

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / DIRLSWEBADDRBKDNL

Source / Collection Definition: PERFMON / LS:WEB - Address Book File Download(*)

Metric: DirectorAddressBookDownloadInstance

> **Description**: instance of perfmon object LS:WEB - Address Book File Download
>
> **Metric SpecName**: DIRADWEBINSTANCE
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: DirectorFailedRequestsperSecond

Description: the per-second rate of failed Address Book file requests

Metric SpecName: DIRFAILEDREQUESTS

Metric Field Name: WEB - Failed File Requests/Second

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 3, Major / 6

Policy: MSBS_DirectorFailedRequestsperSecond

Message text: The value of WEB - Failed File Requests/Second for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Caused by authentication issues or network connectivity issues

Potential Impact: NA

Suggested Action(s): Check Lync Server event log for failure causes and correct

Collect_Edge_DataCollab_WebRelay_Server

This polcy gives us the information for the collaboration of Skype Business Server

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collaboration_Service_Conf

Aspect: Skype Collaboration Service

CIT: Edge Server, Director Server, Front End Server

Data source / Data class: LYNC / LSWEBRELAY

Source / Collection Definition: PERFMON / LS:WebRelay - Data Collab Web Relay Server(*)

Metric: EdgeWebRelayDataCollabInstance

Description: instance of perfmon object LS:WebRelay - Data Collab Web Relay Server

Metric SpecName: WEBRELAYINSTANCE

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: EdgeNofDCClientConnClosedDuetoThrottlingPerSec

Description: the number of Data Collaboration client connections closed due to throttling per second.

Metric SpecName: DCCLNTCONNCLOSED

Metric Field Name: WEBRELAY - Number of Data Collaboration client connections closed due to throttling per second

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 25, Major / 50

Policy: MSBS_EdgeNofDCClientConnClosedDuetoThrottlingPerSec

Message text: The value of WEBRELAY - Number of Data Collaboration client connections closed due to throttling per second for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Client Data Collaboration was closed because client failed to read data in a timely manner. This may indicate a network failure.

Potential Impact: NA

Suggested Action(s): Check client network connectivity to Lync Web App.

Metric: EdgeNoDCConnFailureWithServers

Description: the number of Data Collaboration connection failures with Data Collaboration servers.

Metric SpecName: DCCONFAILURE

Metric Field Name: WEBRELAY - Number of Data Collaboration connection failures with Data Collaboration servers

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 5, Major / 10

Policy: MSBS_EdgeNoDCConnFailureWithServers

Message text: The value of WEBRELAY - Number of Data Collaboration connection failures with Data Collaboration servers for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Connection closed by local party or remote party or network issues.

Potential Impact: NA

Suggested Action(s): Check availability of Web Conferencing Server servers.

Metric: EdgeNoFailedDCAuthRequestsPerSecond

Description: the number of failed Data Collaboration authentication request per second.

Metric SpecName: DATACOLLABAUTHREQ

Metric Field Name: WEBRELAY - Number of failed Data Collaboration authentication request per second

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 10, Major / 20

Policy: MSBS_EdgeNoFailedDCAuthRequestsPerSecond

Message text: The value of WEBRELAY - Number of failed Data Collaboration authentication request per second for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Attempts to authenticate incoming client connections for data collaboration failed.

Potential Impact: NA

Suggested Action(s): Perform

Metric: EdgeNoQueuedBytesForDCServerConnections

Description: the total number of queued bytes for Data Collaboration Server Connections.

Metric SpecName: DATACOLLABSRVCONQ

Metric Field Name: WEBRELAY - Total number of queued bytes for Data Collaboration Server Connections

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 536870912, Major / 1073741824

Policy: MSBS_EdgeNoQueuedBytesForDCServerConnections

Message text: The value of WEBRELAY - Total number of queued bytes for Data Collaboration Server Connections for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Failure to read outgoing date by Web Conferencing Server servers.

Potential Impact: NA

Suggested Action(s): Check availability of Web Conferencing Server servers. Also check network connectivity.

Metric: EdgeSIPConnectionFailuresPerSecond

Description: the number of Sip connection failures per second.

Metric SpecName: SIPCONNFAILURE

Metric Field Name: WEBRELAY - Sip Connection Failures per second

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 25, Major / 50

Policy: MSBS_EdgeSIPConnectionFailuresPerSecond

Message text: The value of WEBRELAY - Sip Connection Failures per second for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Sip connection is terminated unexpectedly due to network issues or unavailability of remote servers.

Potential Impact: NA

Suggested Action(s): Check network and SIP server availability.

Collect_LogicalDisk_Mediation

This Policy monitors the logical disk feature of Microsoft Skype Business Server

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Logical_Disk_Conf

Aspect: Skype Logical Disk

CIT: Edge Server, Director Server, Mediation Server, Front End Server, Persistent Chat Server

Data source / Data class: LYNC / LOGICALDISK

Source / Collection Definition: PERFMON / LogicalDisk(*)

Metric: MedLogicalDiskInstance

> **Description**: instance of perfmon object LogicalDisk
>
> **Metric SpecName**: LGDISKINSTNAME
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: MedPercentageFreeSpace

> **Description**: % Free Space is the percentage of total usable space on the selected logical disk drive that was free.
>
> **Metric SpecName**: FREESPACE
>
> **Metric Field Name**: % Free Space
>
> **Data type**: UINT32
>
> **Alarm**: TRUE
>
> **Category** : MSSkype
>
> **Severity / Threshold** : Warning / 70, Major / 90
>
> **Policy**: MSBS_MedPercentageFreeSpace
>
> **Message text**: The value of % Free Space for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>
>
> **Instructional Text**:
>
> **Probable Cause(s)**: Database size grows indefinitely.
>
> **Potential Impact**: NA
>
> **Suggested Action(s)**: Please check each disk drive and clean up unnecessary files.

ActiveClientConnections

This policy maintains the information about the status for the different services

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_ConferenceProcPerform_2010_Conf

Aspect: Skype Conference Processing Performance

CIT: Mediation Server, Front End Server, Edge Server

Data source / Data class: SKYPE / ACTIVECLIENTCONN

Source / Collection Definition: PERFMON / LS:PDP - TURN(*)

Metric: ActiveClientConnections

> **Description**: This metric captures Active Client Connections
>
> **Metric SpecName**: ActiveClientConn
>
> **Metric Field Name**: ActiveClientConnections
>
> **Data type**: REAL64
>
> **Alarm**: FALSE

Metric: Instance_Name

> **Description**: This is the key for metric
>
> **Metric SpecName**: Instance_Name
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: ActiveEdgeConnections

> **Description**: This metric captures Active Edge Connections
>
> **Metric SpecName**: ActiveEdgeConn
>
> **Metric Field Name**: ActiveEdgeConnections
>
> **Data type**: REAL64
>
> **Alarm**: FALSE

Metric: ActiveClientConnections

Description: This metric captures Active Client Connections

Metric SpecName: ActiveClientConn

Metric Field Name: PDP - Active client connections

Data type: REAL64

Alarm: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: ActiveEdgeConnections

Description: This metric captures Active Edge Connections

Metric SpecName: ActiveEdgeConn

Metric Field Name: PDP - Active edge connections

Data type: REAL64

Alarm: FALSE

Collect_FrontEnd_Edge

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / LSPROCESSOR

Source / Collection Definition: PERFMON / Processor(_Total)

Metric: ProcesserInstance

> **Description**: instance of perfmon object Processor Total
>
> **Metric SpecName**: PROCESSORINST
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: SystemPercentProcessorTime

> **Description**: Percentage Processor Time is the percentage of elapsed time that all of process threads used the processor to execution instructions.
>
> **Metric SpecName**: SYSPCTPROCESSORTIME
>
> **Metric Field Name**: % Processor Time
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

DataMCUHealth

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: SKYPE / DATAMCUHEALTH

Source / Collection Definition: PERFMON / LS:DATAMCU - 04 - MCU Health And Performance(*)

Metric: MCUHealthState

Description: This metric captures MCU Health State

Metric SpecName: MCUHealthState

Metric Field Name: DATAMCU - 005 - MCU Health State

Data type: REAL64

Alarm: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: MCUHealthStateChangedCount

Description: This metric captures MCU Health State Changed Count

Metric SpecName: MCUHelthStatChang

Metric Field Name: DATAMCU - 007 - MCU Health State Changed Count

Data type: UINT32

Alarm: FALSE

Metric: MCUHealthState

Description: This metric captures MCU Health State

Metric SpecName: MCUHealthState

Metric Field Name: DATAMCU - MCU Health State

Data type: REAL64

Alarm: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: MCUHealthStateChangedCount

Description: This metric captures MCU Health State Changed Count

Metric SpecName: MCUHelthStatChang

Metric Field Name: DATAMCU - MCU Health State Changed Count

Data type: UINT32

Alarm: FALSE

MediationServerGateway

This policy maintains the information about the status for the different services

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_ConferenceProcPerform_2010_Conf

Aspect: Skype Conference Processing Performance

CIT: Mediation Server, Front End Server, Edge Server

Data source / Data class: SKYPE / TTLFAILCALUNEXINTGW

Source / Collection Definition: PERFMON / LS:MediationServer - Global Per Gateway Counters(*)

Metric: TotalFailedCallsCausedByUnexpectedInteractionFromAGateway

Description: This metric captures Total Failed Calls Caused By Unexpected Interaction From The Gateway

Metric SpecName: TtlFailCalUnexIntGw

Metric Field Name: - Total Failed Calls Caused By Unexpected Interaction From A Gateway

Data type: UINT32

Alarm: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: TotalFailedCallsCausedByUnexpectedInteractionFromAGateway

Description: This metric captures Total Failed Calls Caused By Unexpected Interaction From The Gateway

Metric SpecName: TtlFailCalUnexIntGw

Metric Field Name: - Total Failed Calls Caused By Unexpected Interaction From A Gateway

Data type: UINT32

Alarm: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Collect_FrontEnd_Process_LyncBackupService

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / CS_PROCESS

Source / Collection Definition: PERFMON / Process(LyncBackupService)

Metric: FELYNCBACKUPInstance

> **Description**: instance of AVMCUSvc process
>
> **Metric SpecName**: INSTANCENAME
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FELYNCBACKUPPercentprocessorTime

> **Description**: Percentage Processor Time is the percentage of elapsed time that all of process threads used the processor to execution instructions.
>
> **Metric SpecName**: PCTPROCESSORTIME
>
> **Metric Field Name**: % Processor Time
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Metric: FELYNCBACKUPWorkingSet

Description: Working Set is the current size, in bytes, of the Working Set of this process. the Working Set is the set of memory pages touched recently by the threads in the process. If free memory in the computer is above a threshold, pages are left in the Working Set of a process even if they are not in use. When free memory falls below a threshold, pages are trimmed from Working Sets. If they are needed they will then be soft-faulted back into the Working Set before leaving main memory.

Metric SpecName: WORKINGSET

Metric Field Name: Working Set

Data type: UINT32

Alarm: FALSE

Metric: FELYNCBACKUPPageFaultsPerSec

Description: Page Faults/sec is the average number of pages faulted per second. It is measured in number of pages faulted per second because only one page is faulted in each fault operation, hence this is also equal to the number of page fault operations. This counter includes both hard faults (those that require disk access) and soft faults (where the faulted page is found elsewhere in physical memory.) Most processors can handle large numbers of soft faults without significant consequence. However, hard faults, which require disk access, can cause significant delays.

Metric SpecName: PAGEFAULTS

Metric Field Name: Page Faults/sec

Data type: UINT32

Alarm: FALSE

Metric: FELYNCBACKUPPrivateBytes

Description: Private Bytes is the current size, in bytes, of memory that this process has allocated that cannot be shared with other processes.

Metric SpecName: PRIVATEBYTES

Metric Field Name: Private Bytes

Data type: UINT32

Alarm: FALSE

Metric: FELYNCBACKUPThreadCount

> **Description**: the number of threads currently active in this process. An instruction is the basic unit of execution in a processor, and a thread is the object that executes instructions. Every running process has at least one thread.
>
> **Metric SpecName**: THREADCOUNT
>
> **Metric Field Name**: Thread Count
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

PoorStreamsBtwnSubnetsPercentage

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / STRBTWNSUBNETS

Source / Collection Definition: SQLDB / select (SELECT SERVERPROPERTY ('MACHINENAME')) as 'SERVERNAME', isnull((100 * (SELECT COUNT(*) as [PoorStreamsBtwnSubnets] FROM [Session] s WITH (NOLOCK) INNER JOIN [MediaLine] AS m WITH (NOLOCK) ON m.ConferenceDateTime = s.ConferenceDateTime AND m.SessionSeq = s.SessionSeq INNER JOIN [AudioStream] AS a WITH (NOLOCK) ON a.MediaLineLabel = m.MediaLineLabel and a.ConferenceDateTime = m.ConferenceDateTime and a.SessionSeq = m.SessionSeq INNER JOIN [User] AS CallerUser WITH (NOLOCK) ON CallerUser.UserKey = s.CallerURI INNER JOIN [User] AS CalleeUser WITH (NOLOCK) ON CalleeUser.UserKey = s.CalleeURI INNER JOIN [IpAddress] AS CallerIpAdr WITH (NOLOCK) ON CallerIpAdr.IpAddressKey = m.CallerSubnet INNER JOIN [IpAddress] AS CalleeIpAdr WITH (NOLOCK) ON CalleeIpAdr.IpAddressKey = m.CalleeSubnet INNER JOIN [NetworkConnectionDetail] AS CallerNcd WITH (NOLOCK) ON CallerNcd.NetworkConnectionDetailKey = m.CallerNetworkConnectionType INNER JOIN [NetworkConnectionDetail] AS CalleeNcd WITH (NOLOCK) ON CalleeNcd.NetworkConnectionDetailKey = m.CalleeNetworkConnectionType INNER JOIN [PayloadDescription] AS PL WITH (NOLOCK) ON PL.PayloadDescriptionKey =

a.AudioPayloadDescription WHERE s.StartTime >= (dateadd(MINUTE,@Duration,GETUTCDATE())) and s.StartTime (dateadd(MINUTE,0,GETUTCDATE())) and CallerIpAdr.IpAddress = '10.164.25.0' and CalleeIpAdr.IpAddress = '10.164.25.0' and m.ClassifiedPoorCall = 1)) / nullif((SELECT COUNT (*) as [TotalStreamsBtwnSubnets] FROM [Session] s WITH (NOLOCK) INNER JOIN [MediaLine] AS m WITH (NOLOCK) ON m.ConferenceDateTime = s.ConferenceDateTime AND m.SessionSeq = s.SessionSeq INNER JOIN [AudioStream] AS a WITH (NOLOCK) ON a.MediaLineLabel = m.MediaLineLabel and a.ConferenceDateTime = m.ConferenceDateTime and a.SessionSeq = m.SessionSeq INNER JOIN [User] AS CallerUser WITH (NOLOCK) ON CallerUser.UserKey = s.CallerURI INNER JOIN [User] AS CalleeUser WITH (NOLOCK) ON CalleeUser.UserKey = s.CalleeURI INNER JOIN [IpAddress] AS CallerIpAdr WITH (NOLOCK) ON CallerIpAdr.IpAddressKey = m.CallerSubnet INNER JOIN [IpAddress] AS CalleeIpAdr WITH (NOLOCK) ON CalleeIpAdr.IpAddressKey = m.CalleeSubnet INNER JOIN [NetworkConnectionDetail] AS CallerNcd WITH (NOLOCK) ON CallerNcd.NetworkConnectionDetailKey = m.CallerNetworkConnectionType INNER JOIN [NetworkConnectionDetail] AS CalleeNcd WITH (NOLOCK) ON CalleeNcd.NetworkConnectionDetailKey = m.CalleeNetworkConnectionType INNER JOIN [PayloadDescription] AS PL WITH (NOLOCK) ON PL.PayloadDescriptionKey = a.AudioPayloadDescription WHERE s.StartTime >= (dateadd(MINUTE,@Duration,GETUTCDATE())) and s.StartTime (dateadd(MINUTE,0,GETUTCDATE())) and CallerIpAdr.IpAddress = '10.164.25.0' and CalleeIpAdr.IpAddress ='10.164.25.0'),0),0) as 'PoorStreamsBtwnSubnetsPercentage'

Metric: PoorStreamsBtwnSubnetsPercentage

Description: This metric captures Poor Streams Between internal Lync desktop users and conferencing and mediation servers and calculates percentage for a given interval At the end of each call, parameters that determine Quality of a call that include network, audio and video parameters are logged into QoE database of Lync Server. Each call is categorized as having Acceptable quality or Poor quality based on the same.

Metric SpecName: PoorStrBtwSubnetsPer

Metric Field Name: PoorStreamsBtwnSubnetsPercentage

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 40, Major / 70

Policy: MSBS_PoorStreamsBtwnSubnetsPercentage

Message text: The Percentage of Poor Streams Between internal Lync desktop users and mediation servers is <VALUE> which exceeds the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Subnet router misconfiguration, noisy network etc may cause packet loss or a high roundtrip

Potential Impact: Poor call quality between subnets

Suggested Action(s): Configuring router rules, checking for network congestion

Metric: ServerName

Description: This is the key for metric

Metric SpecName: ServerName

Metric Field Name: ServerName

Data type: TEXT

Alarm: FALSE

UserRPSSQLCalls

This policy maintains the information about the status for the different services

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_SubscribedUser_Conf

Aspect: Skype Subscribed User

CIT: Front End Server

Data source / Data class: LYNC / USERRPSSQLCALLS

Source / Collection Definition: PERFMON / LS:USrv - Rich presence subscribe SQL calls(*)

Metric: AverageNumberOfUsersPerSubscribeRequest

> **Description**: This metric captures Average Number Of Users Per Subscribe Request
>
> **Metric SpecName**: AvgNumOfUsrPrSubReq
>
> **Metric Field Name**: USrv - Average Number Of Users Per Subscribe Request
>
> **Data type**: REAL64
>
> **Alarm**: FALSE

Metric: Instance_Name

> **Description**: This is the key for metric
>
> **Metric SpecName**: Instance_Name
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: PollingSubscribeReqThrottledByDatabaseStoreThrottlePerSec

> **Description**: This metric captures per-second rate of polling subscribe requests throttled by the polling subscribe database throttling mechanism.
>
> **Metric SpecName**: PlSbRqThrtDBStThrPS
>
> **Metric Field Name**: USrv - Polling Subscribe Requests Throttled By Database Store Throttle/Sec.
>
> **Data type**: REAL64
>
> **Alarm**: FALSE

Metric: PollingSubReqThrottledByPollingSubscribeQueueThrottlePerSec

Description: This metric captures per-second rate of polling subscribe requests throttled by the polling subscribe queue throttling mechanism.

Metric SpecName: PlSbRqThrtPlSubQuPS

Metric Field Name: USrv - Polling Subscribe Requests Throttled By Polling Subscribe Queue Throttle/Sec.

Data type: REAL64

Alarm: FALSE

Metric: RtcBatchQueryCategoriesSprocCallsPerSec

Description: This metric captures Rtc Batch Query Categories Sproc Calls Per Sec

Metric SpecName: RtBatQuryCatSprCIPS

Metric Field Name: USrv - RtcBatchQueryCategories Sproc Calls/Sec

Data type: REAL64

Alarm: FALSE

Metric: RtcBatchSubscribeCategoryListSprocCallsPerSec

Description: This metric captures Rtc Batch Subscribe Category List Sproc Calls Per Sec

Metric SpecName: RtBatSubCatLtSpCIPS

Metric Field Name: USrv - RtcBatchSubscribeCategoryList Sproc Calls/Sec

Data type: REAL64

Alarm: FALSE

Metric: RtcSubscribeSelfSprocCallsPerSec

Description: This metric captures Rtc Subscribe Self Sproc Calls Per Sec

Metric SpecName: RtSubSelfSPCIPS

Metric Field Name: USrv - RtcSubscribeSelf Sproc calls/Sec

Data type: REAL64

Alarm: FALSE

Collect_FrontEnd_LSAVAuth

This Policy Monitors the authentication related metrics of Microsoft Skype Business Server

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Authentication_Conf

Aspect: Skype Authentication

CIT: Edge Server, Director Server, Front End Server

Data source / Data class: LYNC / LSAVAUTH

Source / Collection Definition: PERFMON / LS:A/V Auth - Requests(*)

Metric: AVAuthInstance

> **Description**: instance of perfmon object LS:A/V Auth - Requests
>
> **Metric SpecName**: AVAITHINSYANCE
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: BadRequestsReceived

> **Description**: the number of bad requests received/sec
>
> **Metric SpecName**: BADREQRECEIVED
>
> **Metric Field Name**: - Bad Requests Received/sec
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

BACKUPXDSDBStoreQueueDepth

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / BACKXDSDBSTORQUDEPTH

Source / Collection Definition: PERFMON / LS:USrv - BACKUPXDSDBStore(*)

Metric: BackXDsDBStorQUDepth

> **Description**: This metric captures the average number of database requests waiting to be executed for backup Db Store
>
> **Metric SpecName**: BackXDsDBStorQUDepth
>
> **Metric Field Name**: USrv - Queue Depth
>
> **Data type**: REAL64
>
> **Alarm**: TRUE
>
> **Category** : MSSkype
>
> **Severity / Threshold** : Major / 1000
>
> **Policy**: MSBS_BackXDsDBStorQUDepth
>
> **Message text**: The value of average number of database requests waiting to be executed for backup Db Store is <VALUE> and has crossed the threshold of <THRESHOLD>
>
> **Instructional Text**:
>
> **Probable Cause(s)**: The backend might be busy and is unable to respond to requests quickly
>
> **Potential Impact**: This might be a temporary condition. If the problem persists please ensure that the hardware and software requirements meet the user usage characteristics
>
> **Suggested Action(s)**: Backup database may not be accessible

Metric: Instance_Name

> **Description**: This is the key for metric
>
> **Metric SpecName**: Instance_Name
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Collect_Edge_AV_TCP_Counters

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / AVEDGETCPCOUNTERS

Source / Collection Definition: PERFMON / LS:A/V Edge - TCP Counters(_Total)

Metric: AVEdgeTCPCounterInstance

> **Description**: instance of perfmon object LS:A/V Edge - TCP Counters(_Total)
>
> **Metric SpecName**: AVTCPINSTANAME
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: AVEdgeAllocateRequestExceedingPortLimit

Description: Allocate Requests Exceeding Port Limit/sec over TCP

Metric SpecName: TCPREQEXCPORTLIMIT

Metric Field Name: A/V Edge - Allocate Requests Exceeding Port Limit/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 10, Major / 20

Policy: MSBS_AVEdgeAllocateRequestExceedingPortLimit

Message text: The value of A/V Edge - Allocate Requests Exceeding Port Limit/sec for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): This error occurs when there is an unexpectedly high rate of requests over TCP for ports associated with the same user ID. .

Potential Impact: NA

Suggested Action(s): Check that the profile of network traffic to the A/V Edge Server is in line with expected usage. A network level trace can be used to determine if there is unusual amount of traffic originating from a single source.

Metric: AVEdgeAuthFailurePerSec

Description: Authentication Failures/sec over TCP

Metric SpecName: TCPAUTHFAILURE

Metric Field Name: A/V Edge - Authentication Failures/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 10, Major / 20

Policy: MSBS_AVEdgeAuthFailurePerSec

Message text: The value of A/V Edge - Authentication Failures/sec for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): This error occurs when there is unexpectedly high rate of message authentication failures over TCP. This could be the result of a configuration error.

Potential Impact: NA

Suggested Action(s): If the A/V Edge Server is deployed in a load balanced array verify that the same authentication certificate is deployed on each machine. Check that the profile of network traffic to the A/V Edge Server is in line with expected usage.

Metric: AVEdgePacketsDroppedPerSec

Description: Packets Dropped/sec over TCP

Metric SpecName: TCPPACKETDROPPED

Metric Field Name: A/V Edge - Packets Dropped/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 300, Major / 400

Policy: MSBS_AVEdgePacketsDroppedPerSec

Message text: The value of A/V Edge - Packets Dropped/sec for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): This error occurs when an unexpectedly high rate of TCP packets is received at the A/V Edge Server causing some packets to be discarded.

Potential Impact: NA

Suggested Action(s): Check that the profile of network traffic to the A/V Edge Server is in line with expected usage.

Metric: AVEdgeActiveSessionsExcceedingAvgBWLimit

Description: Active Sessions Exceeding Average Bandwidth Limit over TCP

Metric SpecName: TCPSESSEXCEEDAVGBW

Metric Field Name: A/V Edge - Active Sessions Exceeding Avg Bandwidth Limit

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 10, Major / 20

Policy: MSBS_AVEdgeActiveSessionsExcceedingAvgBWLimit

Message text: The value of A/V Edge - Active Sessions Exceeding Avg Bandwidth Limit for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): This error occurs when there is an unexpectedly high rate of traffic sent through the A/V Edge Server within a UDP session. These sessions will be throttled by the A/V Edge Server.

Potential Impact: NA

Suggested Action(s): Check that the profile of network traffic to the A/V Edge Server is in line with expected usage.

Metric: AVEdgeActiveSessionsExcceedingPeakBWLimit

Description: Active Sessions Exceeding Peak Bandwidth Limit over TCP

Metric SpecName: TCPSESEXCEEDPKBW

Metric Field Name: A/V Edge - Active Sessions Exceeding Peak Bandwidth Limit

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 10, Major / 20

Policy: MSBS_AVEdgeActiveSessionsExcceedingPeakBWLimit

Message text: The value of A/V Edge - Active Sessions Exceeding Peak Bandwidth Limit for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): This error occurs when there is an unexpectedly high rate of traffic sent through the A/V Edge Server within a UDP session. These sessions will be throttled by the A/V Edge Server.

Potential Impact: NA

Suggested Action(s): Check that the profile of network traffic to the A/V Edge Server is in line with expected usage.

ChkEdgeFrontEndServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SERVSTAT

Source / Collection Definition: SERVICECHECK / RTCSRV

Metric: EdgeRTCSRVServName

> **Description**: Name of the Service
>
> **Metric SpecName**: SERVNAME
>
> **Metric Field Name**: Service_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: EdgeRTCSRVServDisplayName

> **Description**: Display Name of the Service
>
> **Metric SpecName**: SRVDISPNAME
>
> **Metric Field Name**: Service_Displayname
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: EdgeRTCSRVServStatus

> **Description**: Status of the Service
>
> **Metric SpecName**: SERVSTATUS
>
> **Metric Field Name**: Service_Status
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: EdgeRTCSRVServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_EdgeRTCSRVServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): Lync Server Front-End' Windows Service is stopped.

Potential Impact: NA

Suggested Action(s): Lync Server Front-End' Windows Service is stopped. Please restart the service.

WEBAddressBook

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: SKYPE / WEBADDRESSBOOK

Source / Collection Definition: PERFMON / LS:WEB - 01 - Address Book File Download(*)

Metric: AverageProcessingTimeForASucceededFileRequestInMilliseconds

Description: This metric captures Average Processing Time For A Succeeded File Request In Milliseconds

Metric SpecName: AvgPrcTimSucFlReqMS

Metric Field Name: WEB - 002 - Average processing time for a succeeded file request in milliseconds

Data type: REAL64

Alarm: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: SucceededFileRequestsPerSecond

Description: This metric captures Succeeded File Requests Per Second

Metric SpecName: SucceededFileReqPS

Metric Field Name: WEB - 001 - Succeeded File Requests/Second

Data type: REAL64

Alarm: FALSE

Metric: AverageProcessingTimeForASucceededFileRequestInMilliseconds

Description: This metric captures Average Processing Time For A Succeeded File Request In Milliseconds

Metric SpecName: AvgPrcTimSucFlReqMS

Metric Field Name: WEB - Average Processing Time For A Succeeded File Request In Milliseconds

Data type: REAL64

Alarm: FALSE

Metric: Instance_Name

> **Description**: This is the key for metric
>
> **Metric SpecName**: Instance_Name
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: SucceededFileRequestsPerSecond

> **Description**: This metric captures Succeeded File Requests Per Second
>
> **Metric SpecName**: SucceededFileReqPS
>
> **Metric Field Name**: WEB - Succeeded File Requests/Second
>
> **Data type**: REAL64
>
> **Alarm**: FALSE

ConferenceMcuAllocator

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / KHICONMCUALLO

Source / Collection Definition: PERFMON / LS:USrv - 26 - Conference Mcu Allocator(*)

Metric: CreateConferenceLatency

Description: This policy monitors the average time (in milliseconds) taken to complete a create conference call.

Metric SpecName: CreateConfLat

Metric Field Name: USrv - 019 - Create Conference Latency (msec)

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 5000, Major / 5000

Policy: MSBS_CreateConferenceLatency

Message text: The current value of CreateConferenceLatency is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): The Mcu or Backend might be busy and may not respond immediately.

Potential Impact: Please ensure that the hardware and software requirements meet the user usage characteristics.

Suggested Action(s): The longer it will take for users to join a conference.

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: CreateConferenceLatency

Description: This policy monitors the average time (in milliseconds) taken to complete a create conference call.

Metric SpecName: CreateConfLat

Metric Field Name: USrv - Create Conference Latency (msec)

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 5000, Major / 5000

Policy: MSBS_CreateConferenceLatency

Message text: The current value of CreateConferenceLatency is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): The Mcu or Backend might be busy and may not respond immediately.

Potential Impact: Please ensure that the hardware and software requirements meet the user usage characteristics.

Suggested Action(s): The longer it will take for users to join a conference.

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Collect_Edge_SIP_AccessEdge_Server_Connections

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / NA

Source / Collection Definition: PERFMON / LS:SIP - 08 - Access Edge Server Connections(*)

Metric: RejectdExEdgeServerConnsPerSec

> **Description**: rate of server connections rejected at the external edge in a second because all federation is disabled
>
> **Metric SpecName**: REJCTDSERVCONNPERSEC
>
> **Metric Field Name**: SIP - 013 - Rejected External Edge Server Connections/sec
>
> **Data type**: UINT32
>
> **Alarm**: TRUE
>
> **Category** : MSSkype
>
> **Severity / Threshold** : Major / 10
>
> **Policy**: MSBS_RejectdExEdgeServerConnsPerSec
>
> **Message text**: The value of the counter 'Rejected External Edge Server Connections/sec' value <VALUE> has crossed the threshold of <THRESHOLD> .
>
> **Instructional Text**:
>
> **Probable Cause(s)**: NA
>
> **Potential Impact**: NA
>
> **Suggested Action(s)**: NA

Metric: RejectdExEdgeClientConnsPerSec

Description: rate at which the number of client connections is rejected, in a second, at the external edge as the remote user access is disabled.

Metric SpecName: REJCTDCLIENTCONNPERSEC

Metric Field Name: SIP - 015 - Rejected External Edge Client Connections/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 10

Policy: MSBS_RejectdExEdgeClientConnsPerSec

Message text: The value of the counter 'Rejected External Edge Client Connections/sec' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: EdgeServerConnectionInstance

Description: instance of perfmon object LS:SIP - 08 - Access Edge Server Connections

Metric SpecName: INSTANCENAME

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

AccessEdgeServer

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: SKYPE / ACCESSEDGESERVER

Source / Collection Definition: PERFMON / LS:SIP - Access Edge Server Connections(*)

Metric: RejectedExternalEdgeClientConnectionsPerSec

> **Description**: This metric captures the per-second rate of client connections rejected at the external edge because remote user access is disabled.
>
> **Metric SpecName**: RejeExtEdgeCntConPS
>
> **Metric Field Name**: SIP - Rejected External Edge Client Connections/Sec
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Metric: Instance_Name

> **Description**: This is the key for metric
>
> **Metric SpecName**: Instance_Name
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: ExternalMessagesDroppedDueToUnresolvedDomain

> **Description**: This metric captures the per-second rate of messages that could not be routed because the message domain is not in the routing table.
>
> **Metric SpecName**: ExtMsgDrpUnresolvDM
>
> **Metric Field Name**: SIP - External Messages Dropped Due To Unresolved Domain
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Metric: ExternalMessagesDroppedDueToUnresolvedDomain

> **Description**: This metric captures the per-second rate of messages that could not be routed because the message domain is not in the routing table.
>
> **Metric SpecName**: ExtMsgDrpUnresolvDM
>
> **Metric Field Name**: SIP - External Messages Dropped Due To Unresolved Domain
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Metric: Instance_Name

> **Description**: This is the key for metric
>
> **Metric SpecName**: Instance_Name
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

AppSharingJitterPoorCallsPercentage

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / APPSHARJITTRCALLS

Source / Collection Definition: SQLDB / select isnull(cast(100.0 * cast((SUM(CASE WHEN [AppSharingJitterInterArrival] > [AppsharingJitterInterArrivalOptimal] THEN 1 ELSE 0 END)) as float) / cast((SUM(CASE WHEN MediaLineLabel is NOT NULL THEN 1 ELSE 0 END)) as float) as decimal (4, 1)),0) as AppSharingJitterPoorCallsPercentage,SERVERPROPERTY('MACHINENAME') AS 'ServerName' from [QoEMetrics].[dbo].[QoEReportsCallDetailView] Where MediaLineLabel = 3 AND ConferenceDateTime >= dateadd(MINUTE,@Duration,GETUTCDATE())

Metric: AppSharingJitterPoorCallsPercentage

Description: This metric captures Poor Application Sharing that have Jitter more than a set threshold value and calculates percentage of poor calls for a given interval At the end of each call, parameters that determine Quality of a call that include network, audio and video parameters are logged into QoE database of Lync Server. Each call is categorized as having Acceptable quality or Poor quality based on the same.

Metric SpecName: AppShareJitrPoorCall

Metric Field Name: AppSharingJitterPoorCallsPercentage

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 40, Major / 70

Policy: MSBS_AppSharingJitterPoorCallsPercentage

Message text: The current value of Percentage App Sharing Jitter Poor Calls is <VALUE> which exceeds the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Variation in the delay time of packets arriving at their destination. Packets are sent at regular intervals from the sender to the receiver, but because of network latency the interval between packets can vary at the destination. Caused by LAN Congestion or issue with device/device drivers, video rendering

Potential Impact: This variation can affect media quality. Jitter is used to determine MOSs as well as in the call detail report. -Delay due to jitter buffering -Distorted rendering

Suggested Action(s): -Use Jitter buffers in Packet Switched Networks -Network Upgrade

Metric: ServerName

Description: This is the key for metric

Metric SpecName: ServerName

Metric Field Name: ServerName

Data type: TEXT

Alarm: FALSE

SimplePortWatcher5065

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / Port5065

Source / Collection Definition: PORTCOL / PORTCHECKER

Metric: SimpleWatcherPort5065

Description: Used for incoming SIP listening requests for application sharing.

Metric SpecName: SimpleWatcherPort5065

Metric Field Name: SimpleWatcherPort5065

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort5065

Message text: The Port No:5065 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

Metric: SimpleWatcherPort5065

Description: Used for incoming SIP listening requests for application sharing.

Metric SpecName: SimpleWatcherPort5065

Metric Field Name: SimpleWatcherPort5065

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort5065

Message text: The Port No:5065 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

> **Description**: This is the key for metric
>
> **Metric SpecName**: HOSTNAME
>
> **Metric Field Name**: HOSTNAME
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

SimplePortWatcher80

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / Port80

Source / Collection Definition: PORTCOL / PORTCHECKER

Metric: SimpleWatcherPort80

Description: Used for communication from Front End Servers to the web farm FQDNs (the URLs used by IIS web components) when HTTPS is not used.

Metric SpecName: SimpleWatcherPort80

Metric Field Name: SimpleWatcherPort80

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_SimpleWatcherPort80

Message text: The Port No:80 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

Metric: SimpleWatcherPort80

Description: Used for communication from Front End Servers to the web farm FQDNs (the URLs used by IIS web components) when HTTPS is not used.

Metric SpecName: SimpleWatcherPort80

Metric Field Name: SimpleWatcherPort80

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_SimpleWatcherPort80

Message text: The Port No:80 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

> **Description**: This is the key for metric
>
> **Metric SpecName**: HOSTNAME
>
> **Metric Field Name**: HOSTNAME
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

ChkAvConfAVConferencingServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / NA

Source / Collection Definition: SERVICECHECK / RTCAVMCU

Metric: AvConfRTCAVMCUServname

> **Description**: Name of the Service
>
> **Metric SpecName**: SERVNAME
>
> **Metric Field Name**: Service_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: AvConfRTCAVMCUDisplayName

Description: Display Name of the Service

Metric SpecName: SRVDISPNAME

Metric Field Name: Service_Displayname

Data type: TEXT

Alarm: FALSE

Metric: AvConfRTCAVMCUServStatus

Description: Status of the Service

Metric SpecName: SERVSTATUS

Metric Field Name: Service_Status

Data type: TEXT

Alarm: FALSE

Metric: AvConfRTCAVMCUServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_AvConfRTCAVMCUServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

SimplePortWatcher5071

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / Port5071

Source / Collection Definition: PORTCOL / PORTCHECKER

Metric: SimpleWatcherPort5071

Description: Used for incoming SIP requests for the Response Group application.

Metric SpecName: SimpleWatcherPort5071

Metric Field Name: SimpleWatcherPort5071

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort5071

Message text: The Port No:5071 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

Metric: SimpleWatcherPort5071

Description: Used for incoming SIP requests for the Response Group application.

Metric SpecName: SimpleWatcherPort5071

Metric Field Name: SimpleWatcherPort5071

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort5071

Message text: The Port No:5071 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

Collect_Monotoring_CDRService_DBCdr

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / NA

Source / Collection Definition: PERFMON / LS:CDR Service - 00 - DBCdr(*)

Metric: MonitoringCDRServiceDBCdrInstance

Description: instance of perfmon object LS:CDR Service - 00 - DBCdr

Metric SpecName: MONCDRSERVCEDBCDRINSTANCE

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: MonitoringQueueLatency

Description: average time (in milliseconds) the database holds a request in queue.

Metric SpecName: QLATENCY

Metric Field Name: CDR Service - 002 - Queue Latency (msec)

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20

Policy: MSBS_MonitoringQueueLatency

Message text: The value of the counter 'CDR Service - 002 - Queue Latency (msec)' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: MonitoringTotalDeadlocks

Description: total number of deadlocks that have occurred since the start of the server.

Metric SpecName: TOTALDEADLOCKS

Metric Field Name: CDR Service - 013 - Total Deadlocks

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20

Policy: MSBS_MonitoringTotalDeadlocks

Message text: The value of the counter 'CDR Service - 013 - Total Deadlocks' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: MonitoringTotalfatalSQLerrors

Description: number of fatal SQL errors that have taken place since the server started.

Metric SpecName: TOTFATALSQLERRORS

Metric Field Name: CDR Service - 019 - Total fatal SQL errors

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20

Policy: MSBS_MonitoringTotalfatalSQLerrors

Message text: The value of the counter CDR Service - 019 - Total fatal SQL errors' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: MonitoringTotalODBCTimeoutFailures

Description: number of ODBC timeout failures that have taken place since the server started.

Metric SpecName: TOTODBCTIMEOUTFAILURES

Metric Field Name: CDR Service - 017 - Total ODBC Timeout Failures

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20

Policy: MSBS_MonitoringTotalODBCTimeoutFailures

Message text: The value of the counter 'CDR Service - 017 - Total ODBC Timeout Failures' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: MonitoringTotalsevereSQLerrors

Description: number of severe SQL errors that occurred since the server started.

Metric SpecName: TOTSEVERESQLERRORS

Metric Field Name: CDR Service - 018 - Total severe SQL errors

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20

Policy: MSBS_MonitoringTotalsevereSQLerrors

Message text: The value of the counter 'CDR Service - 018 - Total severe SQL errors' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: MonitoringTotalthrottledrequests

Description: number of requests that were rejected with a retry-after due to high database queue latency.

Metric SpecName: TOTTHROTLDREQSTS

Metric Field Name: CDR Service - 021 - Total throttled requests

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20

Policy: MSBS_MonitoringTotalthrottledrequests

Message text: The value of the counter 'CDR Service - 021 - Total throttled requests' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Collect_DirectorySearch

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / NA

Source / Collection Definition: PERFMON / LS:USrv - 19 - Directory Search(*)

Metric: DirectorySearchInstance

Description: instance of perfmon object LS:USrv - 19 - Directory Search

Metric SpecName: DIRECTORYSEARCHINST

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: DirectorySearchLatency

Description: average LDAP search time in milliseconds

Metric SpecName: DIRECTORYSEARCHLATENCY

Metric Field Name: USrv - 005 - Search Latency (ms)

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20

Policy: MSBS_DirectorySearchLatency

Message text: The value of the counter 'USrv - 005 - Search Latency (ms)'value <VALUE> has crossed threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: DirNumberofoutstandingsearches

Description: Total number of outstanding searches on this LDAP session in the Directory Search component of the Communications Server User Servers Module associated with a GC.

Metric SpecName: NOFOUTSTNDSEARCH

Metric Field Name: USrv - 000 - Number of outstanding searches

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20

Policy: MSBS_DirNumberofoutstandingsearches

Message text: The value of the counter 'Number of outstanding searches' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: DirNumberofLDAPerrorsPersec

Description: rate at which this LDAP session in communications server's directory search component of the user services module associated with GC

Metric SpecName: NOFLDAPERRORPSEC

Metric Field Name: USrv - 004 - Number of LDAP errors / sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20

Policy: MSBS_DirNumberofLDAPerrorsPersec

Message text: The value of the counter 'Number of LDAP errors / sec' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

AddressBookWebQuery

This policy maintains the information about the status for the different services

Schedule Task Policy: MSBS_SCH_LOW

ConfigFile Policy: MSBS_SyntheticRPC_Conf_2010

Aspect: Skype Test Contacts

CIT: Windows

Data source / Data class: LYNC / SYNRPCADDBKWBQRY

Source / Collection Definition: POWERSHELL / TestCSAddressBookWebQuery TargetFQDN ${fqdn}

Metric: AddressBookWebQuery

Description: This metric gathers the information which confirms that users are able to acess address book web Query

Metric SpecName: AddBkWbQuery

Metric Field Name: AddressBookWebQuery

Data type: TEXT

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_AddressBookWebQuery

Message text: The Address Book Web Query is down

Instructional Text:

Probable Cause(s): 1. User configuration must not have done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: New users cannot be registered

Suggested Action(s): 1. Configuration errors: Most common issues are: Test user password is invalid or expired, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availability: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution errors or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responded to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Metric: TargetFqdn

Description: This is the key for metric

Metric SpecName: TargetFqdn

Metric Field Name: TargetFqdn

Data type: TEXT

Alarm: FALSE

Metric: AddressBookWebQueryLatency

Description: This metric will capture the address book web query latency

Metric SpecName: AddBkWBQueLat

Metric Field Name: AddressBookWebQueryLatency

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Minor / 1000, Minor / 1000

Policy: MSBS_AddressBookWebQueryLatency

Message text: The value of Address Book Web Query Latency(ms) is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): 1. User configuration must not have done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: New users cannot be registered

Suggested Action(s): 1. Configuration errors: Most common issues are: Test user password is invalid or expired, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availibility: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution errors or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responded to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Metric: AddressBookWebQuery

Description: This metric gathers the information which confirms that users are able to acess address book web Query

Metric SpecName: AddBkWbQuery

Metric Field Name: AddressBookWebQuery

Data type: TEXT

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_AddressBookWebQuery

Message text: The Address Book Web Query is down

Instructional Text:

Probable Cause(s): 1. User configuration must not have done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: New users cannot be registered

Suggested Action(s): 1. Configuration errors: Most common issues are: Test user password is invalid or expired, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availability: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution errors or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responded to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Metric: TargetFqdn

Description: This is the key for metric

Metric SpecName: TargetFqdn

Metric Field Name: TargetFqdn

Data type: TEXT

Alarm: FALSE

Metric: AddressBookWebQueryLatency

Description: This metric will capture the address book web query latency

Metric SpecName: AddBkWBQueLat

Metric Field Name: AddressBookWebQueryLatency

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Minor / 1000, Minor / 1000

Policy: MSBS_AddressBookWebQueryLatency

Message text: The value of Address Book Web Query Latency(ms) is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): 1. User configuration must not have done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: New users cannot be registered

Suggested Action(s): 1. Configuration errors: Most common issues are: Test user password is invalid or expired, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availibility: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution errors or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responded to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

MessagesInServer

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / MESSAGESINSERVER

Source / Collection Definition: PERFMON / LS:SIP - Protocol(*)

Metric: MessagesInServer

> **Description**: This metric captures the number of messages currently being processed by the server.
>
> **Metric SpecName**: MessagesInServer
>
> **Metric Field Name**: SIP - Messages In Server
>
> **Data type**: UINT32
>
> **Alarm**: TRUE
>
> **Category** : MSSkype
>
> **Severity / Threshold** : Major / 5000
>
> **Policy**: MSBS_MessagesInServer
>
> **Message text**: The number of Messages processed by Server is <VALUE> and has crossed the threshold of <THRESHOLD>
>
> **Instructional Text**:
>
> **Probable Cause(s)**: This server is too busy and is unable to process user requests in timely fashion
>
> **Potential Impact**: This might be a temporary condition. If the problem persists please ensure that hardware and software requirements for this server meet the user usage characteristics
>
> **Suggested Action(s)**: The user may expereince delay in reciept of messages

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

ChkFrontEnd ResponseGroupServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SERVSTAT

Source / Collection Definition: SERVICECHECK / RTCRGS

Metric: FERTCRGSServName

Description: Name of the Service

Metric SpecName: SERVNAME

Metric Field Name: Service_Name

Data type: TEXT

Alarm: FALSE

Metric: FERTCRGSServDisplayName

Description: Display Name of the Service

Metric SpecName: SRVDISPNAME

Metric Field Name: Service_Displayname

Data type: TEXT

Alarm: FALSE

Metric: FERTCRGSServStatus

Description: Status of the Service

Metric SpecName: SERVSTATUS

Metric Field Name: Service_Status

Data type: TEXT

Alarm: FALSE

Metric: FERTCRGSServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_FERTCRGSServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): Lync Server Response Group' Windows Service is stopped.

Potential Impact: NA

Suggested Action(s): Lync Server Response Group' Windows Service is stopped. Please restart the service.

SimplePortWatcher444

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / Port444

Source / Collection Definition: PORTCOL / PORTCHECKER

Metric: SimpleWatcherPort444

Description: Used for HTTPS communication between the Focus (the Lync Server component that manages conference state) and the individual servers. This port is also used for TCP communication between Survivable Branch Appliances and Front End Servers.

Metric SpecName: SimpleWatcherPort444

Metric Field Name: SimpleWatcherPort444

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_SimpleWatcherPort444

Message text: The Port No:444 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

Metric: SimpleWatcherPort444

Description: Used for HTTPS communication between the Focus (the Lync Server component that manages conference state) and the individual servers. This port is also used for TCP communication between Survivable Branch Appliances and Front End Servers.

Metric SpecName: SimpleWatcherPort444

Metric Field Name: SimpleWatcherPort444

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_SimpleWatcherPort444

Message text: The Port No:444 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

ChkFrontEndAVConferencingServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SERVSTAT

Source / Collection Definition: SERVICECHECK / RTCAVMCU

Metric: FERTCAVMCUServName

Description: Name of the Service

Metric SpecName: SERVNAME

Metric Field Name: Service_Name

Data type: TEXT

Alarm: FALSE

Metric: FERTCAVMCUServDisplayName

Description: Display Name of the Service

Metric SpecName: SRVDISPNAME

Metric Field Name: Service_Displayname

Data type: TEXT

Alarm: FALSE

Metric: FERTCAVMCUServStatus

Description: Status of the Service

Metric SpecName: SERVSTATUS

Metric Field Name: Service_Status

Data type: TEXT

Alarm: FALSE

Metric: FERTCAVMCUServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_FERTCAVMCUServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): Lync Server Audio/Video Conferencing' Windows Service is stopped.

Potential Impact: NA

Suggested Action(s): Lync Server Audio/Video Conferencing' Windows Service is stopped.
Please restart the service.

SimpleURLWatcherDialin

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / URLWATCHDIALIN

Source / Collection Definition: POWERSHELL / Invoke-WebRequest -Uri dialin.{SIPDOMAIN} - UseDefaultCredentials

Metric: URLWatcherDialin

Description: This metric check HTTP response of a Dialin URL

Metric SpecName: URLWatcherDialin

Metric Field Name: StatusCode

Data type: TEXT

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Minor / 1

Policy: MSBS_URLWatcherDialin

Message text: The Dial in URL to access Dial-in Conference is down

Instructional Text:

Probable Cause(s): The page is unreachable. If behind a proxy, check if the proxy settings are correct. Unexpected API call failures. Multiple reasons could cause this, for instance a memory allocation error. The site or URL is not accessible or is down.

Potential Impact: URL cannot be accessed

Suggested Action(s): Try to access the same URL from an internet browser like Internet Explorer.

Metric: ServerName

Description: This metric check HTTP response of a Dialin URL

Metric SpecName: ServerName

Metric Field Name: ServerName

Data type: TEXT

Alarm: FALSE

Collect_Chat_Message_processing

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / CHATMSGPROC

Source / Collection Definition: PERFMON / LS:CHAT - Persistent Chat Message processing(*)

Metric: PersistentChatMessageInstance

> **Description**: instance of perfmon object LS:CHAT - Persistent Chat Message processing
>
> **Metric SpecName**: CHATMSGINSTANCE
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: TotalMessagesWaitingtobeSenttoPeers

> **Description**: Total number of messages waiting to be sent to peers.
>
> **Metric SpecName**: TOTMSGWAITING
>
> **Metric Field Name**: CHAT - Total number of messages waiting to be sent to peers
>
> **Data type**: UINT32
>
> **Alarm**: TRUE
>
> **Category** : MSSkype
>
> **Severity / Threshold** : Warning / 50, Major / 100
>
> **Policy**: MSBS_TotalMessagesWaitingtobeSenttoPeers
>
> **Message text**: The value of Total chat message queued for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>
>
> **Instructional Text**:
>
> **Probable Cause(s)**: The server is unable to send messages to other Persistent Chat servers.
>
> **Potential Impact**: NA
>
> **Suggested Action(s)**: Ensure functional network connectivity between Persistent Chat servers and that all active Persistent Chat are running.

Collect_FrontEnd_WebRelay

This polcy gives us the information for the collaboration of Skype Business Server

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collaboration_Service_Conf

Aspect: Skype Collaboration Service

CIT: Edge Server, Director Server, Front End Server

Data source / Data class: LYNC / LSWEBRELAY

Source / Collection Definition: PERFMON / LS:WebRelay - Data Collab Web Relay Server(*)

Metric: DataCollabWebRelayInstance

> **Description**: instance of perfmon object LS:WebRelay - Data Collab Web Relay Server
>
> **Metric SpecName**: WEBRELAYINSTANCE
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: NumberofDataCollabClinetConnClosed

Description: the number of Data Collaboration client connections closed due to throttling per second.

Metric SpecName: DCCLNTCONNCLOSED

Metric Field Name: WEBRELAY - Number of Data Collaboration client connections closed due to throttling per second

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 25, Major / 50

Policy: MSBS_NumberofDataCollabClinetConnClosed

Message text: The value of Number of Data Collaboration client connections closed due to throttling per second for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Client Data Collaboration was closed because client failed to read data in a timely manner. This may indicate a network failure.

Potential Impact: NA

Suggested Action(s): Check client network connectivity to Lync Web App.

Metric: NumberofDataCollabConnFailureswithDCServers

Description: the number of Data Collaboration connection failures with Data Collaboration servers.

Metric SpecName: DCCONFAILURE

Metric Field Name: WEBRELAY - Number of Data Collaboration connection failures with Data Collaboration servers

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 5, Major / 10

Policy: MSBS_NumberofDataCollabConnFailureswithDCServers

Message text: The value of Number of Data Collaboration connection failures with Data Collaboration servers for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Connection closed by local party or remote party or network issues.

Potential Impact: NA

Suggested Action(s): Check availability of Web Conferencing Server servers.

Metric: NumberofFailedDCAuthRequest

Description: the number of failed Data Collaboration authentication request per second.

Metric SpecName: DATACOLLABAUTHREQ

Metric Field Name: WEBRELAY - Number of failed Data Collaboration authentication request per second

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 10, Major / 20

Policy: MSBS_NumberofFailedDCAuthRequest

Message text: The value of Number of failed Data Collaboration authentication request per second for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Attempts to authenticate incoming client connections for data collaboration failed.

Potential Impact: NA

Suggested Action(s): Perform

Metric: TotalNumberofQueuedBytesForDCServerCon

Description: the total number of queued bytes for Data Collaboration Server Connections.

Metric SpecName: DATACOLLABSRVCONQ

Metric Field Name: WEBRELAY - Total number of queued bytes for Data Collaboration Server Connections

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 536870912, Major / 1073741824

Policy: MSBS_TotalNumberofQueuedBytesForDCServerCon

Message text: The value ofTotal number of queued bytes for Data Collaboration Server Connections for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Failure to read outgoing date by Web Conferencing Server servers.

Potential Impact: NA

Suggested Action(s): Check availability of Web Conferencing Server servers. Also check network connectivity.

Metric: SIPConnectionFailures

Description: the number of Sip connection failures per second.

Metric SpecName: SIPCONNFAILURE

Metric Field Name: WEBRELAY - Sip Connection Failures per second

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 25, Major / 50

Policy: MSBS_SIPConnectionFailures

Message text: The value of Sip Connection Failures per second for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Sip connection is terminated unexpectedly due to network issues or unavailability of remote servers.

Potential Impact: NA

Suggested Action(s): Check network and SIP server availability.

Collect_Edge_SipEps_Dialogs

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / NA

Source / Collection Definition: PERFMON / LS:SipEps - 00 - Sip Dialogs(_Total)

Metric: EdgeSipEpsDialogInstance

Description: instance of perfmon object

Metric SpecName: INSTANCENAME

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: EdgeSipEpsCoreManagerQueueLength

Description: Current Queue Length of events indicated by core manager thread

Metric SpecName: COREMGRQLENGTH

Metric Field Name: SipEps - 003 - CoreManagerQueueLength

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 50, Major / 100

Policy: MSBS_EdgeSipEpsCoreManagerQueueLength

Message text: The value of the counter 'CoreManagerQueueLength' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Collect_FrontEnd_PDPTURN

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / LSPDP

Source / Collection Definition: PERFMON / LS:PDP - TURN(*)

Metric: PDPTurnInstance

> **Description**: instance of perfmon object LS:PDP - TURN
>
> **Metric SpecName**: PDPTURNINSTANCE
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: PDPClientAuthTimeoutFailures

> **Description**: the per-second rate of client connections timing out before receiving an authenticated message.
>
> **Metric SpecName**: CLIENTAUTHTOFAIL
>
> **Metric Field Name**: PDP - Client Authentication timeout failures/sec
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Metric: PDPFirstPacketTimeout

> **Description**: the per-second rate of sessions that have timed out before the first packet arrived.
>
> **Metric SpecName**: FIRPACKTO
>
> **Metric Field Name**: PDP - First packet timeouts/sec
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Metric: PDPServerAuthTimeoutFailures

Description: the per-second rate of server connections timing out before receiving an authenticated message.

Metric SpecName: SERVERAUTHTO

Metric Field Name: PDP - server authentication timeout failures/sec

Data type: UINT32

Alarm: FALSE

Collect_FrontEnd_Web_AddressBook_WebQuery

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / LSWEBADDRBKWEBQRY

Source / Collection Definition: PERFMON / LS:WEB - Address Book Web Query(*)

Metric: AddressBookWebQueryInstance

Description: instance of perfmon object LS:WEB - Address Book Web Query

Metric SpecName: ADDRBKWEBQRYINST

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: FailedSearchRequests

Description: the per-second rate of failed address book search requests

Metric SpecName: FEFAILEDSEARCHREQ

Metric Field Name: WEB - Failed search requests/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 500, Major / 1000

Policy: MSBS_FailedSearchRequests

Message text: The value of Address Book Web Query Failed search requests/sec for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Issues with backend database connectivity

Potential Impact: NA

Suggested Action(s): Verify backend database is running and accessible.

Metric: AvgProcessingTimeForASearchRequest

Description: the average processing time for a address book search request in milliseconds

Metric SpecName: AVGPROCTIME

Metric Field Name: WEB - Average processing time for a search request in milliseconds

Data type: UINT32

Alarm: FALSE

Collect_Archiving_Process_RTCArch

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / CS_PROCESS

Source / Collection Definition: PERFMON / Process(RTCArch)

Metric: ArchivingRTCArchInstance

> **Description**: instance of perfmon object Process(RTCArch)
>
> **Metric SpecName**: INSTANCENAME
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: ArchivingRTCArchPageFaultsPersec

> **Description**: Page Faults/sec counter available in the Lync Server Replica Replicator Agent service.
>
> **Metric SpecName**: PAGEFAULTS
>
> **Metric Field Name**: Page Faults/sec
>
> **Data type**: UINT32
>
> **Alarm**: TRUE
>
> **Category** : MSSkype
>
> **Severity / Threshold** : Major / 100
>
> **Policy**: MSBS_ArchivingRTCArchPageFaultsPersec
>
> **Message text**: The value of the counter 'Page Faults/sec' value <VALUE> has crossed the threshold of <THRESHOLD> .
>
> **Instructional Text**:
>
> **Probable Cause(s)**: NA
>
> **Potential Impact**: NA
>
> **Suggested Action(s)**: NA

Metric: ArchivingRTCArchPrivateBytes

Description: Private Bytes counter available in the Lync Server Replica Replicator Agent service.

Metric SpecName: PRIVATEBYTES

Metric Field Name: Private Bytes

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20000000

Policy: MSBS_ArchivingRTCArchPrivateBytes

Message text: The value of the counter 'Private Bytes' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: ArchivingRTCArchProcessorTime

Description: the % Processor Time counter available in the Lync Server Replica Replicator Agent service.

Metric SpecName: PROCESSORTIME

Metric Field Name: % Processor Time

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 90

Policy: MSBS_ArchivingRTCArchProcessorTime

Message text: The value of the counter '% Processor Time' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: ArchivingRTCArchThreadCount

Description: Thread Count counter available Lync Server Replica Replicator Agent service

Metric SpecName: THREADCOUNT

Metric Field Name: Thread Count

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 150

Policy: MSBS_ArchivingRTCArchThreadCount

Message text: The value of the counter 'Thread Count' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: ArchivingRTCArchWorkingSet

Description: Working Set Counter available in the Lync Server Replica Replicator Agent service.

Metric SpecName: WORKINGSET

Metric Field Name: Working Set

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20000000

Policy: MSBS_ArchivingRTCArchWorkingSet

Message text: The value of the counter 'Working Set' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

AudioJitterPoorCallsPercentage

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / AUDIOJITTERPOORCALLS

Source / Collection Definition: SQLDB / select isnull(cast(100.0 * cast((SUM(CASE WHEN [AudioJitterInterArrival] > [JitterInterArrivalOptimal] THEN 1 ELSE 0 END)) as float) / cast((SUM (CASE WHEN MediaLineLabel is NOT NULL THEN 1 ELSE 0 END)) as float) as decimal(4, 1)),0) as AudioJitterPoorCallsPercentage,SERVERPROPERTY('MACHINENAME') AS 'ServerName' from

[QoEMetrics].[dbo].[QoEReportsCallDetailView] Where MediaLineLabel = 0 AND
ConferenceDateTime >= dateadd(MINUTE,@Duration,GETUTCDATE())

Metric: AudioJitterPoorCallsPercentage

> **Description**: This metric captures Poor Audio that have Jitter more than a set threshold value
> and calculates percentage of poor calls for a given interval At the end of each call, parameters
> that determine Quality of a call that include network, audio and video parameters are logged into
> QoE database of Lync Server. Each call is categorized as having Acceptable quality or Poor
> quality based on the same.
>
> **Metric SpecName**: AudJitterPoorCallPer
>
> **Metric Field Name**: AudioJitterPoorCallsPercentage
>
> **Data type**: REAL64
>
> **Alarm**: TRUE
>
> **Category** : MSSkype
>
> **Severity / Threshold** : Warning / 40, Major / 70, Warning / 40, Major / 70
>
> **Policy**: MSBS_AudioJitterPoorCallsPercentage
>
> **Message text**: The current value of Percentage Audio Jitter Poor Calls is <VALUE> which
> exceeds the threshold of <THRESHOLD>
>
> **Instructional Text**:
>
> **Probable Cause(s)**: Variation in the delay time of packets arriving at their destination. Audio
> packets are sent at regular intervals from the sender to the receiver, but because of network
> latency the interval between packets can vary at the destination. Caused by LAN Congestion or
> issue with device/device drivers.
>
> **Potential Impact**: This variation can affect media quality. Jitter is used to determine MOSs as
> well as in the call detail report. Delay due to jitter buffering
>
> **Suggested Action(s)**: Use Jitter buffers in Packet Switched Networks. Network Upgrade.

Metric: ServerName

Description: This is the key for metric

Metric SpecName: ServerName

Metric Field Name: ServerName

Data type: TEXT

Alarm: FALSE

Metric: AudioJitterPoorCallsPercentage

Description: This metric captures Poor Audio that have Jitter more than a set threshold value and calculates percentage of poor calls for a given interval At the end of each call, parameters that determine Quality of a call that include network, audio and video parameters are logged into QoE database of Lync Server. Each call is categorized as having Acceptable quality or Poor quality based on the same.

Metric SpecName: AudJitterPoorCallPer

Metric Field Name: AudioJitterPoorCallsPercentage

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 40, Major / 70, Warning / 40, Major / 70

Policy: MSBS_AudioJitterPoorCallsPercentage

Message text: The current value of Percentage Audio Jitter Poor Calls is <VALUE> which exceeds the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Variation in the delay time of packets arriving at their destination. Audio packets are sent at regular intervals from the sender to the receiver, but because of network latency the interval between packets can vary at the destination. Caused by LAN Congestion or issue with device/device drivers.

Potential Impact: This variation can affect media quality. Jitter is used to determine MOSs as well as in the call detail report. Delay due to jitter buffering

Suggested Action(s): Use Jitter buffers in Packet Switched Networks. Network Upgrade.

Metric: ServerName

> **Description**: This is the key for metric
>
> **Metric SpecName**: ServerName
>
> **Metric Field Name**: ServerName
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

MCUHealthStateChangedPer

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: SKYPE / MCUHELTHSTATCHANGPS

Source / Collection Definition: PERFMON / LS:AsMcu - 01 - MCU Health And Performance(*)

Metric: MCUHealthStateChangedCount

> **Description**: This metric captures MCU Health State Changed Count
>
> **Metric SpecName**: MCUHelthStatChangPer
>
> **Metric Field Name**: ASMCU - 007 - MCU Health State Changed Count
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Metric: Instance_Name

> **Description**: This is the key for metric
>
> **Metric SpecName**: Instance_Name
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: MCUHealthStateChangedCount

> **Description**: This metric captures MCU Health State Changed Count
>
> **Metric SpecName**: MCUHelthStatChangPer
>
> **Metric Field Name**: ASMCU - MCU Health State Changed Count
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Metric: Instance_Name

> **Description**: This is the key for metric
>
> **Metric SpecName**: Instance_Name
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Collect_FrontEnd_LoadMgmt

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / CS_FRONTEND

Source / Collection Definition: PERFMON / LS:SIP - 07 - Load Management(*)

Metric: SIPLoadManagementInstance

> **Description**: instance of perfmon object LS:SIP - 07 - Load Management
>
> **Metric SpecName**: SIPLOADMGMTINST
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: SIPLoadMgmtAvgHoldTimeForInMessages

> **Description**: average processing time taken by the server for one request.
>
> **Metric SpecName**: HOLDINGTIMEFORINCMSG
>
> **Metric Field Name**: SIP - 000 - Average Holding Time For Incoming Messages
>
> **Data type**: UINT32
>
> **Alarm**: TRUE
>
> **Category** : MSSkype
>
> **Severity / Threshold** : Major / 5
>
> **Policy**: MSBS_SIPLoadMgmtAvgHoldTimeForInMessages
>
> **Message text**: The value of the counter 'Average Holding Time For Incoming Messages' value <VALUE> has crossed the threshold of <THRESHOLD> .
>
> **Instructional Text**:
>
> **Probable Cause(s)**: NA
>
> **Potential Impact**: NA
>
> **Suggested Action(s)**: NA

Collect_FrontEnd_SIPPeers

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / LSSIPPEERS

Source / Collection Definition: PERFMON / LS:SIP - Peers(*)

Metric: SIPPeersInstance

> **Description**: instance of perfmon object LS:SIP - Peers
>
> **Metric SpecName**: PEERSINSTNACE
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: AvgOutgoingQueueDelay

> **Description**: the average time (in seconds) the messages delayed in outgoing (send) queues.
>
> **Metric SpecName**: AVGOUTGOINGQUEDELAY
>
> **Metric Field Name**: SIP - Average Outgoing Queue Delay
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Metric: SIPPeersInstance

> **Description**: instance of perfmon object LS:SIP - 01 - Peers
>
> **Metric SpecName**: PEERSINSTNACE
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: AvgOutgoingQueueDelay

Description: the average time (in seconds) the messages delayed in outgoing (send) queues.

Metric SpecName: AVGOUTGOINGQUEDELAY

Metric Field Name: SIP - Average Outgoing Queue Delay

Data type: UINT32

Alarm: FALSE

Metric: SIPPeersSendsOutstanding

Description: number of outbound requests and responses queued.

Metric SpecName: SENDSOUTSTANDING

Metric Field Name: SIP - 017 - Sends Outstanding

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 200

Policy: MSBS_SIPPeersSendsOutstanding

Message text: The value of the counter 'SIP - 017 - Sends Outstanding' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Collect_FrontEnd_LogRetention

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / LSLOGRETENTION

Source / Collection Definition: PERFMON / LS:LogRetention - LogRetention(*)

Metric: LogRetentionInstance

> **Description**: instance of perfmon object LS:LogRetention - LogRetention
>
> **Metric SpecName**: LOGRETINTANCE
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: AddingTenantAndSyndicatorLatency

> **Description**: Add Tenant and Syndicator' Latency
>
> **Metric SpecName**: TENANTSYNDILATENCY
>
> **Metric Field Name**: - Adding tenant and syndicator latency (ms)
>
> **Data type**: UINT32
>
> **Alarm**: TRUE
>
> **Category** : MSSkype
>
> **Severity / Threshold** : Warning / 10000, Major / 30000
>
> **Policy**: MSBS_AddingTenantAndSyndicatorLatency
>
> **Message text**: The value of Adding tenant and syndicator latency (ms) for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>
>
> **Instructional Text**:
>
> **Probable Cause(s)**: Database addition took long time.
>
> **Potential Impact**: NA
>
> **Suggested Action(s)**: Verify that the database (i.e. lcscdr) is available.

Metric: LogRetentionGetNextPageLatency

Description: GetNextPage' Latency

Metric SpecName: GETNXTPAGLATENCY

Metric Field Name: - GetNextPage latency (ms)

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 10000, Major / 30000

Policy: MSBS_LogRetentionGetNextPageLatency

Message text: The value of GetNextPage latency (ms) for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Active directory query took long time.

Potential Impact: NA

Suggested Action(s): Verify that Active Directory is accessible.

Metric: LogRetentionConferenceMessageQueryLatency

Description: Get Conference Sessions' Latency

Metric SpecName: CONFSESSIONQRYLAT

Metric Field Name: - Conference Session Query latency (ms)

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 10000, Major / 30000

Policy: MSBS_LogRetentionConferenceMessageQueryLatency

Message text: The value of Conference Session Query latency (ms) for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Database query took long time.

Potential Impact: NA

Suggested Action(s): Verify that the database (i.e. lcscdr) is available.

Metric: DeletingSyndicatorCacheLatency

Description: Delete Syndicator Cache' Latency

Metric SpecName: DELSYNDCACHLAT

Metric Field Name: - Deleting syndicator cache latency (ms)

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 10000, Major / 30000

Policy: MSBS_DeletingSyndicatorCacheLatency

Message text: The value of Deleting syndicator cache latency (ms) for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Database delete took long time.

Potential Impact: NA

Suggested Action(s): Verify that the database (i.e. lcscdr) is available.

Metric: GetLogUploadUrlLatency

Description: GetLogUploadUrls' Latency

Metric SpecName: GETLOGUPLURLLAT

Metric Field Name: - GetLogUploadUrls latency (ms)

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 10000, Major / 30000

Policy: MSBS_GetLogUploadUrlLatency

Message text: The value of GetLogUploadUrls latency (ms) for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Calling GetLogUploadUrls took long time.

Potential Impact: NA

Suggested Action(s): Verify that you can connect to Microsoft Online Service.

Metric: FailedGetLogUploadUrlCalls

Description: GetLogUploadUrls' Failures

Metric SpecName: FAILEDLOGUPLURLCALL

Metric Field Name: - Failed GetLogUploadUrls Calls

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 1, Major / 2

Policy: MSBS_FailedGetLogUploadUrlCalls

Message text: The value of Failed GetLogUploadUrls Calls for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Cannot execute GetLogUploadUrls web service call.

Potential Impact: NA

Suggested Action(s): Verify that you can connect to Microsoft Online Service.

Metric: FailedUploadActivityLogCalls

Description: UploadActivityLog' Failures

Metric SpecName: FAILEDUPLACTLOGCALL

Metric Field Name: - Failed UploadActivityLog Calls

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 1, Major / 2

Policy: MSBS_FailedUploadActivityLogCalls

Message text: The value of Failed UploadActivityLog Calls for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Cannot execute UploadActivityLog web service call.

Potential Impact: NA

Suggested Action(s): Verify that you can connect to Microsoft Online Service.

Metric: LogRetentionUnexpectedException

Description: Unexpected failures

Metric SpecName: UNEXPECTEXCEPT

Metric Field Name: - Unexpected Exceptions

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 1, Major / 2

Policy: MSBS_LogRetentionUnexpectedException

Message text: The value of Unexpected Exceptions for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Unexpected exception.

Potential Impact: NA

Suggested Action(s): Notify your organization's support team with the event detail.

Metric: P2PSessionQueryLatency

Description: Get P2P Sessions' Latency

Metric SpecName: P2PSESSIONQRYLAT

Metric Field Name: - P2P Session Query latency (ms)

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 10000, Major / 30000

Policy: MSBS_P2PSessionQueryLatency

Message text: The value of P2P Session Query latency (ms) for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Database query took long time.

Potential Impact: NA

Suggested Action(s): Verify that the database (i.e. lcscdr) is available.

Metric: UpdatingRecordsProcessedLatency

Description: Update Sessions Processed' Latency

Metric SpecName: UPDRECPROCLAT

Metric Field Name: - Updating records Processed latency (ms)

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 10000, Major / 30000

Policy: MSBS_UpdatingRecordsProcessedLatency

Message text: The value of Updating records Processed latency (ms) for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Database update took long time.

Potential Impact: NA

Suggested Action(s): Verify that the database (i.e. lcscdr) is available.

Metric: UploadActivityLogLatency

Description: UploadActivityLog' Latency

Metric SpecName: UPLACTLOGLAT

Metric Field Name: - UploadActivityLog latency (ms)

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 10000, Major / 30000

Policy: MSBS_UploadActivityLogLatency

Message text: The value of UploadActivityLog latency (ms) for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Calling UploadActivityLog took long time.

Potential Impact: NA

Suggested Action(s): Verify that you can connect to Microsoft Online Service.

ChkFrontEndConferencingAnnouncementServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SERVSTAT

Source / Collection Definition: SERVICECHECK / RTCCAS

Metric: FERTCCASServName

Description: Name of the Service

Metric SpecName: SERVNAME

Metric Field Name: Service_Name

Data type: TEXT

Alarm: FALSE

Metric: FERTCCASServDisplayName

Description: Display Name of the Service

Metric SpecName: SRVDISPNAME

Metric Field Name: Service_Displayname

Data type: TEXT

Alarm: FALSE

Metric: FERTCCASServStatus

Description: Status of the Service

Metric SpecName: SERVSTATUS

Metric Field Name: Service_Status

Data type: TEXT

Alarm: FALSE

Metric: FERTCCASServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_FERTCCASServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): Lync Server Conferencing Announcement' Windows Service is stopped.

Potential Impact: NA

Suggested Action(s): Lync Server Conferencing Announcement' Windows Service is stopped. Please restart the service.

Collect_AvConf_AVMCU_CCCPProcessing

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / NA

Source / Collection Definition: PERFMON / LS:AVMCU - 03 - CCCP Processing

Metric: AvConfCCCPProcessingInstance

Description: instance of perfmon object LS:AVMCU - 03 - CCCP Processing

Metric SpecName: AVCONFCCCPROCESSGINSTANCE

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: AvConfNumberofaddconferencerequestsfailed

Description: number of failed response returned by add-conference

Metric SpecName: NOFADDCONFREQSTFAILD

Metric Field Name: AVMCU - 029 - Number of add conference requests failed

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 50, Major / 100

Policy: MSBS_AvConfNumberofaddconferencerequestsfailed

Message text: The value of the counter 'Number of add conference requests failed' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

SimplePortWatcher5076

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / Port5076

Source / Collection Definition: PORTCOL / PORTCHECKER

Metric: SimpleWatcherPort5076

Description: Used for incoming SIP requests for the Audio Test service.

Metric SpecName: SimpleWatcherPort5076

Metric Field Name: SimpleWatcherPort5076

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort5076

Message text: The Port No:5076 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

Metric: SimpleWatcherPort5076

Description: Used for incoming SIP requests for the Audio Test service.

Metric SpecName: SimpleWatcherPort5076

Metric Field Name: SimpleWatcherPort5076

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort5076

Message text: The Port No:5076 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

JoinLauncherService

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / JOINLAUNCHERSERVICE

Source / Collection Definition: PERFMON / LS:JoinLauncher - Join Launcher Service Failures(*)

Metric: JoinFailures

Description: This metric captures Join Failures

Metric SpecName: JoinFailures

Metric Field Name: JOINLAUNCHER - Join Failures

Data type: REAL64

Alarm: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: JoinFailuresDueToBaseURLMappingToMultipleTenants

Description: This metric captures Join Failures Due To Base URL Mapping To Multiple Tenants

Metric SpecName: JoinFailBsURLMapMltT

Metric Field Name: JOINLAUNCHER - Join Failures Due To Base URL Mapping To Multiple Tenants

Data type: REAL64

Alarm: FALSE

Metric: JoinFailuresDueToFailureToLookupBaseURL

Description: This metric captures Join Failures Due To Failure To Lookup Base URL

Metric SpecName: JoiFailFailLkupBsURL

Metric Field Name: JOINLAUNCHER - Join Failures Due To Failure To Lookup Base URL

Data type: REAL64

Alarm: FALSE

Metric: JoinFailuresDueToIncorrectMeetingURLFormat

Description: This metric captures Join Failures Due To Incorrect Meeting URL Format

Metric SpecName: JoinFailIncMetURLFmt

Metric Field Name: JOINLAUNCHER - Join Failures Due To Incorrect Meeting URL Format

Data type: REAL64

Alarm: FALSE

Metric: JoinFailuresDueToJoinTakingLongerThanExpectedTime

Description: This metric captures Join Failures Due To Join Takin Longer Than Expected Time

Metric SpecName: JnFailjoinTakLongExp

Metric Field Name: JOINLAUNCHER - Join Failures Due To Join Taking Longer Than Expected Time

Data type: REAL64

Alarm: FALSE

Metric: JoinFailuresDueToLookupUserFailure

Description: This metric captures Join Failures Due ToLookupUserFailure

Metric SpecName: JnFailLkupUsrFailure

Metric Field Name: JOINLAUNCHER - Join Failures Due To Lookup User Failure

Data type: REAL64

Alarm: FALSE

Metric: JoinFailuresDueToNoMatchingRegexFound

Description: This metric captures Join Failures Due To No Matching Regex Found

Metric SpecName: JoinFailNoMtchRegFnd

Metric Field Name: JOINLAUNCHER - Join Failures Due To No Matching Regex Found

Data type: REAL64

Alarm: FALSE

Metric: JoinFailuresDueToVerifyConferenceKeyFailure

Description: This metric captures Join Failures Due To Verify Conference Key Failure

Metric SpecName: JnFailVerConfKeyFail

Metric Field Name: JOINLAUNCHER - Join Failures Due To Verify Conference Key Failure

Data type: REAL64

Alarm: FALSE

Metric: JoinFailuresToSendConferenceErrorReports.

Description: This metric captures Join Failures Due To Send Conference Error Reports.

Metric SpecName: JoinFailSendCnfErRep

Metric Field Name: JOINLAUNCHER - Join Failures To Send Conference Error Reports.

Data type: REAL64

Alarm: FALSE

ChkFrontEndServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SERVSTAT

Source / Collection Definition: SERVICECHECK / RTCSRV

Metric: FrontEndRTCSRVServName

Description: Name of the Service

Metric SpecName: SERVNAME

Metric Field Name: Service_Name

Data type: TEXT

Alarm: FALSE

Metric: FrontEndRTCSRVServDisplayName

Description: Display Name of the Service

Metric SpecName: SRVDISPNAME

Metric Field Name: Service_Displayname

Data type: TEXT

Alarm: FALSE

Metric: FrontEndRTCSRVServStatus

Description: Status of the Service

Metric SpecName: SERVSTATUS

Metric Field Name: Service_Status

Data type: TEXT

Alarm: FALSE

Metric: FrontEndRTCSRVServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_FrontEndRTCSRVServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): Lync Server Front-End' Windows Service is stopped.

Potential Impact: NA

Suggested Action(s): Lync Server Front-End' Windows Service is stopped. Please restart the service.

Collect_FrontEnd_Process_MasterReplicatorAgent

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / CS_PROCESS

Source / Collection Definition: PERFMON / Process(MasterReplicatorAgent)

Metric: FEMASTERInstance

> **Description**: instance of MasterReplicatorAgent process
>
> **Metric SpecName**: INSTANCENAME
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FEMASTERPercentprocessorTime

> **Description**: Percentage Processor Time is the percentage of elapsed time that all of process threads used the processor to execution instructions.
>
> **Metric SpecName**: PCTPROCESSORTIME
>
> **Metric Field Name**: % Processor Time
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Metric: FEMASTERWorkingSet

Description: Working Set is the current size, in bytes, of the Working Set of this process. the Working Set is the set of memory pages touched recently by the threads in the process. If free memory in the computer is above a threshold, pages are left in the Working Set of a process even if they are not in use. When free memory falls below a threshold, pages are trimmed from Working Sets. If they are needed they will then be soft-faulted back into the Working Set before leaving main memory.

Metric SpecName: WORKINGSET

Metric Field Name: Working Set

Data type: UINT32

Alarm: FALSE

Metric: FEMASTERPageFaultsPerSec

Description: Page Faults/sec is the average number of pages faulted per second. It is measured in number of pages faulted per second because only one page is faulted in each fault operation, hence this is also equal to the number of page fault operations. This counter includes both hard faults (those that require disk access) and soft faults (where the faulted page is found elsewhere in physical memory.) Most processors can handle large numbers of soft faults without significant consequence. However, hard faults, which require disk access, can cause significant delays.

Metric SpecName: PAGEFAULTS

Metric Field Name: Page Faults/sec

Data type: UINT32

Alarm: FALSE

Metric: FEMASTERPrivateBytes

Description: Private Bytes is the current size, in bytes, of memory that this process has allocated that cannot be shared with other processes.

Metric SpecName: PRIVATEBYTES

Metric Field Name: Private Bytes

Data type: UINT32

Alarm: FALSE

Metric: FEMASTERThreadCount

> **Description**: the number of threads currently active in this process. An instruction is the basic unit of execution in a processor, and a thread is the object that executes instructions. Every running process has at least one thread.
>
> **Metric SpecName**: THREADCOUNT
>
> **Metric Field Name**: Thread Count
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Collect_Mediation_MediaRelay

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / NA

Source / Collection Definition: PERFMON / LS:MediationServer - 02 - Media Relay(*)

Metric: MedMediaRelayInstance

> **Description**: instance of perfmon object LS:MediationServer - 02 - Media Relay
>
> **Metric SpecName**: MEDMEDIARELYINSTANCE
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: MedMediaConnectivityCheckFailure

Description: the number of failures in media connectivity check

Metric SpecName: MEDIACONNCHKFAIL

Metric Field Name: 1 - Media Connectivity Check Failure

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 5, Major / 10

Policy: MSBS_MedMediaConnectivityCheckFailure

Message text: The value of the counter 'Media Connectivity Check Failure' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Collect_FrontEnd_CallParkServicePlanning

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / LSCPS

Source / Collection Definition: PERFMON / LS:CPS - Call Park Service Planning(*)

Metric: CPSInstanceName

Description: Instance of perfmon object LS:CPS - Call Park Service Planning

Metric SpecName: CPSINSTANCENAME

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: TotalfailedFallbackAttempts

Description: the total number of failed fallback attempts.

Metric SpecName: TOTFAILEDFBATTEMPTS

Metric Field Name: CPS - Total failed fallback attempts.

Data type: UINT32

Alarm: FALSE

Metric: TotalparkRequestFailedUnavailableOrbit

Description: the total number of park requests failed because no orbit available.

Metric SpecName: TOTPRKREQFAILEDUO

Metric Field Name: CPS - Total park requests failed because unavailable orbit

Data type: UINT32

Alarm: FALSE

Metric: TotalParkRequestsFailed

Description: the total number of park requests that failed.

Metric SpecName: TOTPRKREQFAILED

Metric Field Name: CPS - Total park requests that failed

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 5, Major / 10

Policy: MSBS_TotalParkRequestsFailed

Message text: The value of Total park requests that failed for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): See resolution for next steps.

Potential Impact: NA

Suggested Action(s): Check NT events and logs for further errors as well as Performance Monitor.

Collect_Edge_SIP_Networking

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / EDGESIPNWKNG

Source / Collection Definition: PERFMON / LS:SIP - Networking(*)

Metric: EdgeSIPNetworkingInstance

Description: instance of perfmon object LS:SIP - Networking

Metric SpecName: EDGNWINSTNAME

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: EdgeConnsRefusedDueToServerOverload

Description: the total number of the connections that were refused with Service Unavailable response because the server was overloaded.

Metric SpecName: CONREFSERVLOAD

Metric Field Name: SIP - Connections Refused Due To Server Overload

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 1, Major / 3

Policy: MSBS_EdgeConnsRefusedDueToServerOverload

Message text: The value of SIP - Connections Refused Due To Server Overload for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): This server is overloaded.

Potential Impact: NA

Suggested Action(s): This might be a temporary condition. If the problem persists, please ensure that hardware and software requirements for this server meets the user usage characteristics.

Metric: EdgeSIPNetworkingInstance

Description: instance of perfmon object LS:SIP - 00 - Networking

Metric SpecName: EDGNWINSTNAME

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: EdgeConnectionsFailedToEstablishPerSec

Description: rate of the connections dropped because the peer failed to exchange valid data with the server within establishing timeout.

Metric SpecName: CONNFAILDTESTBLSH

Metric Field Name: SIP - 005 - Connections Failed To Establish/Sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20

Policy: MSBS_EdgeConnectionsFailedToEstablishPerSec

Message text: The value of the counter 'Connections Failed To Establish/Sec' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Collect_Edge_API_Application_Counters

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / NA

Source / Collection Definition: PERFMON / LS:API - 00 - API Application Instance Counters(_
Total)

Metric: APIEdgeTransPendingDispatchCompln

> **Description**: number of established TLS connections that are currently active. TLS Connection
> is considered established when peer certificate and, possibly, host name are verified for trust
> relationship.
>
> **Metric SpecName**: TRANSPENDGDISPATCHCOMP
>
> **Metric Field Name**: API - 026 - Transactions Pending Dispatch Completion
>
> **Data type**: UINT32
>
> **Alarm**: TRUE
>
> **Category** : MSSkype
>
> **Severity / Threshold** : Warning / 500, Major / 1000
>
> **Policy**: MSBS_APIEdgeTransPendingDispatchCompln
>
> **Message text**: The value of the counter 'Transactions Pending Dispatch Completion' value
> <VALUE> has crossed the threshold of <THRESHOLD> .
>
> **Instructional Text**:
>
> **Probable Cause(s)**: NA
>
> **Potential Impact**: NA
>
> **Suggested Action(s)**: NA

Metric: APIEdgeApplicationCounterInstance

> **Description**: instance of perfmon object LS:API - 00 - API Application Instance Counters(_
> Total)
>
> **Metric SpecName**: INSTANCENAME
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

SprocCallsPerSec

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SPROCCALLSPERSEC

Source / Collection Definition: PERFMON / LS:USrv - GetPresence sproc(*)

Metric: SprocCallsPerSec

> **Description**: This metric captures SprocCallsPerSec
>
> **Metric SpecName**: SprocCallsPerSec
>
> **Metric Field Name**: USrv - Sproc Calls/Sec
>
> **Data type**: REAL64
>
> **Alarm**: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Collect_Archiving_ArchService_READ

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / NA

Source / Collection Definition: PERFMON / LS:Arch Service - 01 - READ(*)

Metric: ArchServiceReadInstance

   Description: instance of perfmon object LS:Arch Service - 01 - READ

   Metric SpecName: ARCHSERVCEREADINSTANCE

   Metric Field Name: Instance_Name

   Data type: TEXT

   Alarm: FALSE

Metric: ArchServiceDroppedmessagesfromMQ

Description: number of messages getting dropped

Metric SpecName: DROPPEDMSGFRMMQ

Metric Field Name: Arch Service - 006 - Dropped messages from MQ

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 0, Major / 1

Policy: MSBS_ArchServiceDroppedmessagesfromMQ

Message text: The value of the counter 'Arch Service - 006 - Dropped messages from MQ' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: ArchServiceMessagesthatfailedvalidation

Description: number of messages for which validation has failed

Metric SpecName: MSGFAILDVALIDTION

Metric Field Name: Arch Service - 002 - Messages that failed validation

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 0, Major / 1

Policy: MSBS_ArchServiceMessagesthatfailedvalidation

Message text: The value of the counter 'Arch Service - 002 - Messages that failed validation' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Collect_Edge_SIP_Peers

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / LSSIPPEERS

Source / Collection Definition: PERFMON / LS:SIP - Peers(*)

Metric: EdgeSIPPeersInstance

Description: instance of perfmon object LS:SIP - Peers

Metric SpecName: PEERSINSTNACE

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: EdgeSIPPeersSendsOutstandingLogging

Description: the average time (in seconds) the messages delayed in outgoing (send) queues.

Metric SpecName: AVGOUTGOINGQUEDELAY

Metric Field Name: SIP - Average Outgoing Queue Delay

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 8, Major / 20

Policy: MSBS_EdgeSIPPeersSendsOutstandingLogging

Message text: The value of SIP - Average Outgoing Queue Delay for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Network bandwidth to the destination is insufficient.

Potential Impact: NA

Suggested Action(s): This might be a temporary condition. If the problem persists, please ensure that hardware and software requirements at the destination and network bandwidth allocation meet the user usage characteristics.

Metric: EdgeSIPPeersInstance

Description: instance of perfmon object LS:SIP - 01 - Peers(_Total)

Metric SpecName: PEERSINSTNACE

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: PeersAboveLimitConnsDropd

Description: total number of connections that were dropped because the limit on number of incoming connections from a federated partner or clearing house was exceeded.

Metric SpecName: ABOVELMTCONNDROPPED

Metric Field Name: SIP - 004 - Above Limit Connections Dropped (Access Proxies only)

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 1, Major / 2

Policy: MSBS_PeersAboveLimitConnsDropd

Message text: The value of the counter 'Above Limit Connections Dropped' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: PeersFlowcontrldConns

Description: number of connections that are currently being flow-controlled

Metric SpecName: FLOWCONTRLDCONN

Metric Field Name: SIP - 023 - Flow-controlled Connections

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 50, Major / 100

Policy: MSBS_PeersFlowcontrldConns

Message text: The value of the counter 'Flow-controlled Connections' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: PeersFlowcontrldConnsDropd

Description: total number of connections dropped because of excessive flow-control.

Metric SpecName: FLOWCONTRLDCONNDROPPED

Metric Field Name: SIP - 024 - Flow-controlled Connections Dropped

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 5, Major / 10

Policy: MSBS_PeersFlowcontrldConnsDropd

Message text: The value of the counter 'Flow-controlled Connections Dropped' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: EdgeSIPPeersSendsTimed-Out

Description: total number of sends dropped because they stayed in the outgoing (send) queue for too long.

Metric SpecName: SENDSTIMEOUT

Metric Field Name: SIP - 018 - Sends Timed-Out

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 500, Major / 1000

Policy: MSBS_EdgeSIPPeersSendsTimed-Out

Message text: The value of the counter 'Sends Timed-Out' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

WebThrottlingAuth

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / WEBTHROTTLINGAUTH

Source / Collection Definition: PERFMON / LS:WEB - Throttling and Authentication(*)

Metric: FailedHTTPProxRequest

Description: This metric captures Failed HTTP Proxy Requests

Metric SpecName: FailedHTTPProxyReq

Metric Field Name: WEB - Failed HTTP Proxy Requests

Data type: REAL64

Alarm: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: NumberOfProxyRequestsAwaitingCompletion.

Description: This metric captures Number Of Proxy Requests Awaiting Completion

Metric SpecName: NumPrxReqAwaitCmplt

Metric Field Name: WEB - Number Of Proxy Requests Awaiting Completion.

Data type: UINT32

Alarm: FALSE

Metric: RequestsExceededPerAppLimit

Description: This metric captures Requests Exceeded Per App Limit

Metric SpecName: RequExcPerAppLimit

Metric Field Name: WEB - Requests Exceeded Per-App Limit

Data type: REAL64

Alarm: FALSE

Metric: TotalRequests

Description: This metric captures Total Requests

Metric SpecName: TotalRequests

Metric Field Name: WEB - Total Requests

Data type: UINT32

Alarm: FALSE

Metric: TotalRequestsInProcessing

Description: This metric captures Total Requests In Processing

Metric SpecName: TotalRequestsInProc

Metric Field Name: WEB - Total Requests In Processing

Data type: UINT32

Alarm: FALSE

Metric: UnauthenticatedRequestsInProcessing

Description: This metric captures Unauthenticated Requests In Processing

Metric SpecName: UnauthentiReqProce

Metric Field Name: WEB - Unauthenticated Requests In Processing

Data type: REAL64

Alarm: FALSE

VISSvc

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / KHIVISSVC

Source / Collection Definition: PERFMON / LS:VISSvc - VISSvc

Metric: TotalCallsdeclinedduetoload

> **Description**: This policy monitors the counter that shows the total number of calls rejected because the server is overloaded.
>
> **Metric SpecName**: TotCaldecDuetoload
>
> **Metric Field Name**: VIS - Total Calls declined due to load
>
> **Data type**: UINT32
>
> **Alarm**: TRUE
>
> **Category** : MSSkype
>
> **Severity / Threshold** : Major / 10
>
> **Policy**: MSBS_TotalCallsdeclinedduetoload
>
> **Message text**: The current value of TotalCallsdeclinedduetoload is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:
>
> **Instructional Text**:
>
> **Probable Cause(s)**: Incoming INVITE is rejected because Video Interop Server is under heavy load.
>
> **Potential Impact**: Upgrade existing hardware or lower the calls through this Video Interop Server.
>
> **Suggested Action(s)**: Calls cannot be made.

Metric: TotalProxyLegCallFailures

Description: This policy monitors the counter that shows the total number of Proxy leg call failures.

Metric SpecName: TotPrxLegCalFail

Metric Field Name: VIS - Total Proxy Leg Call Failures

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 10

Policy: MSBS_TotalProxyLegCallFailures

Message text: The current value of TotalProxyLegCallFailures is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): Incoming INVITE is rejected because Video Interop Server is under heavy load.

Potential Impact: Upgrade existing hardware or lower the calls through this Video Interop Server.

Suggested Action(s): Calls cannot be made.

Metric: TotalInteropLegCallFailures

Description: This policy monitors the counter that shows the total number of interop leg call failures.

Metric SpecName: TotIntrpLegCalFail

Metric Field Name: VIS - Total Interop Leg Call Failures

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 10

Policy: MSBS_TotalInteropLegCallFailures

Message text: The current value of TotalInteropLegCallFailures is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): Incoming INVITE is rejected because Video Interop Server is under heavy load.

Potential Impact: Upgrade existing hardware or lower the calls through this Video Interop Server.

Suggested Action(s): Calls cannot be made.

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

PersistantChat

This policy maintains the information about the status for the different services

Schedule Task Policy: MSBS_SCH_LOW

ConfigFile Policy: MSBS_PersistantChat_Conf

Aspect: Skype Test Persistent Chat

CIT: Windows

Data source / Data class: LYNC / SYNCONPERCHAT

Source / Collection Definition: POWERSHELL / Test-CsPersistentChatMessage -TargetFQDN {fqdn}

Metric: PersistantChat

Description: This metric gathers the information which confirms that users can exchange messages by using the Persistent Chat service.

Metric SpecName: PersistentChat

Metric Field Name: PersistantChat

Data type: TEXT

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Minor / 1

Policy: MSBS_PersistantChat

Message text: The Persistant Chat is down

Instructional Text:

Probable Cause(s): 1. User configuration must not have done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: New users cannot be registered

Suggested Action(s): 1. Configuration errors: Most common issues are: Test user password is invalid or expired, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availibility: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution errors or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responded to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Metric: TargetFqdn

Description: This is the key for metric

Metric SpecName: TargetFqdn

Metric Field Name: TargetFqdn

Data type: TEXT

Alarm: FALSE

Metric: PersistantChatLatency

Description: This metric will capture latency which confirms that users can exchange messages by using the Persistent Chat service.

Metric SpecName: PersistentChatLat

Metric Field Name: PersistantChatLatency

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Minor / 1000

Policy: MSBS_PersistantChatLatency

Message text: The current value of Percentage Persistant Chat Latency is <VALUE> which exceeds the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): 1. User configuration must not have done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: New users cannot be registered

Suggested Action(s): 1. Configuration errors: Most common issues are: Test user password is invalid or expired, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availibility: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution errors or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responded to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Collect_FrontEnd_Process_AVMCUSvc

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / CS_PROCESS

Source / Collection Definition: PERFMON / Process(AVMCUSvc)

Metric: FERTCAVMCUInstance

> **Description**: instance of ASMCUSvc process
>
> **Metric SpecName**: INSTANCENAME
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FERTCAVMCUPercentprocessorTime

> **Description**: Percentage Processor Time is the percentage of elapsed time that all of process threads used the processor to execution instructions.
>
> **Metric SpecName**: PCTPROCESSORTIME
>
> **Metric Field Name**: % Processor Time
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Metric: FERTCAVMCUWorkingSet

Description: Working Set is the current size, in bytes, of the Working Set of this process. the Working Set is the set of memory pages touched recently by the threads in the process. If free memory in the computer is above a threshold, pages are left in the Working Set of a process even if they are not in use. When free memory falls below a threshold, pages are trimmed from Working Sets. If they are needed they will then be soft-faulted back into the Working Set before leaving main memory.

Metric SpecName: WORKINGSET

Metric Field Name: Working Set

Data type: UINT32

Alarm: FALSE

Metric: FERTCAVMCUPageFaultsPerSec

Description: Page Faults/sec is the average number of pages faulted per second. It is measured in number of pages faulted per second because only one page is faulted in each fault operation, hence this is also equal to the number of page fault operations. This counter includes both hard faults (those that require disk access) and soft faults (where the faulted page is found elsewhere in physical memory.) Most processors can handle large numbers of soft faults without significant consequence. However, hard faults, which require disk access, can cause significant delays.

Metric SpecName: PAGEFAULTS

Metric Field Name: Page Faults/sec

Data type: UINT32

Alarm: FALSE

Metric: FERTCAVMCUPrivateBytes

Description: Private Bytes is the current size, in bytes, of memory that this process has allocated that cannot be shared with other processes.

Metric SpecName: PRIVATEBYTES

Metric Field Name: Private Bytes

Data type: UINT32

Alarm: FALSE

Metric: FERTCAVMCUThreadCount

> **Description**: the number of threads currently active in this process. An instruction is the basic unit of execution in a processor, and a thread is the object that executes instructions. Every running process has at least one thread.
>
> **Metric SpecName**: THREADCOUNT
>
> **Metric Field Name**: Thread Count
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

REGDBStore

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / KHIREGDBSTORE

Source / Collection Definition: PERFMON / LS:Usrv - 00 - REGDBStore(*)

Metric: REGDBQueueLatency

Description: This policy monitors the average time a request is held in the request queue to RTC database.

Metric SpecName: REGDBQueueLatency

Metric Field Name: Usrv - 002 - Queue Latency (msec)

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 100, Major / 100

Policy: MSBS_REGDBQueueLatency

Message text: The current value of REGDBQueueLatency is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): The backend might be busy and is unable to respond to requests quickly.

Potential Impact: Please ensure that the hardware and software requirements meet the user usage characteristics.

Suggested Action(s): The average time a request is held in the request queue to RTC database would be high which would lead to slow response

Metric: REGDBSprocLatency

Description: This policy monitors the average time it takes to execute a sproc call against RTC database.

Metric SpecName: REGDBSprocLatency

Metric Field Name: Usrv - 004 - Sproc Latency (msec)

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 100, Major / 100

Policy: MSBS_REGDBSprocLatency

Message text: The current value of REGDBSprocLatency is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): The backend might be busy and is unable to respond to requests quickly.

Potential Impact: Please ensure that the hardware and software requirements meet the user usage characteristics.

Suggested Action(s): The average time it takes to execute a sproc call against RTC database would be high and would lead to delayed responses.

Metric: REGDBStoreThrottledrequests

Description: This policy monitors the number of requests that were rejected with a retry since the database queue latency was high.

Metric SpecName: REGDBThrottledreq

Metric Field Name: Usrv - 020 - Throttled requests/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 0, Major / 0

Policy: MSBS_REGDBStoreThrottledrequests

Message text: The current value of REGDBStoreThrottledrequests is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): Registrar database is overloaded.

Potential Impact: Please ensure that the hardware and software requirements meet the user usage characteristics.

Suggested Action(s): The total number of requests that were rejected with a retry-after since the database queue latency would be high and would lead to delayed response from Registrar database

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: REGDBQueueLatency

Description: This policy monitors the average time a request is held in the request queue to RTC database

Metric SpecName: REGDBQueueLatency

Metric Field Name: Usrv - Queue Latency (msec)

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 100, Major / 100

Policy: MSBS_REGDBQueueLatency

Message text: The current value of REGDBQueueLatency is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): The backend might be busy and is unable to respond to requests quickly.

Potential Impact: Please ensure that the hardware and software requirements meet the user usage characteristics.

Suggested Action(s): The average time a request is held in the request queue to RTC database would be high which would lead to slow response

Metric: REGDBSprocLatency

Description: This policy monitors the average time it takes to execute a sproc call against RTC database.

Metric SpecName: REGDBSprocLatency

Metric Field Name: Usrv - Sproc Latency (msec)

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 100, Major / 100

Policy: MSBS_REGDBSprocLatency

Message text: The current value of REGDBSprocLatency is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): The backend might be busy and is unable to respond to requests quickly.

Potential Impact: Please ensure that the hardware and software requirements meet the user usage characteristics.

Suggested Action(s): The average time it takes to execute a sproc call against RTC database would be high and would lead to delayed responses.

Metric: REGDBStoreThrottledrequests

Description: This policy monitors the number of requests that were rejected with a retry since the database queue latency was high.

Metric SpecName: REGDBThrottledreq

Metric Field Name: Usrv - Throttled requests/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 0, Major / 0

Policy: MSBS_REGDBStoreThrottledrequests

Message text: The current value of REGDBStoreThrottledrequests is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): Registrar database is overloaded.

Potential Impact: Please ensure that the hardware and software requirements meet the user usage characteristics.

Suggested Action(s): The total number of requests that were rejected with a retry-after since the database queue latency would be high and would lead to delayed response from Registrar database

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Collect_LogicalDisk_FrontEnd

This Policy monitors the logical disk feature of Microsoft Skype Business Server

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Logical_Disk_Conf

Aspect: Skype Logical Disk

CIT: Edge Server, Director Server, Mediation Server, Front End Server, Persistent Chat Server

Data source / Data class: LYNC / LOGICALDISK

Source / Collection Definition: PERFMON / LogicalDisk(*)

Metric: FELogicalDiskInstance

> **Description**: instance of perfmon object LogicalDisk
>
> **Metric SpecName**: LGDISKINSTNAME
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FEPercentageFreeSpace

> **Description**: % Free Space is the percentage of total usable space on the selected logical disk drive that was free.
>
> **Metric SpecName**: FREESPACE
>
> **Metric Field Name**: % Free Space
>
> **Data type**: UINT32
>
> **Alarm**: TRUE
>
> **Category** : MSSkype
>
> **Severity / Threshold** : Warning / 70, Major / 90
>
> **Policy**: MSBS_FEPercentageFreeSpace
>
> **Message text**: The value of % Free Space for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>
>
> **Instructional Text**:
>
> **Probable Cause(s)**: Database size grows indefinitely.
>
> **Potential Impact**: NA
>
> **Suggested Action(s)**: Please check each disk drive and clean up unnecessary files.

Collect_Edge_Process_MRASSvc

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / CS_PROCESS

Source / Collection Definition: PERFMON / Process(MRASSvc)

Metric: EdgeMRASSvcWorkingSet

> **Description**: Working Set counter available in the Audio/Video Authentication service.
>
> **Metric SpecName**: WORKINGSET
>
> **Metric Field Name**: Working Set
>
> **Data type**: UINT32
>
> **Alarm**: TRUE
>
> **Category** : MSSkype
>
> **Severity / Threshold** : Major / 20000000
>
> **Policy**: MSBS_EdgeMRASSvcWorkingSet
>
> **Message text**: The value of the counter 'Working Set' value <VALUE> has crossed the threshold of <THRESHOLD> .
>
> **Instructional Text**:
>
> **Probable Cause(s)**: NA
>
> **Potential Impact**: NA
>
> **Suggested Action(s)**: NA

Metric: EdgeMRASSvcThreadCount

Description: Thread Count counter available in the Audio/Video Authentication service.

Metric SpecName: THREADCOUNT

Metric Field Name: Thread Count

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 150

Policy: MSBS_EdgeMRASSvcThreadCount

Message text: The value of the counter 'Thread Count' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: EdgeMRASSvcProcessorTime

Description: the % Processor Time counter available in the Audio/Video Authentication service.

Metric SpecName: PROCESSORTIME

Metric Field Name: % Processor Time

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 90

Policy: MSBS_EdgeMRASSvcProcessorTime

Message text: The value of the counter '% Processor Time' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: EdgeMRASSvcPrivateBytes

Description: Private Bytes counter available in the Audio/Video Authentication service.

Metric SpecName: PRIVATEBYTES

Metric Field Name: Private Bytes

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20000000

Policy: MSBS_EdgeMRASSvcPrivateBytes

Message text: The value of the counter 'Private Bytes' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: EdgeMRASSvcIPageFaultsPersec

Description: Page Faults/sec counter available in the Audio/Video Authentication service.

Metric SpecName: PAGEFAULTPERSEC

Metric Field Name: Page Faults/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 100

Policy: MSBS_EdgeMRASSvcIPageFaultsPersec

Message text: The value of the counter 'Page Faults/sec' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: EdgeMRASSvcInstance

Description: instance of perfmon object Process(MRASSvc)

Metric SpecName: MRASSVCINSTANCE

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Collect_Monitoring_CDRService_ ReportError

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / NA

Source / Collection Definition: PERFMON / LS:CDR Service - 03 - Report Error(*)

Metric: MonitoringCDRServiceReportErrorInstance

> **Description**: instance of perfmon object LS:CDR Service - 03 - Report Error
>
> **Metric SpecName**: MONCDRSERVCEREPERRINSTANCE
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: MonitoringNumberoffailuresduetointernallocks

> **Description**: number of error report failures that occurred because of internal locks.
>
> **Metric SpecName**: NOFFAILDUETOINTLOCKS
>
> **Metric Field Name**: CDR Service - 001 - Number of failures due to internal locks
>
> **Data type**: UINT32
>
> **Alarm**: TRUE
>
> **Category** : MSSkype
>
> **Severity / Threshold** : Major / 20
>
> **Policy**: MSBS_MonitoringNumberoffailuresduetointernallocks
>
> **Message text**: The value of the counter 'Number of failures due to internal locks' value <VALUE> has crossed the threshold of <THRESHOLD> .
>
> **Instructional Text**:
>
> **Probable Cause(s)**: NA
>
> **Potential Impact**: NA
>
> **Suggested Action(s)**: NA

Metric: Nofthrotlderrreptsduetomaxreptperminlim

Description: number of error reports throttled because of the limit on maximum reports in a minute.

Metric SpecName: NOFTHROTLDERRREPDTMAXREPMINLIMT

Metric Field Name: CDR Service - 002 - Number of throttled error reports due to max report per minute limit

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20

Policy: MSBS_Nofthrotlderrreptsduetomaxreptperminlim

Message text: The value of the counter 'Number of throttled error reports due to max report per minute limit' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Metric: MonitoringNumberofunknownfailures

Description: number of unknown error report failures.

Metric SpecName: NOFUKNWNFAILS

Metric Field Name: CDR Service - 000 - Number of unknown failures

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20

Policy: MSBS_MonitoringNumberofunknownfailures

Message text: The value of the counter 'Number of unknown failures' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

AddressBookService_FileDownload

This policy maintains the information about the status for the different services

Schedule Task Policy: MSBS_SCH_LOW

ConfigFile Policy: MSBS_SyntheticRPC_Conf_2010

Aspect: Skype Test Contacts

CIT: Windows

Data source / Data class: LYNC / SYNRPCFILEDOWLD

Source / Collection Definition: POWERSHELL / TestCSAddressbookService TargetFQDN ${fqdn}

Metric: AddressBookService_FileDownload

Description: This metric gathers the information which confirms that users are able to download file This test allows you to monitor the ability to connect to an Address Book Download Web Service from a Lync pool. If the Address Book Download Web service is able to supply the requested location of the Address Book files the test is considered successful.

Metric SpecName: AddBkSeFileDwl

Metric Field Name: AddressBookService_FileDownload

Data type: TEXT

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_AddressBookService_FileDownload

Message text: The Address BookService File Download is down

Instructional Text:

Probable Cause(s): 1. User configuration must not have done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: New users cannot be registered

Suggested Action(s): 1. Configuration errors: Most common issues are: Test user password is invalid or expired, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availability: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution errors or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responded to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Metric: TargetFqdn

> **Description**: This is the key for metric
>
> **Metric SpecName**: TargetFqdn
>
> **Metric Field Name**: TargetFqdn
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: AddressBookServiceLatency

Description: This metric will capture the address book service latency

Metric SpecName: AddBkSerLat

Metric Field Name: AddressBookServiceLatency

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Minor / 1000, Minor / 1000

Policy: MSBS_AddressBookServiceLatency

Message text: The value of Address Book Service Latency(ms) is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): 1. User configuration must not have done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: New users cannot be registered

Suggested Action(s): 1. Configuration errors: Most common issues are: Test user password is invalid or expired, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availibility: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution errors or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responded to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Metric: AddressBookService_FileDownload

Description: This metric gathers the information which confirms that users are able to download file This test allows you to monitor the ability to connect to an Address Book Download Web Service from a Lync pool. If the Address Book Download Web service is able to supply the requested location of the Address Book files the test is considered successful.

Metric SpecName: AddBkSeFileDwl

Metric Field Name: AddressBookService_FileDownload

Data type: TEXT

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_AddressBookService_FileDownload

Message text: The Address BookService File Download is down

Instructional Text:

Probable Cause(s): 1. User configuration must not have done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: New users cannot be registered

Suggested Action(s): 1. Configuration errors: Most common issues are: Test user password is invalid or expired, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availability: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution errors or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responded to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Metric: TargetFqdn

Description: This is the key for metric

Metric SpecName: TargetFqdn

Metric Field Name: TargetFqdn

Data type: TEXT

Alarm: FALSE

Metric: AddressBookServiceLatency

Description: This metric will capture the address book service latency

Metric SpecName: AddBkSerLat

Metric Field Name: AddressBookServiceLatency

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Minor / 1000, Minor / 1000

Policy: MSBS_AddressBookServiceLatency

Message text: The value of Address Book Service Latency(ms) is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): 1. User configuration must not have done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: New users cannot be registered

Suggested Action(s): 1. Configuration errors: Most common issues are: Test user password is invalid or expired, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availibility: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution errors or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responded to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

AppSharingOneWayTripPoorCallsPercentage

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / QOEAPPSHARINGONEWAY

Source / Collection Definition: SQLDB / select isnull(cast(100.0 * cast((SUM(CASE WHEN [AppSharingRelativeOneWayAverage] > [AppsharingRelativeOneWayAverageOptimal] THEN 1 ELSE 0 END)) as float) / cast((SUM(CASE WHEN MediaLineLabel is NOT NULL THEN 1 ELSE 0 END)) as float) as decimal(4, 1)),0) as AppSharingOneWayTripPoorCallsPercentage,SERVERPROPERTY('MACHINENAME') AS 'ServerName' from [QoEMetrics].[dbo].[QoEReportsCallDetailView] Where MediaLineLabel = 3 AND ConferenceDateTime >= dateadd(MINUTE,@Duration,GETUTCDATE())

Metric: AppSharingOneWayTripPoorCallsPercentage

Description: This metric captures Poor Video that have Relative Network One Way Average Time more than a set threshold value and calculates percentage of poor calls for a given interval At the end of each call, parameters that determine Quality of a call that include network, audio and video parameters are logged into QoE database of Lync Server. Each call is categorized as having Acceptable quality or Poor quality based on the same.

Metric SpecName: AppShareTripPoorCall

Metric Field Name: AppSharingOneWayTripPoorCallsPercentage

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 40, Major / 70

Policy: MSBS_AppSharingOneWayTripPoorCallsPercentage

Message text: The Percentage of Poor Video that have Relative Network One Way Average Time is <VALUE> which exceeds the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): High round-trip values can be caused by a routing misconfiguration, a long distance call or an overloaded media server.

Potential Impact: - Slow rendering - Distorted Video rendering

Suggested Action(s): Network upgrade Reconfigure routing rules

Metric: ServerName

Description: This is the key for metric

Metric SpecName: ServerName

Metric Field Name: ServerName

Data type: TEXT

Alarm: FALSE

RegDBQueueDepth

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / REGDBQUEUEDEPTH

Source / Collection Definition: PERFMON / LS:USrv - REGDBStore(*)

Metric: RegDBQueueDepth

> **Description**: This metric captures the average number of database requests waiting to be executed for REGDB Store
>
> **Metric SpecName**: RegDBQueueDepth
>
> **Metric Field Name**: USrv - Queue Depth
>
> **Data type**: REAL64
>
> **Alarm**: FALSE

Metric: Instance_Name

> **Description**: This is the key for metric
>
> **Metric SpecName**: Instance_Name
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Collect_FrontEnd_DataCollection_Legal_Intercept_ Adapter

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / LSDCLEGALADAPT

Source / Collection Definition: PERFMON / LS:DATACOLLECTION - Legal Intercept Adaptor(*)

Metric: UDCEmailSendingFailures

> **Description**: This counter shows the total number of email sending failures.
>
> **Metric SpecName**: EMAILSENDFAILURES
>
> **Metric Field Name**: UDC - Email Sending Failures
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Metric: UDCMaxRetriedSessions

> **Description**: This counter shows the total number of permanently failed sessions.
>
> **Metric SpecName**: MAXRETRIEDSESSIONS
>
> **Metric Field Name**: UDC - Max Retried Sessions
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Metric: UDCProcessingFailedSessions

Description: This counter shows the total number of processing failed sessions.

Metric SpecName: PROCFAILEDSESSIONS

Metric Field Name: UDC - Processing Failed Sessions

Data type: UINT32

Alarm: FALSE

Metric: UDCSendEmailLatency

Description: the latency of sending an email.

Metric SpecName: SENDEMAILLATENCY

Metric Field Name: UDC - Send Email latency (ms)

Data type: UINT32

Alarm: FALSE

ChkEdgeReplicaReplicatorServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SERVSTAT

Source / Collection Definition: SERVICECHECK / REPLICA

Metric: EdgeREPLICAServName

Description: Name of the Service

Metric SpecName: SERVNAME

Metric Field Name: Service_Name

Data type: TEXT

Alarm: FALSE

Metric: EdgeREPLICAServDisplayName

Description: Display Name of the Service

Metric SpecName: SRVDISPNAME

Metric Field Name: Service_Displayname

Data type: TEXT

Alarm: FALSE

Metric: EdgeREPLICAServStatus

Description: Status of the Service

Metric SpecName: SERVSTATUS

Metric Field Name: Service_Status

Data type: TEXT

Alarm: FALSE

Metric: EdgeREPLICAServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_EdgeREPLICAServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): Lync Server Replica Replicator Agent' Windows Service is stopped.

Potential Impact: NA

Suggested Action(s): Lync Server Replica Replicator Agent' Windows Service is stopped. Please restart the service.

MediationOutbound

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: SKYPE / MEDIATIONOUTBOUND

Source / Collection Definition: PERFMON / LS:MediationServer - Outbound Calls(*)

Metric: OutboundCurrent

Description: This metric captures Current number of outbound calls

Metric SpecName: OutboundCurrent

Metric Field Name: - Current

Data type: UINT32

Alarm: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: TotalAttemptsoOutBound

Description: This metric captures Total Attempts at outbound calls

Metric SpecName: TotalAttemptOutBound

Metric Field Name: - Total Attempts

Data type: UINT32

Alarm: FALSE

Metric: TotalEstablishedOutBound

Description: This metric captures Total Established outbound calls

Metric SpecName: TotlEstablishOutBond

Metric Field Name: - Total Established

Data type: UINT32

Alarm: FALSE

Metric: TotalRejectedDueToLoadOT

Description: This metric captures Total Rejected outbound calls Due To Load

Metric SpecName: TotlRejecteDueLoadOT

Metric Field Name: - Total Rejected Due To Load

Data type: UINT32

Alarm: FALSE

Metric: OutboundCurrent

Description: This metric captures Current number of outbound calls

Metric SpecName: OutboundCurrent

Metric Field Name: - 000 - Current

Data type: UINT32

Alarm: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: TotalAttemptsoOutBound

Description: This metric captures Total Attempts at outbound calls

Metric SpecName: TotalAttemptOutBound

Metric Field Name: - 002 - Total attempts

Data type: UINT32

Alarm: FALSE

Metric: TotalEstablishedOutBound

Description: This metric captures Total Established outbound calls

Metric SpecName: TotlEstablishOutBond

Metric Field Name: - 001 - Total established

Data type: UINT32

Alarm: FALSE

Metric: TotalRejectedDueToLoadOT

Description: This metric captures Total Rejected outbound calls Due To Load

Metric SpecName: TotlRejecteDueLoadOT

Metric Field Name: - 003 - Total rejected due to load

Data type: UINT32

Alarm: FALSE

Metric: OutboundCurrent

Description: This metric captures Current number of outbound calls

Metric SpecName: OutboundCurrent

Metric Field Name: - Current

Data type: UINT32

Alarm: FALSE

Metric: TotalAttemptsoOutBound

Description: This metric captures Total Attempts at outbound calls

Metric SpecName: TotalAttemptOutBound

Metric Field Name: - Total Attempts

Data type: UINT32

Alarm: FALSE

Metric: TotalEstablishedOutBound

Description: This metric captures Total Established outbound calls

Metric SpecName: TotlEstablishOutBond

Metric Field Name: - Total Established

Data type: UINT32

Alarm: FALSE

Metric: TotalRejectedDueToLoadOT

Description: This metric captures Total Rejected outbound calls Due To Load

Metric SpecName: TotlRejecteDueLoadOT

Metric Field Name: - Total Rejected Due To Load

Data type: UINT32

Alarm: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

ChkFrontEndOnlineProvisioningServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SERVSTAT

Source / Collection Definition: SERVICECHECK / RtcProv

Metric: FERtcProvServName

> **Description**: Name of the Service
>
> **Metric SpecName**: SERVNAME
>
> **Metric Field Name**: Service_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FERtcProvServDisplayName

> **Description**: Display Name of the Service
>
> **Metric SpecName**: SRVDISPNAME
>
> **Metric Field Name**: Service_Displayname
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FERtcProvServStatus

> **Description**: Status of the Service
>
> **Metric SpecName**: SERVSTATUS
>
> **Metric Field Name**: Service_Status
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FERtcProvServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_FERtcProvServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): Lync Online Provisioning Service' Windows Service is stopped.

Potential Impact: NA

Suggested Action(s): Lync Online Provisioning Service' Windows Service is stopped. Please restart the service.

Collect_Director_Distribution_List_Expansion

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / DIRLSWEBDISTRLISTEXP

Source / Collection Definition: PERFMON / LS:WEB - Distribution List Expansion(*)

Metric: DirectorDistributionListExpansionInstance

Description: instance of perfmon object LS:WEB - Distribution List Expansion

Metric SpecName: DISTRLSTEXPANSION

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: DirectorSuccessRequestProcTime

Description: Average processing time for a successful request to be completed

Metric SpecName: DIRSUCREQPROCTIME

Metric Field Name: WEB - Successful Request Processing Time

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 3000, Major / 5000

Policy: MSBS_DirectorSuccessRequestProcTime

Message text: The value of WEB - Successful Request Processing Time for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Issues with Active Directory performance

Potential Impact: NA

Suggested Action(s): Verify CPU load on active directory machines.

Metric: DirectorSoapExceptionPerSecond

Description: the per-second rate of Soap Exceptions

Metric SpecName: DIRSOAPEXCEPT

Metric Field Name: WEB - Soap exceptions/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 3, Major / 6

Policy: MSBS_DirectorSoapExceptionPerSecond

Message text: The value of WEB - Soap exceptions/sec for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Soap Exceptions.

Potential Impact: NA

Suggested Action(s): This is an internal error.

Collect_FrontEnd_LoadMgmtLogging

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / CS_FELOADMGMT

Source / Collection Definition: PERFMON / LS:SIP - Load Management(*)

Metric: SIPLoaManagementInstance

> **Description**: instance of perfmon object LS:SIP - Load Management
>
> **Metric SpecName**: SIPLOADMGMTINST
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: SIPLoadMgmtAvgHoldTimeForInMessagesLogging

> **Description**: the average time that the server held the incoming messages currently being processed.
>
> **Metric SpecName**: HOLDINGTIMEFORINCMSG
>
> **Metric Field Name**: SIP - Average Holding Time For Incoming Messages
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

ChkFrontEndAudioTestServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / SERVSTAT

Source / Collection Definition: SERVICECHECK / RTCATS

Metric: FERTCATSServName

Description: Name of the Service

Metric SpecName: SERVNAME

Metric Field Name: Service_Name

Data type: TEXT

Alarm: FALSE

Metric: FERTCATSSServDisplayName

Description: Display Name of the Service

Metric SpecName: SRVDISPNAME

Metric Field Name: Service_Displayname

Data type: TEXT

Alarm: FALSE

Metric: FERTCATSSServStatus

Description: Status of the Service

Metric SpecName: SERVSTATUS

Metric Field Name: Service_Status

Data type: TEXT

Alarm: FALSE

Metric: FERTCATSSServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_FERTCATSServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): #N/A!

Potential Impact: NA

Suggested Action(s): #N/A!

ChkMonitoringCallDetailRecordingServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / NA

Source / Collection Definition: SERVICECHECK / RTCCDR

Metric: MonitoringRTCCDRServname

Description: Name of the Service

Metric SpecName: SERVNAME

Metric Field Name: Service_Name

Data type: TEXT

Alarm: FALSE

Metric: MonitoringRTCCDRDisplayName

Description: Display Name of the Service

Metric SpecName: SRVDISPNAME

Metric Field Name: Service_Displayname

Data type: TEXT

Alarm: FALSE

Metric: MonitoringRTCCDRServStatus

Description: Status of the Service

Metric SpecName: SERVSTATUS

Metric Field Name: Service_Status

Data type: TEXT

Alarm: FALSE

Metric: MonitoringRTCCDRServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_MonitoringRTCCDRServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

Collect_FrontEnd_Web_Mobile_Comm_Service

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / LSWEBMOBCOMM

Source / Collection Definition: PERFMON / LS:WEB - Mobile Communication Service(*)

Metric: MobileCommServiceInstance

> **Description**: instance of perfmon object LS:WEB - Mobile Communication Service
>
> **Metric SpecName**: MOBCOMMINST
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: CurrActiveSessionCountWithActivePresenceSubscr

> **Description**: the number of currently active sessions with active presence subscriptions
>
> **Metric SpecName**: FECURRENTACTSESCNT
>
> **Metric Field Name**: WEB - Currently Active Session Count With Active Presence Subscriptions
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

SimplePortWatcher5082

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / Port5082

Source / Collection Definition: PORTCOL / PORTCHECKER

Metric: SimpleWatcherPort5082

Description: Used for outgoing SIP requests from the Mediation Server to the PSTN gateway.

Metric SpecName: SimpleWatcherPort5082

Metric Field Name: SimpleWatcherPort5082

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort5082

Message text: The Port No:5082 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

Metric: SimpleWatcherPort5082

Description: Used for outgoing SIP requests from the Mediation Server to the PSTN gateway.

Metric SpecName: SimpleWatcherPort5082

Metric Field Name: SimpleWatcherPort5082

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort5082

Message text: The Port No:5082 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

> **Description**: This is the key for metric
>
> **Metric SpecName**: HOSTNAME
>
> **Metric Field Name**: HOSTNAME
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

PoorStreamsBtwnMSAndAVMCUPercentage

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / STRBTWNMSANDAVMCU

Source / Collection Definition: SQLDB / select (SELECT SERVERPROPERTY ('MACHINENAME')) AS 'ServerName', isnull((100 * (select SUM(case when (PacketLossRate > .01 OR PacketLossRateMax > .05) THEN 1 ELSE null END) as 'PoorCalls' FROM [Session] s WITH (NOLOCK) INNER JOIN [MediaLine] AS m WITH (NOLOCK) ON m.ConferenceDateTime = s.ConferenceDateTime AND m.SessionSeq = s.SessionSeq INNER JOIN [AudioStream] AS a WITH (NOLOCK) ON a.MediaLineLabel = m.MediaLineLabel and a.ConferenceDateTime = m.ConferenceDateTime and a.SessionSeq = m.SessionSeq INNER JOIN [UserAgent] AS CallerUA WITH (NOLOCK) ON CallerUA.UserAgentKey = s.CallerUserAgent INNER JOIN [UserAgent] AS CalleeUA WITH (NOLOCK) ON CalleeUA.UserAgentKey = s.CalleeUserAgent WHERE m.CallerInside = 1 AND m.CalleeInside = 1 and s.StartTime >= (dateadd (MINUTE,@Duration,GETUTCDATE())) AND s.StartTime (dateadd(MINUTE,0,GETUTCDATE())) and CallerUA.UAType in (1, 2) and CalleeUA.UAType in (1, 2) and ((CallerUA.UAType in (2) and CalleeUA.UAType in (1)) or (CallerUA.UAType in (1) and CalleeUA.UAType in (2))))) / ((select SUM (CASE WHEN s.ConferenceDateTime is not null THEN 1 ELSE null END) FROM [Session] s WITH (NOLOCK) INNER JOIN [MediaLine] AS m WITH (NOLOCK) ON m.ConferenceDateTime = s.ConferenceDateTime AND m.SessionSeq = s.SessionSeq INNER JOIN [AudioStream] AS a WITH (NOLOCK) ON a.MediaLineLabel = m.MediaLineLabel and a.ConferenceDateTime = m.ConferenceDateTime and a.SessionSeq = m.SessionSeq INNER JOIN [UserAgent] AS CallerUA

WITH (NOLOCK) ON CallerUA.UserAgentKey = s.CallerUserAgent INNER JOIN [UserAgent] AS CalleeUA WITH (NOLOCK) ON CalleeUA.UserAgentKey = s.CalleeUserAgent WHERE m.CallerInside = 1 AND m.CalleeInside = 1 and s.StartTime >= (dateadd (MINUTE,@Duration,GETUTCDATE())) AND s.StartTime (dateadd(MINUTE,0,GETUTCDATE())) and CallerUA.UAType in (1, 2) and CalleeUA.UAType in (1, 2) and ((CallerUA.UAType in (2) and CalleeUA.UAType in (1)) or (CallerUA.UAType in (1) and CalleeUA.UAType in (2)))),0) as 'PoorStreamsBtwnMSAndAVMCUPercentage'

Metric: PoorStreamsBtwnMSAndAVMCUPercentage

> **Description**: This metric captures Poor Streams between Mediation Server and Audio-Video Conferencing Unit and calculates percentage for a given interval At the end of each call, parameters that determine Quality of a call that include network, audio and video parameters are logged into QoE database of Lync Server. Each call is categorized as having Acceptable quality or Poor quality based on the same.
>
> **Metric SpecName**: PoorStrBtwMSAndAVMCU
>
> **Metric Field Name**: PoorStreamsBtwnMSAndAVMCUPercentage
>
> **Data type**: REAL64
>
> **Alarm**: TRUE
>
> **Category** : MSSkype
>
> **Severity / Threshold** : Warning / 40, Major / 70, Warning / 40, Major / 70
>
> **Policy**: MSBS_PoorStreamsBtwnMSAndAVMCUPercentage
>
> **Message text**: The Percentage of Poor Streams between Mediation Server and Audio-Video Conferencing Unit is <VALUE> which exceeds the threshold of <THRESHOLD>
>
> **Instructional Text**:
>
> **Probable Cause(s)**: The reason would be an overloaded server
>
> **Potential Impact**: Poor Streams between Mediation Server and Audio-Video Conferencing Unit
>
> **Suggested Action(s)**: Ramp up server

Metric: ServerName

Description: This is the key for metric

Metric SpecName: ServerName

Metric Field Name: ServerName

Data type: TEXT

Alarm: FALSE

Metric: PoorStreamsBtwnMSAndAVMCUPercentage

Description: This metric captures Poor Streams between Mediation Server and Audio-Video Conferencing Unit and calculates percentage for a given interval At the end of each call, parameters that determine Quality of a call that include network, audio and video parameters are logged into QoE database of Lync Server. Each call is categorized as having Acceptable quality or Poor quality based on the same.

Metric SpecName: PoorStrBtwMSAndAVMCU

Metric Field Name: PoorStreamsBtwnMSAndAVMCUPercentage

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 40, Major / 70, Warning / 40, Major / 70

Policy: MSBS_PoorStreamsBtwnMSAndAVMCUPercentage

Message text: The Percentage of Poor Streams between Mediation Server and Audio-Video Conferencing Unit is <VALUE> which exceeds the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): The reason would be an overloaded server

Potential Impact: Poor Streams between Mediation Server and Audio-Video Conferencing Unit

Suggested Action(s): Ramp up server

Metric: ServerName

> **Description**: This is the key for metric
>
> **Metric SpecName**: ServerName
>
> **Metric Field Name**: ServerName
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Collect_FrontEnd_LegalIntercept

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / LSLEGALINTERCEPT

Source / Collection Definition: PERFMON / LS:LegalIntercept - LegalIntercept(*)

Metric: LegalInterceptInstanceName

> **Description**: instance of perfmon object LS:LegalIntercept - LegalIntercept
>
> **Metric SpecName**: LEGALINTERCEPTINST
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: ConferenceMessageQueryLatency

Description: Get Conferencing Messages' Latency

Metric SpecName: CONFMSGQRYLATENCY

Metric Field Name: - Conference Message Query latency (ms)

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 10000, Major / 30000

Policy: MSBS_ConferenceMessageQueryLatency

Message text: The value of Conference Message Query latency (ms) for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Database query took long time

Potential Impact: NA

Suggested Action(s): Verify that the database (i.e. lcslog) is available.

Metric: GetNextPageLatency

Description: GetNextPage' Latency

Metric SpecName: GETNXTPAGELATENCY

Metric Field Name: - GetNextPage latency (ms)

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 10000, Major / 30000

Policy: MSBS_GetNextPageLatency

Message text: The value of GetNextPage latency (ms) for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Active directory query took long time.

Potential Impact: NA

Suggested Action(s): Verify that Active Directory is accessible.

Metric: MaxRetryCount

Description: Reached Max Retry Count

Metric SpecName: MAXRETRYCOUNT

Metric Field Name: - Max Retry Count

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 1, Major / 2

Policy: MSBS_MaxRetryCount

Message text: The value of Max Retry Count for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Email Server is not configured correctly or email is not valid.

Potential Impact: NA

Suggested Action(s): Verify the email relay system is configured correctly and email address is correct.

Metric: ProcessingFailedSessions

Description: Archived Session Processing' Failures

Metric SpecName: LEGPROCFAILSESSIONS

Metric Field Name: - Processing Failed Sessions

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 1, Major / 2

Policy: MSBS_ProcessingFailedSessions

Message text: The value of Processing Failed Sessions for instance <OPTION(InstanceName)
> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Processing message failed

Potential Impact: NA

Suggested Action(s): Verify the integrity of data in the database.

Metric: SendingFailedEmails

Description: Send Email' Failures

Metric SpecName: FAILEDSENDINGEMAILS

Metric Field Name: - Sending Failed Emails

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 1, Major / 2

Policy: MSBS_SendingFailedEmails

Message text: The value of Sending Failed Emails for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Failed to send email

Potential Impact: NA

Suggested Action(s): Verify the email relay system is configured correctly.

Metric: PurgingFailedSessions

Description: Update Sessions Purgeable' Failures

Metric SpecName: FAILEDPURGESESSIONS

Metric Field Name: - Purging Failed Sessions

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 1, Major / 2

Policy: MSBS_PurgingFailedSessions

Message text: The value of Purging Failed Sessions for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Cannot update sessions as purgeable.

Potential Impact: NA

Suggested Action(s): Verify that the data is valid and that the database is available.

Metric: LegalInterceptUnexpectedExceptions

Description: Unexpected failures

Metric SpecName: UNEXPECTEDEXCEPT

Metric Field Name: - Unexpected Exceptions

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 1, Major / 2

Policy: MSBS_LegalInterceptUnexpectedExceptions

Message text: The value ofUnexpected Exceptions for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Unexpected exception.

Potential Impact: NA

Suggested Action(s): Notify your organization's support team with the event detail.

Metric: P2PMessageQueryLatency

Description: Get P2P Messages' Latency

Metric SpecName: P2PMSGQRYLATENCY

Metric Field Name: - P2P Message Query latency (ms)

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 10000, Major / 30000

Policy: MSBS_P2PMessageQueryLatency

Message text: The value of P2P Message Query latency (ms) for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Database query took long time.

Potential Impact: NA

Suggested Action(s): Verify that the database (i.e. lcslog) is available.

Metric: UpdatingRecordsPurgeableLatency

Description: Update Sessions Purgeable' Latency

Metric SpecName: UPDTRECPURGELATENCY

Metric Field Name: - Updating records Purgeable latency (ms)

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 10000, Major / 30000

Policy: MSBS_UpdatingRecordsPurgeableLatency

Message text: The value of Updating records Purgeable latency (ms)for instance <OPTION (InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Database update took long time.

Potential Impact: NA

Suggested Action(s): Verify that the database (i.e. lcslog) is available.

Metric: SenEmailLatency

Description: Send Email' Latency

Metric SpecName: SENDMAILLATENCY

Metric Field Name: - send Email latency (ms)

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 10000, Major / 30000

Policy: MSBS_SenEmailLatency

Message text: The value of send Email latency (ms) for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Sending an email took long time.

Potential Impact: NA

Suggested Action(s): Verify the email relay system is configured correctly.

RGSResponseGroup

This policy maintains the information about the status for the different services

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_ConferenceProcPerform_2010_Conf

Aspect: Skype Conference Processing Performance

CIT: Mediation Server, Front End Server, Edge Server

Data source / Data class: SKYPE / RGSRESPONSEGROUP

Source / Collection Definition: PERFMON / LS:RGS - 01 - Response Group Service Call Control(*)

Metric: TotalNumOfIncomingCallsDeclinedBecauseOfHighNumOfActiveCall

Description: This metric captures Total Number Of Incoming Calls Declined Because Of High Number Of Active Calls

Metric SpecName: TtlNumInCalDecHgNumA

Metric Field Name: RGS - 006 - Total number of incoming calls declined because of high number of active calls

Data type: UINT32

Alarm: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: TotalNumberOfIncomingCallsDeclinedBecauseOfMemoryPressure

Description: This metric captures Total Number Of Incoming Calls Declined Because Of Memory Pressure

Metric SpecName: TtlNumInCalDecMemPrs

Metric Field Name: RGS - 004 - Total number of incoming calls declined because of memory pressure

Data type: UINT32

Alarm: FALSE

Metric: TotalNumOfIncomingCallsDeclinedBecauseOfHighNumOfActiveCall

Description: This metric captures Total Number Of Incoming Calls Declined Because Of High Number Of Active Calls

Metric SpecName: TtlNumInCalDecHgNumA

Metric Field Name: RGS - Total Number Of Incoming Calls Declined Because Of High Number Of Active Calls

Data type: UINT32

Alarm: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: TotalNumberOfIncomingCallsDeclinedBecauseOfMemoryPressure

Description: This metric captures Total Number Of Incoming Calls Declined Because Of Memory Pressure

Metric SpecName: TtlNumInCalDecMemPrs

Metric Field Name: RGS - Total Number Of Incoming Calls Declined Because Of Memory Pressure

Data type: UINT32

Alarm: FALSE

IMMcuConference

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: SKYPE / IMMCUCONFERENCE

Source / Collection Definition: PERFMON / LS:ImMcu - 00 - IMMcu Conferences(*)

Metric: ActiveConferences

> **Description**: This metric captures Active Conferences
>
> **Metric SpecName**: ActiveConferencesM
>
> **Metric Field Name**: IMMCU - 000 - Active Conferences
>
> **Data type**: REAL64
>
> **Alarm**: FALSE

Metric: Instance_Name

> **Description**: This is the key for metric
>
> **Metric SpecName**: Instance_Name
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: ConnectedUsers

> **Description**: This metric captures Connected Users
>
> **Metric SpecName**: ConnectedUsers
>
> **Metric Field Name**: IMMCU - 001 - Connected Users
>
> **Data type**: REAL64
>
> **Alarm**: FALSE

Metric: ActiveConferences

Description: This metric captures Active Conferences

Metric SpecName: ActiveConferencesM

Metric Field Name: IMMCU - Active Conferences

Data type: REAL64

Alarm: FALSE

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: ConnectedUsers

Description: This metric captures Connected Users

Metric SpecName: ConnectedUsers

Metric Field Name: IMMCU - Connected Users

Data type: REAL64

Alarm: FALSE

ExternalPoorStreamsPercentage

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / QOEEXTERNALPOORSTR

Source / Collection Definition: SQLDB / select (SELECT SERVERPROPERTY ('MACHINENAME')) as 'SERVERNAME', isnull((100 * (select SUM(CASE WHEN PacketLossRate > .01 OR PacketLossRateMax > .05 THEN 1 ELSE null END) as 'PoorCalls' FROM [Session] s WITH (NOLOCK) INNER JOIN [MediaLine] AS m WITH (NOLOCK) ON m.ConferenceDateTime = s.ConferenceDateTime AND m.SessionSeq = s.SessionSeq INNER JOIN [AudioStream] AS a WITH (NOLOCK) ON a.MediaLineLabel = m.MediaLineLabel and a.ConferenceDateTime = m.ConferenceDateTime and a.SessionSeq = m.SessionSeq INNER JOIN [UserAgent] AS CallerUA WITH (NOLOCK) ON CallerUA.UserAgentKey = s.CallerUserAgent INNER JOIN [UserAgent] AS CalleeUA WITH (NOLOCK) ON CalleeUA.UserAgentKey = s.CalleeUserAgent WHERE s.StartTime >= (dateadd(MINUTE,@Duration,GETUTCDATE())) AND s.StartTime (dateadd (MINUTE,0,GETUTCDATE())) and ((CallerUA.UAType in (4,8,16,64,128,16398,16399,16400,16401,16402,16403,16405,16411) and m.CallerInside=0) or (CalleeUA.UAType in (4,8,16,64,128,16398,16399,16400,16401,16402,16403,16405,16411) and m.CalleeInside=0)))) / ((select SUM(CASE WHEN s.ConferenceDateTime is not null THEN 1 ELSE null END) FROM [Session] s WITH (NOLOCK) INNER JOIN [MediaLine] AS m WITH (NOLOCK) ON m.ConferenceDateTime = s.ConferenceDateTime AND m.SessionSeq = s.SessionSeq INNER JOIN [AudioStream] AS a WITH (NOLOCK) ON a.MediaLineLabel = m.MediaLineLabel and a.ConferenceDateTime = m.ConferenceDateTime and a.SessionSeq = m.SessionSeq INNER JOIN [UserAgent] AS CallerUA WITH (NOLOCK) ON CallerUA.UserAgentKey = s.CallerUserAgent INNER JOIN [UserAgent] AS CalleeUA WITH (NOLOCK) ON CalleeUA.UserAgentKey = s.CalleeUserAgent WHERE s.StartTime >= (dateadd(MINUTE,@Duration,GETUTCDATE())) AND s.StartTime (dateadd(MINUTE,0,GETUTCDATE())) and ((CallerUA.UAType in (4,8,16,64,128,16398,16399,16400,16401,16402,16403,16405,16411) and m.CallerInside=0) or (CalleeUA.UAType in (4,8,16,64,128,16398,16399,16400,16401,16402,16403,16405,16411) and m.CalleeInside=0))),0) as 'ExternalPoorStreamsPercentage'

Metric: ExternalPoorStreamsPercentage

Description: This metric captures Poor Streams between External users talking to internal or external end-points and calculates percentage for a given interval At the end of each call, parameters that determine Quality of a call that include network, audio and video parameters are logged into QoE database of Lync Server. Each call is categorized as having Acceptable quality or Poor quality based on the same.

Metric SpecName: ExternalPoorStrPer

Metric Field Name: ExternalPoorStreamsPercentage

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 40, Major / 70, Warning / 40, Major / 70

Policy: MSBS_ExternalPoorStreamsPercentage

Message text: The Percentage of Poor Streams between External users talking to internal or external end-points is <VALUE> which exceeds the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): This may be caused due to an overloaded Edge Server, external network congestion etc.

Potential Impact: Poor Call quality with external clients

Suggested Action(s): Ramp up Edge Server, configure external gateway, check external network bandwidth

Metric: ServerName

Description: This is the key for metric

Metric SpecName: ServerName

Metric Field Name: ServerName

Data type: TEXT

Alarm: FALSE

Metric: ExternalPoorStreamsPercentage

Description: This metric captures Poor Streams between External users talking to internal or external end-points and calculates percentage for a given interval At the end of each call, parameters that determine Quality of a call that include network, audio and video parameters are logged into QoE database of Lync Server. Each call is categorized as having Acceptable quality or Poor quality based on the same.

Metric SpecName: ExternalPoorStrPer

Metric Field Name: ExternalPoorStreamsPercentage

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 40, Major / 70, Warning / 40, Major / 70

Policy: MSBS_ExternalPoorStreamsPercentage

Message text: The Percentage of Poor Streams between External users talking to internal or external end-points is <VALUE> which exceeds the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): This may be caused due to an overloaded Edge Server, external network congestion etc.

Potential Impact: Poor Call quality with external clients

Suggested Action(s): Ramp up Edge Server, configure external gateway, check external network bandwidth

Metric: ServerName

Description: This is the key for metric

Metric SpecName: ServerName

Metric Field Name: ServerName

Data type: TEXT

Alarm: FALSE

ChkFrontEndReplicaReplicatorServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SERVSTAT

Source / Collection Definition: SERVICECHECK / REPLICA

Metric: FEREPLICAServName

> **Description**: Name of the Service
>
> **Metric SpecName**: SERVNAME
>
> **Metric Field Name**: Service_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FEREPLICAServDisplayName

> **Description**: Display Name of the Service
>
> **Metric SpecName**: SRVDISPNAME
>
> **Metric Field Name**: Service_Displayname
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FEREPLICAServStatus

Description: Status of the Service

Metric SpecName: SERVSTATUS

Metric Field Name: Service_Status

Data type: TEXT

Alarm: FALSE

Metric: FEREPLICAServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_FEREPLICAServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): Lync Server Replica Replicator Agent' Windows Service is stopped.

Potential Impact: NA

Suggested Action(s): Lync Server Replica Replicator Agent' Windows Service is stopped.
Please restart the service.

Metric: REPLICAServName

Description: Name of the Service

Metric SpecName: SERVNAME

Metric Field Name: Service_Name

Data type: TEXT

Alarm: FALSE

Metric: REPLICAServDisplayName

Description: Display Name of the Service

Metric SpecName: SRVDISPNAME

Metric Field Name: Service_Displayname

Data type: TEXT

Alarm: FALSE

Metric: REPLICASErvStatus

Description: Status of the Service

Metric SpecName: SERVSTATUS

Metric Field Name: Service_Status

Data type: TEXT

Alarm: FALSE

Metric: REPLICASErvState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_REPLICASErvState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): Lync Server Replica Replicator Agent' Windows Service is stopped.

Potential Impact: NA

Suggested Action(s): Lync Server Replica Replicator Agent' Windows Service is stopped.
Please restart the service.

VideoJitterPoorCallsPercentage

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / VIDEOJITTERPOORCALLS

Source / Collection Definition: SQLDB / select isnull(cast(100.0 * cast((SUM(CASE WHEN [VideoJitterInterArrival] > [JitterInterArrivalOptimal] THEN 1 ELSE 0 END)) as float) / cast((SUM (CASE WHEN MediaLineLabel is NOT NULL THEN 1 ELSE 0 END)) as float) as decimal(4, 1)),0) as VideoJitterPoorCallsPercentage,SERVERPROPERTY('MACHINENAME') AS 'ServerName' from [QoEMetrics].[dbo].[QoEReportsCallDetailView] Where MediaLineLabel IN (1,2) AND ConferenceDateTime >= dateadd(MINUTE,@Duration,GETUTCDATE())

Metric: VideoJitterPoorCallsPercentage

Description: This metric captures Poor Video that have Jitter more than a set threshold value and calculates percentage of poor calls for a given interval At the end of each call, parameters that determine Quality of a call that include network, audio and video parameters are logged into QoE database of Lync Server. Each call is categorized as having Acceptable quality or Poor quality based on the same.

Metric SpecName: VidJitterPoorCallPer

Metric Field Name: VideoJitterPoorCallsPercentage

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 40, Major / 70, Warning / 40, Major / 70

Policy: MSBS_VideoJitterPoorCallsPercentage

Message text: The current value of Percentage Video Jitter Poor Calls is <VALUE> which exceeds the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Variation in the delay time of packets arriving at their destination. Video packets are sent at regular intervals from the sender to the receiver, but because of network latency the interval between packets can vary at the destination. Caused by LAN Congestion or issue with device/device drivers, video rendering

Potential Impact: This variation can affect media quality. Jitter is used to determine MOSs as well as in the call detail report. -Delay due to jitter buffering -Distorted Video

Suggested Action(s): Use Jitter buffers in Packet Switched Networks Network Upgrade

Metric: ServerName

Description: This is the key for metric

Metric SpecName: ServerName

Metric Field Name: ServerName

Data type: TEXT

Alarm: FALSE

Metric: VideoJitterPoorCallsPercentage

Description: This metric captures Poor Video that have Jitter more than a set threshold value and calculates percentage of poor calls for a given interval At the end of each call, parameters that determine Quality of a call that include network, audio and video parameters are logged into QoE database of Lync Server. Each call is categorized as having Acceptable quality or Poor quality based on the same.

Metric SpecName: VidJitterPoorCallPer

Metric Field Name: VideoJitterPoorCallsPercentage

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 40, Major / 70, Warning / 40, Major / 70

Policy: MSBS_VideoJitterPoorCallsPercentage

Message text: The current value of Percentage Video Jitter Poor Calls is <VALUE> which exceeds the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Variation in the delay time of packets arriving at their destination. Video packets are sent at regular intervals from the sender to the receiver, but because of network latency the interval between packets can vary at the destination. Caused by LAN Congestion or issue with device/device drivers, video rendering

Potential Impact: This variation can affect media quality. Jitter is used to determine MOSs as well as in the call detail report. -Delay due to jitter buffering -Distorted Video

Suggested Action(s): Use Jitter buffers in Packet Switched Networks Network Upgrade

Metric: ServerName

Description: This is the key for metric

Metric SpecName: ServerName

Metric Field Name: ServerName

Data type: TEXT

Alarm: FALSE

ChkFrontEndServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / SERVSTAT

Source / Collection Definition: SERVICECHECK / RTCSrv

Metric: FERTCSrvServName

> **Description**: Name of the Service
>
> **Metric SpecName**: SERVNAME
>
> **Metric Field Name**: Service_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FERTCSrvServDisplayName

> **Description**: Display Name of the Service
>
> **Metric SpecName**: SRVDISPNAME
>
> **Metric Field Name**: Service_Displayname
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FERTCSrvServStatus

Description: Status of the Service

Metric SpecName: SERVSTATUS

Metric Field Name: Service_Status

Data type: TEXT

Alarm: FALSE

Metric: FERTCSrvServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_FERTCSrvServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

PoolConfStatistics

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / POOLCONFSTATISTICS

Source / Collection Definition: PERFMON / LS:USrv - Pool Conference Statistics(*)

Metric: ActiveConferenceCount

> **Description**: This metric captures Active Conference Count
>
> **Metric SpecName**: ActiveConferenceCnt
>
> **Metric Field Name**: USrv - Active Conference Count
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Metric: Instance_Name

> **Description**: This is the key for metric
>
> **Metric SpecName**: Instance_Name
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: ActiveFocusEndpointCount

> **Description**: This metric captures Active Focus Endpoint Count
>
> **Metric SpecName**: ActFocusEndpointCnt
>
> **Metric Field Name**: USrv - Active Focus Endpoint Count
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Metric: ActiveMcuSessionCount

> **Description**: This metric captures Active Mcu Session Count
>
> **Metric SpecName**: ActiveMcuSessionCnt
>
> **Metric Field Name**: USrv - Active Mcu Session Count
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Metric: ActiveParticipantCount

> **Description**: This metric captures Active Participant Count
>
> **Metric SpecName**: ActParticipantCnt
>
> **Metric Field Name**: USrv - Active Participant Count
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Metric: ConferenceCount

> **Description**: This metric captures Conference Count
>
> **Metric SpecName**: ConferenceCount
>
> **Metric Field Name**: USrv - Conference Count
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

AudioFailurePercentage

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / AUDIOFAILURE

Source / Collection Definition: SQLDB / select isnull(cast(100.0 * cast((SUM(CASE WHEN SD.ResponseCode != 200 THEN 1 ELSE 0 END)) as float) / cast((SUM(CASE WHEN SD.ResponseCode is NOT NULL THEN 1 ELSE 0 END)) as float) as decimal(4, 1)),0) as AudioFailurePercentage,SERVERPROPERTY('MACHINENAME') AS 'ServerName' from [LcsCDR].[dbo].SessionDetails SD LEFT OUTER JOIN [LcsCDR].[dbo].Media M ON SD.SessionIdTime = M.SessionIdTime LEFT OUTER JOIN [LcsCDR].[dbo].MediaList ML ON M.MediaId = ML.MediaId Where ML.MediaId = 5 AND SD.SessionIdTime >= dateadd(MINUTE,@Duration,GETUTCDATE())

Metric: AudioFailurePercentage

Description: This metric captures call failures periodically from the CDR database and raises an alert whenever call failures exceed the specified "threshold" percentage value. When an Audio call fails, this failure is reported to the Monitoring Server database (Call Detail Records database).

Metric SpecName: AudFailPer

Metric Field Name: AudioFailurePercentage

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 40, Major / 70, Warning / 40, Major / 70

Policy: MSBS_AudioFailurePercentage

Message text: The current value of Percentage Audio Failure is <VALUE> which exceeds the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): The causes are related to server errors which point out to source of error like Mediatation, Front-end etc Probable causes include server overload, unknown MIME type,timeout, policy violation, protocol errors etc

Potential Impact: Users face issue in connecting a P2P call or establishing a conference

Suggested Action(s): Ramping up server resources, checking health of servers and network, modifying policy Refer Response codes MS Diagnostic codes

Metric: ServerName

Description: This is the key for metric

Metric SpecName: ServerName

Metric Field Name: ServerName

Data type: TEXT

Alarm: FALSE

Metric: AudioFailurePercentage

Description: This metric captures call failures periodically from the CDR database and raises an alert whenever call failures exceed the specified "threshold" percentage value. When an Audio call fails, this failure is reported to the Monitoring Server database (Call Detail Records database).

Metric SpecName: AudFailPer

Metric Field Name: AudioFailurePercentage

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 40, Major / 70, Warning / 40, Major / 70

Policy: MSBS_AudioFailurePercentage

Message text: The current value of Percentage Audio Failure is <VALUE> which exceeds the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): The causes are related to server errors which point out to source of error like Mediatation, Front-end etc Probable causes include server overload, unknown MIME type,timeout, policy violation, protocol errors etc

Potential Impact: Users face issue in connecting a P2P call or establishing a conference

Suggested Action(s): Ramping up server resources, checking health of servers and network, modifying policy Refer Response codes MS Diagnostic codes

Metric: ServerName

Description: This is the key for metric

Metric SpecName: ServerName

Metric Field Name: ServerName

Data type: TEXT

Alarm: FALSE

Collect_LogicalDisk_Director

This Policy monitors the logical disk feature of Microsoft Skype Business Server

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Logical_Disk_Conf

Aspect: Skype Logical Disk

CIT: Edge Server, Director Server, Mediation Server, Front End Server, Persistent Chat Server

Data source / Data class: LYNC / LOGICALDISK

Source / Collection Definition: PERFMON / LogicalDisk(*)

Metric: DirLogicalDiskInstance

> **Description**: instance of perfmon object LogicalDisk
>
> **Metric SpecName**: LGDISKINSTNAME
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: DirPercentageFreeSpace

Description: % Free Space is the percentage of total usable space on the selected logical disk drive that was free.

Metric SpecName: FREESPACE

Metric Field Name: % Free Space

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Warning / 70, Major / 90

Policy: MSBS_DirPercentageFreeSpace

Message text: The value of % Free Space for instance <OPTION(InstanceName)> is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): Database size grows indefinitely.

Potential Impact: NA

Suggested Action(s): Please check each disk drive and clean up unnecessary files.

SimplePortWatcher8060

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / Port8060

Source / Collection Definition: PORTCOL / PORTCHECKER

Metric: SimpleWatcherPort8060

Description: Used to listen for Persistent Shared Object Model (PSOM) connections from the Live Meeting client and previous versions of Lync Server.

Metric SpecName: SimpleWatcherPort8060

Metric Field Name: SimpleWatcherPort8060

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_SimpleWatcherPort8060

Message text: The Port No:8060 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

Metric: SimpleWatcherPort8060

Description: Used to listen for Persistent Shared Object Model (PSOM) connections from the Live Meeting client and previous versions of Lync Server.

Metric SpecName: SimpleWatcherPort8060

Metric Field Name: SimpleWatcherPort8060

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_SimpleWatcherPort8060

Message text: The Port No:8060 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

> **Description**: This is the key for metric
>
> **Metric SpecName**: HOSTNAME
>
> **Metric Field Name**: HOSTNAME
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Collect_Monitoring_CDR Service_WRITE

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / NA

Source / Collection Definition: PERFMON / LS:CDR Service - 02 - WRITE(*)

Metric: MonitoringCDRServiceWriteInstance

> **Description**: instance of perfmon object LS:CDR Service - 02 - WRITE
>
> **Metric SpecName**: MONCDRSERVCEWRITEINSTANCE
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: MonitoringMessagesfailedtobewrittentoDB

Description: number of messages that failed to get written to the SQL database.

Metric SpecName: MSGFAILDTOWRTNTODB

Metric Field Name: CDR Service - 002 - Messages failed to be written to DB

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 20

Policy: MSBS_MonitoringMessagesfailedtobewrittentoDB

Message text: The value of the counter 'CDR Service - 002 - Messages failed to be written to DB' value <VALUE> has crossed the threshold of <THRESHOLD> .

Instructional Text:

Probable Cause(s): NA

Potential Impact: NA

Suggested Action(s): NA

PhysicalDisk

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / KHIPHYSIDISK

Source / Collection Definition: PERFMON / PhysicalDisk(_Total)

Metric: AvgDisksecRead

Description: This policy monitors represents the average time of disk read latency.

Metric SpecName: AvgDisksRead

Metric Field Name: Avg. Disk sec/Read

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 0.025, Major / 0.025

Policy: MSBS_AvgDisksecRead

Message text: The current value of AvgDisksec/Read is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): This condition may be caused by any of the following conditions: Logic board or controller related problems. The hard drive interface speed can form a bottleneck to overall performance if it is too low for the hard disk's maximum sustained transfer rate. When available memory is low, the Virtual Memory Manager writes more pages to swap, resulting in increased disk activity.

Potential Impact: Upgrade or replace existing drive controllers with faster models. Confirm system has the maximum speed hard drive that it can support. Install separate drives on individual controller cards, spreading the read/write activities across multiple controllers, to increase overall performance.

Suggested Action(s): High Disc read latency

Metric: AvgDisksecWrite

Description: This policy monitors represents the average time of disk write latency.

Metric SpecName: AvgDisksWrite

Metric Field Name: Avg. Disk sec/Write

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 0.025, Major / 0.025

Policy: MSBS_AvgDisksecWrite

Message text: The current value of AvgDisksec/Write is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): This condition may be caused by any of the following conditions: Logic board or controller related problems. The hard drive interface speed can form a bottleneck to overall performance if it is too low for the hard disk's maximum sustained transfer rate. When available memory is low, the Virtual Memory Manager writes more pages to swap, resulting in increased disk activity.

Potential Impact: Upgrade or replace existing drive controllers with faster models. Confirm system has the maximum speed hard drive that it can support. Install separate drives on individual controller cards, spreading the read/write activities across multiple controllers, to increase overall performance.

Suggested Action(s): High Disc write latency

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: AvgDisksecRead

Description: This policy monitors represents the average time of disk read latency

Metric SpecName: AvgDisksRead

Metric Field Name: Avg. Disk sec/Read

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 0.025, Major / 0.025

Policy: MSBS_AvgDisksecRead

Message text: The current value of AvgDisksec/Read is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): This condition may be caused by any of the following conditions: Logic board or controller related problems. The hard drive interface speed can form a bottleneck to overall performance if it is too low for the hard disk's maximum sustained transfer rate. When available memory is low, the Virtual Memory Manager writes more pages to swap, resulting in increased disk activity.

Potential Impact: Upgrade or replace existing drive controllers with faster models. Confirm system has the maximum speed hard drive that it can support. Install separate drives on individual controller cards, spreading the read/write activities across multiple controllers, to increase overall performance.

Suggested Action(s): High Disc read latency

Metric: AvgDisksecWrite

Description: This policy monitors represents the average time of disk write latency

Metric SpecName: AvgDisksWrite

Metric Field Name: Avg. Disk sec/Write

Data type: REAL64

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 0.025, Major / 0.025

Policy: MSBS_AvgDisksecWrite

Message text: The current value of AvgDisksec/Write is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): This condition may be caused by any of the following conditions: Logic board or controller related problems. The hard drive interface speed can form a bottleneck to overall performance if it is too low for the hard disk's maximum sustained transfer rate. When available memory is low, the Virtual Memory Manager writes more pages to swap, resulting in increased disk activity.

Potential Impact: Upgrade or replace existing drive controllers with faster models. Confirm system has the maximum speed hard drive that it can support. Install separate drives on individual controller cards, spreading the read/write activities across multiple controllers, to increase overall performance.

Suggested Action(s): High Disc write latency

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Collect_FrontEnd_ASMCUHealthAndPerformance

This policy gives us the information about the Server Health

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Server_Health_Conf

Aspect: Skype Server Health

CIT: Mediation Server, AV Conferencing Server, Front End Server

Data source / Data class: LYNC / LSASMCU

Source / Collection Definition: PERFMON / LS:AsMcu - MCU Health And Performance(*)

Metric: ASMCUHealthInstance

> **Description**: instance of perfmon object LS:AsMcu - MCU Health And Performance
>
> **Metric SpecName**: MCUHEALTHINSTANCE
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: ASMCUHealthInstanceState

> **Description**: the current health of the MCU. 0 = Normal. 1 = Loaded. 2 = Full. 3 = Unavailable.
>
> **Metric SpecName**: MCUHEALTHSTATE
>
> **Metric Field Name**: ASMCU - MCU Health State
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

DataConferencing

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_LOW

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SYNDATACONFERENCING

Source / Collection Definition: POWERSHELL / Test-CsDataConference -TargetFQDN ${fqdn}

Metric: DataConferencing

Description: This metric gathers the information which confirms that users can participate in a data collaboration conference, an online meeting that includes activities such as whiteboards and polls. It will monitor the operation of data conferencing between two test users in a Lync pool. The following functions are tested: • Sign on to the Lync Server • Invitation and acceptance to conduct an data call • Conference creation and joining • Exchange of data • Conference termination •Log out

Metric SpecName: DataConferencing

Metric Field Name: DataConferencing

Data type: TEXT

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_DataConferencing

Message text: The Data Conferencing is down

Instructional Text:

Probable Cause(s): 1. User configuration not done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: Users would not be able to avail peer to peer services

Suggested Action(s): 1. Configuration : Most common issues are invalid or expired Test user password, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availability: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution error or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responds to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

Metric: ServerName

> **Description**: This is the key for metric
>
> **Metric SpecName**: ServerName
>
> **Metric Field Name**: ServerName
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: DataConferenceLatency

Description: This metric will capture latency in group data conference transaction

Metric SpecName: DataConfLat

Metric Field Name: DataConferenceLatency

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1000

Policy: MSBS_DataConferenceLatency

Message text: The value of Data Conference Latency is <VALUE> and has crossed the threshold of <THRESHOLD>

Instructional Text:

Probable Cause(s): 1. User configuration must not have done properly 2. Server/Component is not available 3. Infrastructure issues between Watcher node (where the ST executes) and the Front-end Pool. 4. Other component related errors

Potential Impact: New users cannot be registered

Suggested Action(s): 1. Configuration errors: Most common issues are: Test user password is invalid or expired, Test users have not been configured correctly for this Pool. Please refer Synthetic Transaction Internal Alerts View for more details 2. Component Availibility: Please ensure that you put Synthetic Transactions in maintenance mode before performing server/pool maintenance. To do this, use the Task LS Start Pool maintenance in the Pools view. 3. Infrastructure issues: Look at Alert Context tab for more details on the exact connectivity error such as DNS resolution errors or Connection Timeout. You can also get more details on Connectivity errors by looking at Port Check Alerts view. 4. Other component related errors: Look at Alert Context tab for more details on the component specific error. The specific Front-end server (within the load-balanced Front-end Pool) that responded to this execution of the synthetic transaction is listed in the Alert Context along with the Exception Message associated with the failure.

SimplePortWatcher881

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / Port881

Source / Collection Definition: PORTCOL / PORTCHECKER

Metric: SimpleWatcherPort881

Description: Persistent Chat Front End Server

Metric SpecName: SimpleWatcherPort881

Metric Field Name: SimpleWatcherPort881

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_SimpleWatcherPort881

Message text: The Port No:881 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

> **Description**: This is the key for metric
>
> **Metric SpecName**: HOSTNAME
>
> **Metric Field Name**: HOSTNAME
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

ChkFrontEndWebConferencingServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SERVSTAT

Source / Collection Definition: SERVICECHECK / RTCDATAMCU

Metric: FERTCDATAMCUServName

> **Description**: Name of the Service
>
> **Metric SpecName**: SERVNAME
>
> **Metric Field Name**: Service_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FERTCDATAMCUServDisplayName

Description: Display Name of the Service

Metric SpecName: SRVDISPNAME

Metric Field Name: Service_Displayname

Data type: TEXT

Alarm: FALSE

Metric: FERTCDATAMCUServStatus

Description: Status of the Service

Metric SpecName: SERVSTATUS

Metric Field Name: Service_Status

Data type: TEXT

Alarm: FALSE

Metric: FERTCDATAMCUServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_FERTCDATAMCUServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): Lync Server Web Conferencing' Windows Service is stopped.

Potential Impact: NA

Suggested Action(s): Lync Server Web Conferencing' Windows Service is stopped. Please restart the service.

Collect_FrontEnd_Mediation

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / LSPROCESSOR

Source / Collection Definition: PERFMON / Processor(_Total)

Metric: ProcesserInstance

> **Description**: instance of perfmon object Processor Total
>
> **Metric SpecName**: PROCESSORINST
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: SystemPercentProcessorTime

> **Description**: Percentage Processor Time is the percentage of elapsed time that all of process threads used the processor to execution instructions.
>
> **Metric SpecName**: SYSPCTPROCESSORTIME
>
> **Metric Field Name**: % Processor Time
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

ASP.NETApps

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / KHIASPNET

Source / Collection Definition: PERFMON / ASP.NET v4.0.30319(__Total__)

Metric: RequestsRejected

Description: This policy monitors the number of requests rejected because the request queue was full.

Metric SpecName: RequestsRejected

Metric Field Name: Requests Rejected

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 80, Major / 80

Policy: MSBS_RequestsRejected

Message text: The current value of RequestsRejected is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): A server may be overwhelmed during times of heavy load due to processor or memory constraints that ultimately result in the rejection of requests.

Potential Impact: There may be a larger capacity concerns and adding more servers should be evaluated.

Suggested Action(s): ASP Web Requests are rejected.

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: RequestsRejected

Description: This policy monitors the number of requests rejected because the request queue was full.

Metric SpecName: RequestsRejected

Metric Field Name: Requests Rejected

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 80, Major / 80

Policy: MSBS_RequestsRejected

Message text: The current value of RequestsRejected is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): A server may be overwhelmed during times of heavy load due to processor or memory constraints that ultimately result in the rejection of requests.

Potential Impact: There may be a larger capacity concerns and adding more servers should be evaluated.

Suggested Action(s): ASP Web Requests are rejected.

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

RtcPublishMultipleCategoriesSprocCallsPerSec

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / RTPUBMULTCATSPCALPS

Source / Collection Definition: PERFMON / LS:USrv - Rich presence service SQL calls(*)

Metric: RtcPublishMultipleCategoriesSprocCallsPerSec

> **Description**: This metric captures Rtc Publish Multiple Categories Sproc Calls Per Sec
>
> **Metric SpecName**: RtPubMultCatSpCalPS
>
> **Metric Field Name**: USrv - RtcPublishMultipleCategories Sproc Calls/Sec
>
> **Data type**: REAL64
>
> **Alarm**: FALSE

ServerConnections

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / KHISERVCONN

Source / Collection Definition: PERFMON / LS:DATAPROXY - Server Connections(*)

Metric: Systemisthrottling

Description: This policy monitors indicates that system wide throttling is on.

Metric SpecName: Systemisthrott

Metric Field Name: DATAPROXY - System is throttling

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Minor / 1

Policy: MSBS_Systemisthrottling

Message text: The current value of Systemisthrottling is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): The server is not processing PSOM traffic in a timely fashion

Potential Impact: Verify that the server is not overloaded

Suggested Action(s): System will throttle

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

ChkFrontEndBackupServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SERVSTAT

Source / Collection Definition: SERVICECHECK / LYNCBACKUP

Metric: FELYNCBACKUPServName

> **Description**: Name of the Service
>
> **Metric SpecName**: SERVNAME
>
> **Metric Field Name**: Service_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FELYNCBACKUPServDisplayName

> **Description**: Display Name of the Service
>
> **Metric SpecName**: SRVDISPNAME
>
> **Metric Field Name**: Service_Displayname
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FELYNCBACKUPServStatus

> **Description**: Status of the Service
>
> **Metric SpecName**: SERVSTATUS
>
> **Metric Field Name**: Service_Status
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FELYNCBACKUPServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_FELYNCBACKUPServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): Lync Server Backup Service' Windows Service is stopped.

Potential Impact: NA

Suggested Action(s): Lync Server Backup Service' Windows Service is stopped. Please restart the service.

ChkFrontEndBandwidthAuthPolicyServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SERVSTAT

Source / Collection Definition: SERVICECHECK / RTCPDPAUTH

Metric: FERTCPDPAUTHServName

Description: Name of the Service

Metric SpecName: SERVNAME

Metric Field Name: Service_Name

Data type: TEXT

Alarm: FALSE

Metric: FERTCPDPAUTHServDisplayName

Description: Display Name of the Service

Metric SpecName: SRVDISPNAME

Metric Field Name: Service_Displayname

Data type: TEXT

Alarm: FALSE

Metric: FERTCPDPAUTHServStatus

Description: Status of the Service

Metric SpecName: SERVSTATUS

Metric Field Name: Service_Status

Data type: TEXT

Alarm: FALSE

Metric: FERTCPDPAUTHServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_FERTCPDPAUTHServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): Lync Server Bandwidth Policy Service (Authentication)' Windows Service is stopped.

Potential Impact: NA

Suggested Action(s): Lync Server Bandwidth Policy Service (Authentication)' Windows Service is stopped. Please restart the service.

Collect_Mediation_Health_Indices

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: CS / NA

Source / Collection Definition: PERFMON / LS:MediationServer - 03 - Health Indices(*)

Metric: MedHealthIndicesInstance

> **Description**: instance of perfmon object LS:MediationServer - 03 - Health Indices
>
> **Metric SpecName**: MEDHEALTHINDINS
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: MedLoadCallFailureIndex

> **Description**: index of call failures due to heavy load , The index is scaled between 0 to 100
>
> **Metric SpecName**: LOADCALLFAILINDX
>
> **Metric Field Name**: 0 - Load Call Failure Index
>
> **Data type**: UINT32
>
> **Alarm**: TRUE
>
> **Category** : MSSkype
>
> **Severity / Threshold** : Warning / 5, Major / 10
>
> **Policy**: MSBS_MedLoadCallFailureIndex
>
> **Message text**: The value of the counter ' Load Call Failure Index' value <VALUE> has crossed the threshold of <THRESHOLD> .
>
> **Instructional Text**:
>
> **Probable Cause(s)**: NA
>
> **Potential Impact**: NA
>
> **Suggested Action(s)**: NA

QueueDepth

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / QUEUEDEPTH

Source / Collection Definition: PERFMON / LS:USrv - SHAREDDBStore(*)

Metric: QueueDepth

> **Description**: This metric captures Queue Depth
>
> **Metric SpecName**: QueueDepth
>
> **Metric Field Name**: USrv - Queue Depth
>
> **Data type**: REAL64
>
> **Alarm**: FALSE

Metric: Instance_Name

> **Description**: This is the key for metric
>
> **Metric SpecName**: Instance_Name
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

SimplePortWatcher5070

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / Port5070

Source / Collection Definition: PORTCOL / PORTCHECKER

Metric: SimpleWatcherPort5070

Description: Used by the Mediation Server for incoming requests from the Front End Server.

Metric SpecName: SimpleWatcherPort5070

Metric Field Name: SimpleWatcherPort5070

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort5070

Message text: The Port No:5070 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

> **Description**: This is the key for metric
>
> **Metric SpecName**: HOSTNAME
>
> **Metric Field Name**: HOSTNAME
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: SimpleWatcherPort5070

Description: Used by the Mediation Server for incoming requests from the Front End Server.

Metric SpecName: SimpleWatcherPort5070

Metric Field Name: SimpleWatcherPort5070

Data type: BOOL

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1, Major / 1

Policy: MSBS_SimpleWatcherPort5070

Message text: The Port No:5070 is down

Instructional Text:

Probable Cause(s): The watcher node doesn't have the appropriate permissions. The DNS client side cache has a stale entry. The DNS infrastructure not available. The watcher node DNS settings are out of date or incorrect. DNS has a stale entry for the supplied target name and is returning the wrong IP address. The target computer is offline. There is a firewall between the watcher node and the target IP or device IPSec is required between the watcher node and the target IP or device The target IP:Port is actually not available

Potential Impact: Connection to Port cannot be established

Suggested Action(s): Ensure that if IPSec is configured, that the machine can establish an IPSec connection Telnet to the target IP:Port telnet x.x.x.x #### Where x.x.x.x. is the IP Address or device name and #### is the target port number." Try the following troubleshooting steps to attempt to fix the problem On a Windows Computer, at the command line type: ipconfig /flushdns Then type: ipconfig /registerdns Check with your network or domain administrator if there is any problems with the DNS infrastructure that the watcher node is configured to use. Check the IP Address that is being returned to ensure it is returning the actual device name you expect. Do this by pinging by the device name you supplied in the wizard. Next take the IP Address and type ping -a [IPAddress]. For example, if the IP Address is 10.10.1.1: ping -a 10.10.1.1 If the name returned is different than the name supplied in the wizard there are likely some name resolution issues related to having a misconfigured or stale DNS entry." Check if the Windows Firewall is enabled on either the target machine or the watcher node. If it is, create an exclusion for the application you are monitoring.

Metric: HOSTNAME

Description: This is the key for metric

Metric SpecName: HOSTNAME

Metric Field Name: HOSTNAME

Data type: TEXT

Alarm: FALSE

Peers

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / KHIPEERS

Source / Collection Definition: PERFMON / LS:SIP - 01 - Peers(*)

Metric: SendsTimedOut

Description: This policy monitors the total number of sends dropped because they stayed in the outgoing (send) queue for too long.

Metric SpecName: SendsTimedOut

Metric Field Name: SIP - 019 - Sends Timed-Out/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Minor / 10, Minor / 10

Policy: MSBS_SendsTimedOut

Message text: The current value of SendsTimedOut is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): The destination of the connection might be overloaded or network bandwidth to the destination is insufficient.

Potential Impact: Please ensure that hardware and software requirements at the destination and network bandwidth allocation meet the user usage characteristics.

Suggested Action(s): Slow SIP message transmissions

Metric: AboveLimitConnectionsDropped

Description: This policy monitors the total number of connections that were dropped because the limit on number of incoming connections from a federated partner or clearinghouse was exceeded.

Metric SpecName: AbvLimtConnDrop

Metric Field Name: SIP - 004 - Above Limit Connections Dropped (Access Proxies only)

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Minor / 1, Minor / 1

Policy: MSBS_AboveLimitConnectionsDropped

Message text: The current value of AboveLimitConnectionsDropped is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): he network connectivity with the federated partner or clearinghouse is unstable, or an administrator of the remote domain has configured too many servers to communicate with your domain.

Potential Impact: Check to resolve network connectivity problems with the federated partner or clearinghouse, or ask the administrator of the remote domain to limit the number of servers communicating with your domain.

Suggested Action(s): SIP connections get dropped

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

Metric: SendsTimedOut

Description: This policy monitors the total number of sends dropped because they stayed in the outgoing (send) queue for too long.

Metric SpecName: SendsTimedOut

Metric Field Name: SIP - Sends Timed-Out/sec

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Minor / 10, Minor / 10

Policy: MSBS_SendsTimedOut

Message text: The current value of SendsTimedOut is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): The destination of the connection might be overloaded or network bandwidth to the destination is insufficient.

Potential Impact: Please ensure that hardware and software requirements at the destination and network bandwidth allocation meet the user usage characteristics.

Suggested Action(s): Slow SIP message transmissions

Metric: AboveLimitConnectionsDropped

Description: This policy monitors the total number of connections that were dropped because the limit on number of incoming connections from a federated partner or clearinghouse was exceeded.

Metric SpecName: AbvLimtConnDrop

Metric Field Name: SIP - Above Limit Connections Dropped (Access Proxies only)

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Minor / 1, Minor / 1

Policy: MSBS_AboveLimitConnectionsDropped

Message text: The current value of AboveLimitConnectionsDropped is <VALUE> which exceeds the threshold of <THRESHOLD> that is defined in the policy:

Instructional Text:

Probable Cause(s): he network connectivity with the federated partner or clearinghouse is unstable, or an administrator of the remote domain has configured too many servers to communicate with your domain.

Potential Impact: Check to resolve network connectivity problems with the federated partner or clearinghouse, or ask the administrator of the remote domain to limit the number of servers communicating with your domain.

Suggested Action(s): SIP connections get dropped

Metric: Instance_Name

Description: This is the key for metric

Metric SpecName: Instance_Name

Metric Field Name: Instance_Name

Data type: TEXT

Alarm: FALSE

MEDIAPlanning

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2015

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / NUMOCCCONFPRCDLSIGN

Source / Collection Definition: PERFMON / LS:MEDIA - Planning(*)

Metric: NumberOfOccasionsConferenceProcessingIsDelayedSignificantly

> **Description**: This metric captures Number Of Occasions Conference Processing Is Delayed Significantly
>
> **Metric SpecName**: NumOccConfPrcDISign
>
> **Metric Field Name**: MEDIA - Number of occasions conference processing is delayed significantly
>
> **Data type**: UINT32
>
> **Alarm**: FALSE

Metric: Instance_Name

> **Description**: This is the key for metric
>
> **Metric SpecName**: Instance_Name
>
> **Metric Field Name**: Instance_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

ChkFrontEndMasterReplicatorServStat

The Policy Contains the metric definition xml which will get used by Microsoft Collector to collect metrics

Schedule Task Policy: MSBS_SCH_VERY_HIGH

ConfigFile Policy: MSBS_Collection_Definition_2010

Aspect: Skype Configuration

CIT: Windows

Data source / Data class: LYNC / SERVSTAT

Source / Collection Definition: SERVICECHECK / MASTER

Metric: FEMASTERServName

> **Description**: Name of the Service
>
> **Metric SpecName**: SERVNAME
>
> **Metric Field Name**: Service_Name
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FEMASTERServDisplayName

> **Description**: Display Name of the Service
>
> **Metric SpecName**: SRVDISPNAME
>
> **Metric Field Name**: Service_Displayname
>
> **Data type**: TEXT
>
> **Alarm**: FALSE

Metric: FEMASTERServStatus

Description: Status of the Service

Metric SpecName: SERVSTATUS

Metric Field Name: Service_Status

Data type: TEXT

Alarm: FALSE

Metric: FEMASTERServState

Description: State of the Service

Metric SpecName: SERVSTATE

Metric Field Name: Service_State

Data type: UINT32

Alarm: TRUE

Category : MSSkype

Severity / Threshold : Major / 1

Policy: MSBS_FEMASTERServState

Message text: the service <OPTION(ServiceName)> is in the state <OPTION(ServiceStatus)>

Instructional Text:

Probable Cause(s): Lync Server Master Replicator Agent' Windows Service is stopped.

Potential Impact: NA

Suggested Action(s): Lync Server Master Replicator Agent' Windows Service is stopped. Please restart the service.

Send documentation feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Reference Guide (OMi Management Pack for Microsoft Skype for Business Server 1.00)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to docfeedback@hpe.com.

We appreciate your feedback!