Honeywell

Install and Configure a TPS PDC

Objective

Given an NT Server node, configure it to be the primary domain controller (PDC) for a TPS domain.

In This Module

- Review of PDC Functions
- Review of NT Domain Models
- Overview of PDC Setup
- Configure PDC Security including:
  - Groups
  - Users
  - File Permissions
  - User Rights
  - Audit Policies
  - Proxy Files
- Details of Honeywell added users
- Details of Honeywell added groups
- Configure HOST and LMHOSTS Files
- Create the PDC_COPY.BAT File

Install and Configure a TPS PDC

What is a Primary Domain Controller

Domain controllers are computers running Windows NT Server that use one shared directory to store security and user-account information for the entire domain; they comprise a single administrative unit.

Within a domain, domain controllers manage all aspects of user/domain interactions. Windows NT domain controllers use the information in the directory database to authenticate users logging on to the domain accounts.

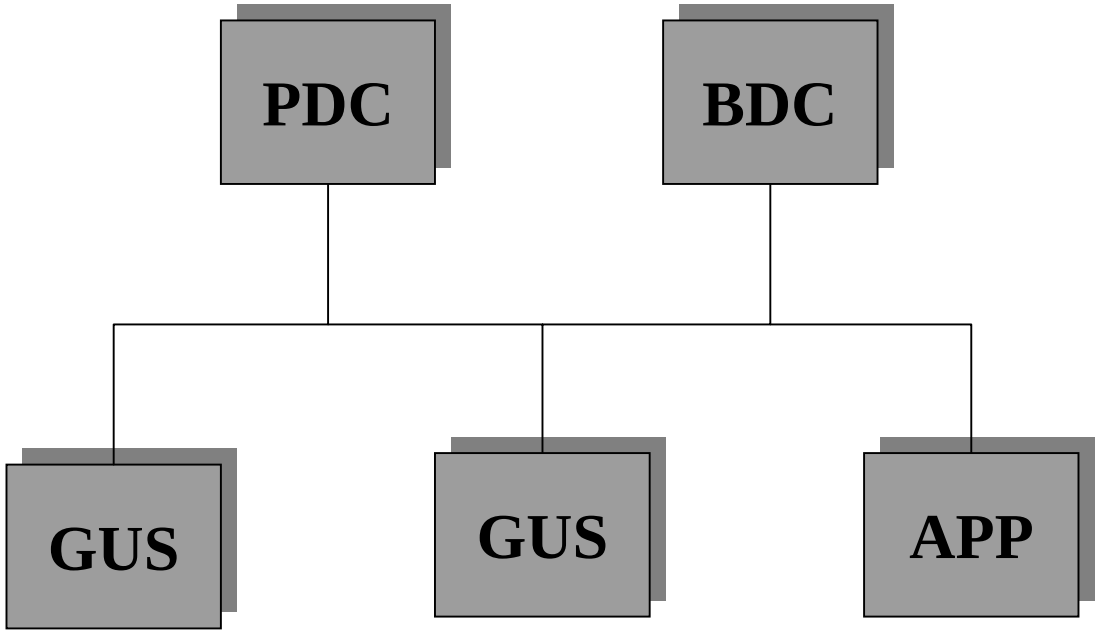
There are two types of domain controllers:

- The *primary domain controller* (PDC), which maintains a copy of the directory database. A domain has one PDC.
- A *backup domain controller* (BDC), which maintains a copy of the directory database. This is periodically synchronized with the directory database on the PDC. A domain can have multiple BDCs.

Install and Configure a TPS PDC

Single Domain

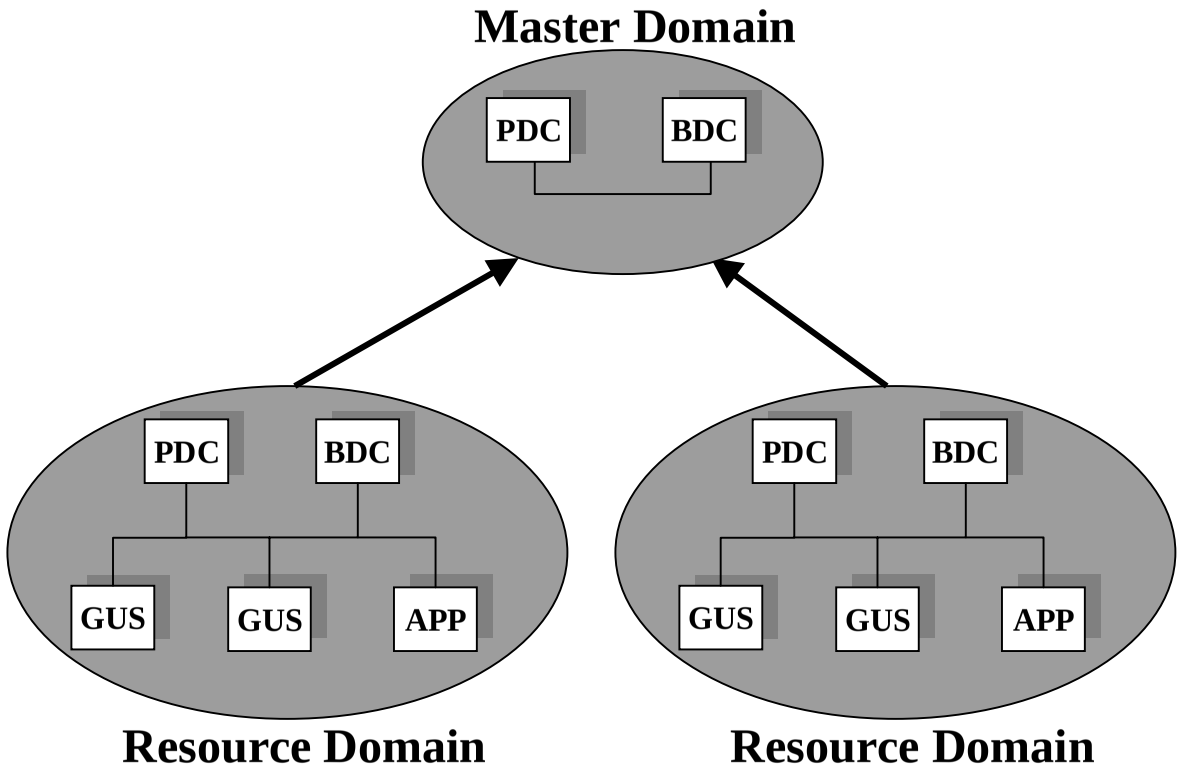
- BDC for fault tolerance and logon load balance
- All machine and user accounts reside in domain



Install and Configure a TPS PDC

Single Master

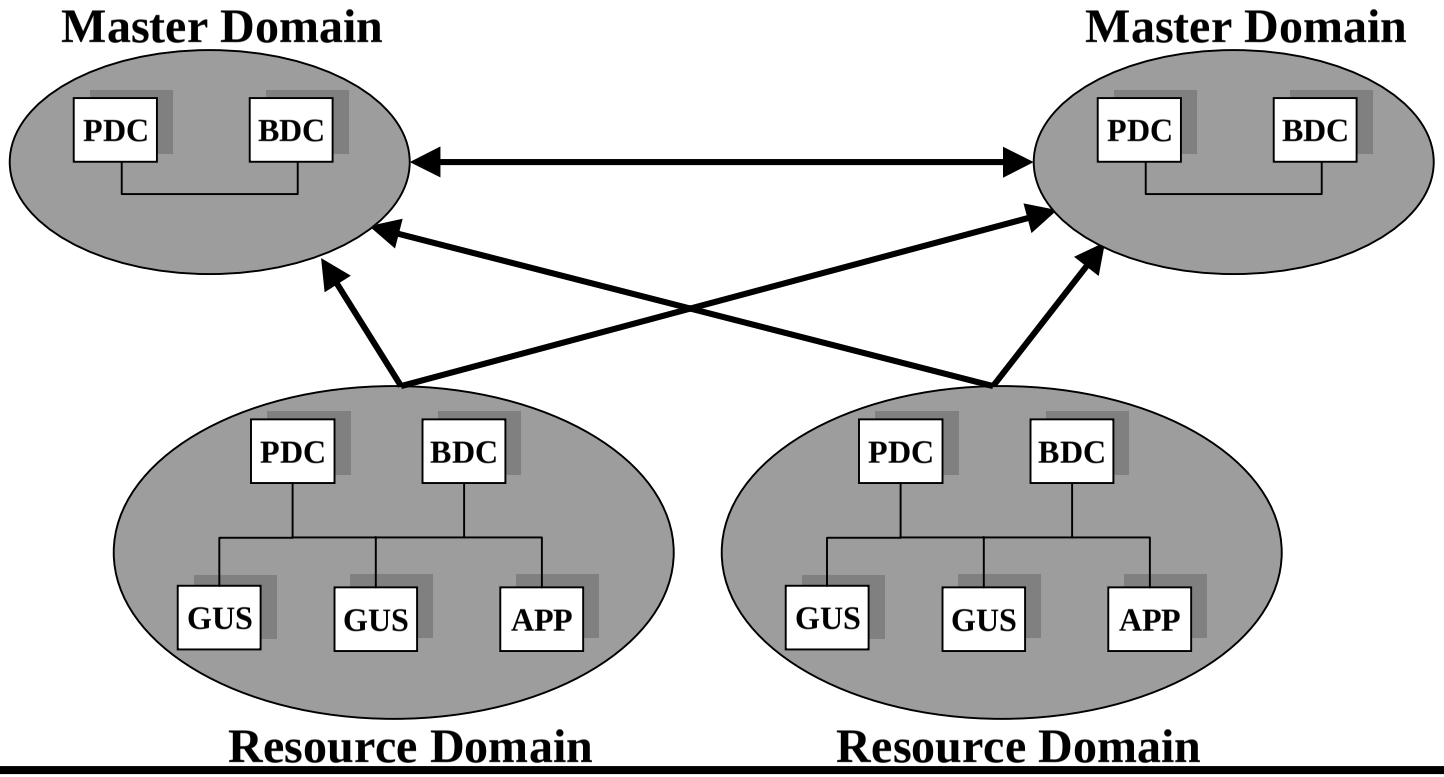
- A PDC in each domain
- Machine accounts reside in respective domain
- User accounts reside in trusted domain



Install and Configure a TPS PDC

Multiple Master

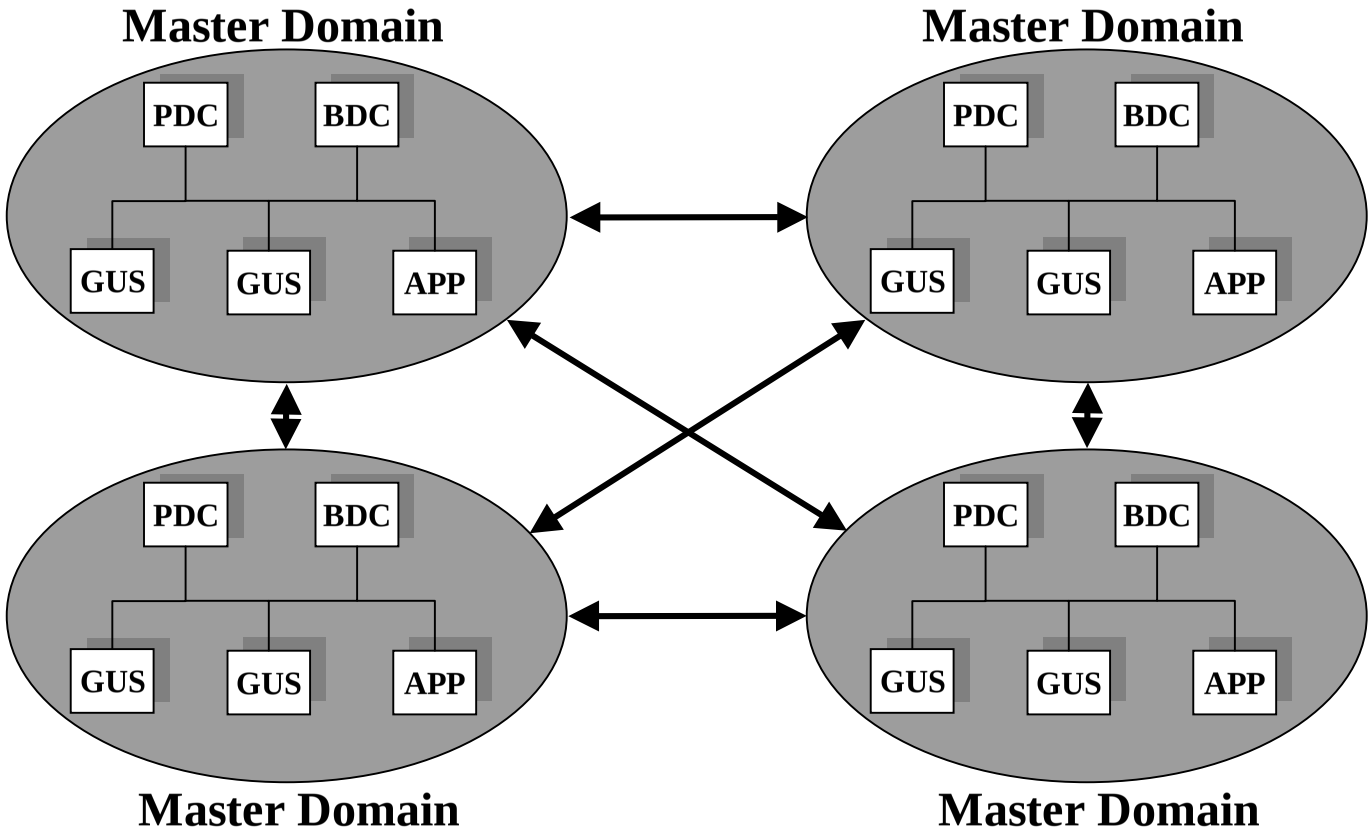
- All master domains would trust each other
- User accounts would be distributed among master domains
- Resource domains must trust all master domains



Install and Configure a TPS PDC

Complete Trust

- All domains trusting all other domains
- All domains maintain their own machine accounts



Install and Configure a TPS PDC

PDC Setup

- Install NT Server software, service pack, drivers
- Set the password for the Administrator account
- Set date and time
- Configure Auditing
- Configure TCP/IP
- Install TPS Security (run a setup utility)
- Add Users
  - Operator, Supervisor, Engineer, TPSAdministrator, View Only
- Configure HOSTS and LMHOSTS files
- Create the PDC_COPY.BAT file (does special replication)
- Create/Update the Emergency Repair Disk (ERD)

Install and Configure a TPS PDC

Install TPS Security (setup utility)

- Add user accounts
  - TPSRepl, TPSComServer, TPSApp, AppDir_EE_Account
- Add domain groups (global groups)
  - TPS Administrators, Intimate Users, Point Builders, Continuous Controls, Programs, Engineers, Supervisors, Operators, View Only Users
- Modify Group Membership
  - Add Domain Admins group to Local Administrators group
  - Add TPSAdministrators group to Local Backup Operators group
  - Add Domain Admins group to Local Backup Operators group
  - Add TPSRepl domain user to Local Replicator group
  - Add TPSApp domain user to Global Programs group
  - Add AppDir_EE_Account domain user to Global TPS Administrators group
  - Make Global Programs group primary group for TPSApp domain user
  - Remove TPSApp domain user from Global Domain Users group

Install and Configure a TPS PDC

Install TPS Security (setup utility), continued

- Create a hidden share called TPSRepl$ on the directory: \winnt\system32\repl\export\HWIAC
  - set permissions on the share:
    - Full Control: Administrators, TPSAdministrators, Replicator
    - Read: Everyone
- Create the following files:
  - \Winnt\system32\Repl\Export\HWIAC\ master.dcl
  - \Winnt\system32 \Repl\Export\scripts\ntconfig.pol
  - \Winnt\system32 \Repl\Export\scripts\ntconfig.pol.sam
  - \Winnt\system32 \Repl\Export\scripts\operator.bat
  - \Winnt\system32 \Repl\Export\scripts\operator.bat.sam
  - \Winnt\system32 \Repl\Export\scripts\pdc_copy.sam
  - \Winnt\Inf\honeywell.adm

Install and Configure a TPS PDC

Install TPS Security (setup utility), continued

- Modify registry permissions
  - HKLM\System\CurrentControlSet\Control\SecurePipeServers\winreg (not recursive)
    - Full Control: Administrators, TPSAdministrators, Replicator
    - Read: Everyone
  - HKLM\Software\Honeywell (recursive)
    - Full Control: TPSAdministrators, Replicator
    - Read: Everyone
  - HKLM\Software\Honeywell IAC (recursive)
    - Full Control: TPSAdministrators
    - Read: Everyone
- Modify user rights (refer to *TPS System Administration Guide*)
- Modify File Permissions (refer to *TPS System Administration Guide- only proxy files listed*)

Install and Configure a TPS PDC

Account Administration

- Local User Database on each Workstation
- Domain Wide User Database on PDC/BDC in each Domain
- Administrative Tool from Microsoft
  - User Manager (on Workstations)
  - User Manager for Domains (on Servers)
    - Also available as part of NT Workstation Resource Kit
- Users and Groups

Install and Configure a TPS PDC

GUS Local User

- Login with no password
- No access to Network, Floppy Drive, Zip Drive, or CD-ROM
- Allowed to run these applications:
  - Native Window, GUS Runtime, TPS System Status Display
- No icons presented on the desktop
- No Screensaver
- Allowed to shut down node
- Environment started at login using a batch file

Install and Configure a TPS PDC

View Only User

- Login with no password
- No access to Floppy Drive, Zip Drive, or CD-ROM
- Allowed to run these applications:
  - Native Window, GUS Runtime, TPS System Status Display
- No icons presented on the desktop
- No Screensaver
- Allowed to shut down node
- Environment started at login using a batch file

Being logged in as a View Only User does NOT stop the user from making changes through the Native Window.

Install and Configure a TPS PDC

Operator

- Login with no password
- No access to Floppy Drive, Zip Drive, or CD-ROM
- Allowed to run these applications:
  - Native Window, GUS Runtime, TPS System Status Display
- No icons presented on the desktop
- No Screensaver
- Allowed to shut down node
- Environment started at login using a batch file

Install and Configure a TPS PDC

Supervisor

- Login with a password
- No access to Floppy Drive, Zip Drive, or CD-ROM
- Allowed to run these applications:
  - Native Window, GUS Runtime, TPS System Status Display
- No icons presented on the desktop
- No Screensaver
- Allowed to shut down node
- Environment started at login using a batch file

Install and Configure a TPS PDC

Engineer

- Login with a password
- Access to Floppy Drive, Zip Drive, or CD-ROM
- Allowed to run any application
  - with restricted write access to files and directories
- Full NT Desktop presented
- Screensaver enabled with password
- Allowed to shut down node
- No access to configuration and registry editing tools

Install and Configure a TPS PDC

TPS Administrators

- Login with password
- Access to Floppy Drive, Zip Drive, or CD-ROM
- Allowed to run any application
  - with full write access to files
- Full NT Desktop presented
- Screensaver enabled with password
- Allowed to shut down node
- No access to registry editing tools
- Access to TPS configuration tools

Install and Configure a TPS PDC

Administrators

- Login with password
- Access to Floppy Drive, Zip Drive, or CD-ROM
- Allowed to run any application
  - with full write access to files
- Full NT Desktop presented
- Screensaver enabled with password
- Allowed to shut down node
- Full access to registry editing tools
- No access to TPS Domain Configuration Utility

Install and Configure a TPS PDC

Local Users

Local Administrator

- Requires end user to set password

Local Users Created During TPS Base Software Installation:

- GUS (for Local Login)
  - No Network Access
  - Restricted Policies
- TPSLocalServer (for Local Servers)
  - Only configured to be used for Services and Batch jobs
  - Will not be used after November 1998

Install and Configure a TPS PDC

Domain Users

- TPSComServer
  - used to run TPN Server
- TPSRepl
  - used to run TPSAdmin service
  - used to commit/replicate TPS configuration (NOT standard NT replication)
- TPSApp
  - used to run CL Server and NT applications invoked by CL Server
  - member of Programs global group
- AppDir_EE_Account
  - used to run the Execution Environment used by Application Director

These accounts:

- are used by the TPS System Infrastructure
- are automatically created by the TPS Security Installation
- passwords are set to **password**

Install and Configure a TPS PDC

Domain Users, continued

User added by installing the Best1 package:

- Best1_User
  - used with the Best1 performance monitoring package when a remote connection is made to the system

This account:

- is automatically created when the Best1 package is installed
- should not be modified

Install and Configure a TPS PDC

Local Group Membership

Domain Groups to Local Group membership required on the TPS PDC:

- Domain Admins member of Local Administrators
- TPS Administrators member of Backup Operators
- Domain Admins member of Backup Operators
- TPSRepl Domain User members of Replicator

Domain Groups to Local Group membership required on TPS Nodes:

- Domain Admins member of Local Administrators
- TPSRepl Domain User members of Replicator
- TPS Administrators member of Local Administrators

Install and Configure a TPS PDC

Proxy Files

TPS introduces Proxy Files for security.

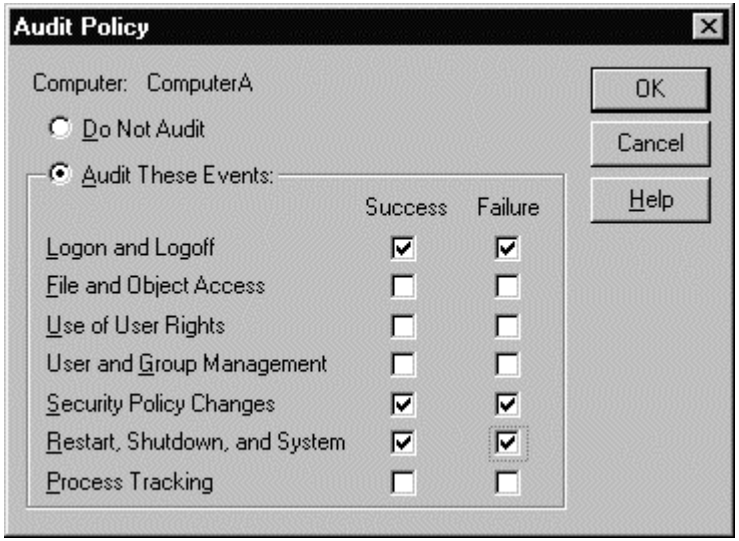
Default Proxy files are:

- Created by the TPS Security Installation
- Duplicated in each TPS Domain
- Defined in the *TPS System Administration Guide*

Install and Configure a TPS PDC

Audit Policy

The recommended audit policy settings:



Install and Configure a TPS PDC

Account Policies

Account Policies are configured through the **User Manager** utility.

- Set Password Age, Minimum Password Length, and Password Uniqueness
- Set Account Lockout Policies

Install and Configure a TPS PDC

PDC_COPY.BAT

- Distributes
  - HOSTS and LMHOSTS
  - Policy Files
  - Batch Files (**operator.bat**)
  - PDC_COPY.BAT – original file is named PDC_COPY.SAM
  - Command Files
- Operator and Supervisor Accounts are more restrictive
  - Execute a batch file on Login - **Operator.bat**
  - **Operator.bat** distributed from the PDC