# Create a Missed SLA Form Procedure

Continuous Performance Enablement

**Purpose**

The Missed SLA Form is used when an Investigation Incident ticket is created to research a missed or breached SLA. Information from the Metric Data Definition, the CI Unavailability record, and the monitoring tool are added to the form by the SLM team. Any Incident or Change tickets which pertain to the application being researched are 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 JET to complete. JET will add their conclusions to the form to either verify that the information discovered by Continuous Performance Enablement is correct, or to provide the actual cause of the outage if the information discovered by Continuous Performance Enablement is not correct.   
***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”.*

For more information see:

[Create an Investigation Ticket for Missed / Breached SLA Procedure](Create%20an%20Investigation%20Ticket%20for%20Missed%20Breached%20SLA%20Procedure.docx)

**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:

* Continuous Performance Enablement

**Procedure**

|  |  |
| --- | --- |
| Step | Action |
| 1 | Create the Missed SLA form:   1. Copy the “Missed SLA Form” located at:   [..\..\SLA Working Spreadsheet\Missed SLA Forms](../../SLA%20Working%20Spreadsheet/Missed%20SLA%20Forms)   1. Re-name the file to represent the date of the missed / breached SLA and the service name. Example: 02-02-2018 JEDI.docx 2. Continuous Performance Enablement fills in the section highlighted in yellow on the form.   Open the Metric Data Definition (MDD) form located on SharePoint for the service being researched:  [Service Level Management/Documents/SLM Documents/Metric Data Definitions](https://sharepoint.jackson.com/sites/itsmsd/servicelevelmanagement/_layouts/15/start.aspx#/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2Fsites%2Fitsmsd%2Fservicelevelmanagement%2FShared%20Documents%2FSLM%20Documents%2FMetric%20Data%20Definitions&FolderCTID=0x012000C3EC5FEE7B19F646BACB9A57478C774E&View=%7B527EAB19%2D8D4A%2D47E6%2DACE1%2D)   1. Take note of the following information on the MDD:    * Requirements      + Service Target      + Percentage 2. Copy the information from the following section on the MDD:    * Monitoring Specifications      + Details on the monitor that will feed the SLM system: 3. 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. Use   the outage minutes from the CI Unavailability record  that are in the Service Target time frame (see d)  above) and divide by the number of minutes that the  application is expected to be available each day.  Multiply the result by 100 to obtain the percentage.  See the percentage in d) above to determine if the SLA  was “Missed” or “Breached”.  For more information see:  [Incident Ticket with CI Unavailability Record Documentation](../SLA%20Reporting%20Documentation/Incident%20Ticket%20with%20CI%20Unavailability%20Record%20Documentation%20.docx)   * **Outage Minutes on SLA Report –** Use the outage minutes from the CI   Unavailability record that are in the Service Target time  frame.   * **Incident Request Number** – Use the Investigation Incident ticket   number that has been created to investigate the  missed / breached SLA.   * **SLM CI Unavailability Incident Ticket Number** – Use the SLM Incident   ticket(s) number in which a CI Unavailability record is  attached.  For more information see:  [Identify and Verify CI Unavailability Record Tickets Documentation](../SLA%20Reporting%20Documentation/Identify%20and%20Verify%20CI%20Unavailabillity%20Record%20Tickets%20Documentation.docx)   * **Details that Feed the Monitor** – Paste the information from e) above   into this section.   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. |
| 2 | 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 JET with verifying or investigating the  outage. |
| 3 | Attach the Missed SLA form to the Investigation Incident ticket that has been created for the missed / breached SLA.  JET Application Delivery or JET Infrastructure are expected to fill in the sections highlighted in blue to either verify the results of the research conducted by Continuous Performance Enablement or provide information to explain the cause of the outage. |
| 4 | **Save the Missed SLA Form**   1. The Missed SLA forms will reside at the following location while the Investigation tickets is still being worked.   [..\..\SLA Working Spreadsheet\Missed SLA Forms](file:///\\jacksonnational.com\GROUP\ITVOL1\VOL1\group\PM%20COE\Forecasting%20&%20Metrics%20Model%20Rollout\SLA%20Reporting\SLA%20Working%20Spreadsheet\Missed%20SLA%20Forms)   1. Once the Missed SLA form has been completed and the Investigation ticket has been resolved, move the form to current month’s folder in the same location. 2. When all of the Missed SLA Forms for the month have been completed and moved to the current month’s folder, move the folder to the following location:   [..\..\Reporting\YYYY\Monthly SLA Report\Month](../../Reporting)   1. Publish all of the Missed SLA forms to SharePoint at the following location:   [Daily Reporting/SLM/YYYY/Daily SLA /Month/Missed SLA Form](http://docs.jackson.local/it/sites/rs/_layouts/15/start.aspx#/Daily%20Reporting/Forms/current.aspx?RootFolder=%2Fit%2Fsites%2Frs%2FDaily%20Reporting%2FSLM&View=%7B1D5400F7%2DF40D%2D4DC8%2DAED7%2DCCDABECB8C2F%7D) |

**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>

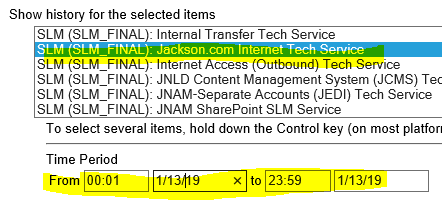
1. Access SiteScope at <https://webadmin.jacksonnational.com:8888/SiteScope/accounts/login137/htdocs/SiteScope.html>
2. Click the “Reports” button at the top of the screen.



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

|  |  |  |
| --- | --- | --- |
| 4:07 AM 1/13/19 | Jackson.com Internet Tech Service | 50% OK, 2 monitors checked, 1 in error (jackson.com: CONSUMER Login: statuscode=ERROR:Failed to retrieve https://www.jackson.com/login/terms-of-service.xhtml. ) |
| 4:11 AM 1/13/19 | Jackson.com Internet Tech Service | 50% OK, 2 monitors checked, 1 in error (jackson.com: CONSUMER Login: statuscode=ERROR:Failed to retrieve https://www.jackson.com/login/terms-of-service.xhtml. ) |

**Appendix B - Nagios Monitoring Tool**

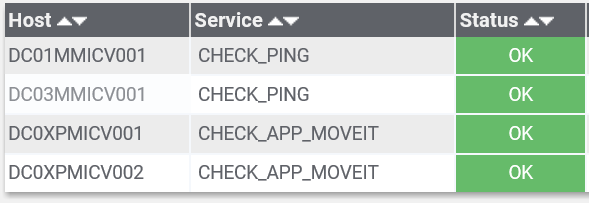
Nagios is a [free](https://en.wikipedia.org/wiki/Free_software) and [open source](https://en.wikipedia.org/wiki/Open_source) [computer](https://en.wikipedia.org/wiki/Computer)-[software application](https://en.wikipedia.org/wiki/Software_application) that [monitors](https://en.wikipedia.org/wiki/Event_monitoring) [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>

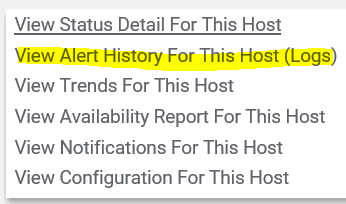
1. The Nagios monitoring site for Windows is located at: <https://dc0xpnagv004.jacksonnational.com/thruk/#cgi-bin/status.cgi?hostgroup=all&style=hostdetail>
2. Perform a search on a host name or an application in the search field. You need to only type in a partial name.

 or 

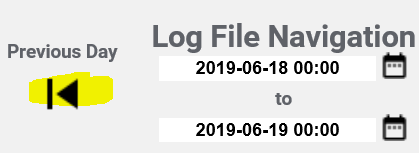
1. The host and service information will appear.



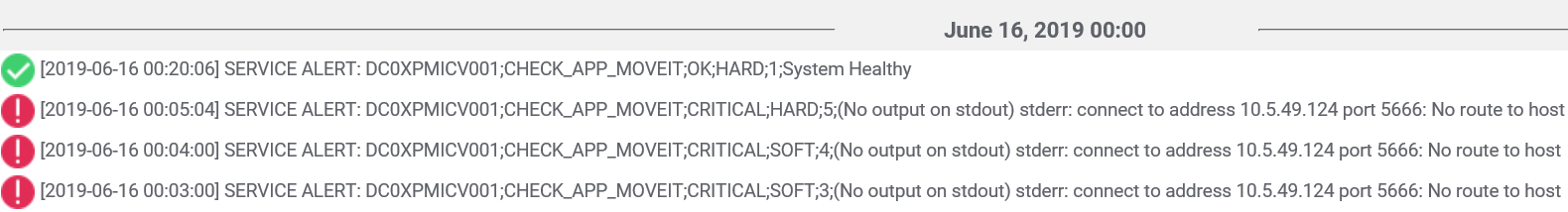
1. Click on the link under the “Host” column.
2. Click the “View Alert History For This Host (Logs) link in the corner of the screen.



1. Use the back-arrow to navigate to the date that is being investigated.



1. Alerts will appear in red.



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

**Modification**

The following associates can make modifications to this document:

* Director, Continuous Performance Enablement
* Vice President, Continuous Performance Enablement
* Chief Technology Officer, JET

|  |  |
| --- | --- |
| Continuous Performance Enablement Process | |
| Responsible Party: CPE Metrics Approving Authority: Bali Bodeddula, Director, JET Continuous Performance Enablement | Date Created: 02-09-2018 Last Modified:  Last Reviewed: |