CSP Vulnerability Scanner 2.00

Sample Reports

Preface

CSP Vulnerability Scanner™ is a reporting product intended to aid in the enforcement of security policies and procedures. CSP Vulnerability Scanner™ can produce reports which:

- Analyze the security settings on a system and report improper practices or security loopholes.
- List the security settings by user.
- List the security settings by object.
- Verify access to particular objects by particular users, taking into account the Safeguard configuration.
- Help identify subvolumes containing similarly secured diskfiles, which might allow for the simplification of your Safeguard configuration.
- Explain the logic that Safeguard uses to arbitrate a particular access request.
- List orphan files – Orphan files are files created by user which no longer exists.

The Safeguard security system is recommended, but not required for the Security Analysis Report. All other reports require that Safeguard be running.
CSP Vulnerability Scanner™ does not secure your system. CSP Vulnerability Scanner™ is a tool designed to quickly and efficiently collect information that will assist you in this task. You must secure your system based on information not only from CSP Vulnerability Scanner™, but from users, support staff, and management.

What's New in Release 2.00

CSP Vulnerability Scanner™ Release 2.00 has the following new reports:

- *Critical File Vulnerability* Report now has a new option:
Critical Objects Vulnerability Report is added. This report verifies only specific objects. These files/objects are saved in a given Critical file. These objects can be subvolumes, disk-volumes, devices, processes, disk-file patterns or saved disk-file patterns.

- ***Weak Password Vulnerability*** Report:
This report compares the password of a given user against a list of 'weak' passwords.

- ***Compare History for Group Members*** Report:
These new reports compare Safeguard groups (and their members). The objectives is to list added/deleted Safeguard groups, and/or their members – between two *Group Members* reports.

- ***New Program Discovery*** Report has a new option:
New TACL Macro Discovery Report is added. This report shows list of TACL macros created from a specific date or in a time frame on a specified sub-volume. This helps identifing suspicious/unauthorized new TACL macros

Sample reports

These are some sample reports in version 2.00 of CSP Vulnerability Scanner:

1. **Compare History of ALL Groups/Members - Summary.**

   This report compares the reults from any 2 reports executed before, on the groups and their members – as summary.

   Example: Report below shows a member was added in group ABCTEST before the execution of GROUPMEMBERS report on 2024-01-26 12:02 and hence one increase in the total members.

```
********************************************************************************

          *** List of GROUPMEMBER reports executed ***

                                          TOTAL
    Run#  Run Date                    Groups       Members
       1  2024-01-26 11:57:45            26           214
       2  2024-01-26 11:58:59            26           214
       3  2024-01-26 12:02:33            26           215

********************************************************************************
--------------------------------------------------------------------------------
\NS3X.$DATA.VS200.CSPHIST Version 2.00 - System \NS3X        26Jan2024, 12:02
Copyright (C) 2022-2023 Computer Security Products Inc.
Run by: SUPER.SUPER (255,255)  at \NS3X.$ZTN0.#PT4YZ46
--------------------------------------------------------------------------------
COMPARE HISTORY GROUPMEMBERS SUMMARY
--------------------------------------------------------------------------------

                           *** GROUPMEMBER History ***
                                    Summary

   Run Date:                          2024-01-26 11:57:45  2024-01-26 12:02:33

   Group                                          Members              Members

   (  101) 001TEST                                    3                    3
   (   16) A                                          6                    6
   (  102) A001TEST                                   8                    8
   (  155) ABCTEST                                    4                    5
   (   29) BL                                        14                   14
   (    1) CSP                                       51                   51
   (  300) fsgroup                                    5                    5
   (    2) GCC                                        1                    1
   (    3) LI                                         1                    1
   (  250) LIGE                                       1                    1
   (  179) LIGE1                                      0                    0
   (  145) LIGE2                                      0                    0
   (   13) MQM                                        2                    2
   (    5) newtest-peter                              0                    0
   (  290) parneet-file-sharing-group                 2                    2
   (    7) QA                                         1                    1
   (48484) QAT                                        6                    6
   (  337) rick                                       2                    2
   (65537) SECURITY-CLIM-ADMIN                        4                    4
   (65536) SECURITY-ENCRYPTION-ADMIN                  1                    1
   (  255) SUPER                                     52                   52
```

```
(   99) TEST                                    35                  35
(  100) TEST001                                  7                   7
(   78) TESTGRP                                  4                   4
(  251) WELLS                                    3                   3
(34255) xxtest801                                1                   1

--------------------------------------------------------------------------------
     Total Groups:                              26                  26
           Members:                            214                 215
```

2. **Compare History of ALL Groups/Members - Detail.**
   This report compares the reults from any 2 reports executed before on the groups and their members – in detailed form.

   Example: Highlighted below is only part of the detailed report produced. It shows the new member added to the group ABCTEST.

```
********************************************************************************

           *** List of GROUPMEMBER reports executed ***

                                          TOTAL
    Run#  Run Date                    Groups       Members
       1  2024-01-26 11:57:45            26           214
       2  2024-01-26 11:58:59            26           214
       3  2024-01-26 12:02:33            26           215

********************************************************************************
--------------------------------------------------------------------------------
\NS3X.$DATA.VS200.CSPHIST Version 2.00 - System \NS3X        26Jan2024, 12:04
Copyright (C) 2022-2023 Computer Security Products Inc.
Run by: SUPER.SUPER (255,255)  at \NS3X.$ZTN0.#PT4YZ46
--------------------------------------------------------------------------------
COMPARE HISTORY GROUPMEMBERS DETAIL
--------------------------------------------------------------------------------

                        *** GROUPMEMBER History ***
                                  Details

 2024-01-26 11:57:45                  2024-01-26 12:02:33

 Group   Members                      Group   Members


 (  101) 001TEST                      (  101) 001TEST
         *Same*                               *Same*

 (   16) A                            (   16) A
         *Same*                               *Same*

 (  102) A001TEST                     (  102) A001TEST
         *Same*                               *Same*

 (  155) ABCTEST                      (  155) ABCTEST
                                              TEST.ABC

 (   29) BL                           (   29) BL
         *Same*                               *Same*
```

(1)	CSP	(1)	CSP
	Same		*Same*
(300)	fsgroup	(300)	fsgroup
	Same		*Same*
(2)	GCC	(2)	GCC
	Same		*Same*
(3)	LI	(3)	LI
	Same		*Same*
(250)	LIGE	(250)	LIGE
	Same		*Same*
(179)	LIGE1	(179)	LIGE1
	Same		*Same*
(145)	LIGE2	(145)	LIGE2
	Same		*Same*
(13)	MQM	(13)	MQM
	Same		*Same*
(5)	newtest-peter	(5)	newtest-peter
	Same		*Same*
(290)	parneet-file-sharing-group	(290)	parneet-file-sharing-group
	Same		*Same*
(7)	QA	(7)	QA
	Same		*Same*
(48484)	QAT	(48484)	QAT
	Same		*Same*
(337)	rick	(337)	rick
	Same		*Same*
(65537)	SECURITY-CLIM-ADMIN	(65537)	SECURITY-CLIM-ADMIN
	Same		*Same*
(65536)	SECURITY-ENCRYPTION-ADMIN	(65536)	SECURITY-ENCRYPTION-ADMIN
	Same		*Same*
(255)	SUPER	(255)	SUPER
	Same		*Same*
(99)	TEST	(99)	TEST
	Same		*Same*
(100)	TEST001	(100)	TEST001
	Same		*Same*
(251)	WELLS	(251)	WELLS
	Same		*Same*
(34255)	xxtest801	(34255)	xxtest801
	Same		*Same*
Total Groups:	26		26
Members:	214		215

3. **Compare History of Groups where a User is a Member.**
   This report compares the reults from any 2 reports executed before for the groups that a user belongs to.

   Example: The report below shows there was a change in the associated groups for user CSP.PTHIND.

```
********************************************************************************


        *** List of reports on Groups ***
            For User CSP.PTHIND (1,5)

    Run#  Run Date                  Num Groups
       1  2024-01-26 12:06:12               2
       2  2024-01-26 12:07:24               3

********************************************************************************
--------------------------------------------------------------------------------
\NS3X.$DATA.VS200.CSPHIST Version 2.00 - System \NS3X        26Jan2024, 12:07
Copyright (C) 2022-2023 Computer Security Products Inc.
Run by: SUPER.SUPER (255,255)  at \NS3X.$ZTN0.#PT4YZ46
--------------------------------------------------------------------------------
COMPARE HISTORY USER csp.pthind
--------------------------------------------------------------------------------


                                *** USER History ***
                                      Details

 User: CSP.PTHIND

 2024-01-26 12:06:12                  2024-01-26 12:07:24

 Primary Group                        Primary Group
 (    1) CSP                          (    1) CSP

 Group                                Group

 (    1) CSP                          (    1) CSP
                                      (   16) A
 (  290) parneet-file-sharing-group   (  290) parneet-file-sharing-group
```

4. **Compare History of Groups where an Alias is a Member.**
   This report compares the reults from any 2 reports executed before for the groups that an alias belongs to.

   Example: The report below shows there was a change in the associated groups for alias 'parneetk'.

```
********************************************************************************

                  *** List of reports on Groups ***
                      For Alias: parneetk

    Run#  Run Date                 Num Groups   Corr. User
       1  2024-01-26 12:08:26               1   CSP.PARN (1,25)
       2  2024-01-26 12:09:32               2   CSP.PARN (1,25)

********************************************************************************
--------------------------------------------------------------------------------
\NS3X.$DATA.VS200.CSPHIST Version 2.00 - System \NS3X        26Jan2024, 12:09
Copyright (C) 2022-2023 Computer Security Products Inc.
Run by: SUPER.SUPER (255,255)  at \NS3X.$ZTN0.#PT4YZ46
--------------------------------------------------------------------------------
COMPARE HISTORY ALIAS parneetk
--------------------------------------------------------------------------------


                              *** Alias History ***
                                    Details

 Alias: parneetk

 2024-01-26 12:08:26                  2024-01-26 12:09:32

 Corr. User                           Corr. User
 CSP.PARN (1,25)                      CSP.PARN (1,25)

 Group                                Group


 (    1) CSP                          (    1) CSP
                                      (    7) QA
```

5. **Safeguard Object Verification Report.**
   This job checks security for specified object – Volume/Sub-Volume/Device/Process/Diskfile-Pattern/Saved Diskfile-pattern.

```
VERIFY OBJ[ECTS] IN <filename>, [VOL[UME]              ]
                                [SUBVOL[UME]           ]
                                [DEVICE                ]
                                [PROCESS               ]
                                [DISKFILE-PATTERN      ]
                                [SAVED-DISKFILE-PATTERN]
```

<Filename> contains object names for specified object-type, separated by newline character.

```
$DATA.VS200.CSPVRPT Version 2.0.0 - System \NS3X  26-Jan-2024 12:20
CSP Vulnerability Scanner Copyright(C) 2024 Computer Security Products Inc
Run by SUPER.SUPER (255,255) at $ZTN0.#PT4YZ3X
--------------------------------------------------------------------------------
VERIFY DISKFILE PATTERNS IN $D2.SPARN.INPUT2
--------------------------------------------------------------------------------

Specified entries:

$D2.SPARN.*
$D1.ORPHAN.*
$d2.ptnp240.*
$d2.parn?.t*
$d*.parnc.*


Verifying Objects
This checks the security for objects of specified type

** M01-07001 WARNING: At least one invalid entry was found in the input file:
                      $D2.SPARN.*
      RECOMMENDATION: Correct the input file.

              WARNING: At least one invalid entry was found in the input file:
                       $D1.ORPHAN.*

              WARNING: At least one invalid entry was found in the input file:
                       $D2.PTNP240.*

              WARNING: At least one invalid entry was found in the input file:
                       $D2.PARN?.T*

              WARNING: At least one invalid entry was found in the input file:
                       $D*.PARNC.*
```

6. **Discover new TACL macros.**
   This job finds TACL macros created since the specified date (or for the last ‘n’ number of days) in a specified location.

   Example: The report below shows three new TACL macros were found on the specified pattern (`$d2.PTVS200A.*`) since 18-Sept-2023.

```
$DATA.VS200.CSPVRPT Version 2.0.0 - System \NS3X  26-Jan-2024 12:18
CSP Vulnerability Scanner Copyright(C) 2024 Computer Security Products Inc
Run by SUPER.SUPER (255,255) at $ZTN0.#PT4YZ3X
--------------------------------------------------------------------------------

New File Discovery Report
Find TACL macros created since the specified date

DISCOVER NEW TACL MACROS , FROM 2023-SEP-18, PATTERN *

--------------------------------------------------------------------------------
DISCOVER NEW TACL MACROS
--------------------------------------------------------------------------------

Looking for new TACL macros

   M01-06101 Observation: The following new TACL macro has been found:
                          $D2.PTVS200A.SECUREVS
          RECOMMENDATION: Check if new macro is expected.

             Observation: The following new TACL macro has been found:
                          $D2.PTVS200A.SETUP

             Observation: The following new TACL macro has been found:
                          $D2.PTVS200A.VSREPORT
```

7. **Weak Passwords Report:**

   The report checks password(s) for a user and its aliases (if any) against known weak passwords. Known weak passwords are defined in an EDIT file used by the report. This file comes with the SETUP and is customizable. Guardian user name can also be specified as input but the intended use is primarily for SUPER.SUPER.

   Example: The report below shows an associated alias for User CSP.PARN has a weak password as per the specified weak-password input file, named WEAKPWD.

```
$DATA.VS200.CSPVRPT Version 2.0.0 - System \NS3X  26-Jan-2024 12:11
CSP Vulnerability Scanner Copyright(C) 2024 Computer Security Products Inc
Run by SUPER.SUPER (255,255) at $ZTN0.#PT4YZ3X
--------------------------------------------------------------------------------

Weak Passwords Report
Check passwords of CSP.PARN and its aliases against known weak passwords

PASSWORDS AGAINST WEAKPWD FOR CSP.PARN

Global settings:

  PASSWORD-ALGORITHM    = HMAC256

$DATA.VS200.CSPVRPT Version 2.0.0 - System \NS3X  26-Jan-2024 12:11
CSP Vulnerability Scanner Copyright(C) 2024 Computer Security Products Inc
Run by SUPER.SUPER (255,255) at $ZTN0.#PT4YZ3X
--------------------------------------------------------------------------------
CHECK PASSWORDS AGAINST KNOWN WEAK PASSWORDS IN WEAKPWD
--------------------------------------------------------------------------------

Checking for weak passwords

** M01-08001 WARNING: Password for the following user / alias is a known weak pa
                      ssword:
                      parneetk
      RECOMMENDATION: Change password for the user / alias.
```

8. Safeguard Globals Report:

The Safeguard Global report displays the current Safeguard setting.

```
--------------------------------------------------------------------------------
$DATA.VS200.CSPSRV Version 2.00 - System \NS3X               26 Jan 24, 11:54
Copyright (C) 2022-2024 Computer Security Products Inc.
Run by: SUPER.SUPER (255,255) at $ZTN0.#PT4YZ46
--------------------------------------------------------------------------------
SAFEGUARD GLOBALS
--------------------------------------------------------------------------------
SAFEGUARD IS CONFIGURED WITH SUPER.SUPER DENIABLE

AUTHENTICATE-MAXIMUM-ATTEMPTS  = 0
AUTHENTICATE-FAIL-TIMEOUT      = 0 SECONDS
AUTHENTICATE-FAIL-FREEZE       = OFF
PROMPT-BEFORE-STOP             = OFF

PASSWORD-REQUIRED              = ON
PASSWORD-HISTORY               = 3
PASSWORD-ENCRYPT               = ON
PASSWORD-MINIMUM-LENGTH        = 4
PASSWORD-MAXIMUM-LENGTH        = 64
PASSWORD-ALGORITHM             = HMAC256
PASSWORD-COMPATIBILITY-MODE    = OFF
PASSWORD-UPPERCASE-REQUIRED    = OFF
PASSWORD-LOWERCASE-REQUIRED    = OFF
PASSWORD-NUMERIC-REQUIRED      = OFF
PASSWORD-SPECIALCHAR-REQUIRED  = OFF
PASSWORD-SPACES-ALLOWED        = OFF
PASSWORD-MIN-QUALITY-REQUIRED  = 0
PASSWORD-MAY-CHANGE            = 0 DAYS BEFORE EXPIRATION
PASSWORD-EXPIRY-GRACE          = 4 DAYS  AFTER EXPIRATION

SYSTEM-WARNING-MODE            = OFF
WARNING-FALLBACK-SECURITY      = GRANT
OBJECT-WARNING-MODE            = OFF

ALLOW-NODE-ID-ACL              = OFF

CHECK-DEVICE                   = ON
CHECK-SUBDEVICE                = ON
DIRECTION-DEVICE               = DEVICE-FIRST
COMBINATION-DEVICE             = ALL
ACL-REQUIRED-DEVICE            = OFF

CHECK-PROCESS                  = ON
CHECK-SUBPROCESS               = ON
DIRECTION-PROCESS              = SUBPROCESS-FIRST
COMBINATION-PROCESS            = FIRST-ACL
ACL-REQUIRED-PROCESS           = OFF

CHECK-VOLUME                   = OFF
CHECK-SUBVOLUME                = ON
CHECK-FILENAME                 = ON
CHECK-DISKFILE-PATTERN         = OFF
DIRECTION-DISKFILE             = VOLUME-FIRST
COMBINATION-DISKFILE           = ALL
ACL-REQUIRED-DISKFILE          = OFF
CLEARONPURGE-DISKFILE          = OFF

--------------------------------------------------------------------------------
CSP Vulnerability Scanner (2.00).                              Page     1
```

9. Orphan Files Report:

The Orphan Files report displays the list of orphan Guardian files – files owned by an undefined user, or files with undefined users in their ACLs.

```
--------------------------------------------------------------------------------
\NS3X.$DATA.VS200.CSPRPT Version 2.00 - System \NS3X       26 Jan 2024, 12:36
Copyright (C) 2022-2024 Computer Security Products Inc.
Run by: SUPER.SUPER (255,255)  at \NS3X.$ZTN0.#PT4YZ46
--------------------------------------------------------------------------------
ORPHAN GUARDIAN-FILES $WORK*.*.T* BYUSER
--------------------------------------------------------------------------------
Searching for Orphaned Files on: \NS3X.$WORK*.*.T*

001,066 (?.?) owns orphaned file \NS3X.$WORK.PP530.T6241LOG
001,066 (?.?) owns orphaned file \NS3X.$WORK.PP530.T9154CFG
001,066 (?.?) owns orphaned file \NS3X.$WORK.PP530.T9154CPY
001,066 (?.?) owns orphaned file \NS3X.$WORK.PP530.T9154CTL
001,066 (?.?) owns orphaned file \NS3X.$WORK.PP530.T9154LOG
001,066 (?.?) owns orphaned file \NS3X.$WORK.PP530.T9154MAP
001,066 (?.?) owns orphaned file \NS3X.$WORK.PP530.TR
001,066 (?.?) owns orphaned file \NS3X.$WORK.PP530B.TR
001,066 (?.?) owns orphaned file \NS3X.$WORK.PP530BKU.T6241LOG
001,066 (?.?) owns orphaned file \NS3X.$WORK.PP530BKU.T9154CFG
001,066 (?.?) owns orphaned file \NS3X.$WORK.PP530BKU.T9154CPY
001,066 (?.?) owns orphaned file \NS3X.$WORK.PP530BKU.T9154CTL
001,066 (?.?) owns orphaned file \NS3X.$WORK.PP530BKU.T9154LOG
001,066 (?.?) owns orphaned file \NS3X.$WORK.PP530BKU.T9154MAP
001,066 (?.?) owns orphaned file \NS3X.$WORK.PP530BKU.TR
001,066 (?.?) owns orphaned file \NS3X.$WORK.PPW5530B.TR

====================
001,066 (CSP.????????)

Total Non-Existent UserIDs       =     1

Number of Orphaned Files         =    16

0 Errors and 0 Warnings were issued.
```

10. Security Analysis Report:

This report displays the security check results performed on users, files, CMON, Guardian or Safeguard.

Example: A sample report follows:

```
 ------------------------------------------------------------------------------
$DATA.VS200.CSPSRV Version 2.00 - System \NS3X               26 Jan 24, 12:49
Copyright (C) 2022-2024 Computer Security Products Inc.
Run by: SUPER.SUPER (255,255) at $ZTN0.#PT4YZ46
------------------------------------------------------------------------------
CHECK GUARDIAN
------------------------------------------------------------------------------

Checking Guardian Settings
This checks Guardian authentication settings.


   M01-04042 Warning: PWCONFIG info shows you have PROMPTPASSWORD set to
                      BLIND.
      RECOMMENDATION: Set PROMPTPASSWORD ECHO, with the PWCONFIG program.


   M01-04043 Warning: PWCONFIG info shows MINPASSWORDLEN set to 4.
      RECOMMENDATION: Set MINPASSWORDLEN 8, with the PWCONFIG program.


   M01-04041 Observe: The CONFIGP file does not contain recognizable values.
      RECOMMENDATION: The PASSWORD settings can not be checked.

------------------------------------------------------------------------------
CHECK TACL
------------------------------------------------------------------------------

Checking TACL configuration
This checks the TACL CONFIGURATION attributes. These values control LOGON and
LOGOFF processing by TACL.


   M01-02004 Warning: The AUTOLOGOFFDELAY attribute is set to -1.
      RECOMMENDATION: Set AUTOLOGOFFDELAY to 15.  Note: The AUTOLOGOFFDELAY
                      setting determines how many minutes TACL delays before
                      logging off an idle terminal.


   M01-02006 Warning: The REMOTESUPERID attribute is set to -1.
      RECOMMENDATION: Set REMOTESUPERID to 0.  Note: If the value of
                      REMOTESUPERID is zero, TACL will not permit users at
                      remote terminals to logon as the SUPER ID. (A remote
                      terminal is one connected to another system in the
                      network).

------------------------------------------------------------------------------
CHECK USERS
------------------------------------------------------------------------------

Checking USERS
This checks various user-related security settings.


   M01-00004 Warning: The PASSWORD-MUST-CHANGE value for user CSP.TESDT is
                      NEVER.
      RECOMMENDATION: Set PASSWORD-MUST-CHANGE for this user to 90.

             Warning: The PASSWORD-MUST-CHANGE value for user CSP.USER1 is
                      NEVER.
```

11. Authorization Report:

This report displays user authorizations on files, sub-volumes, volumes ordered by obejcts or users.

Example: Sample reports follows:

```
*************************************************************************
*                                                                       *
* $DATA.VS200.CSPREP Version 2.00 - System \NS3X       26Jan24, 12:56 *
* CSP Vulnerability Scanner Version 2.00                                *
* Copyright (C) 2022-2024 - Computer Security Products Inc.             *
*                                                                       *
* Run by: SUPER.SUPER (255,255) at: $ZTN0.#PT4YZ46                      *
*                                                                       *
* List ACLs of selected diskfiles, ordered by user                      *
*                                                                       *
* LIST USER AUTHORIZATIONS                                              *
*                                                                       *
* Report is for Objects:                                                *
*                                                                       *
* DISKFILE $D2.PTVE24*.*                                                *
*                                                                       *
* GUARDIAN Protected Files Included                                     *
*                                                                       *
*************************************************************************


SCANNER REPORTS V2.00                                26Jan24, 12:56  Page 1

                       LIST USER AUTHORIZATIONS

  User =            001,110 (         CSP.PARNEET)

DISKFILE
       R,W,E,P,  O  $D2.PTVE240.CRMREQ
-------------------------------------------------------------------------------
  User =            255,255 (         SUPER.SUPER)

DISKFILE
 (G90) R,W,E,P      $D2.PTVE240
                        A0000001  A0000002  ADDGWSVR  AUDITCOM  AUDTVIEW
                        AVHDIR    AVHELP    AVTABLE3  AVTABLE5  AVTABLEL
                        AVTABLEN  AVTABLEP  CONFIN    CR191111  CR210217
```

```
   ************************************************************************
    *                                                                      *
    * $DATA.VS200.CSPREP Version 2.00 - System \NS3X       26Jan24, 12:58 *
    * CSP Vulnerability Scanner Version 2.00                               *
    * Copyright (C) 2022-2024 - Computer Security Products Inc.            *
    *                                                                      *
    * Run by: SUPER.SUPER (255,255) at: $ZTN0.#PT4YZ46                     *
    *                                                                      *
    * List ACLs of selected subvolumes, ordered by user                    *
    *                                                                      *
    * LIST USER AUTHORIZATIONS                                             *
    *                                                                      *
    * Report is for Objects:                                               *
    *                                                                      *
    * SUBVOLUME $D2.PTCA3*                                                 *
    *                                                                      *
    * GUARDIAN Protected Files Included                                    *
    *                                                                      *
    ************************************************************************

SCANNER REPORTS V2.00                                 26Jan24, 12:58  Page 1

                       LIST USER AUTHORIZATIONS

  User =            001,110 (         CSP.PARNEET)

SUBVOLUME
       R,W,E,P,C,O  $D2.PTCA310D
--------------------------------------------------------------------------------
  User =            099,250 (         TEST.ED)

SUBVOLUME
       R,W,E,P,C,O  $D2.PTCA310
--------------------------------------------------------------------------------
  User =            255,255 (         SUPER.SUPER)

SUBVOLUME
       R,W,E,P,C,O  $D2
                        PTCA310   PTCA310D  PTCA320
--------------------------------------------------------------------------------
```