Automated Security Hardening for NonStop Systems and So Much More….

Click to Watch Video
About CSP

Based in Toronto, Canada with Partners, Agents and Distributors worldwide

HPE Partner since 1987.

Develop, Support and Distribute Security, Compliance and Audit Solutions for the HPE NonStop® Market.

Our Customers include:

- Largest Banks
- Defense and Healthcare organizations
- Telecommunications

Customers need choices!

NonStop X Ready
Agenda

Our New Website (and Logo!)

Why Systems Security Hardening?

The CSP-Wiki™

Automating NonStop Security Hardening (and More!)
CSP – New Website

SAFEGUARD & OSS SECURITY HARDENING

HP NonStop is designed for reliability and availability and thus is the platform of choice for mission critical applications that just can’t afford to go down. Yet we know that more and more systems are vulnerable to attacks each day as hackers become more sophisticated and determined to bring down core systems or compromise sensitive user information. This threat becomes even more likely with the advent of NonStop X.
Why Security Hardening?

- Be proactive! Prevent expensive breaches!
- X86 environment offers more challenges
- Don’t use “Out of the Box” settings and hope!
- Prevent Accidents and Unintended Consequences
Why Harden When I have Good Monitoring?

Monitoring is good – but....

Typically alerts you after the fact

Use strong locks for your doors and windows

Make your systems a HARD target

Be pro-active not reactive
Sources of Threat

Three main attack threats:

1. Insider attack (Opportunism)
2. Outside hack attack (Criminal)
3. State sponsored attack (Terrorism)
Insider Attacks

- A 2015 SANS Institute Insider Threat report reveals:
  - Insider attacks becoming more frequent
  - Less than 50% have appropriate controls and about 33% have experienced an attack
  - Cost of an Insider attack typically exceeds $1M and often exceeds $5M
Why a Need to Harden NonStop?

OSS security requirements are not well understood

A baseline is needed to protect against “Drift and Decay”

The demand for knowledge is high – But expertise is in short supply
The Knowledge Challenge
Lack of Safeguard and OSS Security Expertise

Various surveys pointed to lack of security expertise –

Especially with OSS
So What Did CSP Do?

- Collected as much expert knowledge as possible!
- Collected data from FIVE sources of information
  - Public domain
  - External consultants
  - Inside knowledge – UNIX
  - Existing Compliance Reporting Product
  - Our customers
- We put it all together in a unique way
We Built the Wiki for NonStop Security™

- A web-based Wiki containing extensive Guardian and OSS security knowledge
- Over 700 (and growing) Security Hardening Rules for Safeguard and OSS including 200 PCIDSS Recommendations
- Nearly 100 for Linux Systems
- Expert Knowledge at Your Fingertips
Security Hardening Rules

- Initial System Hardening
  - Safeguard Configuration and Management
    - Audit
    - Safeguard Configuration Files
    - Passwords
    - Users and Aliases
    - Security Groups
    - Administrative Groups
    - Authentication
    - Access Control
    - Default Passwords
  - Software Installation Using DSM/SCM and Software Essentials
- User Management
- Guardian File Security
- OSS File Security
- SQL/MP Object Security
- SQL/MX Object Security
- NonStop Server for Java (NSJ)
# 0013 - Optimize Audit Trail Record Writing for Performance

<table>
<thead>
<tr>
<th>Rule Number</th>
<th>0013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>Optimize Audit Trail Record Writing for Performance</td>
</tr>
<tr>
<td>Verifiable</td>
<td>Yes</td>
</tr>
<tr>
<td>Category Level 1</td>
<td>Initial System Hardening</td>
</tr>
<tr>
<td>Category Level 2</td>
<td>Safeguard Configuration and Management</td>
</tr>
<tr>
<td>Category Level 3</td>
<td>Audit</td>
</tr>
<tr>
<td>Description/Reason</td>
<td>Audit trail record writing must be optimized for performance. You can configure Safeguard to either write audit records to disk individually (WRITE-THROUGH CACHE ON) or to cache the records in memory and write multiple records at a time (WRITE-THROUGH CACHE OFF).</td>
</tr>
<tr>
<td>Recommendation</td>
<td>For performance reasons, HP recommends setting WRITE-THROUGH CACHE to OFF (the default). Note: You run a small risk of losing multiple records if the cache is lost.</td>
</tr>
</tbody>
</table>

### WRITE-THROUGH CACHE { ON | OFF }

ON specifies that after each audit record is written, the block in which it resides is written to disk. OFF specifies that a block modified as an audit record is not written to disk immediately. The initial setting of WRITE-THROUGH CACHE is OFF.

```plaintext
PROTECT XP GUI > Safeguard> Audit Service | Write Through Cache ON|OFF
```

### Technical Notes

```plaintext
TACL> SAFECOM INFO AUDIT SERVICE
   CURRENT AUDIT POOL  $AUDIT.SAFE
   CURRENT AUDIT FILE   $AUDIT.SAFE.A0759814
   NEXT AUDIT POOL     
   RECOVERY             RECYCLE FILES
   CURRENT STATE        RECYCLING FILES
   WRITE-THROUGH CACHE  OFF
   EOF REFRESH          ON
```
Pages in category "Initial System Hardening"

The following 68 pages are in this category, out of 68 total.

- 0001 - Configuring Safeguard is Your First Priority
- 0002 - Set All Safeguard OBJECTTYPE Access Rights
- 0003 - Audit Safeguard Configuration Changes
- 0004 - Enable OSS Client Auditing
- 0005 - Test Audit Configuration Prior to Production
- 0006 - Configure the Safeguard Audit Service
- 0007 - Make Audit Pools Large Enough
- 0008 - Place Audit Pools on Disks That Will Not Adversely Affect Production Application Performance
- 0009 - No Audit Pools on $SYSTEM
- 0010 - Ensure Safeguard Audit Pool Volumes are Available During System Load
- 0011 - Configure Safeguard Audit Recycling
- 0012 - Backup Safeguard Audit Trails
- 0013 - Optimize Audit Trail Record Writing for Performance
- 0014 - Export Safeguard Audit to SIEM
- 0015 - Properly Secure the USERID File
- 0022 - Properly Secure Safeguard SAFE File
- 0031 - Carefully Control and Monitor Super Group Members
- 0032 - Create Aliases for Each User of a Shared User ID
- 0033 - Configure Command Interpreter Defaults for Safeguard-Protected Terminals
- 0034 - Populate the Safeguard Security Groups
- 0035 - Use the SECURITY-ADMINISTRATOR Security Group
- 0036 - Consider Populating All Safeguard Security Groups to Avoid Having the Default Memberships Apply
- 0037 - Do Not Add Non-SUPER-Group Users to the SUPER Group as File-Sharing Members
- 0038 - Define a Set of Users With the Authority to Add Other Users
- 0039 - Implement 2-Factor Identification Using CSP Authenticator
- 0040 - Keep $CMON In Sync With Safeguard
- 0041 - Prevent the Display of Passwords
- 0042 - Control How Authentication Failures are Handled
- 0043 - Use CSP PassPort to Control Authentication Failure Handling on a Per-User Basis
- 0044 - Control User Access toCMON
- 0045 - Control User Access to Safeguard Utilities
- 0046 - Control User Access to Safeguard Processes
- 0047 - Control User Access to Safeguard Variables
- 0048 - Control User Access to Safeguard Environment Variables
- 0049 - Control User Access to Safeguard Files
- 0050 - Control User Access to Safeguard Directories
- 0051 - Control User Access to Safeguard Parking
- 0052 - Control User Access to Safeguard Printers
- 0053 - Change the CLIM Password for Root
- 0054 - Change the NonStop Console Password for Adminstrator
- 0055 - Change the iLO Password of Admin on Each Blade
- 0056 - Change the iLO Password of Admin on Each CLIM
- 0057 - Change Passwords on Underlying System Components
- 0058 - Have a Reliable Process for Communicating Passwords to HP Service Providers
- 0059 - Assign DSM/SCM Roles to the Appropriate Users
- 0061 - Configure DSM/SCM Safeguard Running Requirement
- 0062 - Configure DSM/SCM Ownership for New Files
- 0063 - Configure DSM/SCM Security for New Files
- 0064 - Files Replaced by DSM/SCM Assume the Original File's Ownership and Security
- 0065 - Adequate Privileges Are Required to Activate Software Revisions
Introducing ... Protect-X!

- New Nonstop security hardening solution
- Self-Hosted Web Application using HTML5
- Change Control using Workflows
- Task Approval and Scheduling
- Automated Hardening Rules Compliance
- Audit
- Mobile Friendly
Protect-X Dashboard

- Exceptions: 20%
  - Total hardening rules applied
  - Compliance with hardening rules
  - Approved exceptions
  - Failed to comply with hardening rules

- Hardening
  Check system compliance against the hardening rules and make changes to system security to comply with the hardening rules.

- Protect-X Settings
  Set individual settings and user preferences for Protect-X.

- Approvals
  Approve or decline pending changes to security settings.

- Users
  Add, delete, or alter system User ID settings.

- Audit Monitor
  Control audit settings and run audit reports.

- Browse Files
  Browse individual files and directories to view and manage access.

- Command control
  View and manage system command control.

- SUDO Level 0 (No SUDO control)
- SUDO Level 1
- SUDO Level 2
- SUDO Level 3

- Vulnerability Management
  Execute queries to determine access rights to individual file sets.

- CSP
  Computer Security Products, Inc.
Advantages of Protect-X

Runs in any Web Browser

Protect-X has work flows and dialogs to manage Safeguard

Contains hardening rules based on the CSP-Wiki

Automatic implementation of rules

Built in user roles with authorization and audit
### User ACL's

<table>
<thead>
<tr>
<th>#</th>
<th>Node Name</th>
<th>User ID</th>
<th>User Name</th>
<th>Grant</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>ITANIUM</td>
<td>025,002</td>
<td>AGROUP2.ARTEM22</td>
<td>Grant</td>
<td>R</td>
</tr>
<tr>
<td>1</td>
<td>ITANIUM</td>
<td>025,003</td>
<td>AGROUP2.MAGGIE</td>
<td>Grant</td>
<td>R</td>
</tr>
<tr>
<td>2</td>
<td>ITANIUM</td>
<td>027,002</td>
<td>AGROUP3.ARTEM32</td>
<td>Grant</td>
<td>R</td>
</tr>
<tr>
<td>3</td>
<td>ITANIUM</td>
<td>029,002</td>
<td>BL.ONE</td>
<td>Grant</td>
<td>W</td>
</tr>
<tr>
<td>4</td>
<td>ITANIUM</td>
<td>029,053</td>
<td>BL.LOLO</td>
<td>Grant</td>
<td>E</td>
</tr>
<tr>
<td>5</td>
<td>ITANIUM</td>
<td>029,200</td>
<td>BL.ROOT</td>
<td>Grant</td>
<td>E</td>
</tr>
<tr>
<td>6</td>
<td>ITANIUM</td>
<td>102,000</td>
<td>ADDD/DDDA</td>
<td>Grant</td>
<td>R</td>
</tr>
<tr>
<td>7</td>
<td>ITANIUM</td>
<td>155,000</td>
<td>ABCTEST.A</td>
<td>Grant</td>
<td>R,W,E</td>
</tr>
<tr>
<td>8</td>
<td>ITANIUM</td>
<td>155,001</td>
<td>ABCTEST.GEORGE</td>
<td>Grant</td>
<td>R,W</td>
</tr>
<tr>
<td>9</td>
<td>ITANIUM</td>
<td>155,007</td>
<td>ABCTEST.GUEST</td>
<td>Grant</td>
<td>W</td>
</tr>
<tr>
<td>10</td>
<td>ITANIUM</td>
<td>155,012</td>
<td>ABCTEST.ASD</td>
<td>Grant</td>
<td>R</td>
</tr>
<tr>
<td>11</td>
<td>ITANIUM</td>
<td>155,034</td>
<td>ABCTEST.G998U</td>
<td>Grant</td>
<td>R</td>
</tr>
<tr>
<td>12</td>
<td>ITANIUM</td>
<td>155,089</td>
<td>ABCTEST.ARTEM15</td>
<td>Grant</td>
<td>P</td>
</tr>
<tr>
<td>13</td>
<td>ITANIUM</td>
<td>155,101</td>
<td>ABCTEST.ARTEM777</td>
<td>Grant</td>
<td>R,W</td>
</tr>
<tr>
<td>Name</td>
<td>Size</td>
<td>Permissions</td>
<td>Owner</td>
<td>Group</td>
<td>Modified</td>
</tr>
<tr>
<td>---------</td>
<td>------</td>
<td>--------------</td>
<td>-------</td>
<td>-------</td>
<td>-------------------</td>
</tr>
<tr>
<td>bin</td>
<td>4K</td>
<td>drwx-xr-x</td>
<td>root</td>
<td>root</td>
<td>8/17/2015, 6:42:06 AM</td>
</tr>
<tr>
<td>boot</td>
<td>4K</td>
<td>drwx-xr-x</td>
<td>root</td>
<td>root</td>
<td>9/9/2015, 9:27:43 AM</td>
</tr>
<tr>
<td>cdrom</td>
<td>5K</td>
<td>drwxr-xr-x</td>
<td>root</td>
<td>root</td>
<td>7/30/2015, 7:00:02 AM</td>
</tr>
<tr>
<td>dev</td>
<td>12K</td>
<td>drwxr-xr-x</td>
<td>root</td>
<td>root</td>
<td>10/19/2015, 12:49:24 PM</td>
</tr>
<tr>
<td>etc</td>
<td>4K</td>
<td>drwxr-xr-x</td>
<td>root</td>
<td>root</td>
<td>10/19/2015, 8:53:21 AM</td>
</tr>
<tr>
<td>home</td>
<td>4K</td>
<td>drwxr-xr-x</td>
<td>root</td>
<td>root</td>
<td>8/28/2015, 10:18:31 AM</td>
</tr>
<tr>
<td>lib</td>
<td>4K</td>
<td>drwxr-xr-x</td>
<td>root</td>
<td>root</td>
<td>7/30/2015, 7:38:52 AM</td>
</tr>
<tr>
<td>lib64</td>
<td>16K</td>
<td>drw-------</td>
<td>root</td>
<td>root</td>
<td>7/30/2015, 7:32:16 AM</td>
</tr>
<tr>
<td>lost+found</td>
<td>4K</td>
<td>drwx-r-xr-x</td>
<td>root</td>
<td>root</td>
<td>4/22/2015, 8:01:55 AM</td>
</tr>
<tr>
<td>media</td>
<td>4K</td>
<td>drwxr-xr-x</td>
<td>root</td>
<td>root</td>
<td>7/30/2015, 7:17:03 AM</td>
</tr>
<tr>
<td>mnt</td>
<td>4K</td>
<td>drwxr-xr-x</td>
<td>root</td>
<td>root</td>
<td>4/17/2015, 5:34:41 PM</td>
</tr>
<tr>
<td>opt</td>
<td>4K</td>
<td>drwxr-xr-x</td>
<td>root</td>
<td>root</td>
<td>9/14/2015, 12:23:11 PM</td>
</tr>
<tr>
<td>proc</td>
<td>0b</td>
<td>dr-xr-xr-x</td>
<td>root</td>
<td>root</td>
<td>10/16/2015, 11:20:39 AM</td>
</tr>
<tr>
<td>root</td>
<td>12K</td>
<td>drwxr-xr-x</td>
<td>root</td>
<td>root</td>
<td>8/31/2015, 5:31:35 PM</td>
</tr>
<tr>
<td>run</td>
<td>820b</td>
<td>drwxr-xr-x</td>
<td>root</td>
<td>root</td>
<td>10/17/2015, 7:51:29 AM</td>
</tr>
<tr>
<td>sbin</td>
<td>12K</td>
<td>drwxr-xr-x</td>
<td>root</td>
<td>root</td>
<td>8/17/2015, 6:42:06 AM</td>
</tr>
<tr>
<td>srv</td>
<td>4K</td>
<td>drwxr-xr-x</td>
<td>root</td>
<td>root</td>
<td>4/22/2015, 8:01:51 AM</td>
</tr>
<tr>
<td>sys</td>
<td>0b</td>
<td>dr-xr-xr-x</td>
<td>root</td>
<td>root</td>
<td>10/16/2015, 11:20:40 AM</td>
</tr>
<tr>
<td>tmp</td>
<td>4K</td>
<td>drwxwnwxr</td>
<td>root</td>
<td>root</td>
<td>10/20/2015, 12:21:15 PM</td>
</tr>
<tr>
<td>usr</td>
<td>4K</td>
<td>drwxr-xr-x</td>
<td>root</td>
<td>root</td>
<td>4/22/2015, 8:01:51 AM</td>
</tr>
<tr>
<td>var</td>
<td>4K</td>
<td>drwxr-xr-x</td>
<td>root</td>
<td>root</td>
<td>8/5/2015, 1:47:27 PM</td>
</tr>
<tr>
<td>initrd.img</td>
<td>33b</td>
<td>lrwxwnwxr</td>
<td>root</td>
<td>root</td>
<td>9/9/2015, 9:27:07 AM</td>
</tr>
<tr>
<td>initrd.img.old</td>
<td>33b</td>
<td>lrwxwnwxr</td>
<td>root</td>
<td>root</td>
<td>8/19/2015, 6:51:31 AM</td>
</tr>
<tr>
<td>vmlinuz</td>
<td>30b</td>
<td>lrwxwnwxr</td>
<td>root</td>
<td>root</td>
<td>9/9/2015, 9:27:07 AM</td>
</tr>
<tr>
<td>vmlinuz.old</td>
<td>30b</td>
<td>lrwxwnwxr</td>
<td>root</td>
<td>root</td>
<td>8/19/2015, 6:51:31 AM</td>
</tr>
</tbody>
</table>
OSS File Security Management

### Owner Information

<table>
<thead>
<tr>
<th>Existing owner</th>
<th>Existing group owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>aproskuri</td>
<td>aproskuri</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>New owner</th>
<th>New group owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select user</td>
<td>Select group</td>
</tr>
</tbody>
</table>

### Existing Permissions Information

#### Existing permissions

<table>
<thead>
<tr>
<th>Owner</th>
<th>Group</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>r</td>
<td>w</td>
<td>-</td>
</tr>
</tbody>
</table>

#### Special modes

<table>
<thead>
<tr>
<th>Owner</th>
<th>Group</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Recommended values

<table>
<thead>
<tr>
<th>Owner</th>
<th>Group</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Pending changes

- Change file permissions
  - rwx ?????
  - rwx????
  - ????wxx?

### File Basket

<table>
<thead>
<tr>
<th>System Name</th>
<th>Name</th>
<th>Size</th>
<th>Permissions</th>
<th>Owner</th>
<th>Group</th>
<th>Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>aproskuri-pc</td>
<td>/home/aproskuri/test_files/file1</td>
<td>0b</td>
<td>-rw-r--r--</td>
<td>aproskuri</td>
<td>aproskuri</td>
<td>11/3/2015, 11:14:04 AM</td>
</tr>
<tr>
<td>aproskuri-pc</td>
<td>/home/aproskuri/test_files/file2</td>
<td>0b</td>
<td>-rw-r--r--</td>
<td>aproskuri</td>
<td>aproskuri</td>
<td>11/3/2015, 11:14:05 AM</td>
</tr>
<tr>
<td>aproskuri-pc</td>
<td>/home/aproskuri/test_files/file3</td>
<td>0b</td>
<td>-rw-r--r--</td>
<td>aproskuri</td>
<td>aproskuri</td>
<td>11/3/2015, 11:14:07 AM</td>
</tr>
<tr>
<td>aproskuri-pc</td>
<td>/home/aproskuri/test_files/file4</td>
<td>0b</td>
<td>-rw-r--r--</td>
<td>aproskuri</td>
<td>aproskuri</td>
<td>11/3/2015, 11:14:07 AM</td>
</tr>
<tr>
<td>aproskuri-pc</td>
<td>/home/aproskuri/test_files/file5</td>
<td>0b</td>
<td>-rw-r--r--</td>
<td>aproskuri</td>
<td>aproskuri</td>
<td>11/3/2015, 11:14:08 AM</td>
</tr>
</tbody>
</table>
## Protect-X Safeguard Globals Management

### Audit Client Service

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUDIT-CLIENT-GUARDIAN</td>
<td>Delineates whether the Safeguard software accepts Guardian-related audit records from HP privileged subsystems.</td>
</tr>
<tr>
<td>AUDIT-CLIENT-OSS</td>
<td>ON specifies that the Safeguard software will accept OSS related audit records from privileged client subsystems and write.</td>
</tr>
<tr>
<td>AUDIT-OSS-FILTER</td>
<td>Indicates if user level attributes, AUDIT-USER-ACTION-PASS and AUDIT-USER-ACTION-FAIL, enable or disable.</td>
</tr>
</tbody>
</table>

### Audit Object Access

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUDIT-OBJECT-ACCESS-PASS</td>
<td>Defines additional auditing for successful object accesses. This setting supplements the audit settings in all object.</td>
</tr>
<tr>
<td>AUDIT-OBJECT-ACCESS-FAIL</td>
<td>Defines additional auditing for unsuccessful object accesses. This setting supplements the audit settings in all object.</td>
</tr>
</tbody>
</table>

### Misc

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WARNING-FALLBACK-SECURITY</td>
<td>WARNING-FALLBACK-SECURITY controls SAFEGUARD results when WARNING-MODE is ON.</td>
</tr>
<tr>
<td>ALLOW-NODE-ID-ACL</td>
<td>Defines whether ACL entries containing explicit node identifiers for subjects are consulted to determine remote access. The default is ON.</td>
</tr>
</tbody>
</table>

### Warning Mode

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYSTEM-WARNING-MODE</td>
<td>This setting indicates whether or not Safeguard will log the WARNING-RECORD for individual Object.</td>
</tr>
</tbody>
</table>

### Audit Object Authorization Record Access

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUDIT-OBJECT-MANAGE-PASS</td>
<td>Sets the audit object manage pass. The default is LOCAL.</td>
</tr>
<tr>
<td>AUDIT-OBJECT-MANAGE-FAIL</td>
<td>Sets the audit object manage fail. The default is NONE.</td>
</tr>
</tbody>
</table>

### Additional Options

- Submit for approval
- Implement Now

---

**CSP**

**COMPUTER SECURITY PRODUCTS, INC.**
## Protect-X Actions Approval Screen

<table>
<thead>
<tr>
<th>Case number</th>
<th>Status</th>
<th>Timestamp</th>
<th>Affected Items</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>approved</td>
<td>Mon Nov 09 2015 18:07:22 GMT-0500 (EST)</td>
<td>5 file(s)</td>
<td>Change file permissions =&gt; rw????????</td>
</tr>
<tr>
<td>2</td>
<td>awaiting approval</td>
<td>Mon Nov 09 2015 18:07:12 GMT-0500 (EST)</td>
<td>5 file(s)</td>
<td>Change file permissions =&gt; rw-rw-rwx??</td>
</tr>
<tr>
<td>3</td>
<td>awaiting approval</td>
<td>Mon Nov 09 2015 18:07:12 GMT-0500 (EST)</td>
<td>5 file(s)</td>
<td>Change file permissions =&gt; rw-rwx??</td>
</tr>
</tbody>
</table>

**Actions:**
- Approve
- Decline
- Details
- Implement Now
- Filter by user
- Filter by category
- Filter by Node
<table>
<thead>
<tr>
<th>Audit Record Number</th>
<th>Text</th>
<th>Timestamp</th>
<th>Affected Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>#6</td>
<td>Change file permissions, case has been implemented</td>
<td>Mon Nov 09 2015 18:07:30</td>
<td>5 file(s)</td>
</tr>
<tr>
<td>#5</td>
<td>Change file permissions, case has been approved</td>
<td>Mon Nov 09 2015 18:07:22</td>
<td>5 file(s)</td>
</tr>
<tr>
<td>#4</td>
<td>Change file permissions, case has been committed</td>
<td>Mon Nov 09 2015 18:07:13</td>
<td>5 file(s)</td>
</tr>
<tr>
<td>#3</td>
<td>Change file permissions</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
OSS Command Control, Effective Access And More!

This page is under construction!
Protect-X Summary

- Free CSP-Wiki – 700 rules and growing! User base growing daily
- Safeguard User and Globals Management Complete
- Scheduled for next release (Fall 2016):
  - Implementation of Automated Wiki-based Hardening
  - Access Validation Engine
  - OSS Command Control
  - More Graphics and Widgets
- Cross Platform Support for other UNIX Servers (next 12 months)
New Website

“We Built the Wiki for NonStop Security®”

Proven Products to Help Harden NonStop Systems

Protect-X

Automated Expert Security Hardening for NonStop and UNIX systems
THANK YOU!

Please visit our Website for more information

www.CSPsecurity.com