==========

==========

CATEGORY: EventLogs

==========

==========

Windows Event Logs are a primary forensic and operational data source. These SOPs ensure all log access, filtering, and modification performed through RDAM Script Wizard is controlled, auditable, and aligned with enterprise security and compliance standards.

SOP 1 – Get Recent Event Log Entries

Script Name: Get Recent Event Log Entries **Category:** EventLogs **Version:** 1.0 **Approved By:** IT Operations / Security

1. Purpose

This script retrieves the most recent entries from a specified Windows Event Log. It provides a standardized, auditable method for reviewing system, security, and application events during troubleshooting or monitoring.

2. Scope

- **Systems:** Windows servers and workstations accessible to RDAM.
- **Logs:** System, Application, Security, and custom logs.
- **Authorized Personnel:**
    - System administrators
    - Security analysts
    - Helpdesk Tier-2/3
    - Incident response teams

3. Definitions

- **Event Log:** A structured record of system, security, and application events.
- **Event ID:** Numeric identifier for a specific type of event.
- **Provider:** Source of the event (e.g., Microsoft-Windows-Security-Auditing).

4. Preconditions

- Operator must have read access to the target log.
- Remote system must be reachable (if remote execution is supported).
- Log must exist on the system.

5. Required Inputs

- Log name (e.g., System, Application, Security)
- Number of recent entries to retrieve (e.g., 50, 100, 500)

6. Procedure Steps

1. **Input Collection**
    - Wizard prompts for log name and entry count.
    - Validate log name exists on target system.
    - Validate entry count is numeric and within allowed range.
2. **Log Access Initialization**
    - Connect to local or remote event log provider.
    - If connection fails, abort and log.
3. **Event Retrieval**
    - Query the log for the most recent entries.
    - Sort by timestamp descending.
    - Limit results to requested count.
4. **Data Extraction**
    - Extract fields such as:
        - Timestamp
        - Event ID
        - Level (Information, Warning, Error, Critical)
        - Provider
        - Message text
5. **Output Formatting**
    - Present results in structured table or JSON format.
    - Highlight critical or error events if applicable.

6. **Logging**
    - Log operator, log name, entry count, timestamp.

7. Expected Output

- A list of recent events with timestamps, IDs, severity, and messages.

8. Post-Execution Validation

- Operator may cross-check with Event Viewer.
- Security team may correlate with SIEM.

9. Error Handling

- Log not found
- Access denied
- Remote system unreachable
- Invalid entry count

10. Security Considerations

- Security logs contain sensitive data; restrict access.
- Avoid exporting logs outside approved channels.

11. Audit Logging Requirements

- Operator ID
- Log name
- Entry count
- Timestamp
- Success/Failure

12. Organizational Benefit Statement

This script provides a consistent, auditable method for retrieving recent event logs, improving troubleshooting efficiency and supporting security monitoring.

SOP 2 – Search Event Logs by ID

Script Name: Search Event Logs by ID **Category:** EventLogs

1. Purpose

This script searches a specified Windows Event Log for entries matching a specific Event ID. It supports targeted troubleshooting, compliance checks, and security investigations.

2. Scope

- System, Application, Security, and custom logs
- Local or remote systems (if supported)

3. Definitions

- **Event ID:** Numeric identifier representing a specific event type.
- **Filter Query:** A targeted search against event logs.

4. Preconditions

- Operator must have read access to the log.
- Event ID must be known and valid.
- Log must exist.

5. Required Inputs

- Log name
- Event ID
- Optional: Time range filter

6. Procedure Steps

1. **Input Collection**
    - Wizard prompts for log name and Event ID.
    - Validate Event ID is numeric.
2. **Log Resolution**
    - Confirm log exists on target system.
3. **Query Construction**
    - Build filter for Event ID.
    - If time range provided, include in filter.
4. **Event Retrieval**
    - Query log for matching events.

- Handle large result sets with pagination if needed.

5. **Data Extraction**
    - Extract:
        - Timestamp
        - Event ID
        - Provider
        - Level
        - Message
6. **Output Formatting**
    - Present results in structured format.
    - Highlight critical events.
7. **Logging**
    - Log operator, log name, Event ID, timestamp.

7. Expected Output

- A filtered list of events matching the specified Event ID.

8. Post-Execution Validation

- Operator may validate results using Event Viewer.
- Security team may correlate with SIEM.

9. Error Handling

- Event ID not found
- Log not found
- Access denied
- Invalid time range

10. Security Considerations

- Searching security logs may reveal sensitive information; restrict access.
- Ensure Event ID searches align with approved investigative procedures.

11. Audit Logging Requirements

- Operator ID

- Log name
- Event ID
- Timestamp
- Result count

12. Organizational Benefit Statement

This script provides a precise, auditable method for locating specific events, improving troubleshooting speed and supporting forensic investigations.

SOP 3 – Clear Event Log

Script Name: Clear Event Log **Category:** EventLogs

1. Purpose

This script clears all entries from a specified Windows Event Log. It is used during system preparation, controlled maintenance, or after exporting logs for forensic purposes.

2. Scope

- System, Application, and custom logs
- Security log clearing may require elevated permissions and strict approvals

3. Definitions

- **Log Clearing:** Removing all entries from a log.
- **Backup Before Clear:** Optional export of log contents before deletion.

4. Preconditions

- Operator must have write/clear permissions for the log.
- Clearing must be authorized (e.g., maintenance window, forensic workflow).
- If required, log must be exported before clearing.

5. Required Inputs

- Log name
- Optional: Backup path before clearing

6. Procedure Steps

1. **Input Collection**

- Wizard prompts for log name and optional backup path.

2. **Log Resolution**
    - Confirm log exists.
3. **Optional Backup**
    - If backup path provided:
        - Export log to EVTX file
        - Confirm file exists
        - Log backup operation
4. **Clear Confirmation**
    - Script may require explicit confirmation depending on policy.
5. **Clear Operation**
    - Clear the log using appropriate API/cmdlet.
6. **Post-Clear Verification**
    - Requery log to confirm entry count is zero.
7. **Logging**
    - Log operator, log name, backup path (if used), timestamp.

7. Expected Output

- Confirmation that the log was cleared.
- Optional confirmation of backup file.

8. Post-Execution Validation

- Operator may verify via Event Viewer.
- Security team may validate backup integrity.

9. Error Handling

- Access denied
- Log not found
- Backup path invalid
- Clear operation failed

10. Security Considerations

- Clearing logs can impact forensic investigations; strict approvals required.
- Security log clearing should follow incident response procedures.

11. Audit Logging Requirements

- Operator ID
- Log name
- Backup path (if used)
- Timestamp
- Success/Failure

12. Organizational Benefit Statement

This script ensures log clearing is performed safely, consistently, and with full auditability, supporting maintenance workflows and forensic procedures.