Security Automation and Optimization using HP-NA

Florian Ecard

SNE master student

Supervisor: Olivier Willm

4th February 2015

UNIVERSITEIT VAN AMSTERDAM

Security Automation and Optimization using HP-NA

- What is HP Network Automation?

- What were the objectives with it?

- CVE retrieval automation using HP-LNc
- Integrity of the configuration's Security
- New HP-NA certificate
- SSH keys

Research question

- Evaluate the software capabilities to audit the configurations about potential security issues from the CVE database.

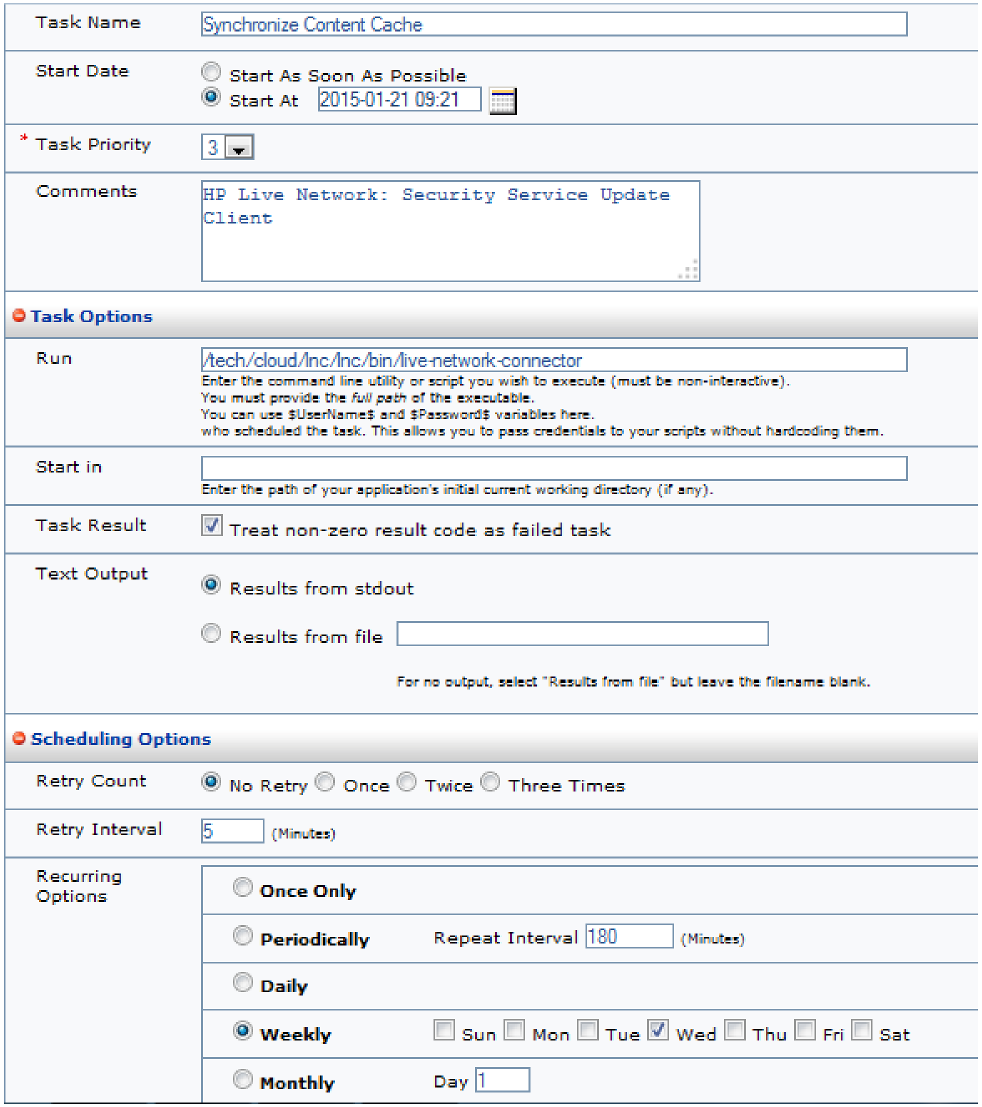
- How to automatically check the configuration's security integrity?

- How does it fit in an overall network security improvement process?

HP-LNc Installation & Configuration

- Linux Redhat server
- Use of the CLI
- Choose the products
- Two users & passwords
- Automation using HP-NA

→ **Documentation**



Task Name	Synchronize Content Cache
Start Date	○ Start As Soon As Possible ● Start At 2015-01-21 09:21
* Task Priority	3
Comments	HP Live Network: Security Service Update Client

Task Options

Run	/tech/cloud/lnc/lnc/bin/live-network-connector Enter the command line utility or script you wish to execute (must be non-interactive). You must provide the *full path* of the executable. You can use $UserName$ and $Password$ variables here. who scheduled the task. This allows you to pass credentials to your scripts without hardcoding them.
Start in	Enter the path of your application's initial current working directory (if any).
Task Result	☑ Treat non-zero result code as failed task
Text Output	● Results from stdout ○ Results from file For no output, select "Results from file" but leave the filename blank.

Scheduling Options

Retry Count	● No Retry ○ Once ○ Twice ○ Three Times
Retry Interval	5 (Minutes)
Recurring Options	○ **Once Only** ○ **Periodically** Repeat Interval 180 (Minutes) ○ **Daily** ● **Weekly** □ Sun □ Mon □ Tue ☑ Wed □ Thu □ Fri □ Sat ○ **Monthly** Day 1

Automate the configuration integrity checking

- **What kind of configuration is verified?**
    - Cisco IOS
    - Cisco NXOS

- **Why checking their integrity?**

Automate the configuration integrity checking

- What is being checked?

- ACLs, AAA & Usernames
- Features & VTY
- NTP
- Logging facilities

- How was it done with HP-NA?

- Create groups, policies and tasks

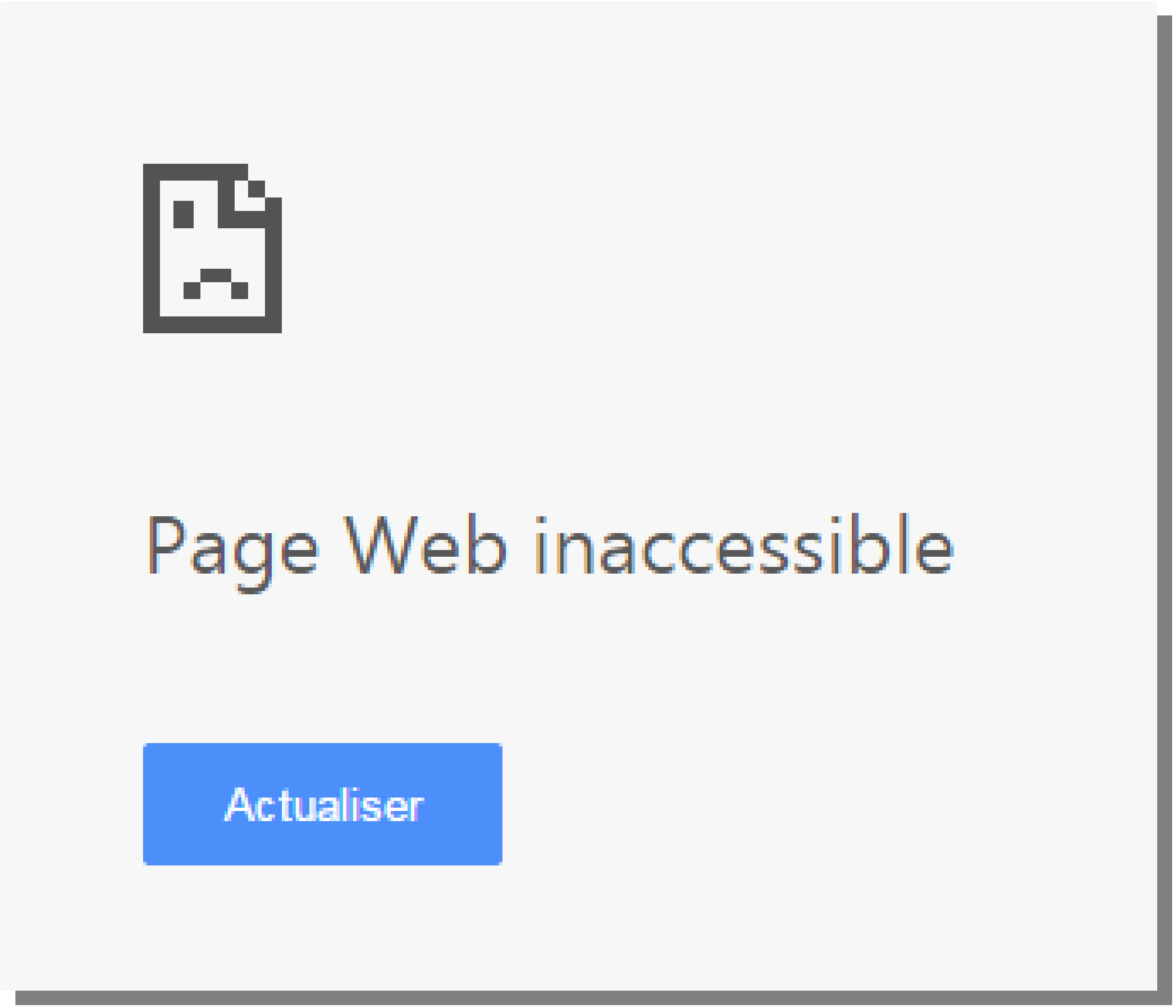
CA-signed HP-NA certificate

- What for?
- What are the *.keystore* and *.truststore* files?
- What steps should be followed?

- public key generation
- CSR generation
- 1 + 3 certificates returned

And the result is → → →

CA-signed HP-NA certificate



Page Web inaccessible

CA-signed HP-NA certificate

- The problems were due to … Stupidity! :-(

- Asked for a www

→ **Documentation**

Problems encountered

- User accounts access
- HP-NA unavailability
- HP-LNc configuration entered using vim
- HP-LNc user access & privileges
- Certificates

Conclusion

RESEARCH QUESTION:

- Evaluate the software capabilities to audit the configurations about potential security issues. Define specific policies from the CVE database.

- How to automatically check the configuration's security integrity?

- How does it fit in an overall network security improvement process?

Conclusion

- Future work

- Perl API
- SSH keys checking

Security Automation and Optimization using HP-NA

Questions ??   :-)