Chaffey College
Chino Information Technology Center

CISNTWK-11

Microsoft Network Server

Chapter 4

User and Group Accounts

Chaffey College
Chino Information Technology Center

Usage Notes

- Throughout these slides, the term ***Active Directory Domain*** implies Domains
  - Based on Windows Server 2008
  - Based on Windows Server 2003
  - Based on Windows 2000 Server
- Throughout these slides, the term ***Domain*** (by itself) implies Domains
  - Based on Windows Server 2008
  - Based on Windows Server 2003

Usage Notes

  - Based on Windows 2000 Server
  - Based on Windows NT Server
- Unless stated otherwise, references to Windows Vista imply
  - Windows Vista Business
  - Windows Vista Enterprise
  - Windows Vista Ultimate
- Unless stated otherwise, references to Windows XP imply
  - Windows XP Professional

User Accounts

- A *User Account* is the name that is used to authenticate on the Windows NT “family” of Operating Systems (including Windows Server 2008)
  - In order to use the system, you must first logon with a valid:
    - User Account
    - password
- User Accounts are what distinguishes one’s identity (and access rights) from another’s
- User Accounts should be unique for each user

User Accounts

  - Exception - an account shared by multiple users, such as “Guest”
- There are two types of user accounts
  - Domain User Accounts
  - Local User Accounts
- Local User Accounts are separate and distinct from Domain User Accounts
  - User “Dilbert” as a Local User Account is separate from user “Dilbert” as a Domain User Account
    - access rights and privileges are treated independently

Domain User Accounts

- Provide access to network resources
  - Either on the Domain in which the User Account exists or a different Domain
    - access to resources in a different Domain will require a trust relationship between the Domains
      - depending on the Domain structure, this may be automatic with Active Directory

Domain User Accounts

  - The resources can be located on different computers in a Domain
    - the computers must be running Windows NT (family) and must have membership in the Domain
- Users can generally authenticate (logon) from any computer in the Domain
- Exist only on Windows Server Domain Controllers
- Are stored on the Domain Controller in
  - Active Directory (AD) (Windows Server 2000 and later versions of Server)
  - The SAM database (Windows NT Server)

Local User Accounts

- Provide access to resources on the local computer only
- Users authenticate (logon) at the computer housing their Local User Account
- Exist on all computers running the following Operating Systems
  - Windows 7, Windows Vista, Windows XP, Windows 2000 Professional,
    and Windows NT Workstation
  - Windows Server 2008, Windows Server 2003, Windows 2000 Server, and
    Windows NT Server acting as stand-alone or member Servers

Local User Accounts

- Local User Accounts do **not** exist on Domain Controllers
- Are stored in the Security Accounts Manager (SAM) database on that computer
- Local User Accounts existing on different computers are treated separately
  - User “Dilbert” on computer “Dogbert” is separate from user “Dilbert” on computer “Catbert”
    - access rights and privileges are treated independently

Groups

- Groups are a collection of (or contain)
  - User Accounts
  - Other Groups
    - Windows Active Directory Domains support multiple levels of nesting [1]
    - Windows NT Domains only supports a single level of nesting
  - Computer accounts
    - supported only on Active Directory Domains
  - Contacts
    - supported only on Active Directory Domains

Groups

- Groups are used to
  - Manage user and computer access to shared resources
    - such as network shares, files, directories, printer queues, and Active Directory objects
  - Filter Group Policy settings
  - Create Email distribution lists
- **Groups are an administrative convenience**

Groups (continued)

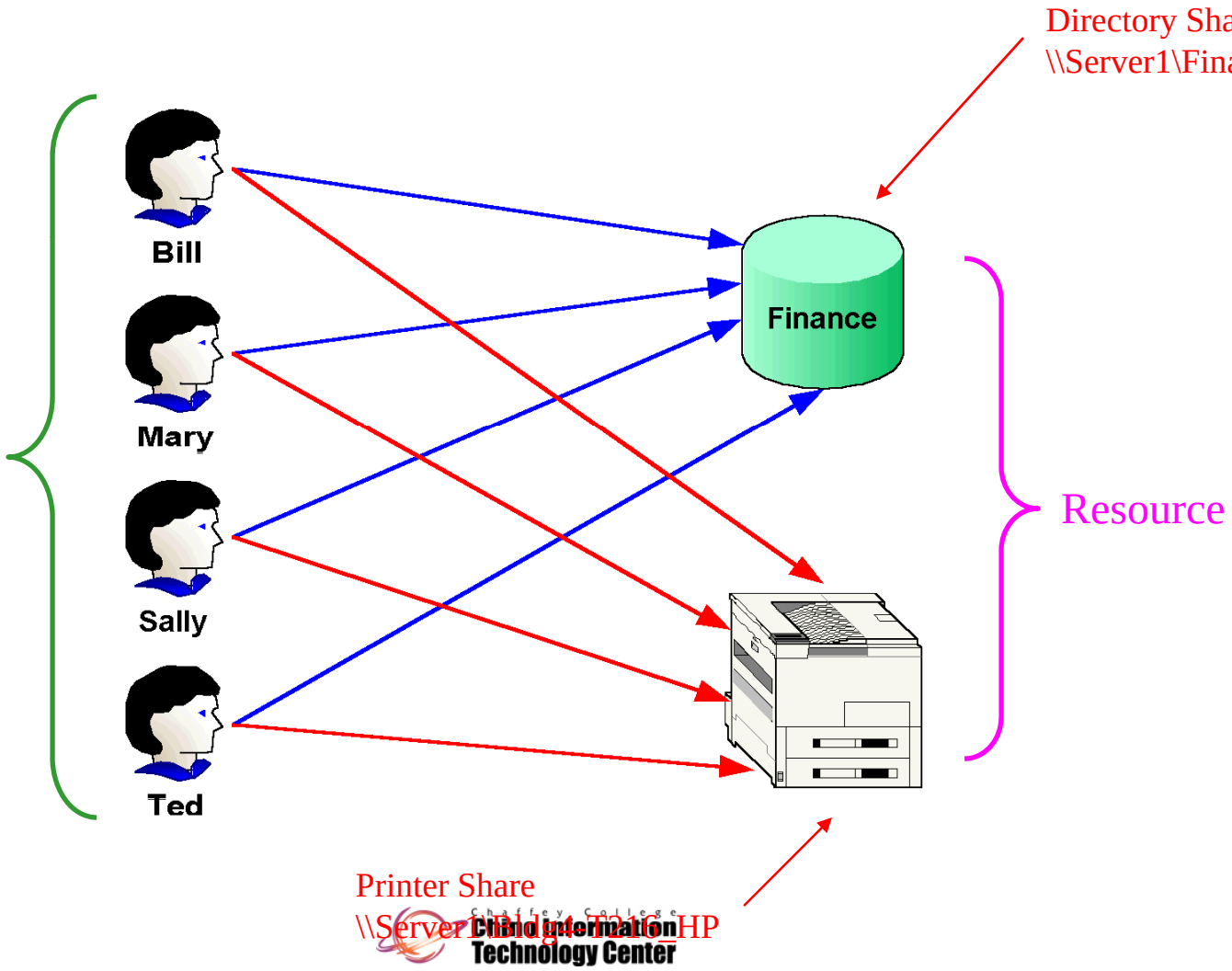
- Users can be members of multiple Groups
  - There are issues with authentication and group policy settings when a user belongs to more than about 120 Groups in a Windows 2000 Domain (pre SP4)
- Members receive the permissions that are given to Groups
- Common types of Groups that you may want to create include
  - Groups for departments within an organization
    - Engineering, Finance, Manufacturing, Marketing, Sales

Groups (continued)

  - Groups for roles within an organization
    - Executives, Supervisors, Secretarial staff, Engineers, Hourly staff
  - Groups for users that use a common application
- A Group can contain no more than 5,000 members in an Active Directory Domain
  - This could be a problem in a “large” Domain because by default every user is a member of the “Domain Users” Group [1]
  - This limitation has been corrected in Windows Server 2003 & 2008 Domains that have been raised to Domain Functional Level “Windows Server 2003” or “Windows Server 2008”

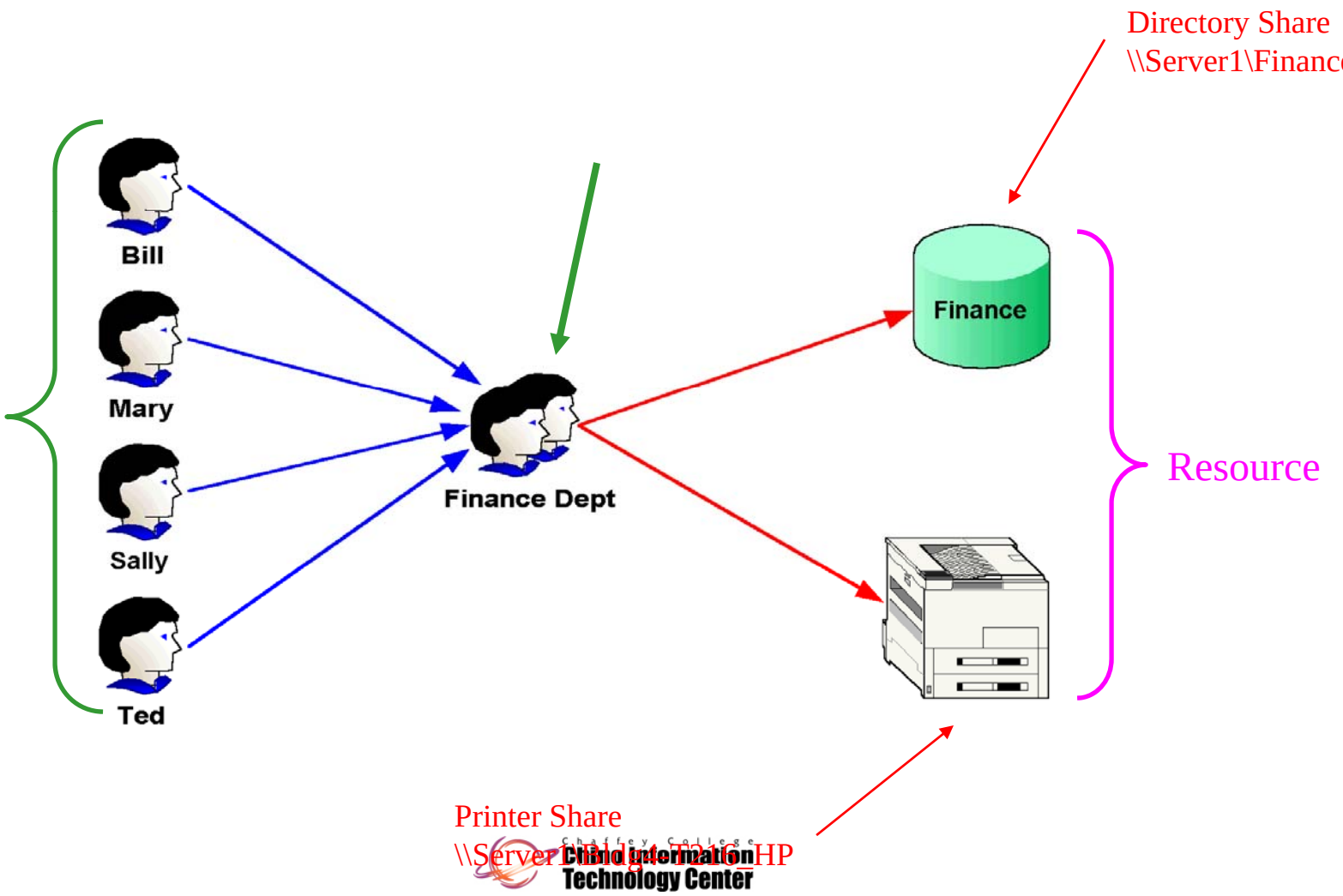
Groups Simplify Administration

- An example without the use of Groups



Groups Simplify Administration (continued)

- An example with the use of Groups



Group Categories

- With Active Directory Domains, there are two categories of Groups
  - Security Groups
  - Distribution Groups
    - this group category does not exist in Windows NT Domains
- **Security Groups**
  - Allow multiple users to be treated as a single administrative unit
    - for permissions (access rights) to objects, and user rights on the local computer

Group Categories

  - The Administrator associates the rights and permissions to a Group, and then “connects” the Group to one or more User Accounts [1]

- **Distribution Groups**
  - Are used for application environments
    - such as an Email mailing list
  - Membership in Distribution Groups does not affect your access rights to resources
  - Was introduced with Windows 2000
    - are only supported in an Active Directory Domain environment

Group Types

- The following types of Groups exist, each providing different scope (visibility)
  - **Local Groups**
    - exist on all computers running Windows NT (family) except Domain Controllers
    - limited in scope - visible on the local computer only
    - Local Groups are used primarily to support a non-Domain environment and provide the same functionality as Windows NT Local Groups
    - when the system is participating in a Domain, the Local Groups are used when a user logs onto the system locally (separate from the Domain)

Group Types

- **Domain Local Groups**
  - exist only on Active Directory Domain Controllers
  - in a "**Windows 2000 mixed**" Domain Functional Level (Windows 2003),
    or "**mixed mode**" Domain (Windows 2000)
    - are visible only on the Domain Controllers within the Domain
    - provide functionality similar to "Local Groups" on Windows NT
  - in a "**Windows 2000 native**", "**Windows Server 2003**", or "**Windows Server 2008**" Domain Functional Level (Windows 2008 and Windows 2003), or a "**native mode**" Domain (Windows 2000)
    - are visible on all computers within the Domain
    - may be nested

Group Types (continued)

- The following types of Groups exist, each providing different scope (visibility)
  - **Domain Global Groups**
    - exist only on Active Directory Domain Controllers
    - provide functionality similar to “Global Groups” on Windows NT
    - are visible on all computers within the Domain
    - are visible within the Active Directory “tree” (trusted Domains)
    - in a “**Windows 2000 native**”, “**Windows Server 2003**”, or “**Windows Server 2008**” Domain Functional Level (Windows 2008 and Windows 2003), or a “**native mode**” Domain (Windows 2000)
      - Global Groups may be nested

Group Types (continued)

- **Universal Groups**
  - exist only on Active Directory Domain Controllers
    - when operating at "**Windows 2000 native**", "**Windows Server 2003**", or "**Windows Server 2008**" Domain Functional Level (Windows 2008 and Windows 2003), or a "**native mode**" Domain (Windows 2000)
  - are stored in the "Global Catalog" within Active Directory
  - are visible throughout the entire Active Directory "forest"
  - Universal Groups may be nested
  - Universal Groups generally have fewer membership restrictions than the other Groups

Rules for Accounts and Groups

- In a Domain environment
  - A Windows User Account (User logon name) can be from 1 to (about) 104 characters in length
  - A “pre Windows 2000” user logon name must also be given [1]
    - it is from 1 to 20 characters in length
    - by default it is set to the first 20 characters of the User logon name
    - this (possibly) alternate name must be unique throughout the Domain

1
2

Rules for Accounts and Groups

- A Group name can be from 1 to 63 characters in length
  - User Account and Group names must be unique throughout the Domain
- In a non-Domain environment
  - A User Account can be from 1 to 20 characters in length

Rules for Accounts and Groups

- Local User Account and Group names must be unique on the computer
- User Account names can contain alphanumeric and “some” special characters
  - These include a period, underscore, hyphen, dollar sign, and space
  - A Group name can be from 1 to 63 characters in length 2

1
2

Rules for Naming User Accounts

- The following list identifies the names of the attributes within a User object (account) and the scope within which that name must be unique
  - First name, initials, last name
    - no uniqueness requirement
  - Display name
    - no uniqueness requirement
  - Full name
    - must be unique within the container

Rules for Naming User Accounts

  - User Principal Name (UPN) [1]
    - must be unique within the forest [1]
  - User logon name (pre-Windows 2000)
    - must be unique within the Domain
- By default, the Full Name is set equal to the Display Name (but can be changed)
- By default, the Display name is generated by using the First name, initials, and last name
  - The Display name is the actual name displayed in most of the administrative tools

Built-in User Accounts

- Windows NT family include two built-in User Accounts
  - this account has implicit access/rights/privileges to the configuration of the local computer
  - this account has access to the entire Domain if it is defined on a Domain Controller
  - the Administrator account is intended for the person who manages the local computer or Domain
  - with Windows Server 2008 and Windows Server 2003, this account can be disabled
  - with Windows 7 and Windows Vista, this account is disabled (by default)
  - if this account is disabled, it can only be logged into by re-starting the system into “Safe Mode”

Built-in User Accounts

- provides limited access to the computer and/or Domain
- access to specific objects will probably need to be explicitly allowed by the Administrator
- this user account is disabled by default

Built-in User Accounts (continued)

- Windows Server 2008, Windows Server 2003, and Windows 2000 Server include additional User Accounts
  - These User Accounts support specific features such as IIS and Terminal Server
  - Domain Controllers have additional User Accounts (e.g.: for key distribution)
- The built-in user accounts cannot be deleted
- The built-in user accounts **can** be renamed
  - Most books recommend renaming the “Administrator” account for added security
  - Unfortunately, this may provide a false sense of security [1]

Built-in Group Accounts

Name	Type	In Domain [1]	In SAM [2]	Active Directory Container	Notes
Account Operators	Local	Yes	No	Builtin	Administrative delegation
Administrators [3]	Local	Yes	Yes	Builtin	Full access to “local” computer
Backup Operators	Local	Yes	Yes	Builtin	Administrative delegation
Domain Admins [3]	Global	Yes	No	Users	Full access to the **entire** Domain
Domain Guests	Global	Yes	No	Users	Limited access
Domain Users	Global	Yes	No	Users	User of Domain (except “Guests”)
Guests	Local	Yes	Yes	Builtin	Limited access
Power Users	Local	No	Yes	N/A	Combines Domain “XXX Operators”
Print Operators	Local	Yes	No [4]	Builtin	Administrative delegation
Replicator	Local	Yes	Yes	Builtin	Domain file and directory replication
Server Operators	Local	Yes	No	Builtin	Administrative delegation
Users	Local	Yes	Yes	Builtin	All users are members of this Group

1

2

3 use with caution

4

Built-in Group Accounts (continued)

- Windows Server 2008, Windows Server 2003, Windows 7, Windows Vista, and Windows XP include the following Groups
  - Light green color means that it is defined only on Windows Server 2003 (and later)

Name	Type	In Domain	In SAM	Active Directory Container	Notes
HelpServicesGroup [1]	Local	Yes	Yes	Users	For Help and Support Center
Incoming Forest Trust Providers [2]	Local	Yes	**No**	Builtin	Can create one-way trusts to this forest
Network Configuration Operators [3]	Local	Yes	Yes	Builtin	Can configure networking features
Performance Log Users	Local	Yes	Yes	Builtin	Can log performance counters
Performance Monitor Users	Local	Yes	Yes	Builtin	Can monitor this computer
Remote Desktop Users	Local	Yes	Yes	Builtin	Can logon remotely
TelnetClients [1]	Local	Yes	Yes	Users	Can access Telnet Server
Windows Authorization Access Group	Local	Yes	**No**	Builtin	Can enumerate Global and Universal Groups

1
2
3

This security Group will eventually be the Forest Root Domain version of the "Pre-Windows 2000 Compatible Access" group - use with caution

Built-in Group Accounts (continued)

- Windows Server 2008, Windows 7, and Windows Vista

Name	Type	In Domain [1]	In SAM [2]	Active Directory Container	Notes
Certificate Service DCOM Access	Local	Yes	Yes	Builtin	Administrative delegation
Cryptographic Operators	Local	Yes	Yes	Builtin	Administrative delegation
Distributed COM Users	Local	Yes	Yes	Builtin	Granular resource access
Event Log Readers	Local	Yes	Yes	Builtin	Administrative delegation
Performance Log Users	Local	Yes	Yes	Builtin	Granular resource access
Performance Monitor Users	Local	Yes	Yes	Builtin	Granular resource access

1
2
3

Built-in Group Accounts (continued)

- Windows Active Directory Domains include the following security Groups
  - This does not include group accounts for specific services (such as DNS, and RAS)
  - Light green color means that it is defined only on Windows Server 2008

Name	Type	Active Directory Container	Notes
Allowed RODC Password Replication Group	Local	Users	User passwords are cached on the RODC
Cert Publishers [1]	Global	Users	Certification and renewal agents
Denied RODC Password Replication Group	Local	Users	User passwords are not cached on the RODC
Domain Computers	Global	Users	This contains computer accounts
Domain Controllers	Global	Users	This contains computer accounts
Enterprise Admins [2] [3]	Global / Universal	Users	Administrators for the **entire** "enterprise"

1

2

3

Built-in Group Accounts (continued)

- Windows Active Directory Domains include the following security Groups
  - This does not include group accounts for specific services (such as DNS, and RAS)
  - Light green color means that it is defined only on Windows Server 2008

Name	Type	Active Directory Container	Notes
Enterprise Read-only Domain Controllers [3]	Universal	Users	This contains computer accounts
Group Policy Creator Owners [1]	Global	Users	For managing Group Policies
Pre-Windows 2000 Compatible Access	Local	Builtin	Provides NT 4 behavior for access to Users and Groups
Read-only Domain Controllers	Global	Users	This contains computer accounts
Schema Admins [2] [3]	Global / Universal	Users	For Active Directory Schema changes
Terminal Server License Servers	Local	Builtin	This contains computer accounts

1

2

3

Built-in Group Accounts (continued)

- The built-in group accounts cannot be deleted
- The built-in Global group accounts can be renamed in an Active Directory Domain
- The built-in group accounts cannot be renamed on Windows NT
- The built-in Local group accounts

Built-in Group Accounts (continued)

  - Can be renamed on non-Domain Controller versions of Window 2000 (or later)
  - Cannot be renamed in an Active Directory Domain
- Group names and Account names **must** be named differently on a local computer or within a Domain
  - A User Account named “Payroll” and a Group named “Payroll” cannot exist in the same “context” at the same time

User Rights

- Apply to the entire computer as a whole
- Are generally unique to the local computer
  - User Rights defined in an Active Directory Domain environment can supercede local User Rights
- Provide the ability for a user to do specific actions on the local computer
  - If you don’t have the right to perform an action, you are unable to do so

User Rights

  - With Windows 2000 (and later) there are a specific set of rights that start with “Deny”
    - these take priority over the same rights that do not start with “Deny”
- User Rights are also known as privileges
- Windows 2000 (and later) define approximately 32 individual “rights”
  - Not all of the User Rights are visible through the user interface

User Rights (continued)

- User Rights that are important to know at this time
  - ***Allow Log on locally*** (Windows Server 2003 and later- including Windows Vista)
    Log on locally (Windows XP, Windows 2000, and Windows NT)
    - without this right, you cannot logon interactively to the local computer
    - this right is restricted to “Administrators and Operators” on Domain Controllers
    - this right is enabled for all users (except Guest) on non-Domain Controllers running
      - Windows Server 2008 and Windows Server 2003
      - Windows 2000 Server and Windows NT Server
    - this right is enabled for all users on the following systems

User Rights (continued)

  - Windows 7, Windows Vista, Windows XP, Windows 2000, Windows NT

- ***Shut down the system***
  - without this right, you cannot shutdown the system
  - this right is restricted to “Administrators and Operators” on Domain Controllers
  - this right is restricted to Administrators, Backup Operators, and Power Users [1] on
    - Windows Server 2008 and Windows Server 2003
    - Windows 2000 Server and Windows NT Server
  - this right is enabled for all users on the following systems
    - Windows 7, Windows Vista, Windows XP, Windows 2000, Windows NT

Password Policy

- **Security Settings -> Account Policies -> Password Policy**

Name	Value Is In	Allowed Range	Default Domain Policy: 2008 / 2003 / 2000	Default Local Policy	Notes
Enforce password history	Passwords remembered	0 - 24	24 / 24 / 1	0	0 does not keep password history
Maximum password age	Days	0 - 999	42 / 42 / 42	42	Expires in “n” days. 0 for password never expires
Minimum password age	Days	0 - 999	1 / 1 / 0	0	Allow changes in “n” days 0 for change immediately
Minimum password length	Characters	0 - 14	7 / 7 / 0	0	0 does not require a password
Passwords must meet complexity requirements	Boolean	Enabled or Disabled	Enabled / Enabled / Disabled	Disabled / Enabled [1]	Uses a “password filter” for enforcement [2]
Store password using reversible encryption for all users in the domain	Boolean	Enabled or Disabled	Disabled / Disabled / Disabled	Disabled	Needed for “legacy” CHAP and Digest protocols used by RAS and IAS

1
2

Password Policy (continued)

- When the "**Passwords must meet complexity requirements**" option is enabled, user passwords must meet the following requirements:
  - **The password is at least six characters long**
  - **The password contains characters from three of the following five categories:**
    - English uppercase characters (A - Z)
    - English lowercase characters (a - z)
    - base 10 digits (0 - 9)
    - non-alphanumeric (for example: !, $, #, or %)
    - Unicode characters not visible on the keyboard
    - the character is entered by simultaneously holding down the **ALT** key while entering three numeric digits (**ddd**) from the numeric keypad

Password Policy (continued)

- **The password does not contain three or more characters from the user's account name**
  - if the account name is less than three characters long, then this check is not performed
  - the following characters are treated as delimiters that separate the name into individual tokens:
    - commas, periods, dashes/hyphens, underscores, spaces, pound-signs and tabs
  - for each token that is three or more characters long, that token is searched for in the password
    - if it is present (even as a substring), the password change is rejected
  - all of these checks are case insensitive

Account Lockout Policy

Name	Value Is In	Range Allowed	Default Domain Policy: 2008 / 2003 / 2000	Default Local Policy	Notes
Account lockout duration	Minutes	0 - 99999	30 [1] / 30 [1] / 30 [1]	Not defined	0 locks account until Administrator unlocks it
Account lockout threshold	Invalid logon attempts	0 - 999	5 [1] / 5 [1] / 0	0	0 does not lock out the account
Reset account lockout counter after	Minutes	1 - 99999	30 [1] / 30 [1] / 5 [1]	Not defined	

Kerberos Policy

- **Security Settings -> Account Policies -> Kerberos Policy** [1]
  - These policies are listed for completeness sake, and should generally be left “as is”

Name	Value Is In	Range Allowed	Default Domain Policy	Default Local Policy	Notes
Enforce user logon restrictions	Boolean	Enabled/ Disabled	Enabled	Not defined	More secure (but slower) if enabled
Maximum lifetime for service ticket	Minutes	0 - 99999	600	Not defined	0 for ticket doesn’t expire
Maximum lifetime for user ticket	Hours	0 - 99999	10	Not defined	0 for ticket doesn’t expire
Maximum lifetime for user ticket renewal	Days	0 - 99999	7	Not defined	0 for ticket renewal doesn’t expire
Maximum tolerance for computer clock synchronization	Minutes	0 - 99999	5	Not defined	

Account Policies Notes

- In an Active Directory Domain environment, the policies are applied in the following sequence
  (the ones listed last take precedence over those listed first if there are “conflicts”)
  - Local Security Settings
  - Domain Security Policy
  - Domain Controller Security Policy
    - this applies only to the Domain Controllers within the Domain
- In an Active Directory Domain environment, the “Account Policies” are only in effect at the Domain level

Account Policies Notes

  - They have no effect at Organizational Units within the Domain
  - They are (usually) configured in the “Default Domain Policy”
- With Windows Server 2008 Domains operating at “Windows Server 2008” Domain Functional Level
  - The “Account Policies” can be applied at a granular level
    - this means different users can have different policies on the same Domain

Account Policies Notes

- Note that by default the “Account Policies” behavior operates at the Domain level
- Refer to the Resources slide “Microsoft Windows Server 2008 resources” for details

Account Policies Notes (continued)

- Password policies apply for all users on the Domain or local computer
  - **Exception** - a User Account with the "Password Never Expires" option enabled
    - however, when the password is changed for this user, the following Password Policies must be met (this includes the "Administrator" account)
      - if the "**Password must meet complexity requirements**" policy is enabled, the password must meet this requirement
      - the password length must be at least as long as the "**Minimum password length**" policy

Account Policies Notes (continued)

- With Windows Server 2008 and Windows Server 2003, the “Administrator” user account can be disabled
  - This circumvents hackers from being able to continually “guess” the password
  - If this account is disabled, it can only be logged into by re-starting the system into “Safe Mode”
- With Windows 7 and Windows Vista, the “Administrator” user account is disabled by default
  - Unless explicitly overridden via an unattended installation

Account Policies Notes (continued)

- With Windows XP and later, you cannot access any user account over a network that has a blank password (or no password) [1]
  - Although not recommended, it is possible to change this behavior by changing the "Security Option"
    - **Accounts: Limit local account use of blank passwords to console logon only** [1]
      - this option can be "***Enabled***" (the default) or "***Disabled***" (to turn off the behavior)

Account Policies Notes (continued)

- The Account Lockout policy applies to all user accounts except Administrator
  - The “Administrator” User Account cannot be locked out via a “denial of service” attack with an interactive logon
  - The “Administrator” User Account can be locked out with the “passprop” utility
    - this utility is limited to the Domain’s “Administrator” account
      - remote logon (access to “share”) will be locked out
      - interactive logons to non-Domain Controllers will be locked out

Account Policies Notes (continued)

- Domain Controllers are exempt
  - to guard against a hacker's "denial of service" attack
- the "passprop" utility is provided with the Windows 2000 Resource Kit (but not 2008/2003)

– The functionality of "passprop" has been integrated into Windows XP (and later)
  - specifically, the Administrator account can be locked when access is done over a network
    - but not interactively
  - this is from observed behavior (and is <u>not</u> documented by Microsoft)

Managing Users and Groups

- User and Group accounts are managed with the Microsoft Management Console Snap-in
  - **Start Menu -> Programs -> Administrative Tools ->**
    Active Directory Users and Computers
    - used in an Active Directory Domain environment
    - available (by default) on Domain Controllers
    - select the appropriate Domain and/or Organizational Unit (OU) in the tree view

Managing Users and Groups

- **Start Menu -> Programs -> Administrative Tools -> Computer Management**
  - primarily used in a non-Domain environment
  - available on all Windows 7, Windows Vista, Windows XP, and Windows 2000 Professional computers
  - available on Windows 2008 Server, Windows 2003 Server, and Windows 2000 Server
    - only when configured as a member Server
  - select the “Local Users and Groups” tree

Managing Account Policies

- Account Policies are managed with the Microsoft Management Console Snap-in
  - On Domain Controllers (Windows Server 2003 and Windows 2000 Server)
    - **Start Menu -> Programs -> Administrative Tools -> Domain Security Policy**
      - policies apply to the Domain as a whole
      - select the “Security Settings -> Account Policies” tree for account policies
      - select the “Security Settings -> Local Policies -> User Rights Assignment” tree for user rights
    - **Start Menu -> Programs -> Administrative Tools -> Domain Controller Security Policy**

Managing Account Policies

- policies apply to to all the Domain Controllers within the Domain
- this replaces the functionality offered by “Local Security Policy” on non-Domain Controllers
- select the “Security Settings -> Account Policies” tree for account policies
- select the “Security Settings -> Local Policies -> User Rights Assignment” tree for user rights

Managing Account Policies

- On Windows Server 2008, Member Servers (non-Domain Controllers), and Windows 7/Vista/XP/2000 Professional
  - **Start Menu -> Programs -> Administrative Tools -> Local Security Policy**
    - select the “Local Policies -> User Rights Assignment” tree
    - select the “Account Policies” tree for password or lockout policies

Security ID (SID)

- A Security Identifier (SID) is part of the security descriptor
  - Windows NT family protect objects with a security descriptor
- A SID is used to uniquely identify the following types of objects
  - User Account
  - Group
  - Computer Name
  - Domain

Security ID (SID)

  - Service (Windows Server 2008, Windows 7, and Windows Vista)
- All User Accounts and Groups have a unique SID
  - The algorithm Windows NT family uses to generate a SID is designed to never duplicate (even across Domains and other stand-alone computers)
    - a given SID value is universally unique and will in theory never recycle

Security ID (SID)

- This means that if you create User Account “Bozo”, delete User Account “Bozo”, and recreate User Account “Bozo”, the SID will be different
  - this is by design to “protect” the integrity of permissions and rights
  - the SID is placed on the object, not the name
- Renaming an object will not change the SID

Security ID (SID) (continued)

- The following is an example of a SID (in textual representation)
  - S-1-5-21-917267712-1342860078-1792151419-500
- This would be a SID for the “Administrator” User Account
- The blue portion varies from computer to computer, and Domain to Domain
- The “-500” is the RID (relative id), and is hard-wired for “Administrator”

Security ID (SID) (continued)

- Renaming the “Administrator” User Account for additional security may be futile
  - This is because programs can easily query Windows NT family and obtain both the SID values and their names
  - Widely available tools can easily “discover” the true Administrator account
    - these tools can generally be run by any user who has access to the computer and/or Domain