==

CATEGORY: WindowsLogs

==

Windows event logs are the forensic backbone of diagnostics, security investigations, compliance audits, and operational monitoring. These SOPs ensure every log-related action performed through RDAM Script Wizard is **controlled**, **auditable**, and aligned with enterprise operational and security standards.

SOP 1 – Get Event Logs

Script Name: Get Event Logs **Category:** WindowsLogs **Version:** 1.0 **Approved By:** IT Operations / Security**

1. Purpose

This script retrieves a list of available Windows event logs, supporting discovery, troubleshooting, and audit preparation.

2. Scope

- Windows servers and workstations
- Classic and modern event logs

3. Definitions

- **Event Log:** A structured record of system, application, and security events.

4. Preconditions

- Operator must have permission to query event logs.

5. Required Inputs

- None

6. Procedure Steps

1. Log Enumeration
    - Retrieve all event logs.
    - Extract log name, record count, and size.
2. Output Formatting
    - Present structured log list.
3. Logging
    - Log operator and timestamp.

7. Expected Output

- List of event logs with metadata.

8. Post-Execution Validation

- Operator may verify via Event Viewer.

9. Error Handling

- Access denied
- Log service unavailable

10. Security Considerations

- Log metadata may reveal system activity patterns.

11. Audit Logging Requirements

- Operator ID
- Timestamp

12. Organizational Benefit Statement

This script provides a consistent, auditable method for enumerating event logs, supporting diagnostics and compliance.

SOP 2 – Get Event Log Details

Script Name: Get Event Log Details **Category:** WindowsLogs**

1. Purpose

This script retrieves detailed entries from a specified event log, supporting troubleshooting, forensic analysis, and compliance.

2. Scope

- Windows servers and workstations
- All event logs

3. Definitions

- **Event Entry:** A single record containing event metadata and message.

4. Preconditions

- Operator must have permission to read the log.
- Log must exist.

5. Required Inputs

- Log name
- Optional: Entry count
- Optional: Event level filter

6. Procedure Steps

1. Input Collection
    - Wizard prompts for log name and optional filters.
2. Validation
    - Confirm log exists.
3. Entry Retrieval
    - Retrieve recent entries.
    - Apply filters (Critical, Error, Warning, Info).
4. Output Formatting
    - Present structured event list.
5. Logging
    - Log log name, filters, operator, timestamp.

7. Expected Output

- Detailed event entries.

8. Post-Execution Validation

- Operator may verify via Event Viewer.

9. Error Handling

- Log not found
- Access denied
- Invalid filter

10. Security Considerations

- Event messages may contain sensitive data.

11. Audit Logging Requirements

- Operator ID
- Log name
- Filters
- Timestamp

12. Organizational Benefit Statement

This script provides a controlled, auditable method for retrieving event log entries, supporting diagnostics and forensic workflows.

SOP 3 – Clear Event Log

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

1. Purpose

This script clears all entries from a specified event log, supporting maintenance, cleanup, and troubleshooting.

2. Scope

- Windows servers and workstations
- All event logs

3. Definitions

- **Log Clearing:** Removing all entries from a log.

4. Preconditions

- Operator must have administrative rights.
- Clearing must be authorized.
- Log must exist.

5. Required Inputs

- Log name

6. Procedure Steps

1. Input Collection
   - Wizard prompts for log name.
2. Validation
   - Confirm log exists.
   - Confirm authorization.
3. Clear Operation
   - Clear event log.
4. Post-Clear Verification
   - Confirm log is empty.
5. Logging
   - Log log name, operator, timestamp.

7. Expected Output

- Confirmation of log clearing.

8. Post-Execution Validation

- Operator may verify via Event Viewer.

9. Error Handling

- Access denied
- Log not found

- Clearing blocked by policy

10. Security Considerations

- Clearing logs may impact forensic investigations.

11. Audit Logging Requirements

- Operator ID
- Log name
- Timestamp

12. Organizational Benefit Statement

This script ensures log clearing is performed safely and with full accountability, supporting maintenance and troubleshooting.

SOP 4 – Export Event Log

Script Name: Export Event Log **Category:** WindowsLogs**

1. Purpose

This script exports an event log to a file, supporting audits, investigations, and archival.

2. Scope

- Windows servers and workstations
- All event logs

3. Definitions

- **Export:** Saving log entries to an external file.

4. Preconditions

- Operator must have permission to read the log.
- Export path must be valid.

5. Required Inputs

- Log name
- Export path

6. Procedure Steps

1. Input Collection
    - Wizard prompts for log name and export path.
2. Validation
    - Confirm log exists.
    - Confirm path is valid.
3. Export Operation
    - Export log to file.
4. Post-Export Verification
    - Confirm file created.
5. Logging
    - Log log name, export path, operator, timestamp.

7. Expected Output

- Confirmation of log export.

8. Post-Execution Validation

- Operator may verify via file system.

9. Error Handling

- Access denied
- Invalid path
- Log not found

10. Security Considerations

- Exported logs may contain sensitive data; secure storage required.

11. Audit Logging Requirements

- Operator ID
- Log name
- Export path
- Timestamp

12. Organizational Benefit Statement

This script ensures log export is performed safely and consistently, supporting audits and investigations.

SOP 5 – Get Recent Critical and Error Events

Script Name: Get Recent Critical and Error Events **Category:** WindowsLogs**

1. Purpose

This script retrieves recent high-severity events, supporting troubleshooting, incident response, and monitoring.

2. Scope

- Windows servers and workstations
- System, Application, and Security logs

3. Definitions

- **Critical/Error Events:** High-severity events requiring attention.

4. Preconditions

- Operator must have permission to read logs.

5. Required Inputs

- Optional: Time range

6. Procedure Steps

1. Input Collection
    - Wizard prompts for optional time range.
2. Event Retrieval
    - Query System, Application, and Security logs.
    - Filter for Critical and Error events.
3. Output Formatting
    - Present structured event summary.
4. Logging
    - Log filters, operator, timestamp.

7. Expected Output

- List of recent high-severity events.

8. Post-Execution Validation

- Operator may verify via Event Viewer.

9. Error Handling

- Access denied
- Log unavailable

10. Security Considerations

- Events may reveal sensitive operational failures.

11. Audit Logging Requirements

- Operator ID
- Filters used
- Timestamp

12. Organizational Benefit Statement

This script provides a fast, auditable method for retrieving critical events, supporting incident response and diagnostics.

SOP 6 – Get Windows Update Event Logs

Script Name: Get Windows Update Event Logs **Category:** WindowsLogs**

1. Purpose

This script retrieves Windows Update–related events, supporting troubleshooting, compliance, and patch-management workflows.

2. Scope

- Windows servers and workstations
- Windows Update logs

3. Definitions

- **Update Event:** Log entry related to update installation or failure.

4. Preconditions

- Operator must have permission to read logs.

5. Required Inputs

- Optional: Date range
- Optional: Event level

6. Procedure Steps

1. Input Collection
    - Wizard prompts for optional filters.
2. Event Retrieval
    - Query Windows Update logs.
    - Apply filters.
3. Output Formatting
    - Present structured update-event list.
4. Logging
    - Log filters, operator, timestamp.

7. Expected Output

- List of update-related events.

8. Post-Execution Validation

- Operator may verify via Event Viewer.

9. Error Handling

- Access denied
- Log unavailable

10. Security Considerations

- Update logs may reveal vulnerability exposure.

11. Audit Logging Requirements

- Operator ID
- Filters used

- Timestamp

12. Organizational Benefit Statement

This script provides a controlled, auditable method for retrieving update logs, supporting patch management and troubleshooting.