Discovery provider · Windows WinRM discovery

Discover Windows hosts through WinRM and PowerShell patterns.

https://docs.qintoravacloud.com/integrations/discovery-provider/winrm/

Prerequisites

- TCP access from a collector to WinRM
- Windows discovery service account
- Kerberos, certificate, or HTTPS transport

Configuration steps

1. Select collector and target ranges
2. Choose transport and port
3. Reference the Windows credential secret
4. Test WinRM, PowerShell, and WMI

Provider fields

Field	Type	Requirement and options
Target CIDRs / hostnames `targetRanges`	textarea	Required
Collector / MID server `collector`	text	Required
WinRM port `port`	number	Required
Discovery username `username`	text	Required
Transport `transport`	select	Required `kerberos`, `ntlm_https`, `certificate`, `basic_https`
Credential secret alias `passwordSecretAlias`	text	Required
Validate HTTPS certificate `validateCertificate`	boolean	Optional

Field	Type	Requirement and options
Use JIT administrative access `useJitAdmin`	boolean	Optional

Verify and troubleshoot

Test with the narrowest supported non-production scope. Confirm that the connection test reaches the expected provider and that the preview or receipt matches the intended scope. Check identity, credential references, network access and provider permissions before retrying. Record the failure stage and redact sensitive payloads when escalating.