Top 10 Service Items - Staying ahead of system issues

MIRION Connect 24
Annual Users' Conference

Introduction

SIS, Life Cycle Managment

- Walt Karrenbauer - Director, Life Cycle Management
  - wkarrenbauer@mirion.com, (412) 316-6724
  - 13 Years w/ Mirion, 10 yrs in LCM
- Chuck Crow - Mgr, LCM AIM Systems
  - ccrow@mirion.com, (972) 523-6498
  - 13 Years w/ Mirion, 9 yrs in LCM
- Brian Sewell - Mgr, LCM Cyber Security
  - bsewell@mirion.com, (757) 338-6046
  - 10 Years w/Mirion, 7 yrs in LCM

Introduction - LCM Engineering Team

LCM, AIM Systems Engineering Team

- Luis Abcede
- Roy Cassel
- Marcus Chin
- Cliff Sipes
- Chris Tinker

LCM Cyber Security Engineering Team

- Grant Logan
- Bill Villaire

How to Stay ahead of System Issues

Agenda

- General
- Personnel
- System Hardware
- AIM Software
- Cyber Software
- After the Issue Occurs
- OnService to ServiceMax

General

- Course is a "Top Ten" and more.
  - Purpose of today's session is to try and help you formulate Maintenance Strategies to aide in the day-to-day support of your systems.
- Today's AIM System and Technology are exponentially more advanced and tightly integrated than systems of ten or twenty years ago.
- No magic bullets that will prevent all failures, but sticking to a regular maintenance plan will have a positive impact.
- Run to Failure is not an option in supporting a good maintenance strategy
- MIRION LCM Team is here to partner with your site in providing support.
  - Goal is to help maintain your systems function and keep it running at its optimal state.

Personnel - Skillset and Training

Do your System Administrators possess the necessary background to effectively manage the AIM SCS?

Skillsets for an AIM SCS System Administrator

- Most important aspect of a good maintenance plan is the people.
- Would you take your brand-new Ferrari to the Bicycle Shop to have the engine worked on?
  - AIM Administration
    - Alarm, Camera, and Device Administration
  - Microsoft Windows Administration
    - Local and domain level, Event Viewer Logs, Active Directory, Group Policy, Application Control (AppLocker)
    - Windows administration functions such as gpupdate /force from a command prompt.
    - Basic hardware (Servers/Workstations)
    - Understanding / troubleshooting of TCP/IP networks
  - Oracle Administration
    - Start and Stop Oracle services, for example the Oracle Listener or Oracle Database.
    - Executing basic SQL statements, such as select, update, and delete.
    - Backing up and restore the database.

Personnel - Skillset and Training

- Basic understanding of Cyber components
  - Switches – commands to login, check port statuses, unlock security violations – sticky MAC
  - Trellix ePO – login and check basic configuration items for HIPS, Virus Scan, and SolidCore

- Other
  - Architecture – Client/Server application
  - What applications run where
  - Where is hardware located and how is it connected
  - Basic Development tools for compiling code
  - Troubleshooting
  - Is the personality appropriate to be effective in your environment

Personnel - Skillset and Training

Do your System Administrators possess the necessary Training to effectively manage your AIM SCS?

Training for an AIM SCS System Administrator

- Standard Course Offerings related to Administration
  - AIM System Administrator
  - Cyber Security Systems Training
  - Hardware Training
- Mirion can customize training to focus on parts of your systems
  - Arrange for Integrated Products, COTS Training - i.e. Qognify, Cisco, Trellix, Acronis, etc...
- Can be done at your Site, in Mirion offices, or via the Web.
- Use your site visits by LCM an opportunity for informal training and Q&A.
  - Use PM and Cyber Patch visits to know what is being updated and why
  - If there is other feedback on desired new features, functions, or out of the ordinary support that would be helpful to the site, please discuss it with your field engineer and they can bring it back the organization.

System Hardware

- All seem simple but our OE suggests that these common items are not always regularly maintained or part of a program.
  - Make Preventative Maintenance a priority and not an afterthought.
  - Keep Hardware clear of Dust and Debris
    - Lack of cleaning can cause the component a shorter life than expected, hard component failures, and intermittent issues
  - Check hard drives regularly
    - Systems are designed to tolerate one drive failure
      - However, two requires system rebuild which is not part of your LCM contract
    - Don't let failed drives sit too long because the second drive will eventually fail.
  - Periodic Shut down and restart
    - Support health of Memory, CPU, overall system health.
  - Spares on Hand
    - Spare Workstations and Servers (1 or 2)
    - Hard Drives for Servers and Workstations
      - Scanned and in the Cyber Program for quicker turn around when drive fails
    - Spare Control Panels, IO Panels, Cameras, Encoders, and other system components

- Procurement of Spares can be made through **Jason Clark, jaclark@mirion.com**

AIM Maintenance

Weekly Maintenance

- Check AIM Host total CPU and Memory utilization so it is compared to your baseline
- Check AIM Logs looking for errors or irregularities
- Check Windows Logs looking for warnings, errors, and irregularities
- Check Server Status, checking to see if there are any warnings or failures
- Check all server drives - Flashing amber/green = predicts the drive will fail, Flashing amber = drive is not configured and predicts the drive will fail, and Solid amber = drive has failed
- Check LINSYS health looking for Rails DOWN, In Progress, or Rails toggling between UP and DOWN
- Check Oracle Exports, verify scheduled night exports exist

AIM Maintenance

Monthly Maintenance

- Perform Backups of all systems

Semi-Annual Maintenance

- Review the User Rights on the Domain
- Review the PSCS_User and the PSCS_Video rights on the Hosts
- Review the Oracle SQLNet parameters
- Test AIM Failover
- Reboot servers (shutdown and restart), this can be done with the Failover process above on the backup Host server. Once completed the system is on the original host and both servers have been cold booted.
- Remove Dust from all equipment (Servers, Workstations, Switches, Firewalls, etc.)
- Examine Network Switch Logs

AIM Maintenance

Annual Maintenance

- Disk De-Fragmentation
  - Keeps drives optimized and allows for faster application execution
  - When de-fragmenting drive we suggest performing this on backup Host with AIM stopped
  - When de-fragmenting the Oracle drive (typically Z: drive) the Oracle services must be stopped
- Oracle backup
  - A recovery point if an accidental change or corruption occurs.
- Remove Dust from all equipment (Servers, Workstations, Switches, Firewalls, etc.)
  - Increases system component longevity

AIM Maintenance

Cyber Software

- Review backup status and storage capacity
  - Current backups are needed during disaster recovery
- Review appliance logs
  - Firewall - review for any errors and identify any issues
  - SIEM - review for devices not receiving logs (Red or Yellow flags)
- Review ePolicy Orchestrator logs
    - Anti-Virus and Firewall - Review blocked applications ports
    - Detected Rogue and USB violations - Review for unauthorized devices
- Review VMWare or other Hypervisor logs - Review errors
- Review local and domain user accounts for unauthorized users (testuser ect.)

AIM Maintenance

Cyber Proficiency

- Be familiar with cyber security controls built into the AIM SCS
  - **Troubleshooting** and **Investigating**
    - System, User, and Network events
    - Cyber alarms sent to AIM
  - **Switches** - Cyber integration, isolation and routing
  - **Antivirus** - Daily, Weekly, On-Access, On-Demand Scans, and Detection Signatures
  - **Firewalls** - Application's unique port/ports
  - **USB** - Whitelisting by device instance path
  - **Rogue System Detection** – MAC Address monitoring

AIM Maintenance

Cyber Auditing Tools

- Recently developed tools that can be customized to support your site
  - CDA Baseline Analyzer
  - HIDS Scripts
  - NRC Inspection Support
  - Services & CVE Evaluations

- Continue to offer traditional services of Microsoft, Trellix, and other 3rd party patching.

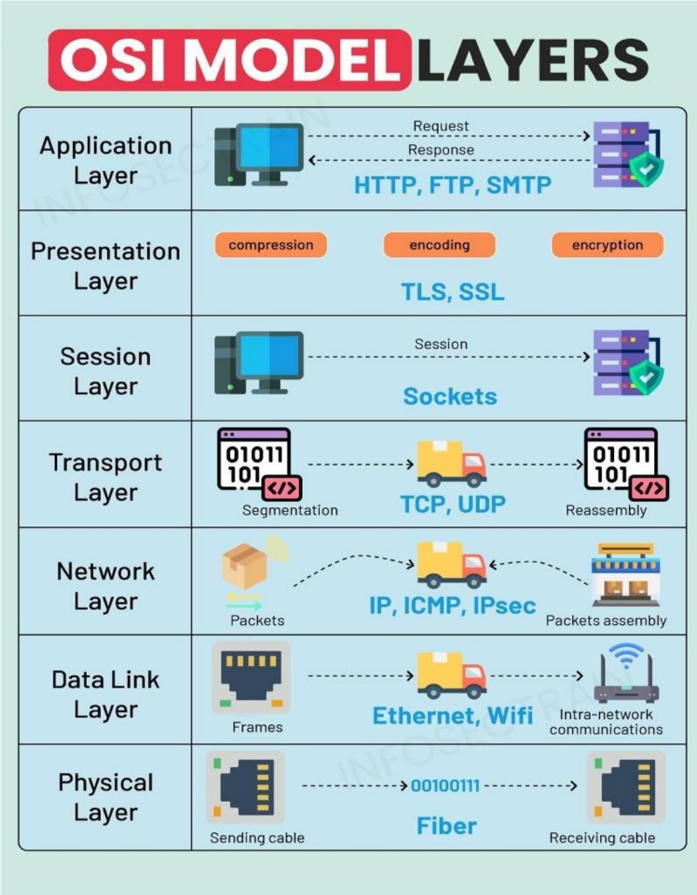
After the Issue Occurs

Troubleshooting

- Start at the Physical Layer and move up the OSI Model Layers.

What is the OSI Model?

OSI Model is a network model having seven different layers. This model was first introduced in 1974 by the ISO (International Organization of Standardization). This model helps to transfer data over the network from one computer device to another. This model is the standard adopted all over the globe.



After the Issue Occurs

Troubleshooting

1. Keep it Simple
   - Is it plugged in?
   - Is it on?
   - Windows or application crash
2. Identify the Problem
   - Gathering information from log files and error messages
   - Identifying symptoms
   - Determining if any recent changes were made
   - Duplicating the problem on MTS
   - Avoid troubleshooting multiple problems one at a time, narrow the scope of the problem
3. Troubleshooting method – OSI bottom up – troubleshooting by going from the physical layer (layer 1) up to the application layer (layer 7)

After the Issue Occurs

Troubleshooting

4. Establish a Theory of Probable Cause
   - Questioning the obvious to identify the cause of the problem
   - Approach of bottom-to-top for layered technologies
5. Test the Theory to Determine the Cause
6. Establish a Plan of Action and Implement the Fix
   - Some fixes require reboots or other more significant forms of downtime
   - You may need to document a series of complex steps, commands and scripts
   - Need to back up data that might be put at risk for the fix
7. Verify Full System Functionality and Implement Preventive Measures

After the Issue Occurs

Logs

- Collection of Logs in a timely manner
  - Many logs are overwritten in as little as a day.
  - Once the logs are overwritten there is not much opportunity to determine the cause

OnService

- Include as many details as possible in the WO’s
- Include a full description of the problem including dates and times.
- What troubleshooting was done and what were the results
- Were there any changes to the systems or environment (ie... password changes, hardware changes, weather events, power outages, etc...)
- - Think - "who, what, where, when" when reporting a problem

Online Experience

Upcoming Change from OnService to ServiceMax

- ServiceMax is the proven CRM tool used by the entire Mirion organization that utilizes the Salesforce platform.
- Includes features that are inclusive of current platforms that are in line with today's technology.
- Ticketing will be similar but will allow for easier communications with better searching and reporting feature.
- Migration is planned for late 3rd to early 4th Qtr of this year
- Details are limited right now but will be communicated as a transition timeline is known.

Thank you