Group Policy

Remote Procedure Call (RPC) Service

> You can use the Group Policy Management Console snap-in to force machines to perform a Group Policy update if the RPC service is running.

Path	Setting	Value
Computer Configuration > Windows Settings > Security Settings > System Services	Remote Procedure Call (RPC)	Automatic

WinRM

> Windows Event Forwarding and Collection depends on WinRM.

Path	Setting	Value
Computer Configuration > Windows Settings > Security Settings > System Services	Windows Remote Management	Automatic
Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Remote… > WinRM Service	- Allow remote server management… - IPv4 filter	- Enabled - *
Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall… > Windows Defender…	- Inbound Rules - Predefined	- New Rule - Windows Remote Management - Remove "Public" profile - Allow the connection
Computer Configuration > Policies > Administrative Templates > Network > Network Connections > Windows Defender… > Domain Profile	- Allow inbound remote… - IPv4 field	- Enabled - *

Logging the "Sexy Six" Event IDs

Path	Setting	Value
Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options	Audit: Force audit policy subcategory settings…	Enabled
Computer Configuration > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies > Detailed Tracking	Audit Process Creation	Success
Computer Configuration > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies > Object Access	Audit File Share	Success
Computer Configuration > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies > Object Access	Audit File System	Success
Computer Configuration > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies > Object Access	Audit Registry	Success
Computer Configuration > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies > Object Access	Audit Filtering Platform Connection	Success
Computer Configuration > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies > Logon/Logoff	Audit Logon	Success, Failure