HP WORLD 2004
Solutions and Technology Conference & Expo

Maintaining HP-UX System Security

Kathy Kwinn
HP-UX Patch Quality Program Manager
Hewlett-Packard

Why be proactive?

- To protect your data
- To minimize your risk of attack
- To avoid unscheduled down time
- Relying on reactive security maintenance is like locking the barn door after the horse has been stolen

Agenda

- Defining a security strategy
- Setting up secure systems
- Maintaining system security
- Recent improvements from HP
- Q&A

Defining a security strategy

Understand the possibilities

- Your institutional policy documents
- Managing Systems and Workgroups, Edition 6, available from http://docs.hp.com
  - Administering a System: Managing System Security (Chapter 8)
  - Configuring HP-UX Bastille Interview (Appendix)
- Available software

Bastille

- A security-hardening, lockdown tool addressing
  - Patches
  - File Permissions
  - Account Security
  - Secure Inetd
  - Miscellaneous Daemons
  - Sendmail
  - DNS
  - Apache
  - FTP
  - HP-UX
  - IPFilter
- More on Bastille later

Graphic from Open-Source Bastille Home Page: http://www.bastille-linux.org

Optional security packages

Tool	Benefit
HP-UX Host Intrusions Detection System	Monitors for & notifies of patterns suggesting break-in or subversive inside activities
HP-UX Shadow Passwords (standard with HP-UX 11i v2)	Makes passwords less susceptible to decryption
Network Information Service Plus (NIS+)	Simplifies network administration by centralizing common configuration info
Pluggable Authentication Modules (PAM)	Allows choice of authentication services, integration of optional security technologies
Secure Internet Services (SIS)	User authentication does not require transmitting a readable password over the network
Strong Random Number Generator (only in HP-UX 11i)	Non-reproducible source of binary sequences provides greater security for cryptographic applications
Security Patch Check	Identifies missing security fixes

Specify your needs

- GOAL: Identify and manage your risks
- Every machine should have a security strategy addressing
  - Who can log in
  - Who has superuser privileges
  - Who can access what data and software
  - Network connectivity & remote access
  - How much auditing and tracking is needed
  - What optional security software is needed
  - Interactions with disaster recovery plan
  - Security maintenance

- Keep the number of variations reasonable
- Document each strategy
- Document which strategy applies to each machine

Select tools

- Tools everyone needs
  - Security Bulletins
  - Bastille
  - Security Patch Check
  - Patch Database
  - Software Depot
- Others
  - Standard HP-UX Patch Bundles
  - Patch Assessment Tool
  - Patch Sets
  - Software Pack

Security bulletins

- Issued whenever HP recommends an action to improve system security
  - Description of problem
  - Recommendation (obtain patch, product update, etc.)
- Subscribe at http://itrc.hp.com
- Read immediately and evaluate need for action on systems and depots
- Archived on ITRC (search technical knowledge base, select Security Bulletins under HP-UX Software, select Security Bulletin Archive under Related Links)

Bastille, cont'd.

- Free at software.hp.com, shipped with HP-UX 11i v2 Operating Environments
- Can be run from cron
- Scans system for violations of your specified security configuration
  - Fixes some problems, logs actions it takes
  - Suggests others for you to fix (TODO.txt)
- Advantages over writing your own tool
  - De facto standard on multiple platforms
  - Based on accepted industry best practices
  - Well-documented, supported by HP
  - Flexible
  - Three pre-defined configurations (in HP-UX 11i v2)
  - Easy to create your own configuration, re-configure
  - Configuration time << tool development and test time
  - Easy to revert to pre-Bastille state

"In real world environments, many people do not have the time or desire to research and implement good security practices. Bastille can help people to take sensible precautions without requiring them to become experts."

Ian Robertson

Research In Motion, Ltd.

Quoted from Open-Source Bastille Home Page: http://www.bastille-linux.org/quotes.html

"The reaction to Bastille has been excellent here. A couple of our department IT contacts and a lot of the students have raved about it, especially the ease-of-use and the run-time explanations."

S. Groppi

Harvard University

Quoted from Open-Source Bastille Home Page: http://www.bastille-linux.org/quotes.html

Predefined Bastille configurations*

Configuration File Name	Description
HOST.config	Host lockdown: no firewall; networking runs normally, including Telnet and FTP.
MANDMZ.config	IPFilter firewall blocks incoming connections except common, secured, management protocols.
DMZ.config	IPFilter firewall blocks all incoming connections except Secure Shell.

* Only for HP-UX 11i v2 or later

Security Patch Check

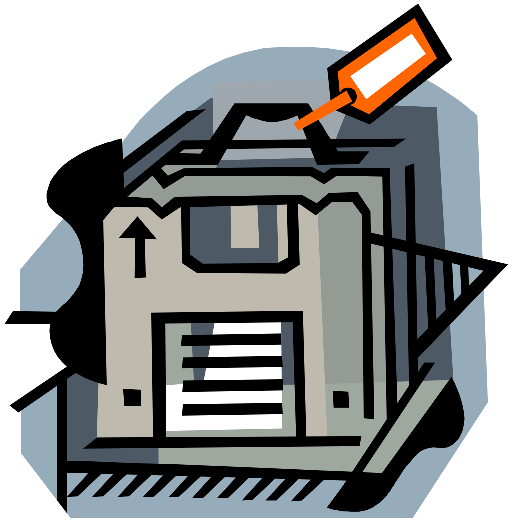
- Identifies upgrades that will make your system more secure and problem patches you may want to replace
  - Missing security patches
  - Missing product updates containing security fixes, beginning with Version B.02.00 (June, 2004)
  - Patches with warnings (not just security-related problems)
- Downloads information from HP that's updated daily
- Runs locally, sends no data to HP
- Checks systems and depots
- Can be run from Bastille or independently
- Free download from http://software.hp.com

Patch Database

- Primary tool for reactive patch maintenance
- Investigate and download a patch recommended in a Security Bulletin or suggested by Security Patch Check
- From http://itrc.hp.com, select “patch database” under “maintenance and support”, then select “find a specific patch”

Software Depot

- Obtain product updates recommended in a Security Bulletin or suggested by Security Patch Check
- Also optional security products
- http://software.hp.com



HP WORLD 2004
Solutions and Technology Conference & Expo

Document your procedures

- Specify
  - What should happen automatically
  - Who does what
  - Schedule for automatic and manual actions
  - What happens with results
  - How to add new machines
  - How to retire machines
  - Interaction with disaster recovery plan
  - Schedule for review and revision of
    - Chosen strategies
    - Mapping of machines to strategies
    - Procedures
- Include your assumptions and rationale

Setting up secure systems

Implement your strategy

- Install and configure Bastille on one machine
- Run Bastille (and Security Patch Check)
- Review results
  - Perform actions recommended in TODO.txt
  - Examine Bastille log for unintended actions
  - Obtain desired security fixes and replacements for patches with warnings
- Modify configuration as necessary
- Deploy to all machines that will have the same Bastille configuration (copy the config file)
- Repeat for all configurations

As you acquire new systems

- Install Bastille
- Copy appropriate Bastille configuration file, run Bastille, and act on recommendations
- Create a new configuration only if necessary

Maintaining system security

Remain vigilant

- Run Bastille regularly
  - Pick a frequency that makes sense for you, use cron
  - After you install a patch or product update
- Examine TODO.txt after every run
  - What does Bastille recommend that you do?
  - Will you follow recommendations now?
  - Will you defer any recommendations?
- Act on Bastille recommendations
- Skim Bastille log

Monitor security bulletins

- Read each new bulletin as it arrives
- Evaluate impact on all your systems
- Decide which systems to fix now, which later

HP WORLD 2004
Solutions and Technology Conference & Expo

Perform proactive maintenance

- Usually once or twice a year
- Consider implementing Bastille and Security Bulletin recommendations you have deferred
- Obtain desired new patches and product updates
- Run Security Patch Check on system and depot
  - Recommended product updates and manual actions
  - Any patches that have warnings
- Run Security Patch Check on system again after you think you're done

Reassess strategy periodically

- Review and update your strategy
  - Whenever an attack has been detected or a significant change occurs
  - At least once a year
- What has changed since last review?
  - Newly acquired systems
  - How each system is used
  - Types of data
  - Tools
  - Threats
  - Corporate policies, laws, etc.

- What changes should you make?
  - Add configurations
  - Alter existing configurations
  - Move a system to a different configuration
  - Change other parts of your strategy (tools, frequency, …)
- Keep your strategy document up to date!!!

Report problems to HP

Report a security alert or potential security vulnerability to HP

To report potential security vulnerabilities in any hp software product, please send an E-mail message to:

» security-alert@ hp.com

Please encrypt any potential exploit information using the security-alert PGP key available from your local key server, or by sending a message with a subject of 'get key' (no quotes) to:

» security-alert@hp.com

Thank you,
HP Software Security Response Team

Recent improvements from HP

New HP processes bring you better security fixes more quickly

- Streamlined patch creation for fixing security defects
  - Patches can be available in days
  - Minimize risk by minimizing change
  - Less need for binaries, manual actions
- Unpackaged solutions may be offered as temporary fixes for special cases
  - Always followed by patches or product updates announced in Security Bulletin updates

Security Patch Check, Version B.02.00 (June, 2004) or later

- Identifies upgrades that will make your system more secure and problem patches you may want to replace
- NEW: Reports manual actions and missing product updates in addition to missing patches
- NEW: Security actions catalog can be downloaded over an HTTPS connection
- Tip: Avoid repeated warnings about manual actions by maintaining an ignore file
  - $HOME/.spc_ignore
  - Actions you have already performed
  - Actions you have decided not to perform

Other improvements

- Patch Assessment has replaced Custom Patch Manager on the ITRC
- Strong Random Number Generator for HP-UX 11i

Q&A

invent

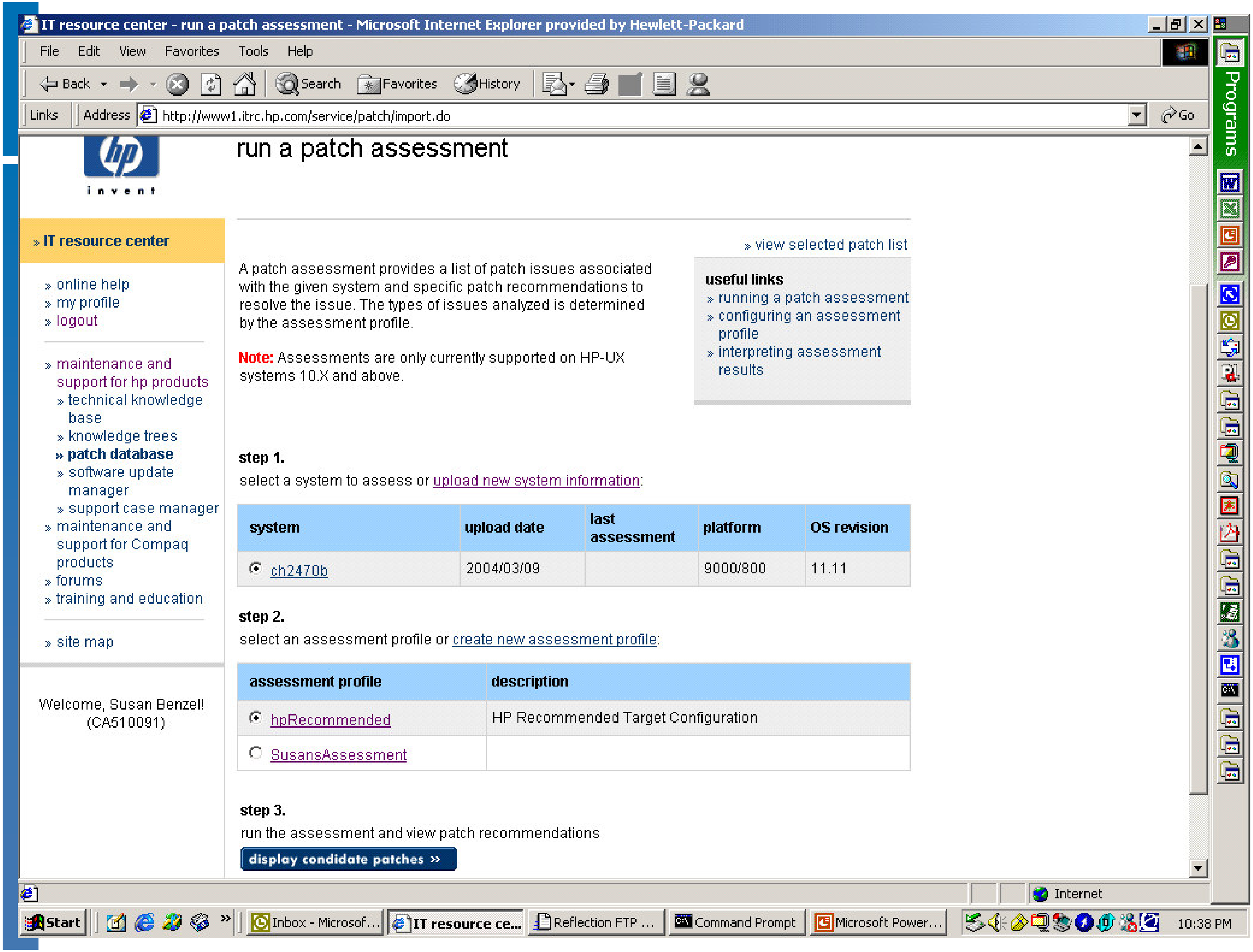
Backup slides

Standard HP-UX Patch Bundles

- Quality Pack Bundle for defect fixes
  - Updated twice a year
  - Patches that have excellent quality track record
  - Simple proactive patch maintenance
  - Latest fixes to security problems may not be included
  - Occasionally a patch warning is issued for a patch in the bundle
  - Use Security Patch Check to identify potential adjustments
- Hardware Enablement Bundle for new drivers, etc.
- Available on media or via download
- From http://itrc.hp.com, select "more…" under "maintenance and support", then select "standard patch bundles – find patch bundles"
- Available to all customers

Patch Assessment Tool

- Tunable proactive patch maintenance for do-it-yourselfers
- Uploads your system configuration to HP for analysis
- Available to all customers
- From http://itrc.hp.com, select "patch database" under "maintenance and support", then select "run a patch assessment"
- You choose a patching strategy – innovative, conservative, or restrictive
- You choose what to look for – security patches is one option
- HP recommends patches
- You decide what recommendations to accept
- Download accepted patches in a single operation


IT resource center - run a patch assessment - Microsoft Internet Explorer provided by Hewlett-Packard
File Edit View Favorites Tools Help
Back
Search
Favorites
History
Links
Address http://www1.itrc.hp.com/service/patch/import.do
Go
Programs
Internet
Start
Inbox - Microsof...
IT resource ce...
Reflection FTP ...
Command Prompt
Microsoft Power...
10:38 PM

run a patch assessment

» IT resource center

» online help
» my profile
» logout

» maintenance and support for hp products
» technical knowledge base
» knowledge trees
» **patch database**
» software update manager
» support case manager
» maintenance and support for Compaq products
» forums
» training and education

» site map

Welcome, Susan Benzel!
(CA510091)

» view selected patch list

A patch assessment provides a list of patch issues associated with the given system and specific patch recommendations to resolve the issue. The types of issues analyzed is determined by the assessment profile.

Note: Assessments are only currently supported on HP-UX systems 10.X and above.

useful links
» running a patch assessment
» configuring an assessment profile
» interpreting assessment results

step 1.
select a system to assess or upload new system information:

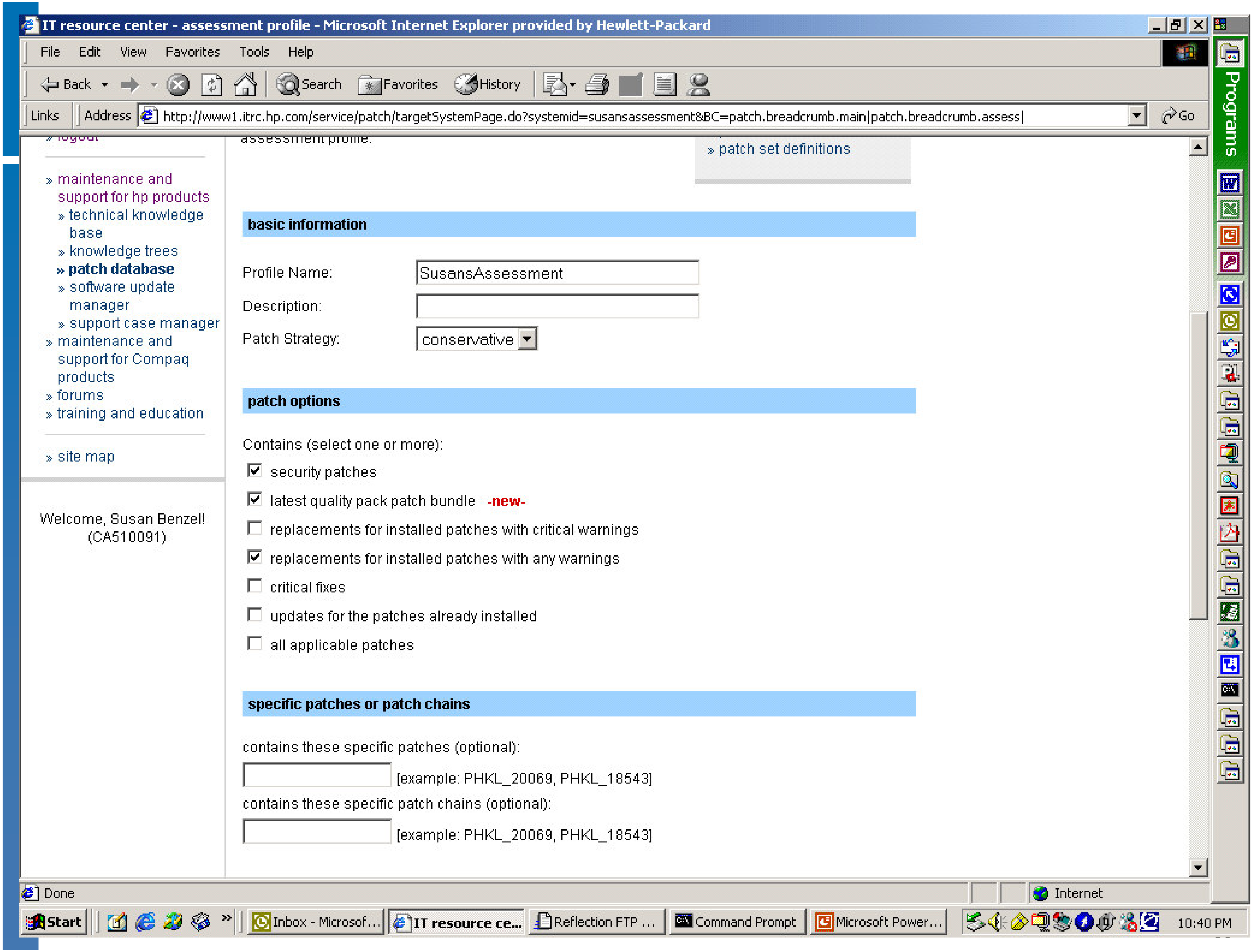
system	upload date	last assessment	platform	OS revision
● ch2470b	2004/03/09		9000/800	11.11

step 2.
select an assessment profile or create new assessment profile:

assessment profile	description
● hpRecommended	HP Recommended Target Configuration
○ SusansAssessment	

step 3.
run the assessment and view patch recommendations

display condidate patches »



http://www1.itrc.hp.com/service/patch/targetSystemPage.do?systemid=susansassessment&BC=patch.breadcrumb.main|patch.breadcrumb.assess|

» logout

» maintenance and support for hp products
- » technical knowledge base
- » knowledge trees
- » **patch database**
- » software update manager
- » support case manager

» maintenance and support for Compaq products

» forums

» training and education

» site map

Welcome, Susan Benzell
(CA510091)

assessment profile.

» patch set definitions

basic information

Profile Name: SusansAssessment

Description:

Patch Strategy: conservative

patch options

Contains (select one or more):

☑ security patches

☑ latest quality pack patch bundle -new-

□ replacements for installed patches with critical warnings

☑ replacements for installed patches with any warnings

□ critical fixes

□ updates for the patches already installed

□ all applicable patches

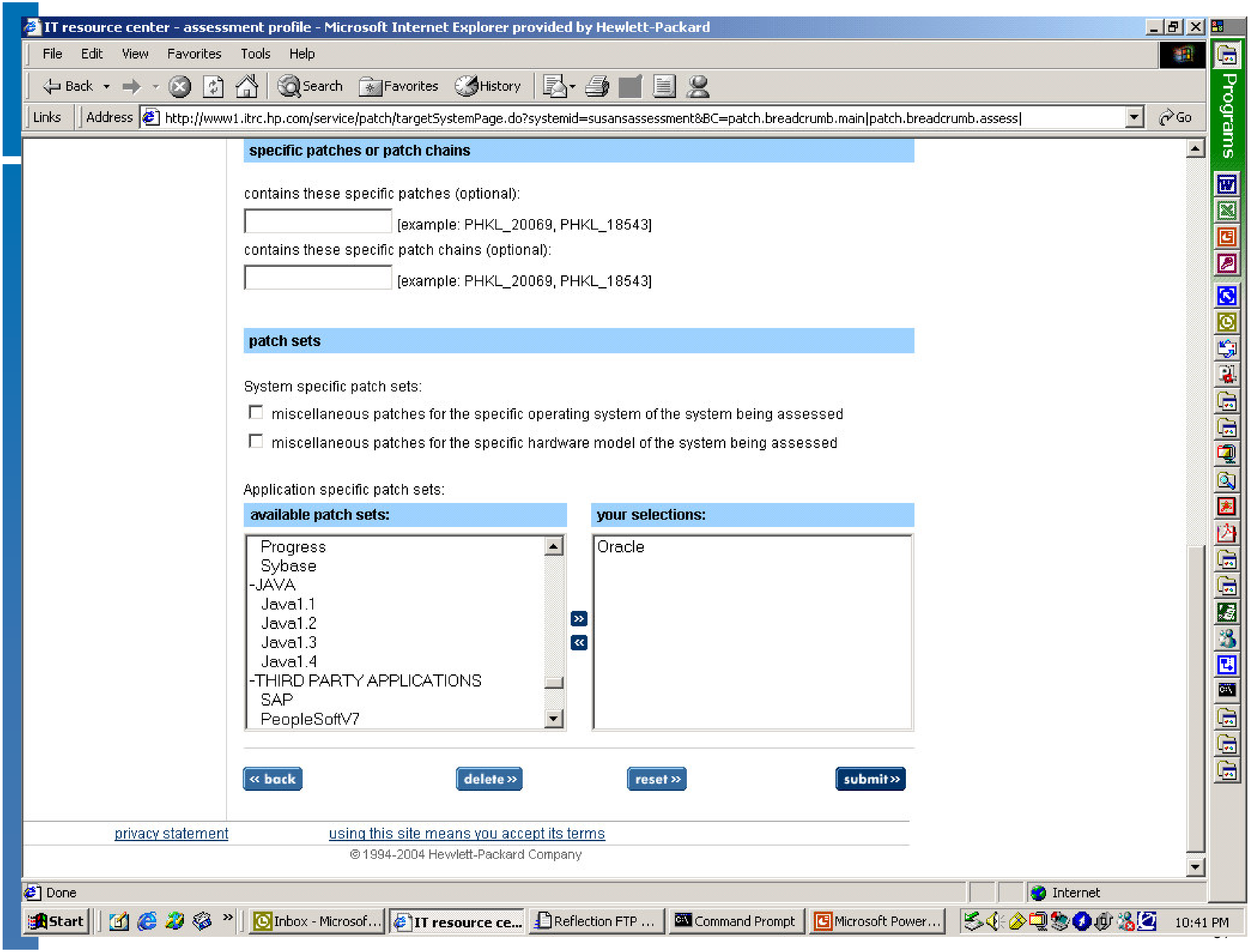
specific patches or patch chains

contains these specific patches (optional):

[example: PHKL_20069, PHKL_18543]

contains these specific patch chains (optional):

[example: PHKL_20069, PHKL_18543]



IT resource center - assessment profile - Microsoft Internet Explorer provided by Hewlett-Packard
File Edit View Favorites Tools Help
Back Search Favorites History
Links Address http://www1.itrc.hp.com/service/patch/targetSystemPage.do?systemid=susansassessment&BC=patch.breadcrumb.main|patch.breadcrumb.assess|
Go
Programs

specific patches or patch chains

contains these specific patches (optional):

[example: PHKL_20069, PHKL_18543]

contains these specific patch chains (optional):

[example: PHKL_20069, PHKL_18543]

patch sets

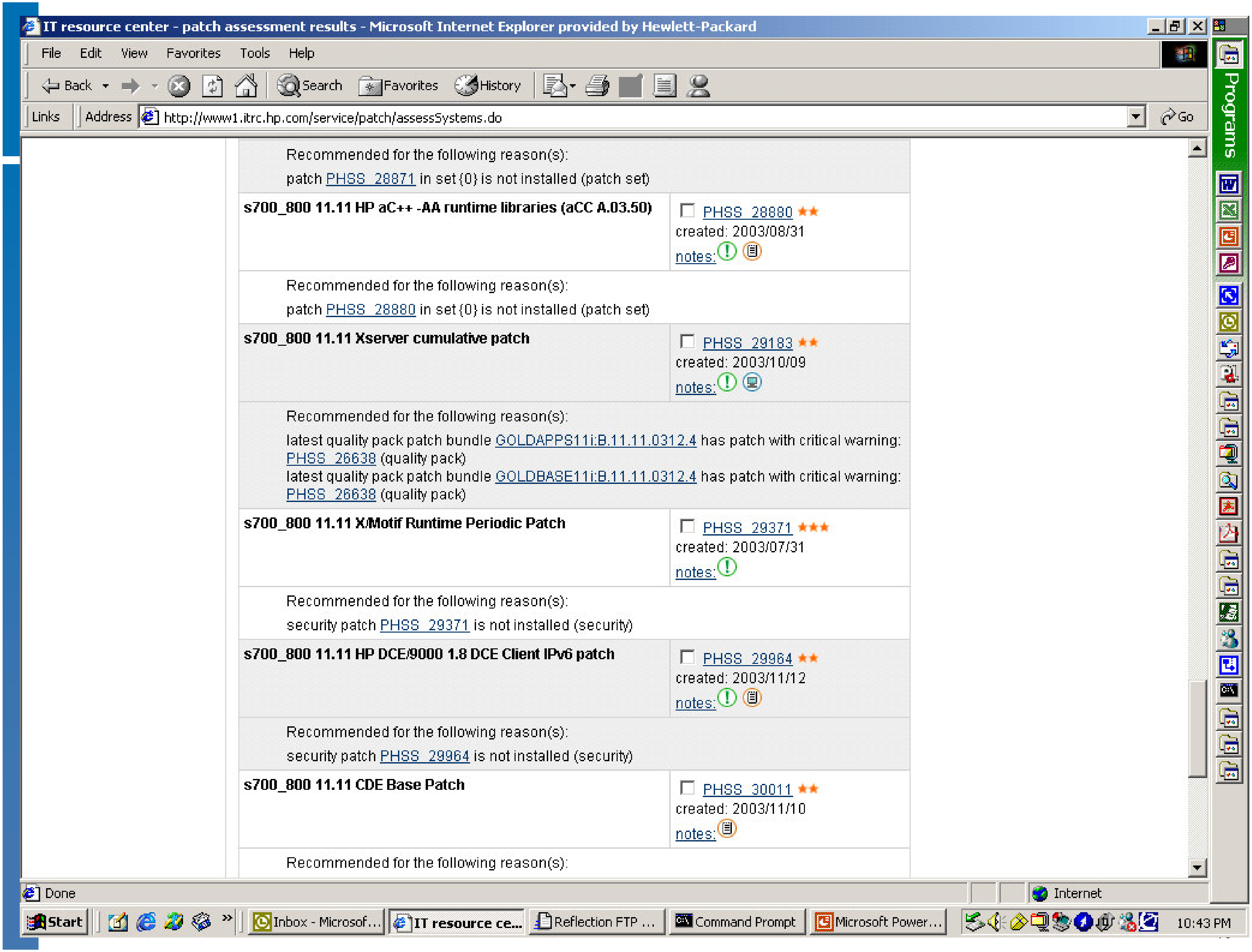
System specific patch sets:

□ miscellaneous patches for the specific operating system of the system being assessed

□ miscellaneous patches for the specific hardware model of the system being assessed

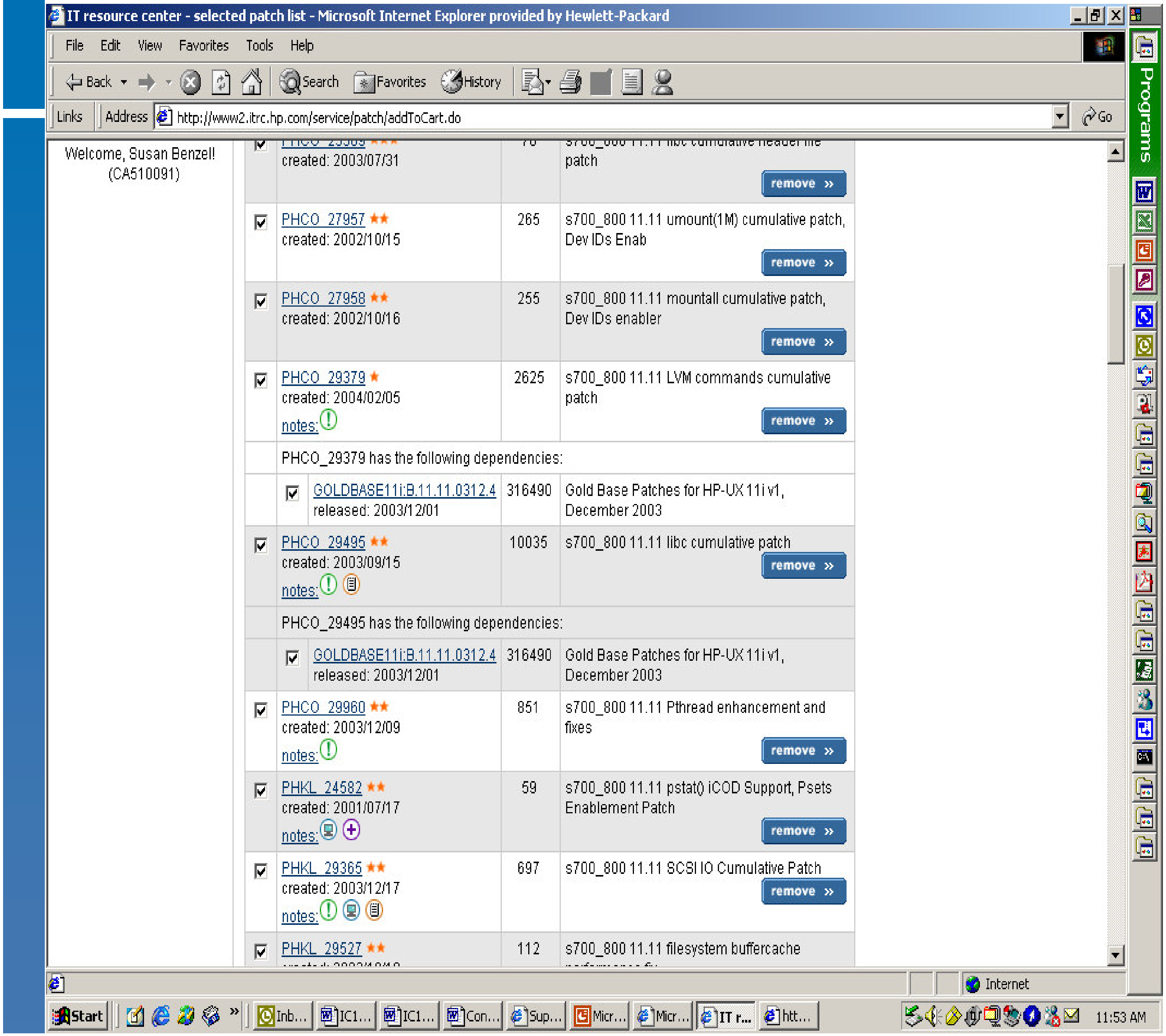
Application specific patch sets:

available patch sets:	your selections:
Progress Sybase -JAVA Java1.1 Java1.2 Java1.3 Java1.4 -THIRD PARTY APPLICATIONS SAP PeopleSoftV7	Oracle


IT resource center - patch assessment results - Microsoft Internet Explorer provided by Hewlett-Packard
File Edit View Favorites Tools Help
Back Search Favorites History
Links Address http://www1.itrc.hp.com/service/patch/assessSystems.do Go
Programs
Done
Internet
Start
Inbox - Microsof...
IT resource ce...
Reflection FTP ...
Command Prompt
Microsoft Power...
10:43 PM

Recommended for the following reason(s): patch PHSS_28871 in set {0} is not installed (patch set)	
s700_800 11.11 HP aC++ -AA runtime libraries (aCC A.03.50)	□ PHSS_28880 ★★ created: 2003/08/31 notes:
Recommended for the following reason(s): patch PHSS_28880 in set {0} is not installed (patch set)	
s700_800 11.11 Xserver cumulative patch	□ PHSS_29183 ★★ created: 2003/10/09 notes:
Recommended for the following reason(s): latest quality pack patch bundle GOLDAPPS11i:B.11.11.0312.4 has patch with critical warning: PHSS_26638 (quality pack) latest quality pack patch bundle GOLDBASE11i:B.11.11.0312.4 has patch with critical warning: PHSS_26638 (quality pack)	
s700_800 11.11 X/Motif Runtime Periodic Patch	□ PHSS_29371 ★★★ created: 2003/07/31 notes:
Recommended for the following reason(s): security patch PHSS_29371 is not installed (security)	
s700_800 11.11 HP DCE/9000 1.8 DCE Client IPv6 patch	□ PHSS_29964 ★★ created: 2003/11/12 notes:
Recommended for the following reason(s): security patch PHSS_29964 is not installed (security)	
s700_800 11.11 CDE Base Patch	□ PHSS_30011 ★★ created: 2003/11/10 notes:
Recommended for the following reason(s):	

“Selected Patch List” – picks up all patch dependencies

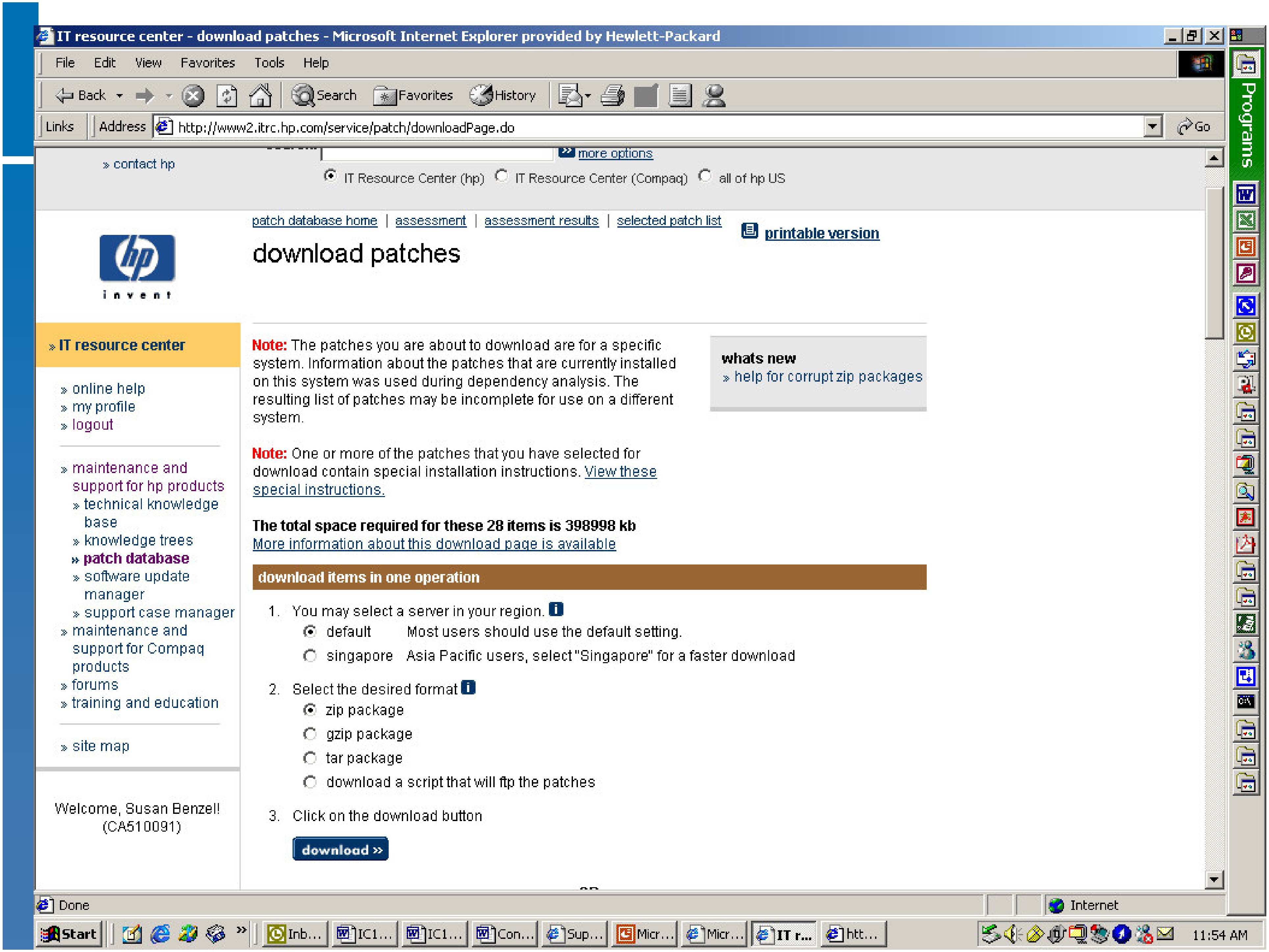


IT resource center - selected patch list - Microsoft Internet Explorer provided by Hewlett-Packard
File Edit View Favorites Tools Help
Back Search Favorites History
Links Address http://www2.itrc.hp.com/service/patch/addToCart.do Go
Programs

Welcome, Susan Benzel!
(CA510091)

☑	created: 2003/07/31		patch remove »
☑	PHCO_27957 ★★ created: 2002/10/15	265	s700_800 11.11 umount(1M) cumulative patch, Dev IDs Enab remove »
☑	PHCO_27958 ★★ created: 2002/10/16	255	s700_800 11.11 mountall cumulative patch, Dev IDs enabler remove »
☑	PHCO_29379 ★ created: 2004/02/05 notes:	2625	s700_800 11.11 LVM commands cumulative patch remove »
	PHCO_29379 has the following dependencies:		
	☑ GOLDBASE11i:B.11.11.0312.4 released: 2003/12/01	316490	Gold Base Patches for HP-UX 11i v1, December 2003
☑	PHCO_29495 ★★ created: 2003/09/15 notes:	10035	s700_800 11.11 libc cumulative patch remove »
	PHCO_29495 has the following dependencies:		
	☑ GOLDBASE11i:B.11.11.0312.4 released: 2003/12/01	316490	Gold Base Patches for HP-UX 11i v1, December 2003
☑	PHCO_29960 ★★ created: 2003/12/09 notes:	851	s700_800 11.11 Pthread enhancement and fixes remove »
☑	PHKL_24582 ★★ created: 2001/07/17 notes:	59	s700_800 11.11 pstat() iCOD Support, Psets Enablement Patch remove »
☑	PHKL_29365 ★★ created: 2003/12/17 notes:	697	s700_800 11.11 SCSI IO Cumulative Patch remove »
☑	PHKL_29527 ★★	112	s700_800 11.11 filesystem buffercache

Internet
Start Inb... IC1... IC1... Con... Sup... Micr... Micr... IT r... htt...
11:53 AM



» contact hp

» more options

● IT Resource Center (hp) ○ IT Resource Center (Compaq) ○ all of hp US

patch database home | assessment | assessment results | selected patch list

printable version

download patches

» IT resource center

» online help
» my profile
» logout

» maintenance and support for hp products
» technical knowledge base
» knowledge trees
» patch database
» software update manager
» support case manager
» maintenance and support for Compaq products
» forums
» training and education

» site map

Welcome, Susan Benzell (CA510091)

Note: The patches you are about to download are for a specific system. Information about the patches that are currently installed on this system was used during dependency analysis. The resulting list of patches may be incomplete for use on a different system.

whats new
» help for corrupt zip packages

Note: One or more of the patches that you have selected for download contain special installation instructions. View these special instructions.

The total space required for these 28 items is 398998 kb
More information about this download page is available

download items in one operation

1. You may select a server in your region.
   - ● default Most users should use the default setting.
   - ○ singapore Asia Pacific users, select "Singapore" for a faster download
2. Select the desired format
   - ● zip package
   - ○ gzip package
   - ○ tar package
   - ○ download a script that will ftp the patches
3. Click on the download button

download »

Patch Sets

- Tunable proactive patch maintenance using patches pre-selected by HP's Software Change Center
- Patch sets are updated weekly
- You specify the strategy and the areas
- Security Patch Set includes all patches recommended in Security Bulletins
- Available to any customer with a support contract
  - Fee-for-service for phone-in support customers
  - No charge with higher-level contracts (up to allowed limit of patch analyses)

Software Pack

- Enhancements to core HP-UX 11i
- Media updated twice a year OR download any time from http://software.hp.com

HP WORLD 2004
Solutions and Technology Conference & Expo

HP WORLD 2004

Solutions and Technology Conference & Expo

Co-produced by:

interex

shared knowledge • shared power

encompass

AN HP USER GROUP

RECOMMENDED TRAINING VENUE FOR THE

HP Certified Professional