==

CATEGORY: WinRM

==

Windows Remote Management (WinRM) is foundational for remote administration, PowerShell remoting, automation frameworks, and secure remote execution. These SOPs ensure every WinRM-related action performed through RDAM Script Wizard is **controlled**, **auditable**, and aligned with **enterprise operational and security standards**.

SOP 1 – Get WinRM Configuration

Script Name: Get WinRM Configuration **Category:** WinRM **Version:** 1.0 **Approved By:** IT Operations / Security

1. Purpose

This script retrieves the current WinRM configuration, supporting troubleshooting, compliance validation, and remote-management readiness checks.

2. Scope

- Windows servers and workstations
- Local or remote systems (if supported)

3. Definitions

- **WinRM Listener:** Endpoint that accepts remote connections.
- **TrustedHosts:** List of allowed remote hosts for non-domain scenarios.

4. Preconditions

- Operator must have permission to query WinRM settings.
- WinRM service must be installed.

5. Required Inputs

- None

6. Procedure Steps

1. Retrieve Service Status
    - Check if WinRM service is running.
2. Retrieve Listener Configuration
    - Extract HTTP/HTTPS listeners.
    - Retrieve certificate bindings (if HTTPS).
3. Retrieve WinRM Settings
    - Authentication settings
    - TrustedHosts
    - Max concurrent operations
    - Max memory per shell
4. Output Formatting
    - Present structured WinRM configuration summary.
5. Logging
    - Log operator and timestamp.

7. Expected Output

- Consolidated WinRM configuration.

8. Post-Execution Validation

- Operator may verify via `winrm get winrm/config`.

9. Error Handling

- Access denied
- WinRM not installed
- Listener query failure

10. Security Considerations

- WinRM configuration may reveal sensitive remote-access settings.

11. Audit Logging Requirements

- Operator ID

- Timestamp

12. Organizational Benefit Statement

This script provides a consistent, auditable method for retrieving WinRM configuration, supporting troubleshooting and compliance.

SOP 2 – Enable WinRM

Script Name: Enable WinRM **Category:** WinRM

1. Purpose

This script enables WinRM on a system, supporting remote administration, automation, and PowerShell remoting.

2. Scope

- Windows servers and workstations
- Domain-joined and standalone systems

3. Definitions

- **Enable WinRM:** Configure listeners, firewall rules, and service startup.

4. Preconditions

- Operator must have administrative rights.
- Action must be authorized.

5. Required Inputs

- Optional: Enable HTTPS listener
- Optional: Certificate thumbprint

6. Procedure Steps

1. Input Collection
    - Wizard prompts for HTTPS and certificate options.
2. Service Configuration
    - Start WinRM service.
    - Set startup type to Automatic.
3. Listener Configuration

    - Create HTTP listener.
    - If HTTPS selected, bind certificate.
4. Firewall Configuration
    - Enable WinRM firewall rules.
5. Post-Enable Verification
    - Confirm listeners active.
    - Confirm service running.
6. Logging
    - Log listener type, operator, timestamp.

7. Expected Output

- Confirmation that WinRM is enabled.

8. Post-Execution Validation

- Operator may verify via `Test-WsMan`.

9. Error Handling

- Certificate not found
- Access denied
- Listener creation failure

10. Security Considerations

- HTTPS listener recommended for secure environments.
- TrustedHosts should not be broadly configured.

11. Audit Logging Requirements

- Operator ID
- Listener type
- Timestamp

12. Organizational Benefit Statement

This script ensures WinRM enablement is performed safely and consistently, supporting remote administration and automation.

SOP 3 – Disable WinRM

Script Name: Disable WinRM **Category:** WinRM

1. Purpose

This script disables WinRM, supporting security hardening, incident response, and configuration rollback.

2. Scope

- Windows servers and workstations
- Domain-joined and standalone systems

3. Definitions

- **Disable WinRM:** Remove listeners and stop service.

4. Preconditions

- Operator must have administrative rights.
- Action must be authorized.

5. Required Inputs

- None

6. Procedure Steps

1. Listener Removal
    - Remove HTTP/HTTPS listeners.
2. Service Shutdown
    - Stop WinRM service.
    - Set startup type to Disabled.
3. Firewall Configuration
    - Disable WinRM firewall rules.
4. Post-Disable Verification
    - Confirm listeners removed.
    - Confirm service stopped.
5. Logging

    - Log operator and timestamp.

7. Expected Output

- Confirmation that WinRM is disabled.

8. Post-Execution Validation

- Operator may verify via `winrm enumerate winrm/config/listener`.

9. Error Handling

- Access denied
- Listener removal failure

10. Security Considerations

- Disabling WinRM may break remote-management workflows.

11. Audit Logging Requirements

- Operator ID
- Timestamp

12. Organizational Benefit Statement

This script ensures WinRM disablement is performed safely and with full accountability, supporting security hardening and incident response.

SOP 4 – Test WinRM Connectivity

Script Name: Test WinRM Connectivity **Category:** WinRM

1. Purpose

This script tests WinRM connectivity to a remote system, supporting troubleshooting, validation, and remote-management readiness.

2. Scope

- Windows servers and workstations
- Domain-joined and standalone systems

3. Definitions

- **Connectivity Test:** Validates listener, firewall, and authentication.

4. Preconditions

- Operator must have permission to test remote connectivity.
- Remote system must be reachable.

5. Required Inputs

- Remote computer name or IP

6. Procedure Steps

1. Input Collection
    - Wizard prompts for remote host.
2. Connectivity Test
    - Attempt WinRM connection.
    - Capture:
        - Listener response
        - Authentication result
        - Error details
3. Output Formatting
    - Present structured connectivity results.
4. Logging
    - Log remote host, operator, timestamp.

7. Expected Output

- Connectivity status and diagnostic details.

8. Post-Execution Validation

- Operator may verify via `Test-WsMan`.

9. Error Handling

- Host unreachable
- Authentication failure
- Listener not configured

10. Security Considerations

- Testing connectivity may reveal network topology.

11. Audit Logging Requirements

- Operator ID
- Remote host
- Timestamp

12. Organizational Benefit Statement

This script provides a controlled, auditable method for validating WinRM connectivity, supporting troubleshooting and remote-management readiness.

SOP 5 – Set WinRM TrustedHosts

Script Name: Set WinRM TrustedHosts **Category:** WinRM

1. Purpose

This script updates the WinRM TrustedHosts list, supporting remote management in non-domain or cross-domain environments.

2. Scope

- Windows servers and workstations
- WinRM client configuration

3. Definitions

- **TrustedHosts:** Hosts allowed for unencrypted or non-Kerberos connections.

4. Preconditions

- Operator must have administrative rights.
- Action must be authorized.
- TrustedHosts must be restricted to approved systems.

5. Required Inputs

- Hostname(s) or wildcard pattern

6. Procedure Steps

1. Input Collection
    - Wizard prompts for host list.
2. Validation
    - Confirm hostnames are valid.
    - Warn if wildcard is broad.
3. Update Operation
    - Apply TrustedHosts configuration.
4. Post-Update Verification
    - Confirm new TrustedHosts list.
5. Logging
    - Log host list, operator, timestamp.

7. Expected Output

- Confirmation of TrustedHosts update.

8. Post-Execution Validation

- Operator may verify via `winrm get winrm/config/client`.

9. Error Handling

- Access denied
- Invalid host format

10. Security Considerations

- Broad TrustedHosts entries increase security risk.
- Should be used only when Kerberos is not available.

11. Audit Logging Requirements

- Operator ID
- Host list
- Timestamp

12. Organizational Benefit Statement

This script ensures TrustedHosts changes are performed safely and with full accountability, supporting remote-management workflows in complex environments.