



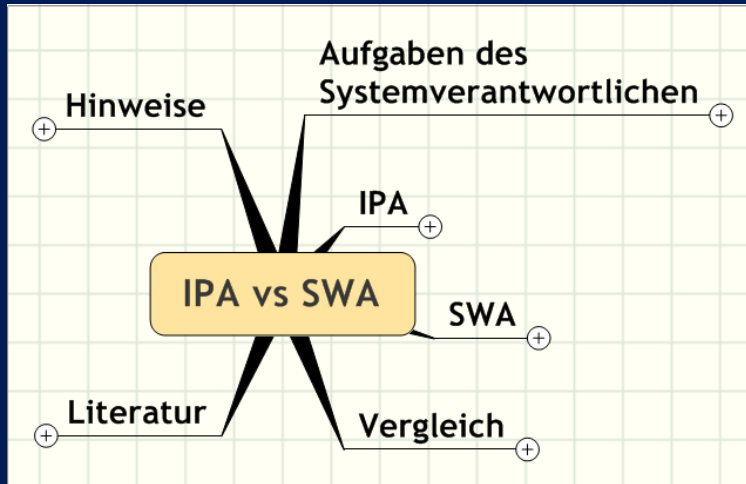
ITRC Patch Assessment (IPA) VS HPUX Software Assistant (SWA)

Thomas Brix
Remote Support Account Advocate, HP Services
Global Value Solution Center, Germany/Austria/Switzerland (GVSC
DACH)



© 2007 Hewlett-Packard Development Company, L.P.
The information contained herein is subject to change without notice

IPA vs SWA



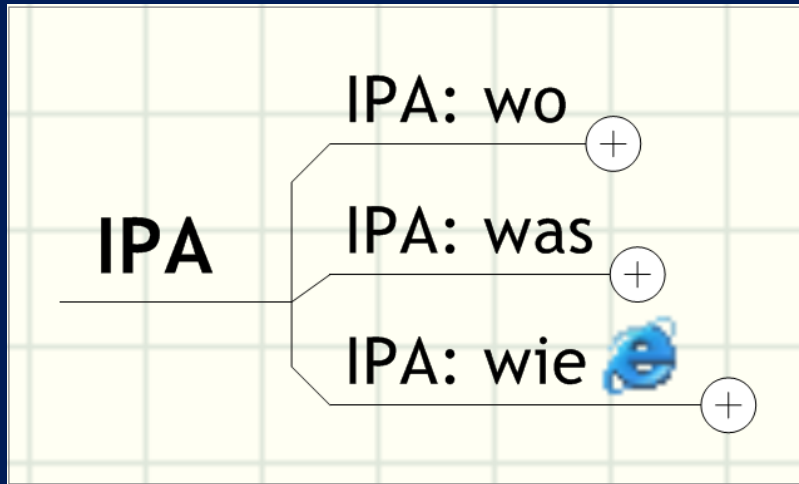
Aufgaben des Systemverantwortlichen

Aufgaben des Systemverantwortlichen

Aktualisierung des OS
Überwachung bzgl
Verfügbarkeit
sicherheitsrelevanter
Aktualisierungen



IPA



IPA: wo

- Web: Funktion in HP's IT Resource Center
itrc.hp.com
 - "run a patch assessment"



IPA: was

- Running a patch assessment is one step in the proactive patching of your HP-UX system.
- Proactive patching ensures that your system has a consistent and recent collection of patches installed.
- Be sure to review "how to proactively patch HP-UX systems", which describes all of the steps in the process.

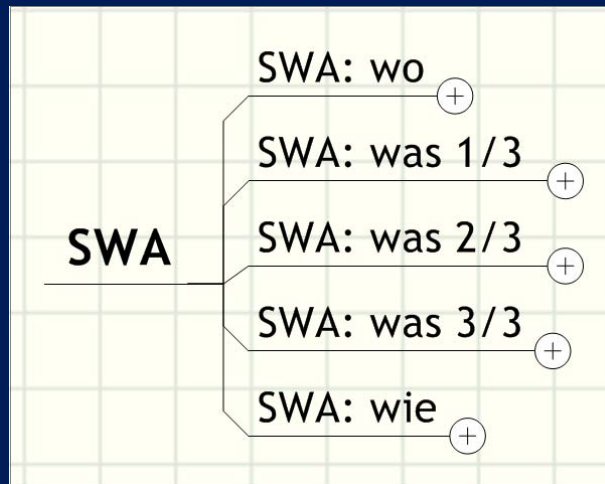


IPA: wie

- Specifying your system configuration.
- Specify the assessment profile appropriate for the uploaded system.
- Run the assessment.
- Review the results of the assessment.
- Take delivery of the recommended items.
- siehe Vorträge der vergangenen Jahre unter [1]



SWA



SWA: wo

- HPUX System
 - 11.11/11.23/11.31
 - Internet-Zugang für Katalog-Download
 - lokale Analyse auf dem eigenen System
 - Analyse anderer HPUX system möglich



SWA: was 1/3

- befeilszeilenbasierendes Werkzeug, das die Verwaltung von Patches und Sicherheitshinweisen auf HP-UX Systemen konsolidiert und vereinfacht. [5]
 - Ist für Systemverwalter gedacht, die für Patches und die Verwaltung der Sicherheitsfunktionen bei HP-UX Systemen zuständig sind.
 - Die Software wird auf HP-UX 11i Systemen unterstützt.
 - Sie bietet eine Befehlszeilenoberfläche.
 - Es handelt sich um ein client-seitiges Werkzeug für Patches und die Analyse/Verbesserung der Systemsicherheit. Es werden die Funktionen von ITRC Patch Assessment Tool und Security Patch Check (SPC) mit wenigen kleinen Ausnahmen, nämlich der Patch-Gruppenanalyse, bereitgestellt.



SWA: was 2/3

- befeilszeilenbasierendes Werkzeug, das die Verwaltung von Patches und Sicherheitshinweisen auf HP-UX Systemen konsolidiert und vereinfacht. [5]
 - Analyse eines Systems (und einiger Typen von Depots) auf Patch-Warnungen, kritische Defekte, Sicherheitshinweise, fehlende Quality Pack-Patch-Pakete und von Benutzern angegebene Patches und Patch-Ketten.
 - Analyse Ihres Systems und Erzeugen von Berichten anhand einer von HP bereitgestellten Katalogdatei.
 - Optimierung der automatischen Auswahl von Patch-Abhängigkeiten durch Zugriff auf die Qualität der Abhängigkeit, Bereitstellen des besten Fallszenarien für die Abhängigkeit, Minimieren von Änderungen am System und Einschätzen künftiger Patch-Abhängigkeitsänderungen.



SWA: was 3/3

- befeilszeilenbasierendes Werkzeug, das die Verwaltung von Patches und Sicherheitshinweisen auf HP-UX Systemen konsolidiert und vereinfacht. [5]
 - Erzeugung der Aktions-, Problem- und Detailberichte sowie eines konsolidierten HTML-Berichts, damit Sie sehen, welche Probleme für die Software im System oder im Depot relevant sind.
 - Möglichkeit zum Herunterladen von Patches und Erzeugen eines Software Distributor (SD-UX)-Depots, wodurch viele der Probleme im Bericht behoben werden. SWA kann auch verwendet werden, um empfohlene zusätzliche Aktionen im Bericht zu sehen, die manuell ausgeführt werden müssen.
 - Automatische Überprüfung der Patch-Integrität (mit MD5-Kryptographie-Hash-Verfahren) vor dem Entpacken heruntergeladener Patches.

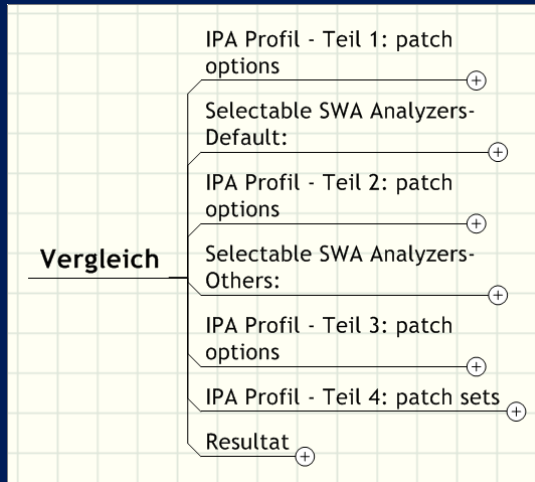


SWA: wie

- `# swa report -x http_proxy=http://web-proxy:8088`
- `inventory: $HOME/.swa/cache/swa_inventory_n.xml`
- `# swa report -a SEC > swa-sec.txt`
- NOTE: See HTML-formatted report `"/.swa/report/swa_report.html"`
- `"~/swa/ignore"`
- `# swa get -p -t swa-depot-t1`
 - -p: preview
- `# swa get -t swa-depot-t1`
- siehe [2], [3]



Vergleich



IPA Profil - Teil 1: patch options

- security patches
- latest quality pack patch bundle
- replacements for installed patches with critical warnings



Selectable SWA Analyzers- Default:

- QPK – Quality pack
 - Identify any newer quality pack bundles
- SEC – Security issues
 - Identify actually/potentially applicable security bulletins
- PCW – Patches with critical warnings
 - Criticality determined by impact of issue, not probability of occurrence



IPA Profil - Teil 2: patch options

- replacements for installed patches with any warnings
- request specific patches
- request specific patch chains
- request specific mandatory patches
- critical fixes



Selectable SWA Analyzers- Others:

- PW – Patches with any warnings (a superset of PCW)
- PATCH – Include a specific patch or patches
- CHAIN – Include a patch or recommended successor
- CRIT – Patches that fix critical problems



IPA Profil - Teil 3: patch options

- all applicable patches
- updates for the patches already installed



IPA Profil - Teil 4: patch sets

- miscellaneous patches for the specific operating system of the system being assessed
- miscellaneous patches for the specific hardware model of the system being assessed
- Application specific patch sets (only available for 11.00, 11.11, & 11.23):
- available patch sets: your selections:

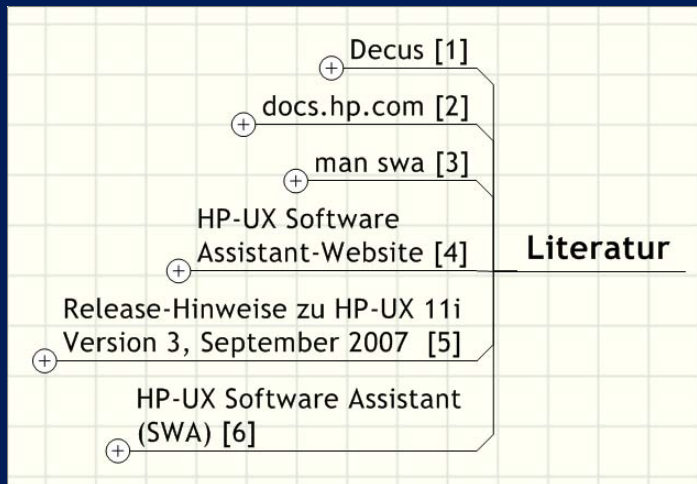


Resultat

- IPA vs SWA
- 4:2
- Analysemöglichkeiten: klarer Vorteil IPA
- Automatisierung: Vorteil SWA
- Reporting: Vorteil SWA



Literatur



Decus [1]

- Decus2007, Vortrag 1H06 [1.1]
 - ITRC Patch Assessment (IPA)
 - http://www.decus.de/slides/sy2007/17_04/1H06.pdf
- Decus2006, Vortrag 2H04 [1.2]
 - ITRC Patch Assessment (IPA)
 - http://www.hp-user-society.de/slides/sy2006/17_05/2H04.pdf



docs.hp.com [2]

- <http://docs.hp.com/en/oshpux11iv3.html#Patch%20Management>
- HP-UX Software Assistant Administration Guide, March 2008 HP-UX 11i v1, HP-UX 11i v2, HP-UX 11i v3 [2.1]
 - [PDF] <http://docs.hp.com/en/5992-3930/5992-3930.pdf>
 - 70Seiten
 - 0.7MB
 - [HTML] <http://docs.hp.com/en/5992-3930/index.html>
- HP-UX Software Assistant Release Notes, March 2008 HP-UX 11i v1, HP-UX 11i v2, HP-UX 11i v3 [2.2]
 - [PDF] <http://docs.hp.com/en/5992-3929/5992-3929.pdf>
 - 11Seiten
 - 0.3MB
 - [HTML] <http://docs.hp.com/en/5992-3929/index.html>
- Patch Management User Guide for HP-UX 11.x Systems, March 2008 HP-UX 11i v1, HP-UX 11i v1.6, HP-UX 11i v2, HP-UX 11i v3 [2.3]
 - [PDF] <http://docs.hp.com/en/5992-4020/5992-4020.pdf>
 - 136Seiten
 - 1.4MB
 - [HTML] <http://docs.hp.com/en/5992-4020/index.html>
- Patch Management User Guide for HP-UX 11.x Systems, September 2007 HP-UX 11i v1, HP-UX 11i v1.6, HP-UX 11i v2, HP-UX 11i v3 [2.4]
 - [PDF] <http://docs.hp.com/en/5992-0674/5992-0674.pdf>
 - 128Seiten
 - 1.3MB
 - [HTML] <http://docs.hp.com/en/5992-0674/index.html>



man swa [3]

- swa(1M)
- swa-report(1M)
- swa-get(1M)
- swa-step(1M)
- swa-clean(1M)



HP-UX Software Assistant-Website [4]

- <https://www.hp.com/go/swa>
 - Produktübersicht
 - Links zum Herunterladen
 - Installationsanweisungen



Release-Hinweise zu HP-UX 11i Version 3, September 2007 [5]

- Aktualisierungsrelease der Betriebsumgebungen
- Kapitel 8 Sicherheitsfunktionen: HP-UX Software Assistant
- <http://docs.hp.com/de/5992-1703/ch08s07.html>

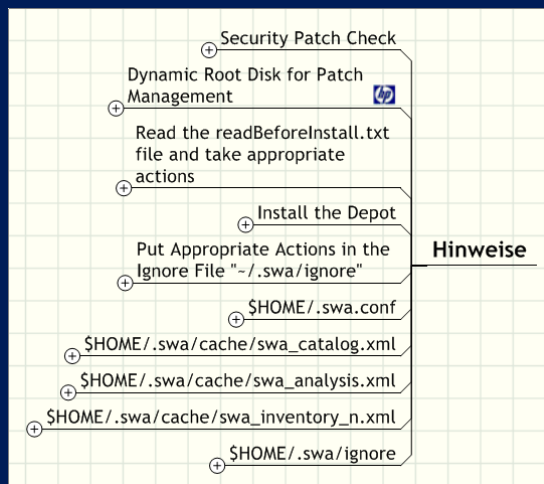


HP-UX Software Assistant (SWA) [6]

- kostenfreier download
- <http://software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=B6834AA>



Hinweise



Security Patch Check

- The security_patch_check utility has been replaced by Software Assistant. See swa(1M).
- After November 1, 2008 the use of the security_patch_check -m option will generate a compatible report through the swa command. Other options will either be ignored or will cause security_patch_check to terminate with an error.
- Previous versions of Security Patch Check will continue to function as intended until the security catalog is no longer provided.
- The security catalog will be available until at least November 1, 2008.
- Unless otherwise specified, the remainder of this DESCRIPTION section describes the behavior of Security Patch Check before November 1, 2008.
- siehe [2.1], security_patch_check(1M), Seite 20



Dynamic Root Disk for Patch Management

- <http://docs.hp.com/en/DRD/index.html>



Read the readBeforeInstall.txt file and take appropriate actions

- The readBeforeInstall.txt is located in the target depot directory.
- This file lists special installation instructions and dependencies to take under consideration for all the patches downloaded from HP. Review this file before installing the depot.



Install the Depot

- The recommended method to install HP-UX patches and patch bundles from a depot is with the command:
- `# swinstall -s depot -x patch_match_target=true -x autoreboot=true`
- Note that this command should only be used within a maintenance window as the system might require a reboot. Any reboot will be performed automatically when required.



Put Appropriate Actions in the Ignore File "~/.swa/ignore"

- It might make sense for you to ignore the following types of issues:
- Manual actions — SWA can't detect if security bulletin manual actions (other than installing specific versions of patches or software) have been taken, so after applying a manual action, add it to the ignore file to track that the action has been taken.
- Deferred actions — If you've made a decision to defer addressing a particular issue for some period of time, after taking into account the risk of not addressing it, you might wish to add it to the ignore file until the issue is revisited or fixed. Be careful not to forget about these types of issues, since SWA will stop warning about them.
- HP advises you include comments in the ignore file explaining who added an issue, why, and when. Auditors are likely to want this information documented and traceable.
- The ignore file, `$HOME/.swa/ignore`, includes comments with instructions regarding syntax and how to add an issue.



`$HOME/.swa.conf`

- The per-user SWA configuration file. This file takes precedence over the system-wide SWA configuration file.



`$HOME/.swa/cache/swa_catalog.xml`

- An HP-supplied catalog file from the ITRC website that contains known security issues and other defects along with their solutions. This file is downloaded with the command `swa report` or `swa step catalog`.



`$HOME/.swa/cache/swa_analysis.xml`

- The analysis of the inventory file and the catalog file created with `swa report` or `swa step analyze`.



`$HOME/.swa/cache/swa_inventory_n.xml`

- The inventory of installed software created by swa inventory or swa step inventory.



`$HOME/.swa/ignore`

- Use this file to specify issues for analyzers to ignore. You may have more than one of these files.



