# SLM Create a Missed SLA Form

Service Level Management

**Purpose**

The Missed SLA Form is used when research is being performed regarding a missed or breached SLA based on error minutes that appear for a service on the Daily SLA Report. Information from the Metric Data Definition, the Daily SLA Report, and the monitoring tool are added to the form by the SLM team. Any Change or Incident tickets that exist during the time frame of the outage are also included as part of the research. The Missed SLA Form is attached to the Work Log of the Investigation Incident ticket, which is then assigned to SIG or JTS to complete. SIG or JTS should add their conclusions to the form to either verify that the information discovered by Service Level Management is correct, or to provide the actual cause of the outage if the information discovered by Service Level Management is not correct.

**Related Policy**

* [IT Service Management Policy](https://sharepoint.jackson.com/sites/integrity/_layouts/15/WopiFrame.aspx?sourcedoc=%7be34fe42a-654a-469a-9d38-6612f00486dc%7d&action=view)

**Audience**

The following groups are responsible for adhering to this document:

* Service Level Management

**Procedure**

|  |  |
| --- | --- |
| Step | Action |
| 1 | An Investigation Incident ticket is created whenever error minutes appear on the Daily SLA Report. Error minutes indicate a missed or breached SLA.  See the ***SLM Reviewing the Daily SLA Report Procedure*** for more information.  ***Note:*** *If the “Actual %” is less than 100% but is above the compliance target percentage, the SLA is considered “Missed”. If the “Actual %” is less than the compliance target, the SLA is considered “Breached”.* |
| 2 | Create the Missed SLA form:   1. Copy the “Missed SLA Form” located at:   [O:\Service Delivery\Service Level Management\SLA Information\SLA Excell Spreadsheet\Missed SLA Forms](../../../SLA%20Information/SLA%20Excell%20Spreadsheet/Missed%20SLA%20Forms)     1. Rename the file to represent the date of the missed / breached SLA and the service name. Example: 02-02-2018 JEDI.docx 2. Service Level Management fills in the section highlighted in yellow on the form.   Open the Metric Data Definition (MDD) form for the service being researched:  [O:\Service Delivery\Service Level Management\SLA Information\SLA Excell Spreadsheet\Metric Data Definitions](../../../SLA%20Information/SLA%20Excell%20Spreadsheet/Metric%20Data%20Definitions)   1. Start filling out the Missed SLA Form:  * **Service Name** – Enter the service name from the ITSM Service Catalog.   It is the same name used in the MDD.   * **Breached or Missed SLA -** Use the drop down list to select one. The   percentage is found in the “Actual” column  on the SLA report. Determine if the SLA is  missed or breached compared to the  compliance target found on the SLA  Report (on the same line as the service  name) or the MDD.   * **Outage Minutes on SLA Report -** Use the number from the “Error”   column on the SLA Report.   * **Incident Request Number –** Use the Incident ticket number that has   been created to investigate the missed  SLA.   * **Details that Feed the Monitor** – Copy this information from the MDD   form.   1. Access the correct monitoring tool (SiteScope or Nagios) to view the time of the outage. The correct monitor to use will be found in the “Details that Feed the Monitor” section of the MDD.   See ***Appendix A*** and ***Appendix B*** for more information.   1. Use the information from the monitoring tool to add data to the following sections of the Missed SLA Form:  * **SiteScope / Nagios Alerts** – Paste the alerts from the monitoring tool in this   field.   * **Date / Time** – Based on the alerts from the monitoring tool, type in the start /   end date and time in these fields. |
| 3 | Conduct research to attempt to find out why the SLA was missed:   1. Use information from the MDD and monitoring tools to perform searches on the following reports to try and find incidents, changes, and problems that coincide with the time frame that the service outage occurred:  * Run the Change Control Management Report * Click the Smart Reporting tab in the “Applications” side bar in BMC Remedy. * Click on “Smart Reporting Console” * Click on “Service Delivery” under the “By Folder” section * Click on “Change Management”. Several reports will appear. * Locate and double click on “CM – Change Control Meeting Report” * Use the calendar prompts to set the report date and time range: * Enter value for Task Scheduled Start Date: * Previous Date / 12:00:00 AM * Enter value for Task scheduled End Date: * Current Date / 12:00:00 PM * Enter value for Task Scheduled Start Date: * Previous Date / 12:00:00 AM * Enter value for Task scheduled End Date: * Current Date / 12:00:00 PM * Click the “Go” button * Once the report has been created, click the export button at the top of the screen and save the report in the PDF format to your U: drive.      1. Review the following reports:  * [Non-Job Abend Tickets: Opened Since Last Business Day Report](http://docs.jackson.local/it/sites/rs/_layouts/15/start.aspx" \l "/Daily%20Reporting/Forms/current.aspx) * Navigate to the current year * Click on “Incidents Opened in Cycle and Outstanding” * Navigate to the current month * Click on the “Production Infrastructure Non-Job Abend Report – Opened Since Last Business Day MMDDYY” report * [Job Abend Tickets: Opened Since Last Business Day Report](http://docs.jackson.local/it/sites/rs/_layouts/15/start.aspx#/Daily%20Reporting/Forms/current.aspx) * Navigate to the current year * Click on “Incidents Opened in Cycle and Outstanding” * Navigate to the current month * Click on the “Production Infrastructure Job Abend Report – Opened Since Last Business Day MMDDYY” report. * [Production Problem Report: Opened Since Last Business Day Report](http://docs.jackson.local/it/sites/rs/_layouts/15/start.aspx#/Daily%20Reporting/Forms/current.aspx) * Navigate to the current year * Click on “Incidents Opened in Cycle and Outstanding” * Navigate to the current month * Click on the “Production Problem Report – Opened Since Last Business Day MMDDYY” report.  1. Use the BMC Remedy Incident search functionality:  * When performing a search, use the dropdown list in the “Services” field. This will show all incidents in which the service had an issue or was subject to change * The most recent incident tickets will be at the top. * Try to match the dates and times to when the monitoring tool reported the outage.      1. If any incident, change, or problem tickets are found that match the time frame of the outage, add the information to the following field on the Missed SLA Form:  * **Research Results** – Type the incident, change, or problem ticket(s)   found. Include the summary of the problem, the  resolution, and any additional information that may  assist SIG or JTS with verifying or investigating the  outage. |
| 4 | Attach the form to the Investigation Incident ticket that has been created for the missed / breached SLA.  SIG / JTS are expected to fill in the sections highlighted in blue to either verify the results of the research conducted by Service Level Management or provide information to explain the cause of the outage. SIG / JTS will reattach the updated Missed SLA form to the ticket. |

**Appendix A – SiteScope Monitoring Tool**

SiteScope is an agentless [monitoring](https://en.wikipedia.org/wiki/System_Monitoring) software focused on monitoring the availability and performance of distributed IT infrastructures, including [Servers](https://en.wikipedia.org/wiki/Server_(computing)), [Network devices and services](https://en.wikipedia.org/wiki/Computer_network), [Applications and application components](https://en.wikipedia.org/wiki/Application_software), [operating systems](https://en.wikipedia.org/wiki/Operating_systems) and various IT enterprise components.

<https://en.wikipedia.org/wiki/HP_SiteScope>

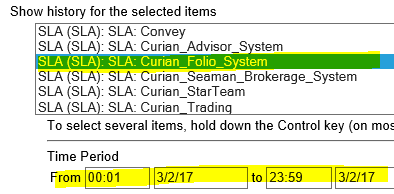
1. Access SiteScope at <https://webadmin.jacksonnational.com:8888/SiteScope/accounts/login137/htdocs/SiteScope.html>
2. Click the “Reports” button at the top of the screen.



1. Click the “Quick” link.



1. Find the SLA / Service from the list and type in the time frame from the “Service Target” information found on the SLA Report.



1. Click the “Show Quick” button
2. The Quick Report Form will appear, showing all the availability and unavailability of the service during the specified time frame.
3. An “Errors” section will appear in the middle of the Quick Report Form. This will show the time of the errors, the service being monitored, and the status of what the monitor experienced.

|  |  |  |
| --- | --- | --- |
| **Errors from 12:01 AM 3/2/17 to 11:59 PM 3/2/17** | | |
| **Time** | **Monitor** | **Status** |
| 3:06 AM 3/2/17 | SLA: Curian\_Folio\_System | 75% OK, 4 monitors checked, 1 in error (aip90a1: Folio Login (SLA): unable to connect to server on (step 1), http://aip90a1:41001/institutional/login/loginFormFolio.jspstatus=-998 URL: http://aip90a1:41001/institutional/login/loginFormFolio.jsp, host: ai |
| 3:11 AM 3/2/17 | SLA: Curian\_Folio\_System | 75% OK, 4 monitors checked, 1 in error (aip90a2: Folio Login (SLA): unable to connect to server on (step 1), http://aip90a2:41001/institutional/login/loginFormFolio.jspstatus=-998 URL: http://aip90a2:41001/institutional/login/loginFormFolio.jsp, host: ai |
| 3:16 AM 3/2/17 | SLA: Curian\_Folio\_System | 75% OK, 4 monitors checked, 1 in error (aip90a2: Folio Login (SLA): unable to connect to server on (step 1), http://aip90a2:41001/institutional/login/loginFormFolio.jspstatus=-998 URL: http://aip90a2:41001/institutional/login/loginFormFolio.jsp, host: ai |

1. This information should be used for researching the cause of the outage.

**Appendix B - Nagios Monitoring Tool**

Nagios is a [free](https://en.wikipedia.org/wiki/Free_software) and [open source](https://en.wikipedia.org/wiki/Open_source) [computer](https://en.wikipedia.org/wiki/Computer)-[software application](https://en.wikipedia.org/wiki/Software_application) that [monitors](https://en.wikipedia.org/wiki/Event_monitoring) [systems](https://en.wikipedia.org/wiki/System_monitor), [networks](https://en.wikipedia.org/wiki/Network_monitoring) and infrastructure. Nagios offers monitoring and alerting services for servers, switches, applications and services. It alerts users when things go wrong and alerts them a second time when the problem has been resolved.

<https://en.wikipedia.org/wiki/Nagios>

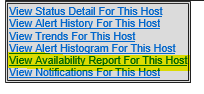
1. The Nagios monitoring site is located at <https://nagiosp4.jacksonnational.com/nagiosp4/>
2. Services are not listed in Nagios so a search needs to be performed on a server name or host. In the field, only the partial name needs to be typed in.



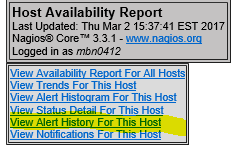
1. The host and service information will appear.



1. Click on the link under the “Host” column.
2. Click the “View Availability Report For This Host” link in the corner of the screen.



1. Click the “View Alert History For This Host”



1. The next screen will allow you to go back to the date you are looking for.



1. Alerts will appear in red.



1. This information should be used when researching the cause of the outage.
2. Also, note that a second Nagios site is located at <https://nagiosp5.jacksonnational.com/nagiosp5/>

This is mainly used for monitoring databases.

**Modification**

The following associates can make modifications to this document:

* Manager, Service Level Management
* Director, IT Service Management
* Vice President, Service Delivery
* Chief Technology Officer, PGDS

|  |  |
| --- | --- |
| Service Level Management Process | |
| Responsible Party: Anna Carter, Manager, Service Level Management Approving Authority: Abdul Golden, Director, IT Service Management | Date Created: 02-09-2018 Last Modified:  Last Reviewed: |