Device Status Monitoring: Local Picture on a Global Scale

Alexei Suvorov, Sr. Security Engineer
Forward-looking statements

This is a rolling (up to three year) Roadmap and is subject to change without notice.

This document contains forward looking statements regarding future operations, product development, product capabilities and availability dates. This information is subject to substantial uncertainties and is subject to change at any time without prior notification. Statements contained in this document concerning these matters only reflect Hewlett Packard's predictions and / or expectations as of the date of this document and actual results and future plans of Hewlett-Packard may differ significantly as a result of, among other things, changes in product strategy resulting from technological, internal corporate, market and other changes. This is not a commitment to deliver any material, code or functionality and should not be relied upon in making purchasing decisions.
HP confidential information

This is a rolling (up to three year) Roadmap and is subject to change without notice.

This Roadmap contains HP Confidential Information. If you have a valid Confidential Disclosure Agreement with HP, disclosure of the Roadmap is subject to that CDA. If not, it is subject to the following terms: for a period of 3 years after the date of disclosure, you may use the Roadmap solely for the purpose of evaluating purchase decisions from HP and use a reasonable standard of care to prevent disclosures. You will not disclose the contents of the Roadmap to any third party unless it becomes publically known, rightfully received by you from a third party without duty of confidentiality, or disclosed with HP’s prior written approval.
Agenda

Device Status Monitoring content

* Included in the ESM next beta

- Business need and use case
- Definition of device
- Connector component “Device Status Monitoring”
- Content architecture overview
- Environment scenarios
- Summary
Use cases examples

- Which Firewall is inactive?
- Which Web Server is new?
- Is a critical device inactive for more than one hour?
Definition: Device

Device is a unique combination of these five fields:

- deviceHostName
- deviceVendor
- deviceProduct
- deviceZone
- customer
Definition: Active or inactive

Device status

• Active:
  o connector received events from the device since last check

• Inactive
  o connector did not receive events from the device since last check
The “Device Status Monitoring” Connector feature

Device Status Monitoring (DSM) is a connector functionality

![Device Status Monitoring Connector Feature](image_url)
Connector Device Status Events (agent:043)

**Connector Device Status** internal event includes:

- Device Event Class ID = agent:043
- Device Vendor
- Device Product
- Device Address
- Device Host Name
- Event Count
- Time stamp Last Event Received
Content architecture overview
Content architecture and design

- Device Monitoring content is new in ESM next beta
- Part of the standard Arcsight Administration package

All product views are illustrations and might not represent actual product screens
Content architecture and design, continued

Dashboards

Query viewers

Reports

Queries

Active Lists

Rules

agent:043 events
**Content architecture and design, continued**

**Dashboards:**
- All monitored devices
- Critical monitored devices
- Panels color-coded on inactivity time
Content architecture and design, continued

Reports:

- Devices detected inactive - Last N Days
- New devices detected - Last N Days

Report example:

![Critical Devices Detected Inactive - Last 24 Hours](image)
Content architecture and design, continued

Active lists

1. Monitored Devices All – populated automatically by rule
2. Monitored Devices Whitelist – populated manually
3. Monitored Devices Critical – populated with critical devices (entries copied over manually)
4. Critical Devices – used to import critical devices from a CSV file
Content architecture and design, continued

**Rules**

- Trigger on agent:043 events
- Update active lists
- Send email notification when device is inactive
Environment scenarios
Scenario 1

- Original Connector has Device Status Monitoring (DSM) enabled
- agent:043 events from Original Connector sent to ESM
Scenario 2

- Connector parses IP addresses and host names of original devices
- agent:043 events have information about original devices
Summary

Events from devices

Connectors
agent: 043 events

ESM

(!) Inactive device detected
Summary

Device Monitoring Content

• Distributed computing: stats gathered at Connectors, not ESM
• Light: ESM does not process tons of base events
• Efficient: minimum impact on ESM performance
• Accurate: fully tested in multiple environments
• User friendly: simple and easy to use
• Scalable: new devices added automatically
For more information

Attend these sessions

• Session TB3069ID, HP ArcSight ESM 24/7

After the event

• Contact your sales rep
• Visit the website at: https://protect724.hp.com/community/arcsight

Your feedback is important to us. Please take a few minutes to complete the session survey.
Please give me your feedback

Session TT3079  Speaker Alexei Suvorov

Please fill out a survey.

Hand it to the door monitor on your way out.

Thank you for providing your feedback, which helps us enhance content for future events.
Thank you