Overview of Administrator Features

An electronic version of the pcAnywhere, 9.0 Administrative Guide is provided in the Documentation folder on the CD. The administrator guide is intended for network administrators and contains information on the following advanced administrative features:

- **Advanced installation**: options available for advanced installations of pcAnywhere, including network and standalone workstation installations.
- **pcAConfig**: A utility that allows an administrator to customize pcAnywhere configuration files before distributing them to the end users.

📖 pcAConfig.exe is a separate component from pcAnywhere. For information on custom configuration utilities, please refer to the pcaCfg online help or the Administrator guide located on the pcAnywhere installation CD.

- **Centralized management**: pcAnywhere integration into network management applications such as Norton System Center (NSC), IBM Tivoli, Computer Associates UniCenter TNG, and Microsoft SMS.

Centralized Management Overview

pcAnywhere offers a Microsoft Management Console (MMC) Snap-In — an advanced configuration and management tool that allows administrators to use Microsoft's latest computer and network management tools.

Integration with network management platforms like Computer Associates UniCenter TNG, IBM Tivoli TMS, and Microsoft's System management Server (SMS), allows a network administrator to install, configure, and distribute pcAnywhere from a single location.

Host Administrator MMC Snap In

The Host Administrator is a Microsoft Management Console (MMC) Snap-in that allows an administrator to remotely control and configure multiple pcAnywhere hosts on a network. One of the more powerful features of the host administrator is the ability to group systems together to allow convenient management and distribution of pcAnywhere connection items.

Using the host administrator, a network administrator can:

- Create configuration groups that allow the administrator to distribute a single pcAnywhere host configuration to multiple workstations on the network.
- Remotely start, stop, and connect to pcAnywhere hosts anywhere on the network.
- Retrieve a pcAnywhere log report from any remote PC on the network.

Norton System Center (NSC) Snap In

Norton System Center (NSC) provides a single point for managing the remote installation and configuration of several Symantec products, as well as a Central LiveUpdate. pcAnywhere integrates into NSC with custom install sets, pcAnywhere Custom Config, and the new MMC Host administrator. For more information, refer to the Norton System Center documentation.

Centralized Logging

pcAnywhere has extended it’s logging utilities to allow logging to central servers. An administrator can collect logging information from every pcAnywhere host on the network to a single PC to simplify tracking and to ensure system integrity.

The pcAnywhere Host Administrator Snap-In can retrieve log files from a remote PC on the network and allow the administrator to view and process them locally. This enhancement to logging supports writing on shared file systems on the network, and using Windows security to allow PCs to write log files to the shared file system without requiring access to the drive.

In addition to the enhanced logging utility, pcAnywhere has added Simple Network Management Protocol (SNMP) technology to the logging utilities. SNMP is used to send SNMPv1 events to a compatible console which records the information. pcAnywhere provides a management information base (MIB) containing the SNMP events supported. pcAnywhere supports multiple event destinations that allows an administrator to direct the SNMP logging to multiple consoles.

Directory Services

A directory is a database, a source of information stored in records, and indexed on one or more of the record's attributes. Each of these records is stored as a directory entry. The directory *service* includes not only the entry but the services that make that information available to users.

The new Directory Services feature of pcAnywhere is an example of an LDAP client application that needs to store and lookup information about users.

Using the service with pcAnywhere

The host starts up and waits for incoming connections as usual. However, in this case, it connects to an LDAP compliant server and updates the user's entry by adding an attribute that stores the current IP address, the machine name and the current status of the host. When the remote is started, a new application is launched, called the Directory Services Browser, which connects to an LDAP compliant server and queries it for all entries that satisfy the filter criteria and displays them in a list view that contains columns for all of the relevant information. The user interface should look familiar - it is designed to look and feel like pcAnywhere's current host browser list. When the user double clicks on one of the entries, a remote is launched to connect to the selected host.

Configuring an LDAP Compliant Server

For all of this to work, however, some minor configuration need to be done on the server. The main goal is to be able to use a company's user directory without having to duplicate any user information. The LDAP protocol allows us to modify what information each entry stores by adding or removing objectclass values that describe the attributes that we can store with this particular entry. For pcAnywhere to work we must add a custom objectclass description to the server's configuration that describes the information we need to store for each host that a user starts. Once the custom objectclass is available, all existing entries can be modified to store values that belong to the new objectclass. The administrator only needs to add the new objectclass to the server, they don't need to change any existing entries. When a host is configured with an LDAP entry is started and that entry is automatically modified to use the new objectclass in addition to any other objectclass values it may contain.

pcAnywhere's custom objectclass

objectclass: pcaHost

pcaHostEntry: binary

The custom pcAnywhere objectclass must be called pcaHost and contain a single attribute called pcaHostEntry whose type is binary. This is done through the user interface, allowing administrators to edit and add objectclasses to a server, or by editing the server configuration files.

SNMP event consoles

pcAnywhere 9.0 supports any SNMP event console that handles SNMPv1 type events, such as UniCenter TNG, SMS, and Tivoli TEC and NetView. The event console usually has a way to automate actions depending on the incoming SNMP trap and the variable it contains. The capabilities of the automated action, or rule, vary for each network management platform. Most include the facility to start any program that can be run from the command line.

Distributed Component Object Model (DCOM)

pcAnywhere uses Microsoft's DCOM technology for all point-to-point communications used for remote management tasks. DCOM is used by the enhanced Host Administrator as well as by every pcAnywhere integration into network management applications.

DCOM runs on a variety of network protocols and, by default, attempts to make connections on all installed protocols. After connecting to the network, it uses Windows NT Authentication to verify that you have the necessary rights for the tasks you want to perform. For example, an administrator with access rights, can perform management tasks on a locked pcAnywhere host from any location.

To ensure that NT Authentication is used for pcAnywhere's DCOM management tasks, it is recommended that the pcAnywhere connection items be configured to use the same Windows NT domain.

Windows DCOM configuration requirements

pcAnywhere configures DCOM during the installation process. All default settings should be sufficient to allow pcAnywhere management applications to function normally and maintain a sufficient level of security. However, modifications can be made to DCOM to modify the default security and allow an administrator to explicitly allow or deny DCOM access to a system.

To configure Windows NT for DCOM:

To remotely configure and control pcAnywhere on Windows NT from a network management system, the network administrator must comply to the following requirements:

- The network administrator must be logged in as a domain administrator.
- Both the administrator PC and the client PC must be in the same domain.
- The Windows NT default DCOM configuration requires all manager activity be authenticated on the NT domain.

To configure Windows 9*x* for DCOM:

To remotely configure and control pcAnywhere on Windows 9*x* from a network management system, the network administrator must comply to the following requirements:

- The Windows 9x PC must log into the same Windows NT domain as the network administrator.
- The Domain name and the workgroup name on the Windows 9x PC must be the same.
- The Windows 9x PC must be configured to user level access. This is a requirement for DCOMCNFG.EXE to allow adjusting the DCOM security settings for a Windows 9x computer.
- File and print sharing for Microsoft Windows Networks should be installed and enabled on the Windows 9x PC.

If you selected **Allow pcAnyhwere to be remotely managed** during the pcAnywhere installation, the DCOM settings were automatically modified to the required defaults. It is only necessary to configure your network as noted above.

The above configuration procedures should resolve any connectivity problems encountered while using the pcAnyhwere Host Administrator, or any of pcAnywere's Network Management integration components.

The most common error experienced is an Access Denied error. This is usually due to incorrect DCOM settings. Use the DCOMCNFG.EXE utility to modify the security settings for the client to resolve this error. Edit the default security and add only the Domain users or administrators to the list of callers allowed to access this host. You can also use the DCOM utility to deny access to selected callers.

Note: If you correctly configure the Windows environment as noted in the procedures above, this error should not occur.

Please consult DCOMCNFG.exe online documentation for more information on modifying configurations.

pcAnywhere management Shim (AwShim.exe)

AwShim is the pcAnywhere management shim. This shim is between pcAnywhere and the network management integration's mentioned earlier. The new and enhanced Host Administrator uses AwShim to accomplish some of the administrator functions.

AwShim uses the following parameters:

- -A Action
- -B Bhf File Name
- -C Chf File Name
- -H HostName to perform action on
- -R Remote PC to connect to

Supported with -A parameter:

- STARTHOST
- STARTREMOTE
- STOPHOST

The -B and -C parameters specify Be Host and Call Host items that exist in the CMS subfolder in the pcAnywhere installation directory.

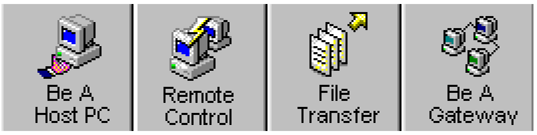
The -H parameter identifies the name or address of the host PC you want the action performed on.

The -R parameter is only used with STARTREMOTE to specify the name of the host PC the remote connects to. Whenever a remote is started, all connection parameters specified in the CHF file are used with the exception of the host PC address. This must be specified with the -R parameter.

Password protected connection items

When you run a password protected connection item on a managed PC, the password prompt appears on the managed PC.   The connection item is not launched until the correct password is provided.

The pcAnywhere action bar



Microsoft's Systems Management Server (SMS) integration

This integration is performed by using the SMSAddin tool. The SMSAddin tool creates registry entries that allow you to add programs to the menubar. The registry keys we add are as follows:

```
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SMS\Applications\Symantec]

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SMS\Applications\Symantec\ SymantecConnectToPCAHost]

"ApplicationName"="Connect To PCA Host"

"Order"=dword:0000000b

"Command"="awshim.exe"

"Description"="Connect To PCA Host"

"WorkingDir"=hex(2):63,3a,5c,00

"RunWindow"="Normal"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SMS\Applications\Symantec\ SymantecConnectToPCAHost\
SMSMachine]

"EnableRule"=hex(7):00,00,00

"PresentRule"=hex(7):00,00,00

"Arguments"=hex(7):2d,61,00,73,74,61,72,74,72,65,6d,6f,74,65, 00,2d,63,00,73,6d,\
73,2e,63,68,66,00,2d,72,00,24,28,41,74,74,72,28,4d,49,43,52, 4f,53,4f,46,54,\
7c,49,44,45,4e,54,49,46,49,43,41,54,49,4f,4e,7c,31,2e,30,3a, 4e,61,6d,65,29,\ 29,00,00,00,00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SMS\Applications\Symantec\ SymantecStartPCAHost]

"ApplicationName"="Start PCA Host"

"Order"=dword:00000009

"Command"="awshim.exe"

"Description"="Start PCA Host"

"WorkingDir"=hex(2):63,3a,5c,00

"RunWindow"="Normal"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SMS\Applications\Symantec\ SymantecStartPCAHost\
SMSMachine]

"EnableRule"=hex(7):00,00,00

"PresentRule"=hex(7):00,00,00

"Arguments"=hex(7):2d,61,00,73,74,61,72,74,68,6f,73,74,00,2d, 62,00,73,6d,73,2e,\
62,68,66,00,2d,68,00,24,28,41,74,74,72,28,4d,49,43,52,4f,53, 4f,46,54,7c,49,\
44,45,4e,54,49,46,49,43,41,54,49,4f,4e,7c,31,2e,30,3a,4e,61, 6d,65,29,29,00,\ 00,00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SMS\Applications\Symantec\ SymantecStopPCAHost]

"ApplicationName"="Stop PCA Host"

"Order"=dword:0000000a

"Command"="awshim.exe"
```

```
"Description"="Stop PCA Host"

"WorkingDir"=hex(2):63,3a,5c,00

"RunWindow"="Normal"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SMS\Applications\Symantec\ SymantecStopPCAHost\
SMSMachine]

"EnableRule"=hex(7):00,00,00

"PresentRule"=hex(7):00,00,00

"Arguments"=hex(7):2d,61,00,73,74,6f,70,68,6f,73,74,00,2d,68,
00,24,28,41,74,74,72,28,4d,49,43,52,4f,53,4f,46,54,7c,49,44,
45,4e,54,49,46,49,43,41,54,49,4f,4e,7c,31,2e,30,3a,4e,61,6d, 65,29,29,00,00,00
```

These registry keys add three new menu items to the Tools menu when you have a computer opened in the SMS console. The SMS12.REG file that creates these entries can be found in the CMS subfolder under the pcAnywhere install directory. Usually this directory is: \ProgramFiles\Symantec\pcAnywhere\CMS

In addition to this file there are the three ATD files created by SMSAddin. These files can be used to modify or adjust the SMS1.2 integration. The SMS.BHF and SMS.CHF files used whenever SMS starts, stops, or connects with pcAnywhere are found in the CMS subfolder. If your site requires specific configurations to your caller items, modify these two files on the install before distributing the install images to your managed hosts. This ensures that your organization has SMS connection items that meet your site's needs.

To update these files

1 Open the install image in the Windows Explorer and right-click the file.

2 Select Properties from the popup menu.

All the options for this object can be adjusted from here. After the image is updated you can install pcAnywhere to your managed nodes.

Tivoli NetView integration

The Tivoli NetView integration is performed by placing a pcAnywhere Application Registration File (or ARF) in the registration directory for Netview. This file is called PCACONN.ARF. This file defines the three actions that are available from within the NetView integration. These options are start, stop, and connect. The menu items for this command are available when one or more devices are selected with the Computer and Node properties. The PCACONN.ARF file that creates these entries can be found in the CMS directory under the pcAnywhere install directory. The directory is:

\Program Files\Symantec\pcAnywhere\CMS

Also in this directory are NETVIEW.BHF and NETVIEW.CHF files. These connection objects are used whenever NetView starts, stops, or connects with pcAnywhere. If your site requires specific adjustments to your caller objects, update these two files on the install before sending the install images to your managed nodes. This will ensure that your organization has NetView connection objects that meet your site's needs.

To update these files, open the install image in the windows explorer and right click on the file. Select properties from the popup menu. All the options for this object can be adjusted from here. After the image is updated you can install pcAnywhere to your managed nodes.

The PCACONN.ARF file

```
Application "pcANYWHERE"

{

        Version "9.0";

    Description {

        "pcAnywhere Remote Control"

    }

Copyright {

        "(C) 1999 Symantec Corporation."

        }

    MenuBar "Tools" {

        "pcAnywhere" _S f.menu PCAItem;

    }

    Menu PCAItem {

        <100> "Start PCA Host      "_S f.action PcaStart;

        <90>   "Stop PCA Host              "_T f.action PcaStop;

        <80>   "Connect to PCA Host        "_C f.action PcaConnect;

    }

    Action "PcaStart"

    {

        SelectionRule isNode && isComputer;

        MinSelected 1;

        Command "awshim.exe -a STARTHOST -b NetView.bhf -h $OVwSelection1";
}
Action "PcaStop"
{
    SelectionRule isNode && isComputer;
    MinSelected 1;
    Command "awshim.exe -a STOPHOST -h $OVwSelection1";
}
Action "PcaConnect"
{
    SelectionRule isNode && isComputer;
    MinSelected 1;
        MaxSelected 1;
    Command "awshim.exe -a STARTREMOTE -c NetView.chf -r $OVwSelection1";
}}
```

Computer Associates Unicenter TNG integration

The Unicenter TNG, including the 2D and 3D map user interfaces, is accessible whenever the TNG popup menu is available.

For the TNG integration we extend the popup menu for the Managed Object class of device to include three additional menu items for starting, stopping, and connecting to pcAnywhere. This integration uses TRIX, the TNG Repository Import-Export program. These menu items can be re-created by rebuilding the TNG repository and re-importing the script. Once created, these items can be modified to meet your site's requirements by using the Unicenter TNG Class wizard. The pcAnywhere.TNG file that creates these items is located in the CMS subfolder in the pcAnywhere install folder:

\Program files\Symantec\pcAnywhere\CMS

The TNG.CHF and TNG.BHF files are also located in the CMS subfolder. These files represent pcAnywhere remote control connection items and are used whenever TNG starts, stops, or connects with pcAnywhere. You can modify these connection items by updating these two files on the install prior to distributing the install images to your managed nodes. This ensures that your organization has TNG connection object that meet your site's requirements.

The PCA.TNG TRIX script that integrates pcAnywhere into Unicenter TNG

```
ADDOBJECT="PCA_ConnectToHost" Method

BEGIN

type TNGWV_OT_INT 0 0

exe_name TNGWV_OT_STRING "awshim.exe" 0

parameter TNGWV_OT_STRING "-a startremote -c tng.chf -r \"&address&\"" 0

END


ADDOBJECT="PCA_StartHost" Method

BEGIN

type TNGWV_OT_INT 0 0

exe_name TNGWV_OT_STRING "awshim.exe" 0

parameter TNGWV_OT_STRING "-a starthost -b tng.bhf -h   \"&address&\"" 0

END


ADDOBJECT="PCA_StopHost" Method

BEGIN

type TNGWV_OT_INT 0 0

exe_name TNGWV_OT_STRING "awshim.exe" 0

parameter TNGWV_OT_STRING "-a stophost -h   \"&address&\"" 0

END
```

```
ADDOBJECT="ManagedObject" Popup_Menu
BEGIN
sequence_no TNGWV_OT_INT 500 0
label TNGWV_OT_STRING "0" 0
method_name TNGWV_OT_STRING "0" 0
flag TNGWV_OT_INT 1 0
END

ADDOBJECT="ManagedObject" Popup_Menu
BEGIN
sequence_no TNGWV_OT_INT 501 0
label TNGWV_OT_STRING "Start PCA Host" 0
method_name TNGWV_OT_STRING "PCA_StartHost" 0
flag TNGWV_OT_INT 0 0
END

ADDOBJECT="ManagedObject" Popup_Menu
BEGIN
sequence_no TNGWV_OT_INT 502 0
label TNGWV_OT_STRING "Stop PCA Host" 0
method_name TNGWV_OT_STRING "PCA_StopHost" 0
flag TNGWV_OT_INT 0 0
END

ADDOBJECT="ManagedObject" Popup_Menu
BEGIN
sequence_no TNGWV_OT_INT 503 0
label TNGWV_OT_STRING "Connect to PCA Host" 0
method_name TNGWV_OT_STRING "PCA_ConnectToHost" 0
flag TNGWV_OT_INT 0 0
END
```

To perform the import you can use the Unicenter TNG Repository Import/Export program (TRIX). To do this, launch TRIX and open the file pca.tng from the CMS directory under the pcAnywhere install directory. The directory is: \Program Files\Symantec\pcAnywhere\CMS

Once this file is opened select the import repository option. To edit the menu integration you can either alter the

TRIX script directly, or you can use the Unicenter TNG Class Wizard to edit the menu interactively. See the Unicenter TNG Books Online for more information.

To use the Unicenter TNG Repository to import:

1. Run TRIX

2. Open pcA.tng from the CMS subfolder in the pcAnywhere install folder.

   Modify the TRIX script directly.

3. Choose the import repository option.

4. Once you’ve completed the import, do the following:

5. Use the Unicenter TNG Class Wizard to modify the script.

ℹ Refer to the Unicenter TNG Books Online for more information.

SNMP and Central Logging

An important part of any distributed computing environment is security, accountability, and logging. pcAnywhere addresses these concerns with new logging features as well as improved security used for pcAnywhere management tasks.

pcAnywhere has extended it's logging utility to allow logging to central servers. An administrator can collect logging information from every pcAnywhere host on the network to a single PC to simplify tracking and to ensure that systems are not misused.

The pcAnywhere's Host Administrator MMC Snap-In can retrieve log files from a remote PC on the network and allow the administrator to view and process them locally. This enhancement to pcAnywhere's logging utility supports writing on shared file systems on the network, and using Windows Security to allow PCs to write log files to the shared file system without requiring access to the drive.

In addition to the enhanced logging utility, pcAnywhere has added Simple Network Management Protocol (SNMP) technology to the logging utilities. SNMP is used to send SNMPv1 events to a compatible console which records this information. pcAnywhere provides a management information base (MIB) containing over forty different SNMP events that we can generate. pcAnywhere supports multiple event destinations that allows an administrator to direct the SNMP logging to multiple consoles.

Event Consoles

pcAnywhere, version 9.0 supports any SNMP event console that handles SNMP traps, such as Computer Associates Unicenter TNG, Microsoft's SMS, and IBM Tivoli. The event console usually has a way to automate actions depending on the incoming SNMP trap and the variable it contains. The capabilities of the automated action, typically referred to as a rule or action, vary for each network management platform. Most include the facility to start any program that can be run from the command line.

For example, you can create a rule that starts with AWSHIM.EXE to automatically run a pcAnywhere remote whenever a host is started on the network.

pcAnywhere Management Information Base (MIB)

The pcAnywhere MIB outlines over 40 different SNMP traps that pcAnywhere can generate. You can use the MIB we provide as a tool to help you build automated responses to pcAnywhere events that occur anywhere on your network. The MIB is installed in the CMS directory under the pcAnywhere install path. This is usually: \Program Files\Symantec\pcAnywhere

```
--

--   pcANYWHERE MIB Definitions

--   Copyright 1999, Symantec Corporation.

--

PCA-Alert-MIB DEFINITIONS ::= BEGIN

IMPORTS

    enterprises

            FROM RFC1155-SMI

    OBJECT-TYPE

          FROM RFC-1212

    TRAP-TYPE

                                              FROM RFC-1215

                                    DisplayString

                                    FROM RFC1213-MIB;

symantec                                            OBJECT IDENTIFIER ::= { enterprises 393 }

pcanywhere                                          OBJECT IDENTIFIER ::= { symantec 100 }

pcaversionnine                                      OBJECT IDENTIFIER ::= { pcanywhere 9 }


PcaHost                                             OBJECT IDENTIFIER ::= { pcaversionnine 1 }

PcaRemote                                           OBJECT IDENTIFIER ::= { pcaversionnine 2 }

PcaFileXfer                                         OBJECT IDENTIFIER ::= { pcaversionnine 3 }

PcaGateway                                          OBJECT IDENTIFIER ::= { pcaversionnine 4 }

PcaMonitor                                          OBJECT IDENTIFIER ::= { pcaversionnine 5 }

PcaInstall                                          OBJECT IDENTIFIER ::= { pcaversionnine 6 }

PcaReset                                            OBJECT IDENTIFIER ::= { pcaversionnine 7 }

PcaLDAP                                             OBJECT IDENTIFIER ::= { pcaversionnine 8 }

PcaObject                                           OBJECT IDENTIFIER ::= { pcaversionnine 9 }


-- Pca Alert Objects - These are not able to be queried,

-- however they are used for the trap variables we will bind
-- to specific traps.   Now I only have generic data bindings
-- listed, this will change to properly reflect the type of
-- data in the variables being sent. NOTE:   Check to see
-- whether the access is set properly, ie use not-accessible
-- instead!!!

HostComputerName   OBJECT-TYPE
             SYNTAX      DisplayString (SIZE (0..128))
             ACCESS      read-only
             STATUS      optional
             DESCRIPTION
"The computer that is running the PCA Host"
             ::= { PcaObject 1 }

RemoteComputerName   OBJECT-TYPE
             SYNTAX      DisplayString (SIZE (0..128))
             ACCESS      read-only
             STATUS      optional
             DESCRIPTION
"The computer that is running the PCA Remote"
             ::= { PcaObject 2 }

CallerName      OBJECT-TYPE
             SYNTAX      DisplayString (SIZE (0..128))
             ACCESS      read-only
             STATUS      optional
             DESCRIPTION
"The name of the remote caller."
             ::= { PcaObject 3 }

HostConnectionObject      OBJECT-TYPE
             SYNTAX      DisplayString (SIZE (0..255))
             ACCESS      read-only
             STATUS      optional
```

```
            DESCRIPTION
"The name of the connection object used to start the PCA Host"
            ::= { PcaObject 4 }

RemoteConnectionObject    OBJECT-TYPE
            SYNTAX    DisplayString (SIZE (0..255))
            ACCESS    read-only
            STATUS    optional
            DESCRIPTION
"The name of the connection object used to start the PCA Remote"
            ::= { PcaObject 5 }

XferFiles OBJECT-TYPE
            SYNTAX  INTEGER
            ACCESS  read-only
            STATUS  optional
            DESCRIPTION
"Number of files transferred by file transfer"
            ::= { PcaObject 6 }

XferBytes OBJECT-TYPE
            SYNTAX  INTEGER
            ACCESS  read-only
            STATUS  optional
            DESCRIPTION
"Number of bytes transferred by this file transfer operation"
            ::= { PcaObject 7 }

XferOperation OBJECT-TYPE
            SYNTAX  INTEGER
            ACCESS  read-only
            STATUS  optional
            DESCRIPTION
"The operation last performed by file transfer"
```

```
            ::= { PcaObject 8 }

XferVirusFlag OBJECT-TYPE
            SYNTAX   INTEGER
            ACCESS   read-only
            STATUS   optional
            DESCRIPTION
"This is the file transfer virus flag."
            ::= { PcaObject 9 }



XferSourceFile     OBJECT-TYPE
            SYNTAX      DisplayString (SIZE (0..255))
            ACCESS      read-only
            STATUS      optional
            DESCRIPTION
"The name of the source file in a file transfer operation"
            ::= { PcaObject 10 }

XferDestFile     OBJECT-TYPE
            SYNTAX      DisplayString (SIZE (0..255))
            ACCESS      read-only
            STATUS      optional
            DESCRIPTION
"The name of the destination file in a file transfer operation"
            ::= { PcaObject 11 }

HostEncryptionLevel   OBJECT-TYPE
            SYNTAX   INTEGER
            ACCESS   read-only
            STATUS   optional
            DESCRIPTION
"The desired encryption level of the PCA Host"
```

```
            ::= { PcaObject 12 }

RemoteEncryptionLevel OBJECT-TYPE
            SYNTAX   INTEGER
            ACCESS   read-only
            STATUS   optional
            DESCRIPTION
"The desired encryption level of the PCA Remote"
            ::= { PcaObject 13 }

HostEndedReason OBJECT-TYPE
            SYNTAX   INTEGER
            ACCESS   read-only
            STATUS   optional
            DESCRIPTION
"The reason a PCA Host was terminated"
            ::= { PcaObject 14 }



DeviceType OBJECT-TYPE
            SYNTAX   INTEGER
            ACCESS   read-only
            STATUS   optional
            DESCRIPTION
"This represents the type of device in which a connection was made."
            ::= { PcaObject 15 }

XferFailedFlag OBJECT-TYPE
            SYNTAX   INTEGER
            ACCESS   read-only
            STATUS   optional
            DESCRIPTION
"Flag is set if a file transfer operation had failed."
```

```
            ::= { PcaObject 16 }

-- Pca Host Alert Traps

PcaHostStarted    TRAP-TYPE
ENTERPRISE   PcaHost

VARIABLES    { DeviceType, HostConnectionObject}
DESCRIPTION "PCA Host was started"
              ::= 1

PcaHostEndSession TRAP-TYPE
ENTERPRISE   PcaHost
VARIABLES    {HostEndedReason}
DESCRIPTION "PCA Host has shut down"
              ::= 2

PcaHostAbnormalEnd    TRAP-TYPE
ENTERPRISE   PcaHost
DESCRIPTION "PCA Host has shut down abnormally"
              ::= 3
PcaHostConnFailDeviceError    TRAP-TYPE
ENTERPRISE   PcaHost
VARIABLES    {DeviceType}
DESCRIPTION "PCA Host connection failed - device error"
              ::= 4


PcaHostStopped    TRAP-TYPE
ENTERPRISE   PcaHost
VARIABLES    {HostEndedReason}
DESCRIPTION "PCA Host was stopped"
              ::= 5
```

```
PcaHostInSession    TRAP-TYPE
ENTERPRISE   PcaHost
VARIABLES    {RemoteComputerName, CallerName}
DESCRIPTION "PCA Host is in session"
                    ::= 6

PcaHostConnFailAccessDenied    TRAP-TYPE
ENTERPRISE   PcaHost
VARIABLES    {RemoteComputerName, CallerName}
DESCRIPTION "PCA Host connection failed - access denied"
                    ::= 7

PcaHostConnFailEncrypt    TRAP-TYPE
ENTERPRISE   PcaHost
VARIABLES    {HostEncryptionLevel, RemoteEncryptionLevel}
DESCRIPTION "PCA Host connection failed - encryption error"
                    ::= 8

PcaHostUnsecuredHostStarted    TRAP-TYPE
ENTERPRISE   PcaHost
VARIABLES    {HostConnectionObject}
DESCRIPTION "PCA Host was launched insecurely"
                    ::= 9

PcaHostRebooting    TRAP-TYPE
ENTERPRISE   PcaHost
DESCRIPTION "PCA Host rebooting the system"
                    ::= 10

PcaHostLockingWorkstation TRAP-TYPE
ENTERPRISE   PcaHost
DESCRIPTION "PCA Host locking workstation"
          ::= 11
```

```
PcaHostLoggingOffUser TRAP-TYPE
ENTERPRISE   PcaHost
DESCRIPTION "PCA Host is logging off the current user"
        ::= 12

-- PCA Remote Generated Traps

PcaRemoteStarted     TRAP-TYPE
ENTERPRISE   PcaRemote
VARIABLES     {DeviceType, RemoteConnectionObject}
DESCRIPTION "PCA Remote was started"
                ::= 1

PcaRemoteInSession     TRAP-TYPE
ENTERPRISE   PcaRemote
VARIABLES     {HostComputerName}
DESCRIPTION "PCA Remote is in session"
                ::= 2

PcaRemoteEndSession     TRAP-TYPE
ENTERPRISE   PcaRemote
DESCRIPTION "PCA Remote has ended the session"
                ::= 3

PcaRemoteAbnormalEndSession     TRAP-TYPE
ENTERPRISE   PcaRemote
DESCRIPTION "PCA Remote has ended the session abnormally"
                ::= 4

PcaRemoteConnFailDeviceError     TRAP-TYPE
ENTERPRISE   PcaRemote
```

```
VARIABLES    {DeviceType}

DESCRIPTION "PCA Remote connection failure - device error"

                  ::= 5


PcaRemoteConnFailHostBusy    TRAP-TYPE

ENTERPRISE   PcaRemote

DESCRIPTION "PCA Remote connection failure - host busy"

                  ::= 6


PcaRemoteConnFailHostNotFound    TRAP-TYPE

ENTERPRISE   PcaRemote

DESCRIPTION "PCA Remote connection failure - host not found"

                  ::= 7


PcaRemoteConnFailBadPassword    TRAP-TYPE

ENTERPRISE   PcaRemote

DESCRIPTION "PCA Remote connection failure - bad password"

                  ::= 8


PcaRemoteConnFailEncryption    TRAP-TYPE

ENTERPRISE   PcaRemote

VARIABLES    {RemoteEncryptionLevel, HostEncryptionLevel}

DESCRIPTION "PCA Remote connection failure - encryption error"

                  ::= 9

-- PCA File Transfer Generated Traps


PcaFileXferStarted    TRAP-TYPE

ENTERPRISE   PcaFileXfer

VARIABLES    {HostComputerName, RemoteComputerName, HostConnectionObject, RemoteConnectionObject,
DeviceType}

DESCRIPTION "PCA File Transfer started"

                  ::= 1


PcaFileXferEnded    TRAP-TYPE

ENTERPRISE   PcaFileXfer
```

```
VARIABLES     {XferFiles, XferBytes}
DESCRIPTION "PCA File Transfer ended"
                        ::= 2

PcaFileXferAbnormalEnd     TRAP-TYPE
ENTERPRISE   PcaFileXfer
VARIABLES     {ComputerName}
DESCRIPTION "PCA File Transfer ended abnormally"
                        ::= 3

PcaFileXferOperationCancelled     TRAP-TYPE
ENTERPRISE   PcaFileXfer
DESCRIPTION "PCA File Transfer operation cancelled"
                        ::= 4

PcaFileXferOperation     TRAP-TYPE
ENTERPRISE   PcaFileXfer
VARIABLES     { XferOperation, XferSourceFile, XferDestFile, XferBytes, XferVirusFlag, XferFailedFlag}
DESCRIPTION "PCA File Transfer received file"
                        ::= 5

-- PCA Monitor Traps

PcaMonitorFullProductNotInstalled     TRAP-TYPE
ENTERPRISE   PcaMonitor
DESCRIPTION "PCA Monitor - The PCA Full product is not installed"
                        ::= 1

PcaMonitorHostNotInstalled     TRAP-TYPE
ENTERPRISE   PcaMonitor
DESCRIPTION "PCA Monitor - The PCA Host is not installed"
                        ::= 2

PcaMonitorRemoteNotInstalled     TRAP-TYPE
```

```
ENTERPRISE   PcaMonitor
DESCRIPTION "PCA Monitor - The PCA Remote is not installed"
                        ::= 3

PcaMonitorHostNotWaiting     TRAP-TYPE
ENTERPRISE   PcaMonitor
DESCRIPTION "PCA Monitor - The PCA Host is not waiting for a connection"
                        ::= 4

PcaMonitorHostNotAutoStart     TRAP-TYPE
ENTERPRISE   PcaMonitor
DESCRIPTION "PCA Monitor - The PCA Host is not set to auto start"
                        ::= 5
PcaMonitorHostNotWaitingOnDialup     TRAP-TYPE
ENTERPRISE   PcaMonitor
DESCRIPTION "PCA Monitor - The PCA Host is not waiting on a dialup"
                        ::= 6

PcaMonitorHostLanOnlyNotInstalled     TRAP-TYPE
ENTERPRISE   PcaMonitor
DESCRIPTION "PCA Monitor - The PCA Host LAN only is not installed"
                        ::= 7

PcaMonitorLiveUpdateNotRun     TRAP-TYPE
ENTERPRISE   PcaMonitor
DESCRIPTION "PCA Monitor - Live Update was not run on this host"
                        ::= 8
-- Reset Events
-- These events are defined so that when generated by
-- the monitor they can be used to clear the status of
-- previously generated events.

PcaResetNotInstalledReset     TRAP-TYPE
ENTERPRISE   PcaReset
```

```
DESCRIPTION "PCA Monitor - Reset install traps"
                ::= 1

PcaResetHostNotWaitingReset     TRAP-TYPE
ENTERPRISE   PcaReset
DESCRIPTION "PCA Monitor - Reset Host not waiting traps"
                ::= 2

PcaResetHostNotAutoStartReset     TRAP-TYPE
ENTERPRISE   PcaReset
DESCRIPTION "PCA Monitor - Reset Host not auto start traps"
                ::= 3

PcaResetHostWaitingOnDialupReset     TRAP-TYPE
ENTERPRISE   PcaReset
DESCRIPTION "PCA Monitor - Reset Host waiting on dialup traps"
                ::= 4

PcaResetLiveUpdateNotRunReset     TRAP-TYPE
ENTERPRISE   PcaReset
DESCRIPTION "PCA Monitor - Reset Live Update not run traps"
                ::= 5
-- pcA Install Traps

PcaInstallRebootRequired   TRAP-TYPE
ENTERPRISE   PcaInstall
DESCRIPTION "PCA Install - A reboot is required"
                ::= 1
        END
```

LDAP (Lightweight Directory Protocol)

The LDAP directory stores information in a hierarchical tree-like structure that is very similar to a file system with subdirectories and files. Each object in the directory is called an entry. Entries can be either containers or leaf entries. Containers are entries that can hold other entries while leaf entries are the 'endpoints' of the tree. These types of entries are used to show an organizational structure by creating entries that represent countries, organizational units and people that fit into the various areas of the organization. The following example has entries representing countries at the top of the tree. Below them are entries representing states or national organizations. Below them might be entries representing people, organizational units, printers or any other type of information.

LDAP also allows you to store attributes with each entry that might provide further information about the entry such as a person's name, an email address, a phone number, or title. Each entry may contain many values for the same attribute. The kind of attributes that can be stored with an entry, the schema, is decided by what objectclass they belong to. An LDAP server has a list of all the objectclasses that it knows about. Administrators can add new and edit existing objectclass entries to enable client applications that might need to store specific types of attributes. The objectclass is stored as an attribute of the entry and it controls which attributes are required and allowed in an entry. Some common objectclass values are person, organizationalUnit and organizationalPerson. An entry can have many combinations of objectclasses to represent complex entries such as employees in a company.

To modify DCOM settings

Do one of the following:

- On a windows NT PC, run DCOMCNFG.EXE from the WinNT\System32 folder.
- On a Windows 9x PC, run DCOMCNFG.EXE from the Windows\System folder.

Modifying DCOM security settings on a managed PC may require that adjustments be made to the DCOM settings on the administrator PC. Be sure that all managed PCs are authenticating on the same Windows NT Domain, or on trusted domains.

When an administrator connection is made to a remote PC, the management software attempts to impersonate the user making the connection. If the connecting user is not logged into a Windows NT system with administrator privileges, this impersonation fails.

To further ensure security, a caller without Windows NT administrator privileges cannot perform administrator functions, or have access beyond what they would normally have, when logged into the PC directly.

Note: To avoid connection problems due to access denied errors, make sure the PC running the management shim and host administrator can access the shared drives on the remote system without having to enter a password. Please consult DCOMCNFG.EXE online documentation for more information on modifying configurations.

To add the Host Administrator Snap-In

1 Start the Microsoft Management Console (MMC).

2 Choose Add/Remove Snap-In from the Console menu.

3 Click Add on the Standalone tab.

4 Select pcAnywhere Administrator from the Add Snap-In dialog box.

5 Click Add.

ℹ After the Host Administrator is added to the MMC console, the administrator can access all Host Administrator features.

To run the Host Administrator Snap-In

▸ Do one of the following:

- Choose pcAnywhere Administrator from the Windows Start menu.
- Perform the following steps:

1 Start the Microsoft Management Console (MMC).

2 Choose Add/Remove Snap-In from the Console menu.

3 Click Add on the Standalone tab.

4 Select pcAnywhere Administrator from the Add Snap-In dialog box.

5 Click Add.

To access PCs on the network with the Host Administrator

1 Expand the pcAnywhere Administrator item in the MMC left window pane, continuing the expansion to the Systems item.

2 Expand the Microsoft Windows Network item in the MMC left window pane.

3 Select a domain or workgroup.

4 Do one of the following:

- Click the explorer icon on the MMC taskbar.
- Right-click the domain and choose Explore Machines from drop-down menu.

5 Click the explorer icon to expand the domain item and view the PCs configured in the selected domain.

Note: The first time you run the host administrator and expand the tree, two items appear in the tree's view: Configuration groups and Microsoft Windows Network. The Microsoft Windows Network is similar to Microsoft's Network Neighborhood. When you expand this item, a list of domains or workgroups accessible from your location appears.

To create a new Configuration Group

1. Right-click Configuration Groups in the MMC left window pane.
2. Choose New > Configuration Group from the menu.
3. Type a name for this group and click OK.

To add a PC to the configuration group

▸ Do one of the following:

- Right-click Systems in the MMC left window pane, choose New > System from the menu, and enter the name of the system you are adding.
- Click any PC listed in the Microsoft Windows Network and drag it to the Systems section.

To create host files

1 Right-click Connection Items in the MMC left window pane.

2 Choose New > Be A Host or Call a Host from the menu.

3 Type a name for this connection item and click OK.

To distribute host files

1 Right-click Configuration Groups in the MMC left window pane.

2 Choose Distribute Host Files

3 Select the PC you want to distribute the file to from the dialog box.

4 Select the file to distribute and Click OK.

After the connection items have been distributed, you can start, stop, and connect to any managed host by right-clicking on any system in the Configuration Group list or the Microsoft Windows Network list.

The pcAnywhere standard installation installs an ADMIN1n.BHF file in the CMS subfolder in the pcAnywhere program directory. This file can be configured prior to installing to allow you to customize the settings to satisfy your organization's requirement.

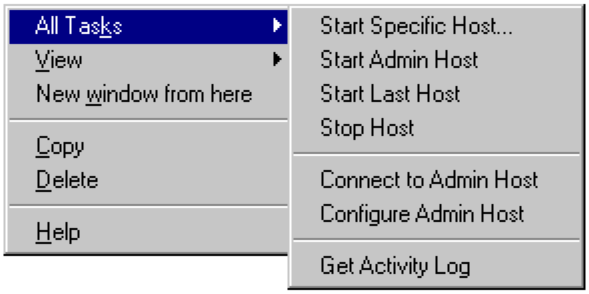
Selecting Start Administrator Host from the Host Administrator Snap-In, runs the ADMIN1n.BHF host file.

Selecting Connect from the Host Administrator Snap-In, runs a corresponding ADMIN1n.CHF file that connects to the selected host.

To manage a host PC on the network

1 Right-click the host in the Configuration Group

2 Choose any of the following actions from the All Tasks menu:



- **Start Specific Host** - runs a host selected from a list of centrally managed hosts, or any host configured on the destination PC..
- **Start Admin Host** - runs the configuration in the Administrator Host file (ADMIN1n.BHF).
- **Start Last Host** - runs the host configuration file that was most recently used.
- **Stop Host** - cancels a host and disconnects any active sessions on the host.
- **Connect to Admin Host** -connects to the administrator host PC.
- **Configure Admin Host** - allow the administrator to reconfigure the settings on the admin host PC.
- **Get Activity Log** - retrieves the remote and host session log to the host administrator console.

To run the pcAConfig utility

1 Double-click pcAConfig.exe located in the Utility\pcAConfig folder on the pcAnywhere CD.

2 Do one of the following:

§ Type the location of the Disk1 folder.

§ Click Browse to select the Disk1 folder.

3 Click OK.

📖 Please click Help on the pcAConfig property pages for information on pcAConfig options.

Configuring pcAnywhere for Directory Services

LDAP servers that are being used with pcAnywhere must be added to the Directory Servers page in the Network Options property sheet.

To configure the PC for directory services:

1 Select Network Options from the Tools menu.

2 Click the Directory Services tab and click Add.

3 Type a display name that clearly describes this Directory Server.

4 Type the address of the Directory Server.

5 Type the Common Name and password of the entry used to authenticate the user on the directory server.

6 Click Advanced to configure the port number and the search base of the directory tree.

Note: See the Novell Administrator Guide to change the port.

7 Click OK.

pcAnywhere attempts to connect to the directory server and search for the entry specified in the Name field. If multiple entries are found, a user must select their own entry. Once the entry is identified, pcAnywhere stores its Distinguished Name in the registry for each identification and labels the entry as Verified.

To enable directory services on the host

1. Right-click a host connection item and choose Properties from the menu.
2. Click the Settings tab.
3. Click **Directory Services**.
4. Choose the appropriate directory Server from the drop-down box.

   The directory server entry that is selected from the Directory Servers drop-down box is used to register this host when it is started. The remote is configured similarly, with the addition of a search filter that helps to filter the search to avoid listing a large number of entries in the list displayed in the Directory Services Browser.

Enable directory services on the remote

Right-click a remote control connection item and choose Properties from the menu.

Click the Settings tab.

Click Use Directory Services.

Select the directory server entry from the drop-down list.

Set initial filter settings

To configure Directory Services with Netscape Directory Server 3.1

1 Connect to the Server Administration page with Netscape Communicator.

2 Click the button that represents the directory server you are configuring.

3 Select the Schema option from the top selection bar.

4 Select Edit or View Attributes from the left selection bar.

5 Enter pcaHostEntry in the Attribute Name field.

6 Choose Binary from the Syntax combo box.

7 Click Add New Attribute under Manage Attributes section.

8 Enter the password for the Directory Manager and click the Submit button.

9 Click Create Objectclass on the left selection bar and enter pcaHost in the ObjectClass Name field.

10 Find the objectclass attribute in the Available Attributes list and add it to the Required Attributes list by clicking on the Add button.

11 Find the pcaHostEntry attribute in the Available Attributes list and add it to the Allowed attributes list by clicking on the Add button.

12 Click Create New ObjectClass.

13 Enter the password for Directory Manager and click the Submit button.

14 Restart the server for the new settings to take effect.

To configure Directory Service with Netscape Directory Server 4.0

1 Start the netscape Console 4.0 application.

Note: Administrator rights are needed to perform this task.

2 Open the item that represents this server in the left-hand tree view.

3 Open up the Server Group.

4 Double-click the Directory Server item to open the server window.

5 Click the Configuration tab.

6 In the left-hand tree view, open the Database item.

7 Select the Schema sub-item and click the Attributes tab.

8 Click Create at the bottom of the window.

9 In the Create Attribute dialog, type **pcaHostEntry** in the field labeled Attribute Name.

10 Select Binary from the Syntax combo-box.

11 Check **Multi-Valued** and click OK.

12 Click the Object Classes tab.

13 Click Create at the bottom of the window.

14 Type **pcaHost** in the Name field of the Create Object Class dialog box.

15 Select objectclass in the Available Attributes list box and click Add to include the Required Attributes list.

16 Select **pcaHostEntry** in the Available Attributes list and click add to include the Allowed Attributes list.

17 Click OK to add the object class.

18 Click the Tasks tab.

19 Click Restart the Directory Server.

20 Reply YES to the Restart Server dialog box.

Configure Novell v5.0 directory server

Note: The following steps only apply if LDAP is installed, configured, and functioning on the Novell v5.0, with NDS V8.0 server. Administrator rights to the server are needed to perform these steps.

To create the pcaHostEntry in ConsoleOne:

1 Log into the LDAP server that contains the LDAP group object.

2 Open ConsoleOne from **sys:public\mgmt\ConsoleOne\1.2\bin\ConsoleOne.exe**.

3 Select Schema Manager from the Tools drop-down menu.

4 Select the Attribute Tab, the click Create.

5 Click Next.

6 In the attribute name field, type **pcaHostEntry**, leaving the ASNI ID field blank.

Note: All entries are case sensitive.

7 Click Next.

8 Select Octet String from the drop-down box for the attribute syntax.

9 Select public read as the attribute flag.

10 Click Next, then Finish.

To create the pcaHost object in ConsoleOne:

1 Open up ConsoleOne from sys:public\mgmt\ConsoleOne\1.2\bin\ConsoleOne.exe.

2 Select Schema Manager from the Tools menu.

3 Click the Class tab, then click Create.

4 Click Next.

5 Type **pcaHost** in the name field, leaving the ASNI ID blank.

Note: This entry is case sensitive.

6 Click Next

7 Select Auxiliary Class, the click Next.

8 Double-click Top and add it to the Inherit From box.

9 Click Next.

Objectclass appears in the Add These Attributes window.

10 Click Next.

11 Double-click the pcaHostEntry and add it to the Add These Attributes window.

12 Click Next.

13 Review the summary for the new class to be created and click Finish.

Map the LDAP attribute to the NDS attribute

1 Double-click the LDAP Group icon in the right window pane to view the properties for the LDAP Group.

2 Click the Attribute Map tab, then click Add.

3 Type **pcaHostEntry;binary** in the LDAP attribute field.

4 Select pcaHostEntry from the NDS Attribute drop-down box and click OK.

5 Type **pcaHostEntry** in the LDAP attribute field.

6 Select pcaHostEntry from the NDS Attribute drop-down box.

Note: These entries are case sensitive and must be entered exactly as configured above.

7 Click OK.

8 Click Apply to map other attributes or click OK to finish.

Note: To modify the attributes for this map, highlight the attribute and click Modify.

Map the NDS class to the LDAP class

1 Double-click the LDAP Group icon in the right window pane.

2 Click the Class Map tab, then click Add.

3 Type **pcaHost** in the LDAP class field.

Note: These entries are case sensitive and must be entered exactly as configured above.

4 Select pcaHost from the NDS Attribute drop-down box and click OK.

5 Click Apply to map other attributes, or click OK to finish.

Create an LIDF file

Note: To perform these steps, access to a text editor, such as Notepad, is required. In addition, access to the server is required through RCONAG6.NLM, and RCONJ.EXE.

1. Open Notepad.
2. An entry is required for each user who requires the use of pcAnywhere.
3. Type the following four lines for each user:

   DN:cn=user, ou=organization_unit, o=organization

   Changetype:modify

   Add:objectclass

   Objectclass:pcaHost

4. Save this file locally and copy it to: sys:system\schema\.
5. At the server prompt type: **Load Bulkload.nlm**.

   Note: Use RCONJ.EXE to manage the server remotely.

6. Select Apply LDIF file.
7. At the command prompt type the log path. Typically, this path is: sys:system\schema\.

Assign rights to an individual user

1 Select the LDAP server to view a list of users in the right-side window pane.

2 Right-click on a user.

3 Select Trustees of the Object.

4 Select the user and click Assigned Rights.

5 Click Add a Property.

6 Uncheck Show Only Properties of the Object Class.

7 Select pcaHostEntry and click OK.

8 Choose the write access rights to apply to this property and click OK.

Assign rights to multiple users

To assign rights to multiple users:

1 Create a group object and name it pcAnywhere_group.

- Select the container to place the group.
- Right-click on the container and select Group from the New menu.
- Type a name for the group.

2 Right-click on the group name and select Properties.

3 Click the Members tab, then click add to include other users.

Note: Hold down the Ctrl key to select multiple users.

4 Select **Properties of Multiple Objects** from the File menu to grant access rights.

5 Click the NDS Rights tab.

6 Click Add Trustee, then select the pcAnywhere group and click OK.

7 Click Add Property.

8 Uncheck **Show Only Properties of this Object Class**.

9 Select **pcaHostEntry** and click OK.

10 Choose the write access rights to apply to this user group and click OK.