Configure SCOM Integration in
Goliath Performance Monitor and Goliath Application Availability Monitor

This document will guide you through the process of configuring Goliath Performance Monitor and Goliath Application Availability Monitor to send notifications and alerts to Microsoft SCOM

Contents

I. Choose an Alert Communication Methodology 1
II. Configure Syslog Notifications 1
III. Configure SNMP Notifications 2
I. Appendix 4
A. Macro Substitution 4

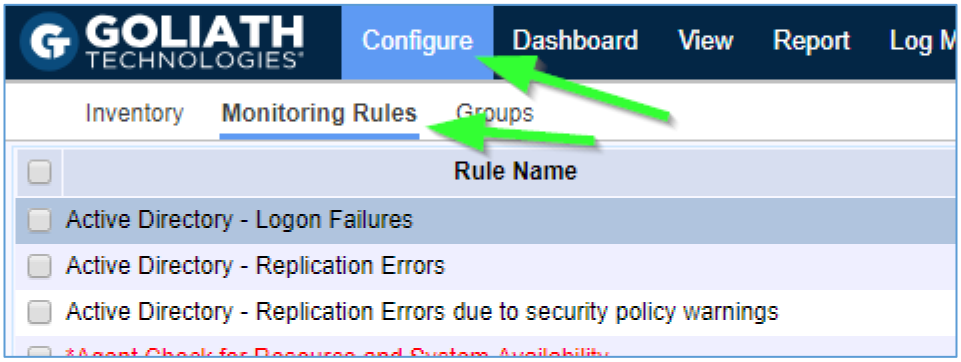
I. Choose an Alert Communication Methodology

Communication to Microsoft SCOM can happen via Syslog or SNMP. Most implementations are utilizing Syslog. Configure the SCOM environment to accept alerts via the communication protocol of your choice based on available documentation from Microsoft. Once the SCOM environment is configured, move to the appropriate section below to configure Goliath Performance Monitor or Goliath Application Availability Monitor to transmit alerts to your SCOM deployment.

II. Configure Syslog Notifications

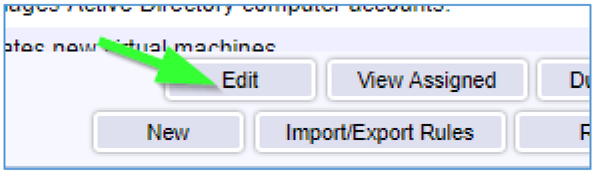
Before starting this section, please ensure that the items in Section I have been completed.

1. Open the Goliath Console
2. Select the **'Configure'** tab, and then the **'Monitoring Rules'** sub menu



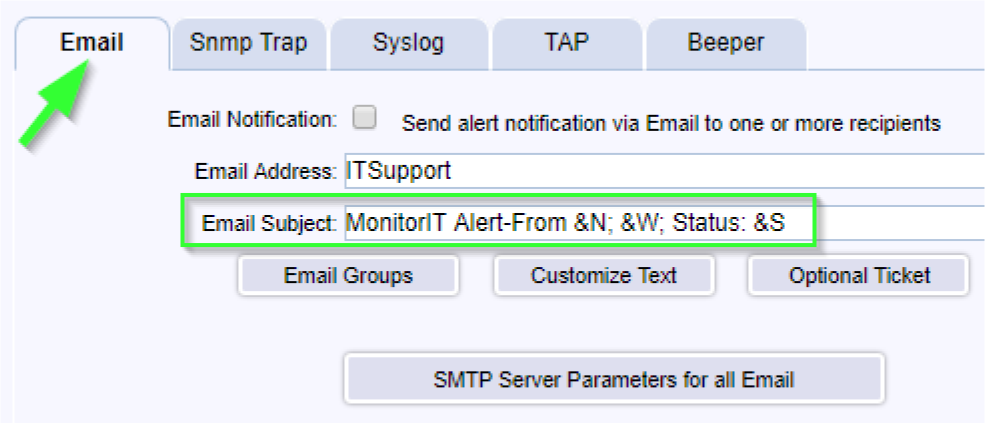
□	Rule Name
□	Active Directory - Logon Failures
□	Active Directory - Replication Errors
□	Active Directory - Replication Errors due to security policy warnings
□	*Agent Check for Resource and System Availability

3. Select the alert condition in which you'd like to enable email or text message notifications
4. Click the **'Edit'** button at the bottom of the page


ages Active Directory computer accounts.
ates new virtual machines
Edit
View Assigned
Du
New
Import/Export Rules
F

5. A new pane will open, choose the **'Notifications'** tab
6. The subsection for **'Email'** will be selected by default, on this tab please use the **'Email Subject'** field to define the subject for the syslog message. Please note, by default you will see characters like '&N' in the subject, this is

a part of our macro functionality. A full list of macros is provided in the Appendix at the end of this document.

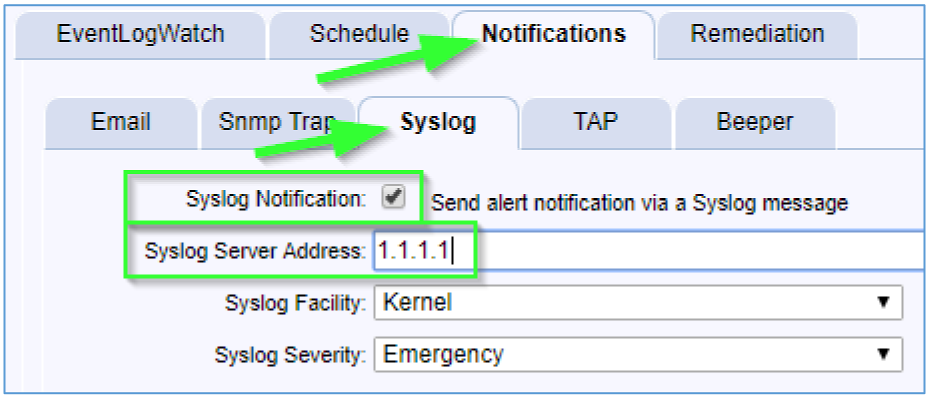


Email Notification: □ Send alert notification via Email to one or more recipients

Email Address: ITSupport

Email Subject: MonitorIT Alert-From &N; &W; Status: &S

7. Click the tab for **'Syslog'** and select the checkbox at the top of the subsection to enable syslog notifications.
8. In the **'Syslog Server Address'** field, define the IP address or machine name where the syslog alert notification will be sent.



Syslog Notification: ☑ Send alert notification via a Syslog message

Syslog Server Address: 1.1.1.1

Syslog Facility: Kernel

Syslog Severity: Emergency

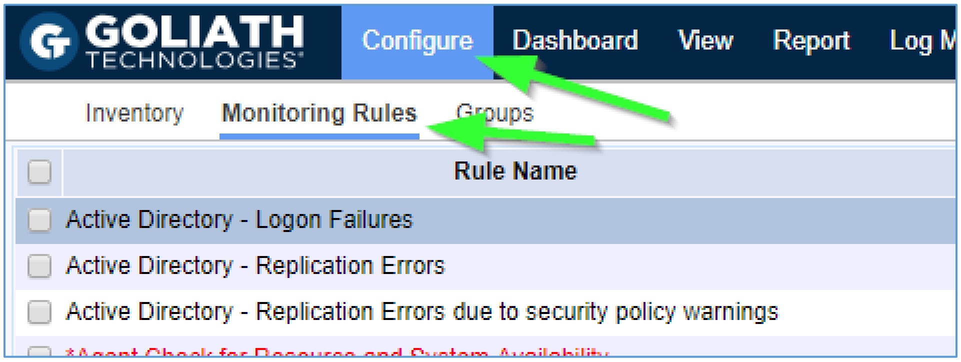
9. For the **'Syslog Facility'** drop down menu, chose the Facility that defines where the Syslog message is originating. This field is used in conjunction with the Severity field to form the syslog message priority code.
10. For the **'Syslog Severity'** drop down menu, chose the Severity that defines the severity level of the Syslog message. This field is used in conjunction with the Facility field to form the syslog message priority code.
11. When finished, you can click the **'Test Syslog'** button to confirm that the Syslog message is received by appropriately by the Syslog server.
12. Click **'Save'** when ready to enable this configuration.

III. Configure SNMP Notifications

Before starting this section, please ensure that the items in Section I have been completed.

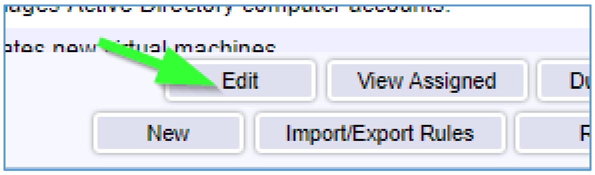
1. Open the Goliath Console

2. Select the **'Configure'** tab, and then the **'Monitoring Rules'** sub menu

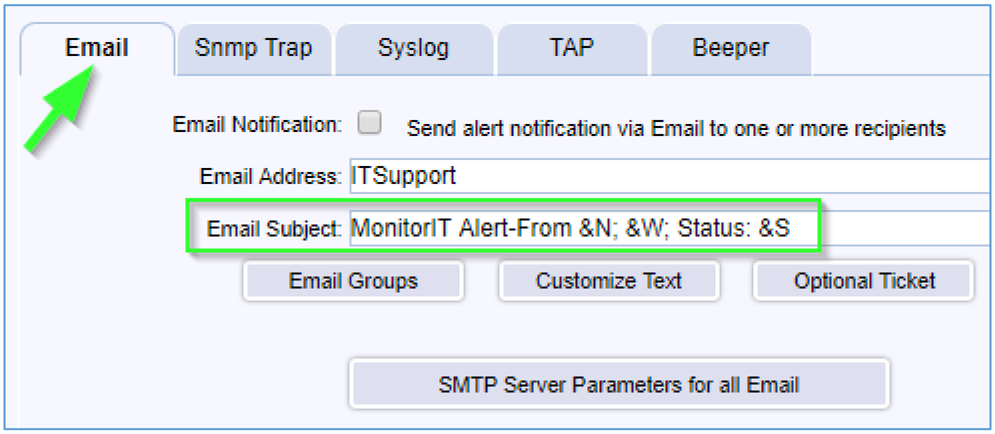


- □ Active Directory - Logon Failures
- □ Active Directory - Replication Errors
- □ Active Directory - Replication Errors due to security policy warnings
- □ *Agent Check for Resources and System Availability

3. Select the alert condition in which you'd like to enable email or text message notifications
4. Click the **'Edit'** button at the bottom of the page


ages Active Directory computer accounts.
ates new virtual machines
Edit
View Assigned
Du
New
Import/Export Rules
R

5. A new pane will open, choose the **'Notifications'** tab
6. The subsection for **'Email'** will be selected by default, on this tab please use the **'Email Subject'** field to define the subject for the SNMP message. Please note, by default you will see characters like '&N' in the subject, this is a part of our macro functionality. A full list of macros is provided in the Appendix at the end of this document.



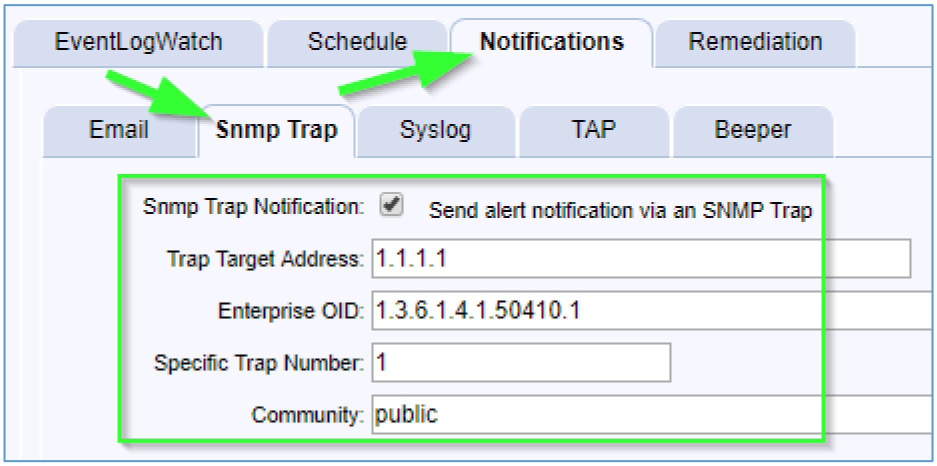
Email Notification: □ Send alert notification via Email to one or more recipients

Email Address: ITSupport

Email Subject: MonitorIT Alert-From &N; &W; Status: &S

7. Click the tab for **'SNMP Trap** and select the checkbox at the top of the subsection to enable SNMP notifications.

8. In the **'Trap Target Address'** field, define the IP address or machine name where the SNMP Trap notification will be sent.



Snmp Trap Notification: ☑ Send alert notification via an SNMP Trap

Trap Target Address: 1.1.1.1

Enterprise OID: 1.3.6.1.4.1.50410.1

Specific Trap Number: 1

Community: public

9. For the **'Enterprise OID'** menu, enter 1.3.6.1.4.1.50410.x where **'x'** is the category of alert based on the table below.

	Category
1	Goliath Performance Monitor
2	VMware
3	XenServer
4	Citrix Role Servers
5	Citrix XenApp
6	Citrix XenDesktop
7	VMware View
8	Remote Desktop Services
9	Goliath Application Availability Monitor
10	Microsoft Windows

10. For the **'Specific Trap Number'** option, define a number representing the specific trap/alert/notification. These numbers are typically sequential and specific to each Monitoring Rule that will be sending notifications.
11. Define your SNMP Community string in the **'Community'** field.
12. When finished, you can click the **'Test Trap'** button to confirm that the SNMP trap is received by appropriately by the target device/service.
13. Click **'Save'** when ready to enable this configuration.

I. Appendix

A. Macro Substitution

Custom Email and SMS Text Notifications supports fourteen ***'Macros'*** that are substituted with the appropriate data for a particular alert when it occurs. The parameters are **case sensitive and must be upper case.**

- &N: which is replaced by the name of the server/device causing the alert
- &A: which is replaced by the IP Address of the server/device causing the alert
- &W: which is replaced by the name of the Monitoring Rule
- &S: which is replaced by the Status message associated with this failure causing the alert status information is source dependent and differs based upon the watch type.
  - For Example:

    - ServerWatch: 429 Mb memory free; 2% available
    - ProcessWatch: Process not running no restart attempted
    - EventLogWatch: Event ID, Source, & Description
    - Logon Simulator: The full simulation details log
- &D: which is replaced by the date of the alert
- &T: which is replaced by the time of the alert
- &P: which is replaced by the Server/Device Description
- &O: which is replaced by the Server/Device Notes
- &G: which is replaced by the name of the Group that the Server/Device belongs
- &C: which is replaced by the Group Description
- &R: which is replaced by the Monitoring Rule ‘Description’ text
- &L: which is replaced by the for the Monitoring Rule ‘Severity’ level
- &E: which is replaced by the for the Monitoring Rule Notes
- &V: (only for CounterWatch) is replaced by the Counter value that exceeded the threshold and caused an alert.