Discovery provider · SSH discovery

Discover Linux and Unix hosts using credentialed command patterns.

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

Prerequisites

- TCP access from a collector to SSH
- Least-privilege discovery account
- Approved sudo commands for privileged attributes

Configuration steps

1. Select collector and target ranges
2. Choose key, certificate, or password authentication
3. Define OS scope and sudo behavior
4. Test login and pattern execution

Provider fields

Field	Type	Requirement and options
Target CIDRs / hostnames `targetRanges`	textarea	Required
Collector / MID server `collector`	text	Required
SSH port `port`	number	Required
Discovery username `username`	text	Required
Authentication mode `authMode`	select	Required `private_key`, `password`, `certificate`
Credential secret alias `privateKeySecretAlias`	text	Required
Operating systems `operatingSystems`	tag_list	Optional

Field	Type	Requirement and options
Use approved sudo commands useSudo	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.