Solution Brief

Check Point + Indeni

Highlights

- Automate repetitive maintenance tasks
- Create cluster high availability assurance
- Gain network visibility
- Implement best practices
- Leverage remediation best practices from SecureKnowledge™
- Get started in minutes

Automate Validation Tasks for Check Point

Check Point customers use Indeni to automate repetitive network and security tasks such as ongoing maintenance, best practices, high availability validation steps and much more. Indeni crowdsources the latest runbook steps from industry experts and Fortune 1000 companies from around the globe, turning their tribal knowledge into code. This allows Indeni to know out of the box how to collect data from IT infrastructure components and analyze them according to known best practices.

Solution Overview

With Indeni Crowd and Indeni Knowledge Check Point customers gain access to living repository of scripts that automate tasks such as maintenance, high availability, network visibility, security, compliance and vendor best practices.

Automate Maintenance Tasks

Automate repetitive and manual intensive maintenance tasks such as identifying if:

- Licenses about to expire
- License usage limit approaching
- Contracts about to expire
- BGP peers down
- Hardware is faulty

Create Cluster High Availability Assurance

Proactively automate tasks to ensure seamless failover in the event of firewall failure. Check active and standby devices for mismatches such as:

- Static routing table does not match
- Radius/TACACS servers
- Time zone
- Bond interfaces
- SecureXL configuration mismatch
- Configuration files, and many more.

Gain Network Visibility

Continuously evaluate of critical resources to avoid outages:

- System – Core CPU, VSes CPU, Chassis and Blade CPU, Memory, Disk, critical processes, kernel tables, hardware components
- Protocols – routing tables, Layer 2 & layer 3 protocols (BGP)
- Connections – VPN tunnel(s) down, connection to SDN controllers and management applications
- Management resources – identity servers, Certificate Authority

Demonstrate Compliance & Audits

Ensure your infrastructure meets internal and external compliance requirements:

- Configuration and misconfiguration avoiding human errors
- Ensure static routing tables match
- Checks for OS software version, hotfixes, DNS servers to ensure compliance

Implement Security Best Practices

Reduce your attack surface and provide defense against security threats:

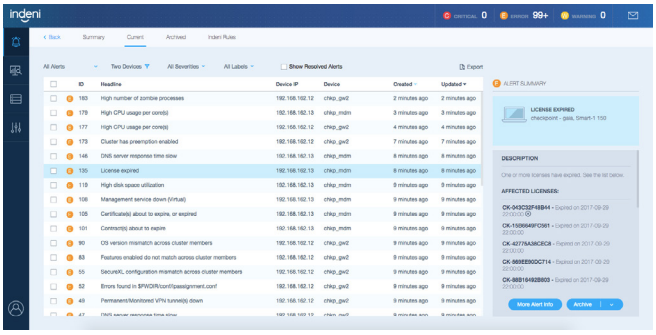
- Hotfixes installed do not match
- SmartEvent log handling too slow
- Track CPU utilization
- Number of connections
- SNMPv2c/v1 used

Indeni KnowledgeTM is built through contributions of Check Point users, their networks, and Check Point partners, and public sources, validated through the Indeni Open Development process.

How it works

Indeni connects to Check Point devices using SSH and collects data 24/7 by automatically running commands administrators generally have to run manually, such as, "ifconfig -a", "cpstat fw", "fw ctl get int <kernel_param>" and also collects and analyzes files such as objects_5_0.C and fwkern.conf. When Indeni finds a configuration issue, a notification is sent describing the issue and the best course of action to resolve it. In many cases, Indeni refers to the relevant SecureKnowledge article in Check Point's support center.

Example notification:

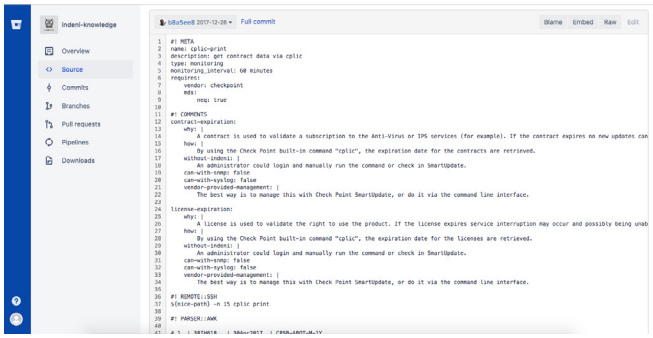


Alert Summary Remediation Steps

View example here: https://indeni.com/alerts/license-expiration-nearing-for-check-point/

Supporting Script:

View code here



What Makes Indeni Unique?

There are three major differences between Indeni and network monitoring and management solutions:

1. Indeni continuously validates that Check Point devices are operating as intended with automation scripts.
2. Indeni connects to network and security devices through the native protocol including SSH and API.
3. Indeni Knowledge is constantly updated by the certified professionals in Indeni Crowd ensuring you have the latest automation scripts and prescriptive remediation steps.

What Makes Check Point Unique?

Check Point plays a leading role in securing corporate networks and the Internet. An important part of this is monitoring networks to see the breadth and depth of threats that hit current and future customers. Check Point has developed a comprehensive suite of threat prevention technologies that adapt as threats evolve to keep customers secure. Check Point offers a unified next-generation solution that prevents advanced threats and malware, including stopping application-specific attacks, botnets, targeted attacks, APTs, and zero-day threats.

Three ways to get started

Get up and running in minutes and automate the identification of issues across network and security infrastructure. Have complete visibility into the commands used and customize to your heart's content.

1. **Test Drive**. Try Indeni without the hassle of a virtual machine. View test drive
2. **Community**. Engage in Indeni Crowd and keep five licenses of Indeni forever. Download
3. **Enterprise**. Contact us to connect Indeni to five or more devices. Contact Us

About Indeni

Indeni is the crowd-sourced automation platform for network and security infrastructure. With Indeni Crowd and Indeni Knowledge organizations gain access to living repository of automation tasks across maintenance, high availability, network visibility, security, compliance and vendor best practices. Teach your team co-development processes alongside the largest community of certified IT professionals and reduce total cost of ownership with prescriptive steps to resolve issues across firewall, router and switches. For more information visit www.indeni.com.

Corporate Headquarters
San Francisco, CA USA
Tel: +1-877-778-8991
Email: info@indeni.com

European Headquarters
Tel Aviv, Israel
Tel: +1-809-494-190
Email: info@indeni.com