

# 

[Date]

Ryan Woolsey

Loop1 systems, inc

http://www.loop1.com

[Document title]

Loop1 Systems – SolarWinds Orion Health Check Report

Table of Contents

[0](#_Toc19194860)

[1. OVERVIEW 1](#_Toc19194861)

[2. SUMMARY OF RECOMMENDATIONS 2](#_Toc19194862)

[3. CURRENT SOFTWARE INVENTORY 2](#_Toc19194863)

[i. OBSERVATIONS 2](#_Toc19194864)

[ii. RECOMMENDATIONS 2](#_Toc19194865)

[4. GENERAL OBSERVATIONS 2](#_Toc19194866)

[a. Architecture 2](#_Toc19194867)

[i. OBSERVATIONS 2](#_Toc19194868)

[ii. RECOMMENDATIONS 3](#_Toc19194869)

[b. Overall Elements and Polling 3](#_Toc19194870)

[i. OBSERVATIONS 3](#_Toc19194871)

[ii. RECOMMENDATIONS 5](#_Toc19194872)

[c. Website Design 5](#_Toc19194873)

[i. OBSERVATIONS 5](#_Toc19194874)

[ii. RECOMMENDATIONS 6](#_Toc19194875)

[d. Custom Properties 6](#_Toc19194876)

[i. OBSERVATIONS 6](#_Toc19194877)

[ii. RECOMMENDATIONS 6](#_Toc19194878)

[e. Groups and Dependencies 6](#_Toc19194879)

[i. OBSERVATIONS 6](#_Toc19194880)

[ii. RECOMMENDATIONS 6](#_Toc19194881)

[f. Alerting 6](#_Toc19194882)

[i. OBSERVATIONS 6](#_Toc19194883)

[ii. RECOMMENDATIONS 6](#_Toc19194884)

[g. Reports 6](#_Toc19194885)

[i. OBSERVATIONS 6](#_Toc19194886)

[ii. RECOMMENDATIONS 6](#_Toc19194887)

[h. Accounts 6](#_Toc19194888)

[i. OBSERVATIONS 6](#_Toc19194889)

[ii. RECOMMENDATIONS 6](#_Toc19194890)

[i. Windows Event Logs 6](#_Toc19194891)

[i. OBSERVATIONS 6](#_Toc19194892)

[ii. RECOMMENDATIONS 6](#_Toc19194893)

[j. SolarWinds Logs 6](#_Toc19194894)

[i. OBSERVATIONS 6](#_Toc19194895)

[ii. RECOMMENDATIONS 7](#_Toc19194896)

[5. MODULE OBSERVATIONS 7](#_Toc19194897)

[a. Network Performance Monitor (NPM) 7](#_Toc19194898)

[i. OBSERVATIONS 7](#_Toc19194899)

[ii. RECOMMENDATIONS 7](#_Toc19194900)

[b. Network Configuration Manager (NCM) 7](#_Toc19194901)

[i. OBSERVATIONS 7](#_Toc19194902)

[ii. RECOMMENDATIONS 7](#_Toc19194903)

[c. NetFlow Traffic Analyzer (NTA) 7](#_Toc19194904)

[i. OBSERVATIONS 7](#_Toc19194905)

[ii. RECOMMENDATIONS 7](#_Toc19194906)

[d. IP Address Manager (IPAM) 7](#_Toc19194907)

[i. OBSERVATIONS 7](#_Toc19194908)

[ii. RECOMMENDATIONS 7](#_Toc19194909)

[e. VOIP and Network Quality Manager (VNQM) 7](#_Toc19194910)

[i. OBSERVATIONS 7](#_Toc19194911)

[ii. RECOMMENDATIONS 7](#_Toc19194912)

[f. User Device Tracker (UDT) 7](#_Toc19194913)

[i. OBSERVATIONS 7](#_Toc19194914)

[ii. RECOMMENDATIONS 7](#_Toc19194915)

[g. Server and Application Monitor (SAM) 8](#_Toc19194916)

[i. OBSERVATIONS 8](#_Toc19194917)

[ii. RECOMMENDATIONS 8](#_Toc19194918)

[h. Patch Manager Integration (PM) 8](#_Toc19194919)

[i. OBSERVATIONS 8](#_Toc19194920)

[ii. RECOMMENDATIONS 8](#_Toc19194921)

[i. Web Performance Monitor (WPM) 8](#_Toc19194922)

[i. OBSERVATIONS 8](#_Toc19194923)

[ii. RECOMMENDATIONS 8](#_Toc19194924)

[j. Storage Resource Monitor (SRM) 8](#_Toc19194925)

[i. OBSERVATIONS 8](#_Toc19194926)

[ii. RECOMMENDATIONS 8](#_Toc19194927)

[k. Virtualization Manager (VMAN) 8](#_Toc19194928)

[i. OBSERVATIONS 8](#_Toc19194929)

[ii. RECOMMENDATIONS 8](#_Toc19194930)

[l. High Availability 8](#_Toc19194931)

[i. OBSERVATIONS 8](#_Toc19194932)

[ii. RECOMMENDATIONS 8](#_Toc19194933)

[m. Log Analyzer (LA) 8](#_Toc19194934)

[i. OBSERVATIONS 8](#_Toc19194935)

[ii. RECOMMENDATIONS 8](#_Toc19194936)

[n. Database Performance Analyzer Integration (DPAIM) 9](#_Toc19194937)

[i. OBSERVATIONS 9](#_Toc19194938)

[ii. RECOMMENDATIONS 9](#_Toc19194939)

[o. Enterprise Operations Console (EOC) 9](#_Toc19194940)

[i. OBSERVATIONS 9](#_Toc19194941)

[ii. RECOMMENDATIONS 9](#_Toc19194942)

[p. Server Configuration Manager (SCM) 9](#_Toc19194943)

[i. OBSERVATIONS 9](#_Toc19194944)

[ii. RECOMMENDATIONS 9](#_Toc19194945)

[q. AppOptics Integration (APM) 9](#_Toc19194946)

[i. OBSERVATIONS 9](#_Toc19194947)

[ii. RECOMMENDATIONS 9](#_Toc19194948)

[r. Engineer’s Toolset (ETS) 9](#_Toc19194949)

[i. OBSERVATIONS 9](#_Toc19194950)

[ii. RECOMMENDATIONS 9](#_Toc19194951)

[6. DATABASE OBSERVATIONS FOR ORION 9](#_Toc19194952)

[a. SQL – Database Settings 9](#_Toc19194953)

[i. OBSERVATIONS 9](#_Toc19194954)

[ii. RECOMMENDATIONS 9](#_Toc19194955)

[b. SQL – Maintenance Plan 10](#_Toc19194956)

[i. OBSERVATIONS 10](#_Toc19194957)

[ii. RECOMMENDATIONS 10](#_Toc19194958)

[7. DATABASE OBSERVATIONS FOR NTA 10](#_Toc19194959)

[a. SQL – Database Settings 10](#_Toc19194960)

[i. OBSERVATIONS 10](#_Toc19194961)

[ii. RECOMMENDATIONS 10](#_Toc19194962)

[b. SQL – Maintenance Plan 10](#_Toc19194963)

[i. OBSERVATIONS 10](#_Toc19194964)

[ii. RECOMMENDATIONS 10](#_Toc19194965)

[8. DATABASE OBSERVATIONS FOR LA 10](#_Toc19194966)

[a. SQL – Database Settings 10](#_Toc19194967)

[i. OBSERVATIONS 10](#_Toc19194968)

[ii. RECOMMENDATIONS 10](#_Toc19194969)

[b. SQL – Maintenance Plan 10](#_Toc19194970)

[i. OBSERVATIONS 10](#_Toc19194971)

[ii. RECOMMENDATIONS 10](#_Toc19194972)

[9. APPENDIX 10](#_Toc19194973)

[a. L1M3 Model Information 10](#_Toc19194974)

[THIS PAGE INTENTIONALLY LEFT BLANK]

# OVERVIEW

<CLIENT> has contracted Loop1 Systems, Inc. to provide a Health Check from a certified SolarWinds Engineer on their existing SolarWinds environment and provide recommendations on these findings.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| A close up of a screen  Description automatically generated | **CURRENT MONITORING LEVELS** | | | | |
| **ENVIRONMENT** | **Ad-Hoc** | **Fragmented** | **Typical** | **Optimized** | **Insightful** |
| **Application** | ☐ | ☐ | ☐ | ☐ | ☐ |
| **Server** | ☐ | ☐ | ☐ | ☐ | ☐ |
| **Database** | ☐ | ☐ | ☐ | ☐ | ☐ |
| **Virtualization** | ☐ | ☐ | ☐ | ☐ | ☐ |
| **Storage** | ☐ | ☐ | ☐ | ☐ | ☐ |
| **Network** | ☐ | ☐ | ☐ | ☐ | ☐ |

[Full L1M3 Model](#_L1M3_Model_Information)

# SUMMARY OF RECOMMENDATIONS

# CURRENT SOFTWARE INVENTORY

### OBSERVATIONS

|  |  |  |  |
| --- | --- | --- | --- |
| **MODULE** | **LICENSE** | **VERSION** | **HEALTH STATUS** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### RECOMMENDATIONS

# GENERAL OBSERVATIONS

## Architecture

### OBSERVATIONS

|  |  |  |
| --- | --- | --- |
| **SERVER** | **HARDWARE** | **HEALTH STATUS** |
| <PRIMARY> | OS: |  |
| CPU: |  |
| RAM: |  |
| DRIVES: |  |
| <APE/AWE/HA> | OS: |  |
| CPU: |  |
| RAM: |  |
| DRIVES: |  |
| <SQL> | SQL VERSION: |  |
| CPU: |  |
| RAM: |  |
| DRIVES: |  |
| SW DB SIZE: |  |
| <NTA SQL> | SQL VERSION: |  |
| CPU: |  |
| RAM: |  |
| DRIVES: |  |
| SW DB SIZE: |  |
| <LA SQL> | SQL VERSION: |  |
| CPU: |  |
| RAM: |  |
| DRIVES: |  |
| SW DB SIZE: |  |

### RECOMMENDATIONS

## Overall Elements and Polling

### OBSERVATIONS

|  |  |  |
| --- | --- | --- |
| **STATISTIC** | **VALUE** | **NOTES** |
| NPM ELEMENTS PER POLLING ENGINE | <PRIMARY>  ELEMENTS:  NODES:  INTERFACES:  VOLUMES:  <APE>  ELEMENTS:  NODES:  INTERFACES:  VOLUMES: |  |
| NPM SYSLOG AND TRAPS | SYSLOGS:  TRAPS:  TRAPVARBINDS: |  |
| NPM POLLING INTERVALS | NODE:  INTERFACE:  VOLUME:  REDISCOVERY: |  |
| NPM STATISTICS POLLING INTERVALS | NODE:  INTERFACE:  VOLUME:  TOPOLOGY:  NODE WARNING LEVEL: |  |
| NPM DATA RETENTION | NODE DETAIL:  NODE HOURLY:  NODE DAILY:  INTERFACE DETAIL:  INTERFACE HOURLY:  INTERFACE DAILY:  EVENTS:  AUDIT LOG:  SYSLOG:  TRAPS:  BASELINE COLLECTION: |  |
| NPM POLLING COMPLETION | <PRIMARY>: %  <APE>: % |  |
| NPM POLLING RATE (LOAD) | <PRIMARY>: %  <APE>: % |  |
| NPM GROUPS | # TOTAL  # DYNAMIC |  |
| NPM DEPENDENCIES | # TOTAL  #AUTO |  |
| SAM APPLICATION MONITORS | # TOTAL  # DOWN  # CRITICAL |  |
| SAM DATA RETENTION | DETAIL:  HOURLY:  DAILY:  EVENT LOG:  BASELINE COLLECTION: |  |
| SAM POLLING RATE  (LOAD) | <PRIMARY>: %  <APE>: % |  |
| APPINSIGHT FOR SQL DATA RETENTION | DETACHED DBs:  HISTORY:  DETAIL: |  |
| APPINSIGHT FOR EXCHANGE DATA RETENTION | DELETED DBs:  MAILBOX HISTORY:  DETAIL: |  |
| NCM NODES | # |  |
| NCM INVENTORY | % FAILING |  |
| NCM CONFIG BACKUPS | % FAILING |  |
| NCM JOBS | # BACKUP ERRORS |  |
| NCM EOS | # OF NODES WITH DATES |  |
| IPAM ELEMENTS | MANUAL SUBNETS: #  DHCP SERVERS: #  DNS SERVERS: # |  |
| IPAM POLLING INTERVALS | DHCP:  DNS:  SUBNETS: |  |
| IPAM DATA RETENTION | EVENTS:  HISTORY: |  |
| VNQM ELEMENTS | IP SLA NODES:  IP SLA OPERATIONS:  VOICE GATEWAYS:  VOIP SITES:  CALL MANAGERS: |  |
| VNQM POLLING INTERVALS | VOICE GATEWAYS:  CALL MANAGERS: |  |
| VNQM DATA RETENTION | IP SLA OPERATIONS:  VOICE GATEWAYS: |  |
| NTA SOURCES | # |  |
| NTA FLOWS PER SECOND | # |  |
| NTA IP ADDRESS GROUPS | # |  |
| NTA RETENTION PERIOD | # |  |
| WPM TRANSACTION MONITORS | # |  |
| WPM DATA RETENTION | DETAIL:  HOURLY:  DAILY:  SCREENSHOT:  CAPTURING: |  |
| UDT ELEMENTS | PORTS:  WATCH LIST:  DOMAIN CONTROLLERS:  WHITE LIST RULES:  ROGUE DEVICES: |  |
| UDT POLLING INTERVALS | LAYER 2:  LAYER 3:  DOMAIN CONTROLLER:  AD USER UPDATE: |  |
| UDT DATA RETENTION | HISTORY:  DETAIL:  HOURLY:  DAILY: |  |
| VMAN ELEMENTS | CLUSTERS:  DATACENTERS:  VCENTERS:  HOSTS:  VMS: |  |
| VMAN POLLING INTERVALS | STANDARD:  CONFIGURATION: |  |
| VMAN DATA RETENTION | DETAIL:  HOURLY:  DAILY: |  |
| SRM ELEMENTS | ARRAYS:  PROVIDERS: |  |
| SRM POLLING INTERVALS | STATISTICS:  REDISCOVERY:  TOPOLOGY: |  |
| LA ELEMENTS | NODES: |  |
| LA DATA RETENTION | SYSLOG:  TRAPS:  WINDOWS EVENTS:  VMWARE EVENTS: |  |
| SCM ELEMENTS | NODES:  PROFILES: |  |
| SCM POLLING SETTINGS | DETECTION ENABLED: Y/N  EXCLUSIONS: |  |
| SCM DATA RETENTION | DETAIL:  HOURLY:  DAILY: |  |

### RECOMMENDATIONS

## Website Design

### OBSERVATIONS

### RECOMMENDATIONS

## Custom Properties

### OBSERVATIONS

### RECOMMENDATIONS

## Groups and Dependencies

### OBSERVATIONS

### RECOMMENDATIONS

## Alerting

### OBSERVATIONS

### RECOMMENDATIONS

## Reports

### OBSERVATIONS

### RECOMMENDATIONS

## Accounts

### OBSERVATIONS

### RECOMMENDATIONS

## Windows Event Logs

### OBSERVATIONS

### RECOMMENDATIONS

## SolarWinds Logs

### OBSERVATIONS

### RECOMMENDATIONS

# MODULE OBSERVATIONS

## Network Performance Monitor (NPM)

### OBSERVATIONS

### RECOMMENDATIONS

## Network Configuration Manager (NCM)

### OBSERVATIONS

### RECOMMENDATIONS

## NetFlow Traffic Analyzer (NTA)

### OBSERVATIONS

### RECOMMENDATIONS

## IP Address Manager (IPAM)

### OBSERVATIONS

### RECOMMENDATIONS

## VOIP and Network Quality Manager (VNQM)

### OBSERVATIONS

### RECOMMENDATIONS

## User Device Tracker (UDT)

### OBSERVATIONS

### RECOMMENDATIONS

## Server and Application Monitor (SAM)

### OBSERVATIONS

### RECOMMENDATIONS

## Patch Manager Integration (PM)

### OBSERVATIONS

### RECOMMENDATIONS

## Web Performance Monitor (WPM)

### OBSERVATIONS

### RECOMMENDATIONS

## Storage Resource Monitor (SRM)

### OBSERVATIONS

### RECOMMENDATIONS

## Virtualization Manager (VMAN)

### OBSERVATIONS

### RECOMMENDATIONS

## High Availability

### OBSERVATIONS

### RECOMMENDATIONS

## Log Analyzer (LA)

### OBSERVATIONS

### RECOMMENDATIONS

## Database Performance Analyzer Integration (DPAIM)

### OBSERVATIONS

### RECOMMENDATIONS

## Enterprise Operations Console (EOC)

### OBSERVATIONS

### RECOMMENDATIONS

## Server Configuration Manager (SCM)

### OBSERVATIONS

### RECOMMENDATIONS

## AppOptics Integration (APM)

### OBSERVATIONS

### RECOMMENDATIONS

## Engineer’s Toolset (ETS)

### OBSERVATIONS

### RECOMMENDATIONS

# DATABASE OBSERVATIONS FOR ORION

## SQL – Database Settings

### OBSERVATIONS

### RECOMMENDATIONS

## SQL – Maintenance Plan

### OBSERVATIONS

### RECOMMENDATIONS

# DATABASE OBSERVATIONS FOR NTA

## SQL – Database Settings

### OBSERVATIONS

### RECOMMENDATIONS

## SQL – Maintenance Plan

### OBSERVATIONS

### RECOMMENDATIONS

# DATABASE OBSERVATIONS FOR LA

## SQL – Database Settings

### OBSERVATIONS

### RECOMMENDATIONS

## SQL – Maintenance Plan

### OBSERVATIONS

### RECOMMENDATIONS

# APPENDIX

## L1M3 Model Information

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| L1M3 | Ad-Hoc | Fragmented | Typical | Optimized | Insightful |
| **Application** | Outages addressed only when end users complain. Extensive, unaddressed application security risks. | Application owners attempting to monitor and address vulnerabilities on their own. | Business applications are mostly monitored, false positive alerts are rampant. Audits are done, but vulnerabilities remain. | Correlated application monitoring with automated provisioning and alerting. Consistent audit and remediation. | Intelligent application monitoring data informs forecasts and budgets with positive impacts to financial performance. |
| **Server** | Ad-hoc server provisioning, excessive licensing costs, reactionary server maintenance, no patching standards. | Limited and inaccurate server documentation. Monitoring only for mission critical servers. Inadequate compliance and patching solutions. | Procedural server provisioning. Basic server documentation with limited correlation visibility. Regular patching efforts. Excessive server alerts. | Automated, correlated performance, event and configuration visibility. Effective vulnerability remediation and alerting solutions. | Data shared by DevOps teams. Intelligent hybrid workload distribution with dynamic monitoring, complete compliance and precision alerting. |
| **Database** | Vendor required databases scattered among servers with break-fix support only. Unmitigated data risks. | Accidental DBA’s focused only on critical systems. Severe sprawl, no tools for audit or compliance. | Dedicated administrators, monitoring key indicators, patching and applying basic security best practices. Limited information-sharing. | Correlated database utilization mapping and performance data. Shared visibility, quality alerts and compliance. | Business insights from multi-platform, federated data to control costs, inform business strategy and increase revenue. |
| **Virtualization** | Ad-hoc hosts, no central administration. Default admin access, severe sprawl. Unsupported ‘free’ hypervisors. | Some use of native tools for administration and reporting. Severe resource conflicts and orphaned VM’s. | Regular use of vendor administration tools or basic third-party monitoring solutions. Alerting on severe issues, no planning tools. | Specialized monitoring, sizing and capacity plans. Automated alerting and dashboards with cross-functional correlation. | Hybrid environment with dynamic load processing. Integrations drive business impact reporting and incident management. |
| **Storage** | Little to no investment in shared arrays. Wasteful disk allocations, ineffective redundancy, no monitoring. | Shared storage solutions on a per cluster basis. Severe allocation issues, app owners devising their own alerts. | Improved visibility to sprawl, over-allocation and orphaned data, limited security, compliance and remediation of issues. | Quality performance, allocation and correlated utilization data for on-prem and cloud with full audit and compliance. | Pro-active management of tiered storage. Integrated tools allow informed performance and financial decisions across teams. |
| **Network** | No standards, random device procurement, break-fix administration, Limited monitoring via ICMP, no SNMP visibility. | Some SNMP monitored devices. Spreadsheet based device tracking, excessive false alerts, minimal compliance. | Full SNMP monitoring. Simple alerts, dashboards and reports. Standards for back-up, compliance and device authentication. | Reduced alert noise, user centric dashboards, correlated traffic and application utilization. Compliance remediation. | Integrated and automated device and incident management. Utilization data informs technical and business decisions. |