# SLM Working the Daily SLM Report Procedure

Service Level Management

**Purpose**

The SLM Report is run and reviewed daily so that error minutes for monitored services can be investigated prior to the publication of the Monthly SLM Report. Error minutes indicate an issue in which an SLA may be missed / breached or the monitor that is checking the SLA is not working correctly. This procedure should be followed whenever down time minutes appear on the Daily SLM Report.

**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 | To run the SLM Report and understand the different fields that appear, see the ***SLM Run & Review the SLM Report Procedure***. |
| 2 | Open the current month’s “SLA Spreadsheet for Month YYYY” located at:  [O:\Service Delivery\Service Level Management\SLA Information\SLA Excell Spreadsheet](file:///O:\Service%20Delivery\Service%20Level%20Management\SLA%20Information\SLA%20Excell%20Spreadsheet)   1. In the spreadsheet, create a new tab. 2. Rename the tab to the current date (example; 10-09). |
| 3 | For daily review, the SLM report should be opened as an Excel document. There is no need to save this spreadsheet:   1. Click the “Export” icon at the top of the screen. 2. Select “Export Document As”. 3. Select ‘Excel” from the drop down list.      1. Select “Open with”. 2. Click the “OK” button.      1. Copy the entire contents of the spreadsheet into the tab that was just created in the “SLA Spreadsheet for Month YYYY” spreadsheet. |
| 4 | Review the report, verifying that the correct dates appear for each service and look for error minutes in the “Down Time (mins)” column. When error minutes appear in the “Down Time (mins”) field:   1. Copy the entire line (including “Date”, “Minutes Available”, “Carve Out (mins)”, etc.,)   *Note: An investigation should be performed for any service that has down time minutes, regardless if the service actually breached the SLA for the day or not.*    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”   1. Click on the “Master” tab of the spreadsheet and locate the service that is showing down time minutes.      1. Paste the row under the correct service that had down time minutes. 2. Highlight the “Comments” section in green to indicate that the investigation is unresolved.      1. Create a Service Request Incident ticket to investigate the down time minutes. The ticket should be assigned to yourself and the status needs to be set to “Work in Progress”. 2. Review the Metric Data Definition for the Service to find out what monitoring tool will need to be viewed.  * Monitoring Specifications * Details on the monitor that will feed the SLM system  1. Copy the “*Details that will feed the monitor*” section of the form and paste it in the “Notes” section of the Incident Request ticket that was created. 2. Access the correct monitoring tool (SiteScope or Nagios) to view the time of the outage.   See *Appendix A* and *Appendix B* for more information.   1. Add any information from the monitoring tools that correspond with the outage into the “Notes” section of the Incident Request ticket that was created above. 2. Use the following reports to research incidents and changes that could have caused the down time minutes.  * [Change Control Management Report](http://docs.jackson.local/it/sites/rs/Daily%20Reporting/2017/Daily%20Change%20Control%20Report%20(Model%20and%20Production)) * [Non-Job Abend Tickets: Opened Since Last Business Day Report](http://docs.jackson.local/it/sites/rs/Daily%20Reporting/2017/Incidents%20Opened%20in%20Cycle%20and%20Outstanding) * [Problem Tickets: Opened Since Last Business Day Report](http://docs.jackson.local/it/sites/rs/Daily%20Reporting/2017/Problems%20Opened%20in%20Cycle%20and%20Outstanding)  1. Use the *Service+* field in Remedy to search for additional Incidents that may not have appeared in the reports.  * 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 a change. * The most recent ones will be at the top. * Try to match the dates and times to when the monitoring tool reported the outage.      * If the cause of the down time minutes is found using the tools above continue to l). * If the cause of the down time minutes is not found using the tools above skip to m).  1. Annotate the work log of the Service Request ticket that was created for investigation.  * Include the ticket number and summary of the issue that you believe caused the down time minutes. * Request that the team responsible for the service verify that your findings are the true cause of the outage, and if not, to provide the actual cause of the outage. * Assign the ticket to the group responsible for the service.   *Note: Use the AC Incident Management group when assigning tickets to SIG.*  *Note: If the cause was due to a Major Outage, the ticket does not need to be assigned out. Relate the ticket to the Major Outage ticket and resolve the ticket with information regarding the Major Outage. A discussion must take place with the IT Incident Manager to review the issue, the resolution, and the actual duration of the outage.*   * When reviewing the SLM Report each day, check the status of the Service Request ticket to see if an explanation has been added. * If it is related to your findings or another reason, relate the ticket to the Incident or Change ticket that was responsible for the outage.   *Note: If it is noted that an incident is to blame and that incident states it was caused by a change ticket, ensure that the change ticket is related to that incident. If it is not, relate the ticket using the “caused by” relationship type.*   * If it is noted that there were no issues found, re-assign the ticket to Technical Services. Include a new Work Detail log entry asking them to verify if it was a true outage or a monitoring issue. If Technical Services states it was a monitoring issue, create a Problem Ticket. * If any information was communicated via email, attach the email to the work log.  1. Annotate the work log of the Service Request ticket that was created for investigation.  * Make note that you could not find any Incidents or Change tickets that appear to have caused an issue during the time frame of the outage. * Request that the team responsible for the service provide information on the cause of the down time minutes. * Assign the ticket to the group responsible for the service.   *Note: Use the AC Incident Management group when assigning tickets to SIG.*   * When reviewing the SLM Report each day, check the status of the Service Request ticket to see if an explanation has been added. * If an incident or change is noted, relate the ticket to the incident or change ticket that is responsible.   *Note: If it is noted that an incident is to blame and that incident states it was caused by a change ticket, ensure that the change ticket is related to that incident. If it is not, relate the ticket using the “caused by” relationship type.*   * If it is noted that there were no issues found, re-assign the ticket to Technical Services. Include a new Work Detail log entry asking them to verify if it was a true outage or a monitoring issue. If Technical Services states it was a monitoring issue, create a Problem Ticket. * If any information was communicated via email, attach the email to the work log.  1. Add information to the “Comments” section of the SLA spreadsheet’s “Master” tab for the service in question.  * If the issue is under investigation, make a note of that.      * If the issue is resolved, note the cause of the down time minutes. * Make any notes necessary in the spreadsheet. This can include additional Incident or Change ticket numbers that were discovered, or information from the investigation ticket that possibly explains the issue in more detail. * Highlight the resolved investigation tickets in yellow. * All finalized comments should include an incident or a change number. See the example below. |
| 5 | If the investigation incident ticket is not resolved within two business days, send an email to the group, the group’s manager, and Service Level Management.  If the investigation incident ticket is not resolved with four business days, notify the Service Level Manager to discuss it with the group’s manager. |
| 6 | Based on the information provided by SIG or JTS, add a comment to the SLM Report.  See the ***SLM Add Comments to SLA Report Procedure*** for more information. |
| 7 | Based on the your research and the information provided by SIG or JTS, apply a blackout if down time minutes appear for the following reasons:   * Pre-Approved Change Window. * Monitoring issue. * A report was not printed on a holiday. * Outages reported by SiteScope in which no user impact was found.   See the ***SLM Apply a Carve Out to SLM Report Procedure*** for more information. |
| 8 | The Daily SLM Report is to be published in SharePoint each day after it is has been reviewed and comments and carve-outs have been applied.   1. Re-Run the SLM Report and save as a PDF file to the following location:   [O:\Service Delivery\Service Level Management\Reporting\Daily SLA Report](file:///O:\Service%20Delivery\Service%20Level%20Management\Reporting\Daily%20SLA%20Report)  See Step 3 of the ***SLM Run & Review the SLM Report Procedures*** for more information.   1. Publish to [SharePoint](http://docs.jackson.local/it/sites/rs/_layouts/15/start.aspx#/Daily%20Reporting/Forms/current.aspx?RootFolder=%2Fit%2Fsites%2Frs%2FDaily%20Reporting%2FSLM&FolderCTID=0x012000AF1427B489A1CD4BA12B90F950303DFE&View=%7B1D5400F7%2DF40D%2D4DC8%2DAED7%2DCCDABECB8C2F%7D) |
| 9 | All of the information gathered throughout the month is presented in the Monthly SLM Report.  See the **SLM Create Monthly SLM Report Procedure** for more information. |

**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>

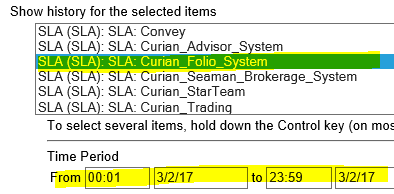
1. Access SiteScope at <https://webadmin.jacksonnational.com:8888/SiteScope/accounts/login137/htdocs/SiteScope.html>
2. Click the “Reports” button at the top of the screen.



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>

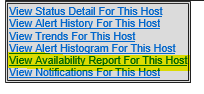
1. The Nagios monitoring site is located at <https://nagiosp4.jacksonnational.com/nagiosp4/>
2. Services are not listed in Nagios so a search needs to be performed on a server name or host. In the field, only the partial name needs to be typed in.



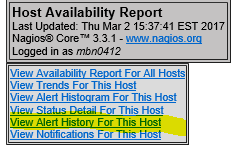
1. The host and service information will appear.



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: 10/27/2017 Last Modified:  Last Reviewed: |