IBM Tivoli Directory Server for z/OS

Password policy

This education topic provides a high-level overview of the password policy support in the IBM Tivoli® Directory Server for z/OS®. It is applicable to customers running at z/OS 1.12 and above.

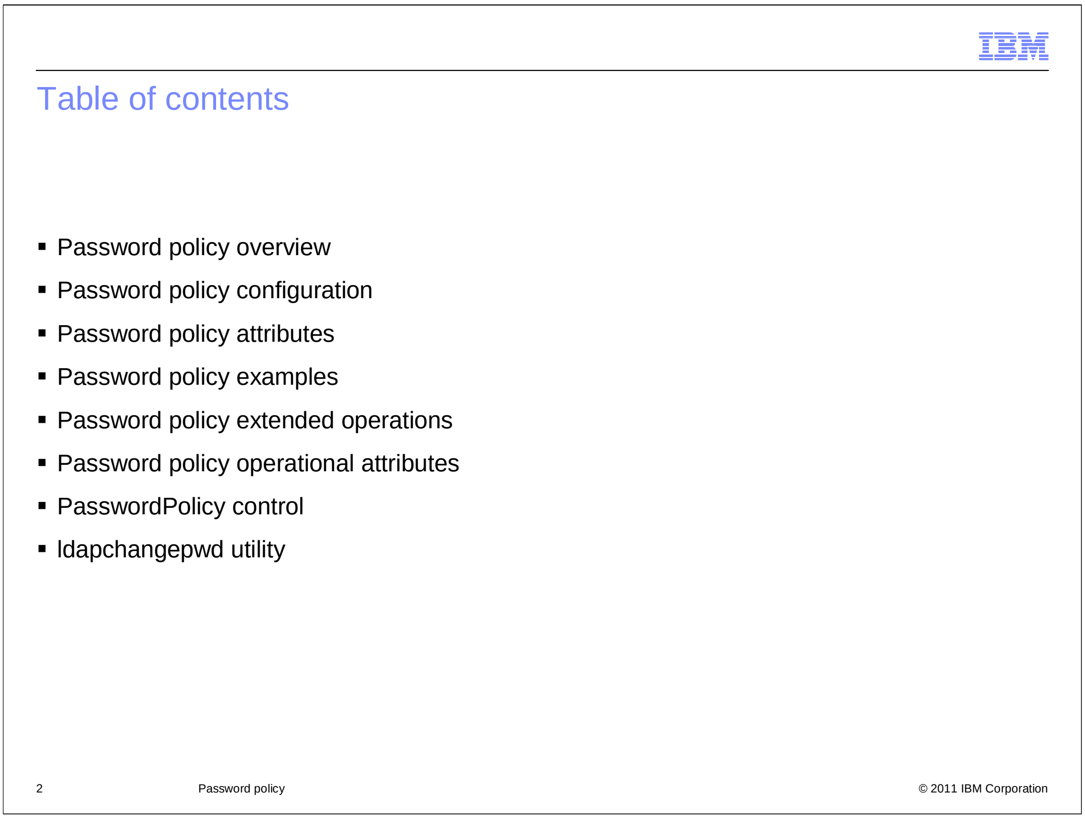
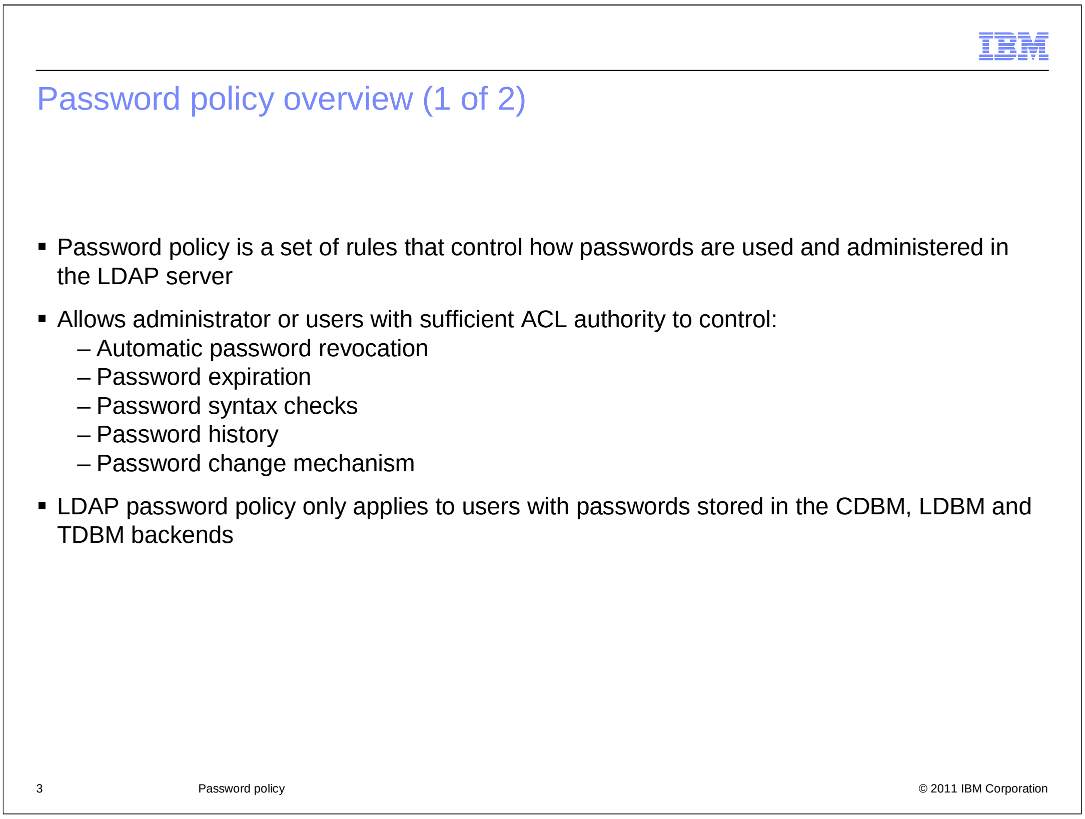


Table of contents

- Password policy overview
- Password policy configuration
- Password policy attributes
- Password policy examples
- Password policy extended operations
- Password policy operational attributes
- PasswordPolicy control
- ldapchangepwd utility

This presentation will begin with an overview of what password policy is. It will then move on to discuss the configuration of password policy in the IBM Tivoli Directory Server for z/OS and discuss what types of password policy configuration are possible in the IBM Tivoli Directory Server for z/OS. It will then move on to discuss the password policy operational attributes, the PasswordPolicy control, and the new ldapchangepwd utility.

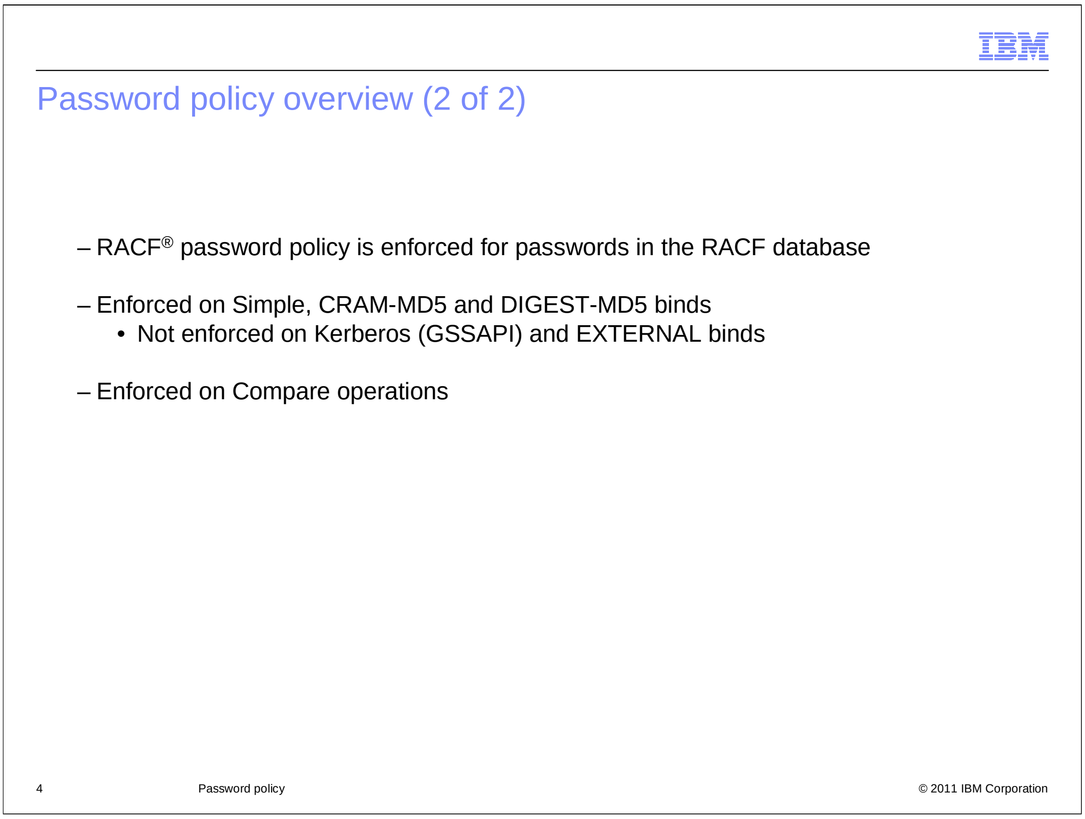


Password policy overview (1 of 2)

- Password policy is a set of rules that control how passwords are used and administered in the LDAP server
- Allows administrator or users with sufficient ACL authority to control:
  - Automatic password revocation
  - Password expiration
  - Password syntax checks
  - Password history
  - Password change mechanism
- LDAP password policy only applies to users with passwords stored in the CDBM, LDBM and TDBM backends

Password policy is a set of rules that controls how passwords are used and administered in the LDAP server. These password policy rules are enforced to ensure that password values are changed periodically and meet the syntactic password requirements of your organization. These rules also restrict the reuse of old passwords, ensure that users are locked out after a defined number of failed bind attempts, automatically expire passwords after a period of time, and specify how password values are allowed to be changed.

Password policy support was added to the IBM Tivoli Directory Server for z/OS in z/OS V1.12. This support allows an LDAP administrator or users with sufficient authorization in the directory to setup and configure password policies for users whose passwords are stored in the LDBM, TDBM, or CDBM backends in the **userPassword** attribute value.

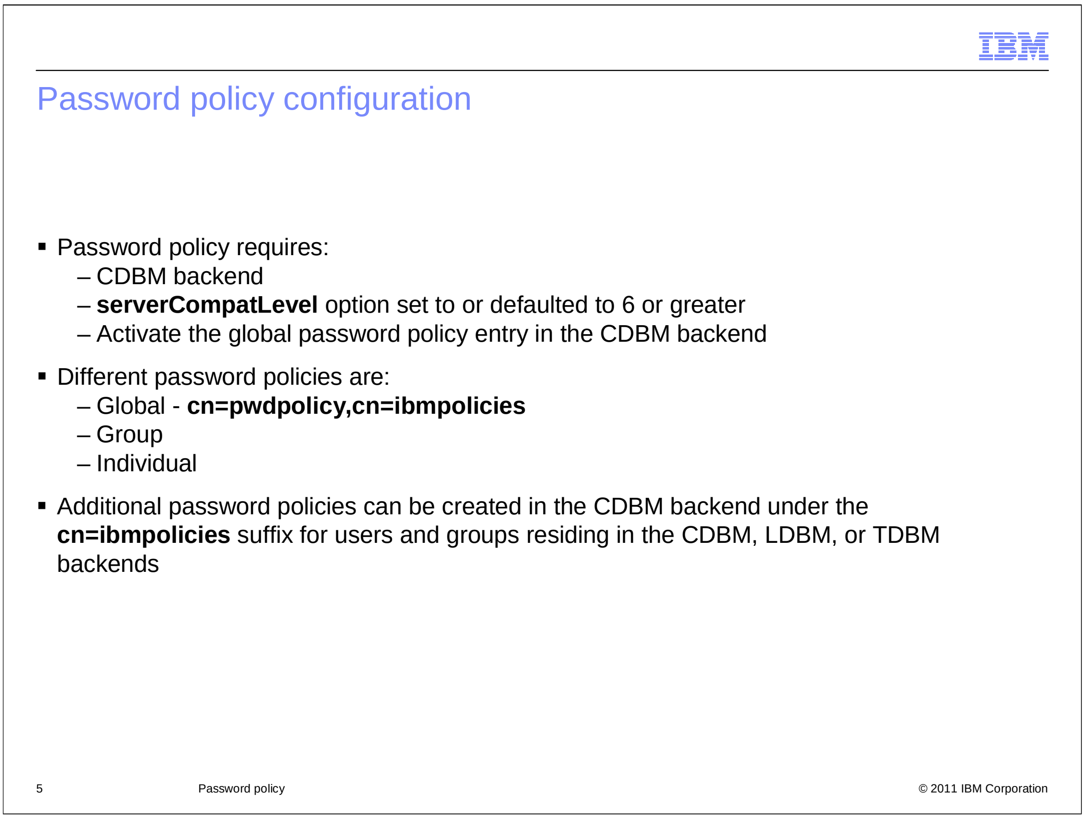


Password policy overview (2 of 2)

- RACF® password policy is enforced for passwords in the RACF database
- Enforced on Simple, CRAM-MD5 and DIGEST-MD5 binds
  - Not enforced on Kerberos (GSSAPI) and EXTERNAL binds
- Enforced on Compare operations

LDAP password policy support is not enforced for users whose password or password phrases are stored in the RACF database. LDAP password policy does not apply to TDBM, LDBM, or CDBM entries participating in native authentication or entries in the SDBM backend. RACF handles the password policy for these users.

LDAP password policy is checked during authentication and compare operations involving the **userPassword** attribute value to ensure that the password has not expired or the user's account has not been locked from authenticating to the directory. The only supported bind mechanisms for password policy checking are simple, CRAM-MD5, and DIGEST-MD5 when the authenticating user's entry and password resides in a TDBM, LDBM, or CDBM backend. LDAP password policy is not checked during anonymous, Kerberos (GSSAPI), or EXTERNAL binds as these authentication mechanisms do not access a password value.



Password policy configuration

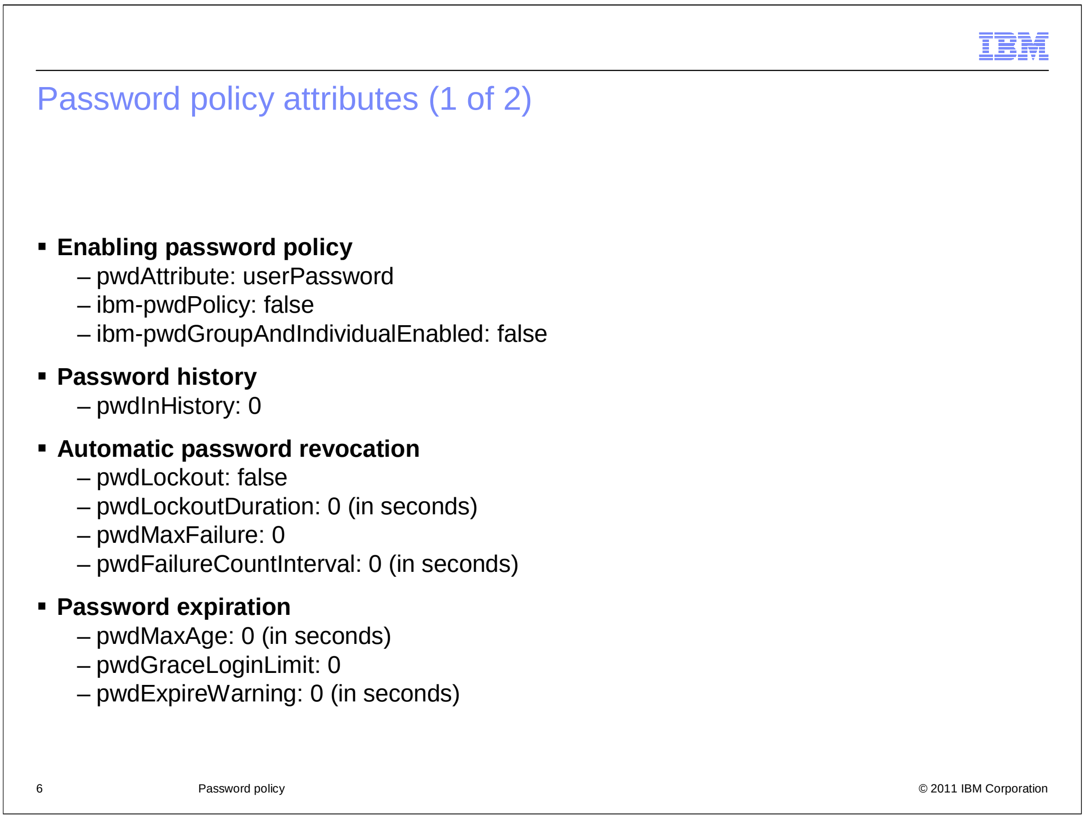
- Password policy requires:
  - CDBM backend
  - **serverCompatLevel** option set to or defaulted to 6 or greater
  - Activate the global password policy entry in the CDBM backend
- Different password policies are:
  - Global - **cn=pwdpolicy,cn=ibmpolicies**
  - Group
  - Individual
- Additional password policies can be created in the CDBM backend under the **cn=ibmpolicies** suffix for users and groups residing in the CDBM, LDBM, or TDBM backends

5 Password policy © 2011 IBM Corporation

There are several updates that may be needed in the LDAP server configuration file prior to configuring password policy in the IBM Tivoli Directory Server for z/OS. First, a CDBM backend must be specified in the LDAP server configuration file. The CDBM backend was added to the IBM Tivoli Directory Server for z/OS in 1.11. Next, the **serverCompatLevel** configuration option must be set to or default to 6 or greater. When the server compatibility option is 6 or greater, the cn=pwdpolicy,cn=ibmpolicies entry is created and initialized in the CDBM backend if it does not already exist. The cn=pwdpolicy,cn=ibmpolicies entry is also referred to as the global password policy entry. When the global password policy is initially created, it is not active however it can be activated by setting the **ibm-pwdPolicy** attribute value in the entry to true.

When the global password policy is activated, the password policy applies to all entries or users in the LDBM, TDBM, or CDBM backend that have an userpassword attribute value. In the global password policy entry, there are attributes that control how often user's passwords must be changed, the syntax of a password value (for example minimum length), the number of passwords kept in history, and when passwords automatically expire. An explanation of these attributes will follow later in this presentation.

If there is a need for a user or group to have a different password policy than the global one, additional password policies can be added under the cn=ibmpolicies entry in the CDBM backend. These additional password policies can apply either to a specific individual or a group entry. User entries can be updated to use a specific password policy by adding the **ibm-pwdIndividualPolicyDN** attribute value. Group entries can be updated to use a specific password policy by adding the **ibm-pwdGroupPolicyDN** attribute value.



Password policy attributes (1 of 2)

- **Enabling password policy**
  - – pwdAttribute: userPassword
  - – ibm-pwdPolicy: false
  - – ibm-pwdGroupAndIndividualEnabled: false
- **Password history**
  - – pwdInHistory: 0
- **Automatic password revocation**
  - – pwdLockout: false
  - – pwdLockoutDuration: 0 (in seconds)
  - – pwdMaxFailure: 0
  - – pwdFailureCountInterval: 0 (in seconds)
- **Password expiration**
  - – pwdMaxAge: 0 (in seconds)
  - – pwdGraceLoginLimit: 0
  - – pwdExpireWarning: 0 (in seconds)

6 Password policy © 2011 IBM Corporation

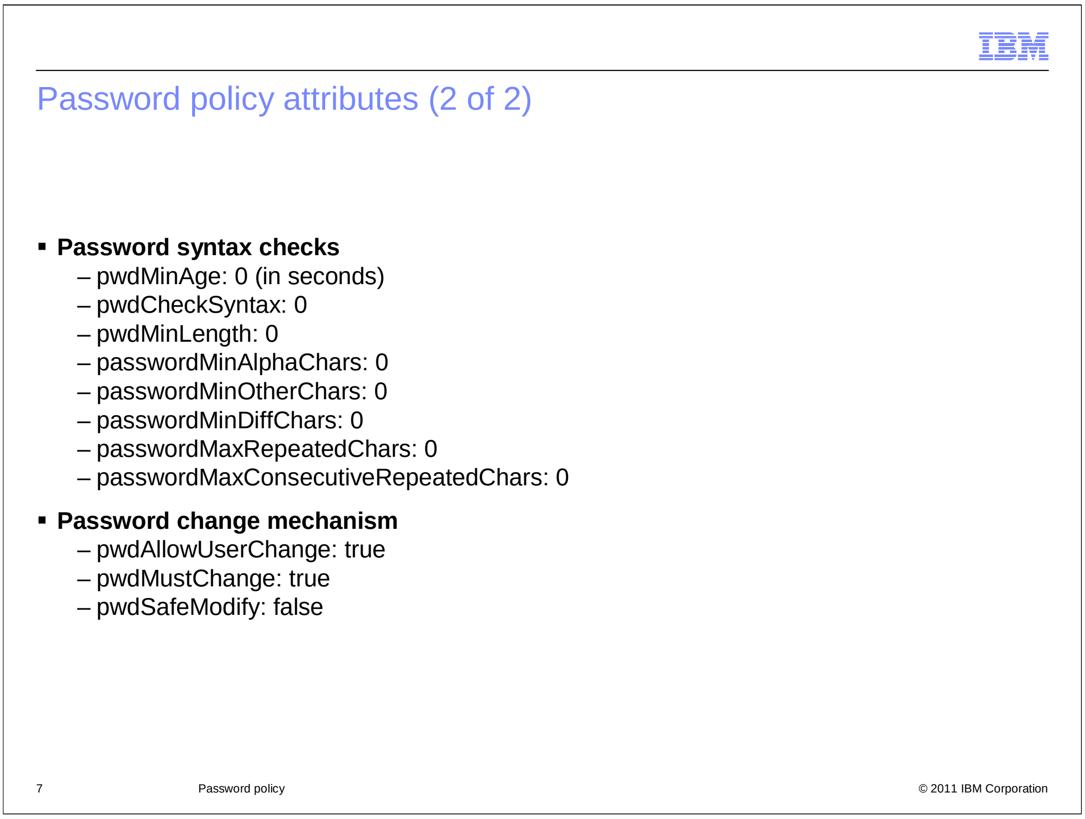
The attributes in password policy entries can be placed into different categories which control different aspects of password policy enforcement. These attributes can be used when creating additional password policies for specific users or groups. The default values for these attributes are listed on this slide.

The three attributes that enable password policy are pwdAttribute, ibm-pwdPolicy, and ibm-pwdGroupAndIndividualEnabled. The pwdAttribute attribute specifies the attribute type that is subject to the password policy, which is only allowed to be set to userPassword. The ibm-pwdPolicy attribute indicates if this password policy is evaluated or not. The ibm-pwdGroupAndIndividualEnabled attribute is only allowed to be specified in the global password policy and it indicates if group and individual password policies are enabled when added to the directory. Note that the ibm-pwdPolicy attribute in these additional individual or group password policy entries must be set to true so that these additional policies can be evaluated for these users and groups.

The only attribute in the password history category is the pwdInHistory. This attribute specifies the number of previous password values that are stored in user entries. This attribute is used to prevent password re-use by users.

The pwdLockout, pwdLockoutDuration, pwdMaxFailure, and pwdFailureCountInterval attributes are used to enforce automatic password revocation. The pwdLockout attribute determines whether or not a password can be used for authentication when the number of failures exceeds the pwdMaxFailure value. The pwdMaxFailure value specifies the maximum number of consecutive authentication failures that are allowed before the user is locked out. The pwdLockoutDuration value controls how long the user is locked out. The pwdFailureCountInterval specifies the number of seconds when password failures are removed from the failure counter although no successful authentication has occurred.

The three attributes in the password expiration category are pwdMaxAge, pwdGraceLoginLimit, and pwdExpireWarning. The pwdMaxAge attribute specifies the maximum age in seconds of a password value. When the maximum age is exceeded, the password is expired. The pwdGraceLoginLimit specifies the number of grace authentications that are allowed when the password is expired. The pwdExpireWarning attribute specifies the number of seconds before a password is due to expire that expiration warning messages are returned during authentication in the **PasswordPolicy** response control.



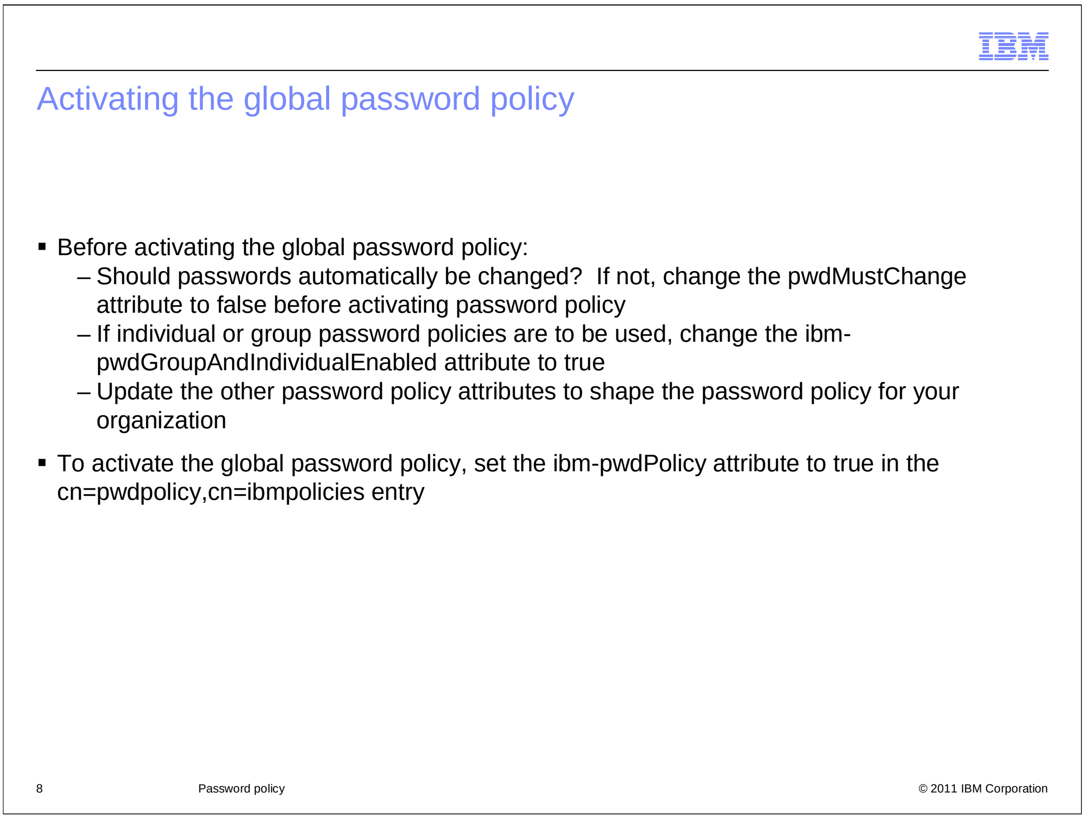
Password policy attributes (2 of 2)

- **Password syntax checks**
  - – pwdMinAge: 0 (in seconds)
  - – pwdCheckSyntax: 0
  - – pwdMinLength: 0
  - – passwordMinAlphaChars: 0
  - – passwordMinOtherChars: 0
  - – passwordMinDiffChars: 0
  - – passwordMaxRepeatedChars: 0
  - – passwordMaxConsecutiveRepeatedChars: 0
- **Password change mechanism**
  - – pwdAllowUserChange: true
  - – pwdMustChange: true
  - – pwdSafeModify: false

7 Password policy

There are a number of attributes in the password policy which control the syntax of password values. The pwdMinAge specifies the number of seconds that must elapse between modifications to the password. The pwdCheckSyntax indicates whether password syntax is enforced when adding or modifying a user's password value. The pwdMinLength controls the minimum length of a user's password value. The passwordMinAlphaChars specifies the minimum number of alphabetic characters (uppercase and lowercase a-z) that a password value must have, while passwordMinOtherChars specifies the minimum number of numeric and special characters (other than uppercase and lowercase a-z) that a password value must have. The passwordMinDiffChars specifies the minimum number of characters in the new password that must be different from the characters in the old password value. The passwordMaxRepeatedChars specifies the maximum number of times a given character is used in a password value. The passwordMaxConsecutiveRepeatedChars specifies the maximum number of successive repetitions of a given character in a password value.

The three attributes that control how passwords are changed are pwdAllowUserChange, pwdMustChange, and pwdSafeModify. The pwdAllowUserChange attribute specifies whether users who have the authority to do so are allowed to change their password values. The pwdMustChange attribute indicates whether users must change their passwords after their first successful authentication to the server after a password is set or reset by the LDAP administrator. The pwdSafeModify attribute indicates if the existing or current password value must be sent when changing a password value.



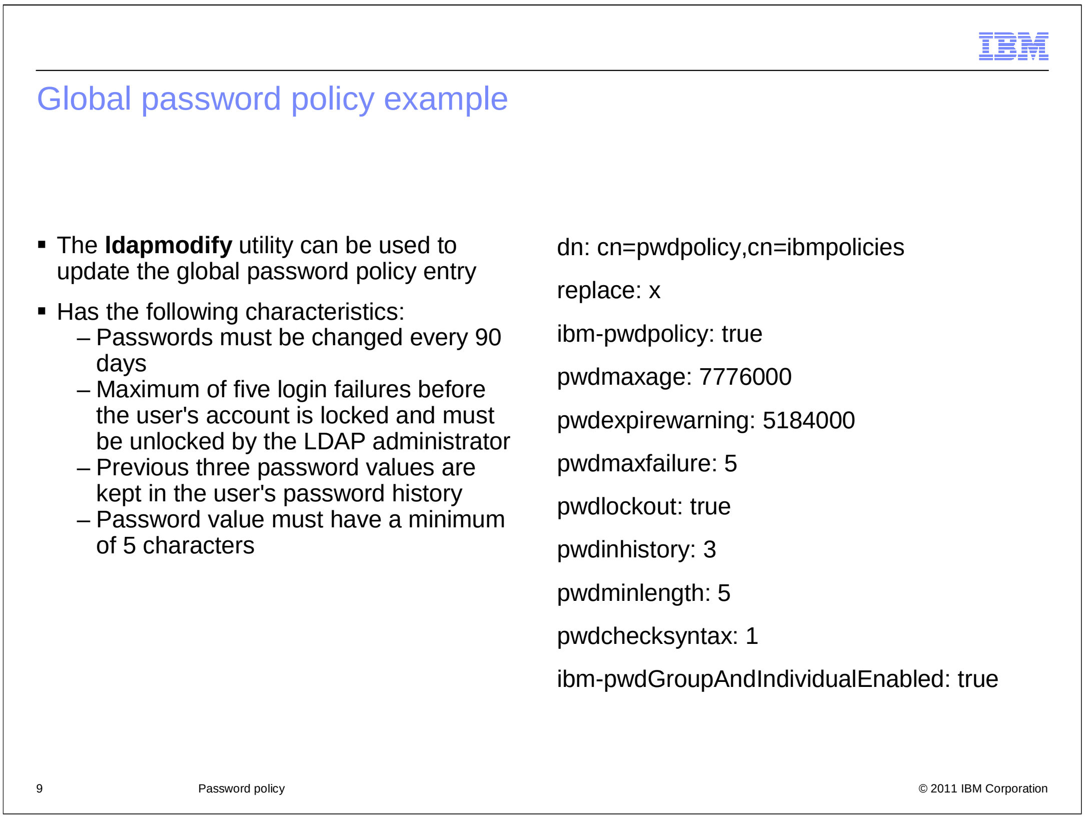
Activating the global password policy

- Before activating the global password policy:
  - Should passwords automatically be changed? If not, change the pwdMustChange attribute to false before activating password policy
  - If individual or group password policies are to be used, change the ibm-pwdGroupAndIndividualEnabled attribute to true
  - Update the other password policy attributes to shape the password policy for your organization
- To activate the global password policy, set the ibm-pwdPolicy attribute to true in the cn=pwdpolicy,cn=ibmpolicies entry

8 Password policy © 2011 IBM Corporation

Before activating the global password policy, there are some important factors to consider. First, the default value for the pwdMustChange attribute in the global password policy entry is set to true which means that all current users must change their password values when the password policy is activated. If this behavior is not desired, set the pwdMustChange attribute value to false. If it is desired to force users to have stronger password values, then leaving this option to default to true is fine. Another thing to consider when activating the global password policy entry is whether to allow evaluation of individual and group password policies. The ibm-pwdGroupAndIndividualEnabled attribute must be set to true to allow this to occur. However keep in mind, the ibm-pwdPolicy attribute in these additional password policies must be set to true to allow evaluation of these password policy entries. You should also evaluate the other password policy attribute types on the previous slides to determine if they ought to be set to enforce your organization’s password policy.

Once you feel comfortable with the global password policy entry, it is activated by setting the ibm-pwdPolicy attribute to true.



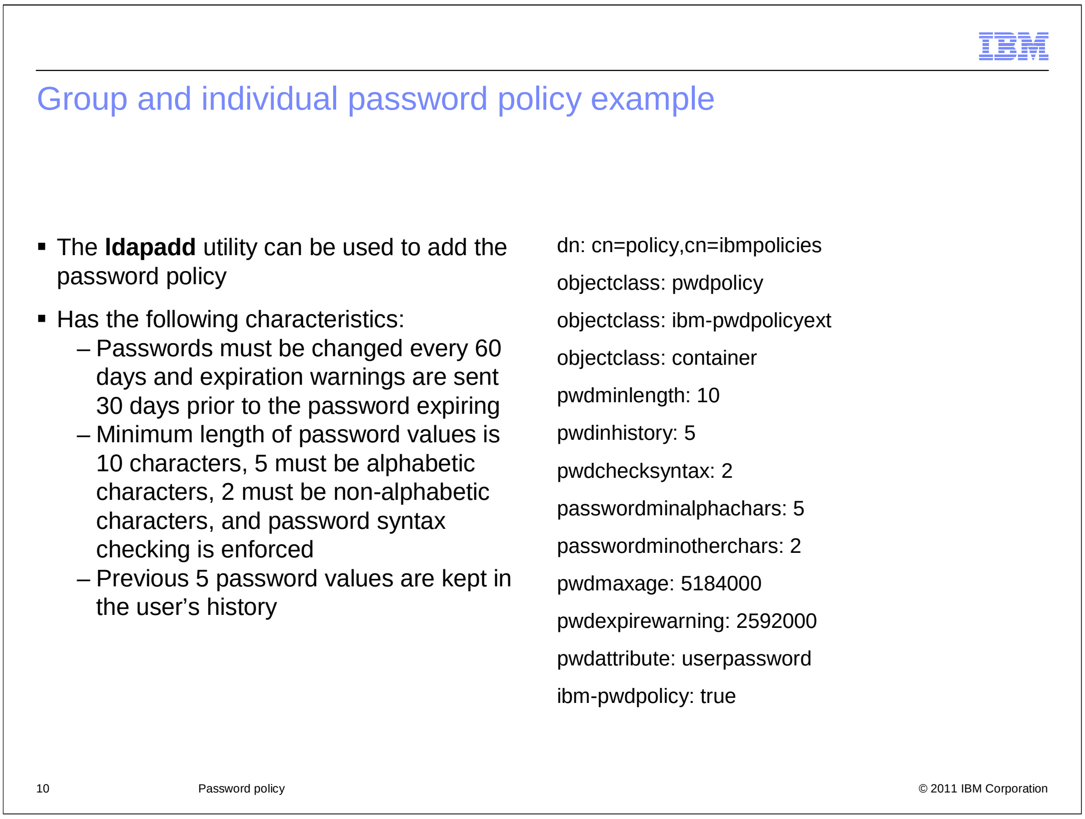
Global password policy example

- The **ldapmodify** utility can be used to update the global password policy entry
- Has the following characteristics:
  - Passwords must be changed every 90 days
  - Maximum of five login failures before the user's account is locked and must be unlocked by the LDAP administrator
  - Previous three password values are kept in the user's password history
  - Password value must have a minimum of 5 characters

```
dn: cn=pwdpolicy,cn=ibmpolicies
replace: x
ibm-pwdpolicy: true
pwdmaxage: 7776000
pwdexpirewarning: 5184000
pwdmaxfailure: 5
pwdlockout: true
pwdinhistory: 3
pwdminlength: 5
pwdchecksyntax: 1
ibm-pwdGroupAndIndividualEnabled: true
```

The LDIF on the right-hand side of this slide can be used with the ldapmodify utility to update and activate the global password policy entry in the server.

In this example when the global password policy is activated, any existing user’s passwords must be changed because the pwdMustChange attribute is still set to true. This global password policy requires that passwords are changed every 90 days or 7776000 seconds, there are a maximum of 5 login failures before the user’s account is locked and must be unlocked by the LDAP administrator. Also, the previous 3 password values are kept in the user’s password history and the user is unable to reuse these password values and new password values must have a minimum of 5 characters. The global password policy is also updated to enable evaluating group and individual password policy entries as long as the ibm-pwdPolicy in those entries is set to true.



Group and individual password policy example

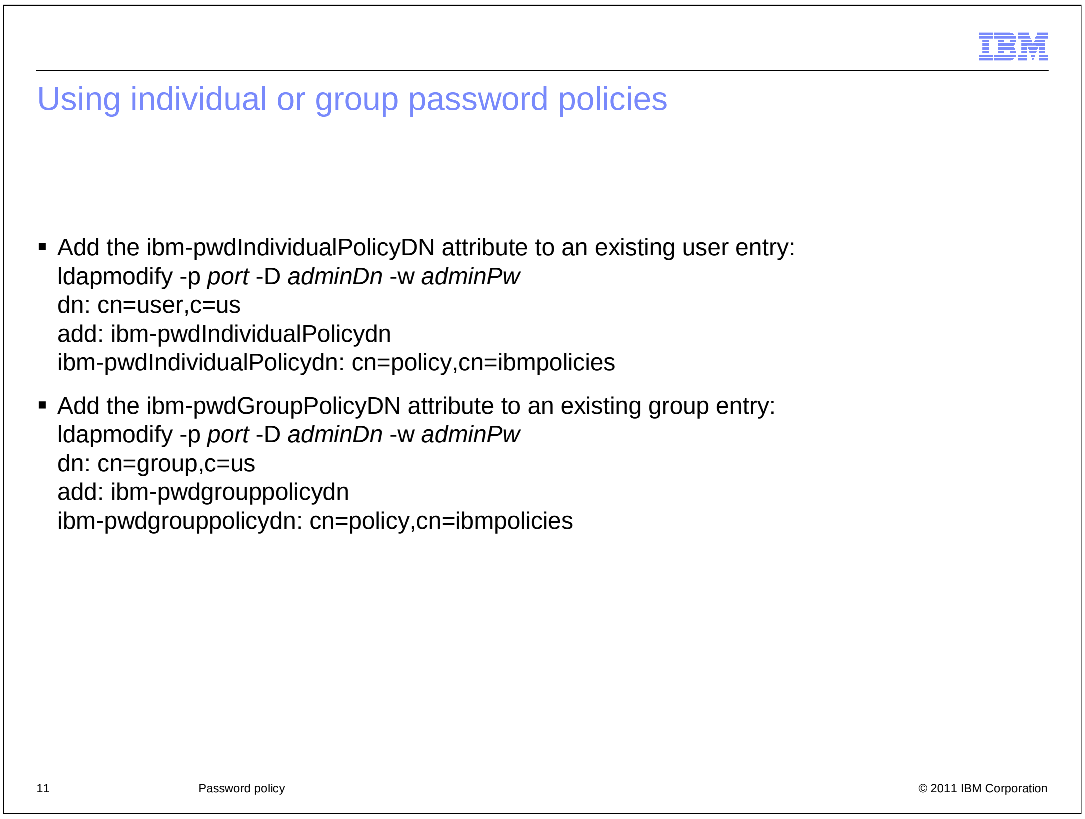
- The **ldapadd** utility can be used to add the password policy
- Has the following characteristics:
  - Passwords must be changed every 60 days and expiration warnings are sent 30 days prior to the password expiring
  - Minimum length of password values is 10 characters, 5 must be alphabetic characters, 2 must be non-alphabetic characters, and password syntax checking is enforced
  - Previous 5 password values are kept in the user's history

```
dn: cn=policy,cn=ibmpolicies
objectclass: pwdpolicy
objectclass: ibm-pwdpolicyext
objectclass: container
pwdminlength: 10
pwdinhistory: 5
pwdchecksyntax: 2
passwordminalphachars: 5
passwordminotherchars: 2
pwdmaxage: 5184000
pwdexpirewarning: 2592000
pwdattribute: userpassword
ibm-pwdpolicy: true
```

10 Password policy © 2011 IBM Corporation

The LDIF on the right-hand side of this slide can be added to the LDAP server using the ldapadd utility.

When this password policy is used, it requires that passwords must be changed every 60 days or 5184000 seconds and password expiration warnings are sent on the **PasswordPolicy** response control starting 30 days or 2592000 seconds before the password is set to expire. The minimum length of password values is 10 characters, five must be alphabetic characters, two must be non-alphabetic characters, and syntax checking is enforced because the **pwdCheckSyntax** attribute is set to two, Also the previous five password values are kept in the user's password history and the user is unable to reuse these password values.



Using individual or group password policies

- Add the ibm-pwdIndividualPolicyDN attribute to an existing user entry:

  ```
  ldapmodify -p port -D adminDn -w adminPw
  dn: cn=user,c=us
  add: ibm-pwdIndividualPolicydn
  ibm-pwdIndividualPolicydn: cn=policy,cn=ibmpolicies
  ```

- Add the ibm-pwdGroupPolicyDN attribute to an existing group entry:

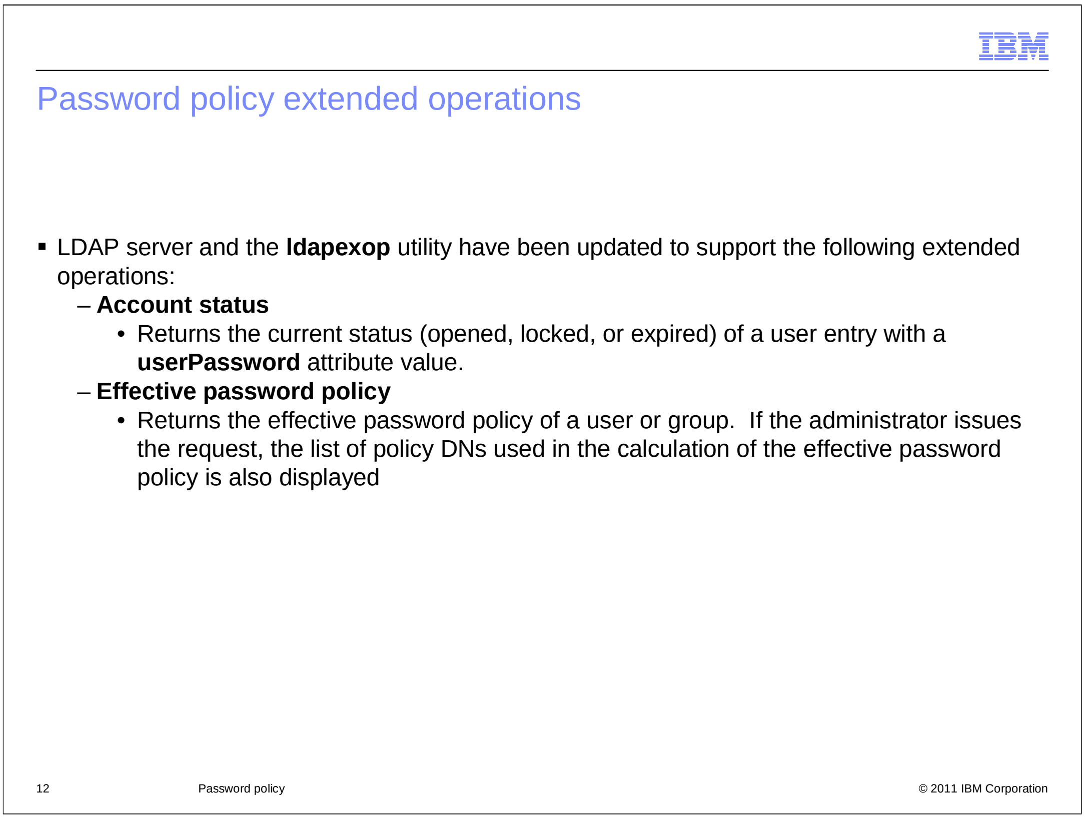
  ```
  ldapmodify -p port -D adminDn -w adminPw
  dn: cn=group,c=us
  add: ibm-pwdgrouppolicydn
  ibm-pwdgrouppolicydn: cn=policy,cn=ibmpolicies
  ```

11 Password policy © 2011 IBM Corporation

If a user must have a password policy that differs from the global password policy, the user entry can be updated to specify the ibm-pwdIndividualPolicyDN which points to that password policy. In this example, the cn=user,c=us entry is updated to use the cn=policy,cn=ibmpolicies entry created on the previous slide.

If a group must have a password policy that differs from the global password policy, the group entry can be updated to specify the ibm-pwdGroupPolicyDN which points to that password policy. In this example, the cn=group,c=us entry is updated to use the cn=policy,cn=ibmpolicies entry created on the previous slide. Therefore, any users that belong to that group are subject to the cn=policy,cn=ibmpolicies password policy. Note the group entry can be a static, dynamic, or nested group entry supported by the IBM Tivoli Directory Server for z/OS.

Since the global password policy has already been updated to enable group and individual policies two slides earlier, there is no need to update the ibm-pwdGroupAndIndividualEnabled attribute in the cn=pwdpolicy,cn=ibmpolicies entry.



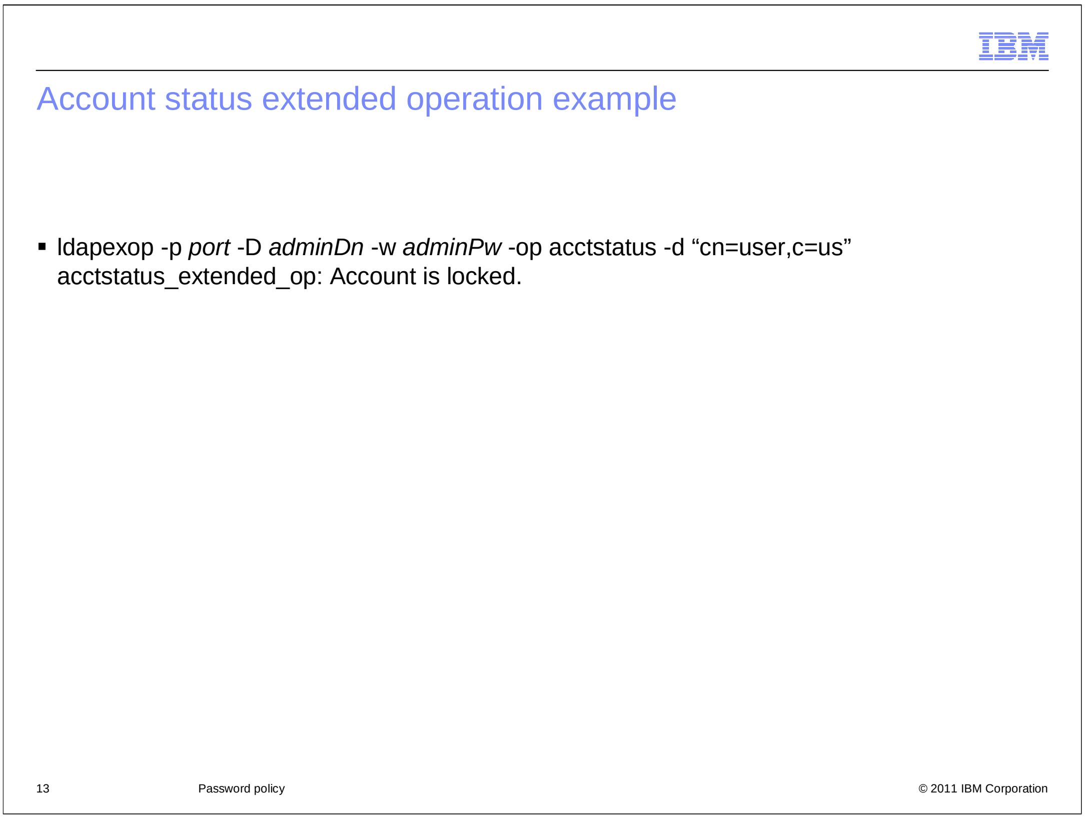
Password policy extended operations

- LDAP server and the **ldapexop** utility have been updated to support the following extended operations:
  - **Account status**
    - Returns the current status (opened, locked, or expired) of a user entry with a **userPassword** attribute value.
  - **Effective password policy**
    - Returns the effective password policy of a user or group. If the administrator issues the request, the list of policy DNs used in the calculation of the effective password policy is also displayed

12 Password policy © 2011 IBM Corporation

In z/OS V1.12, the IBM Tivoli Directory Server for z/OS has been updated to support the Account status and Effective password policy extended operations. The **Account status** extended operation returns the current status of a user entry with a **userPassword** attribute value. The current status is either open, locked, or expired. The **Effective password policy** extended operation returns the effective password policy of a user or group. For example, this extended operation is especially useful if a user belongs to multiple groups and each of these groups have a password policy and there is also an individual password policy associated with the user.

The ldapexop utility has also been updated to support these extended operations.

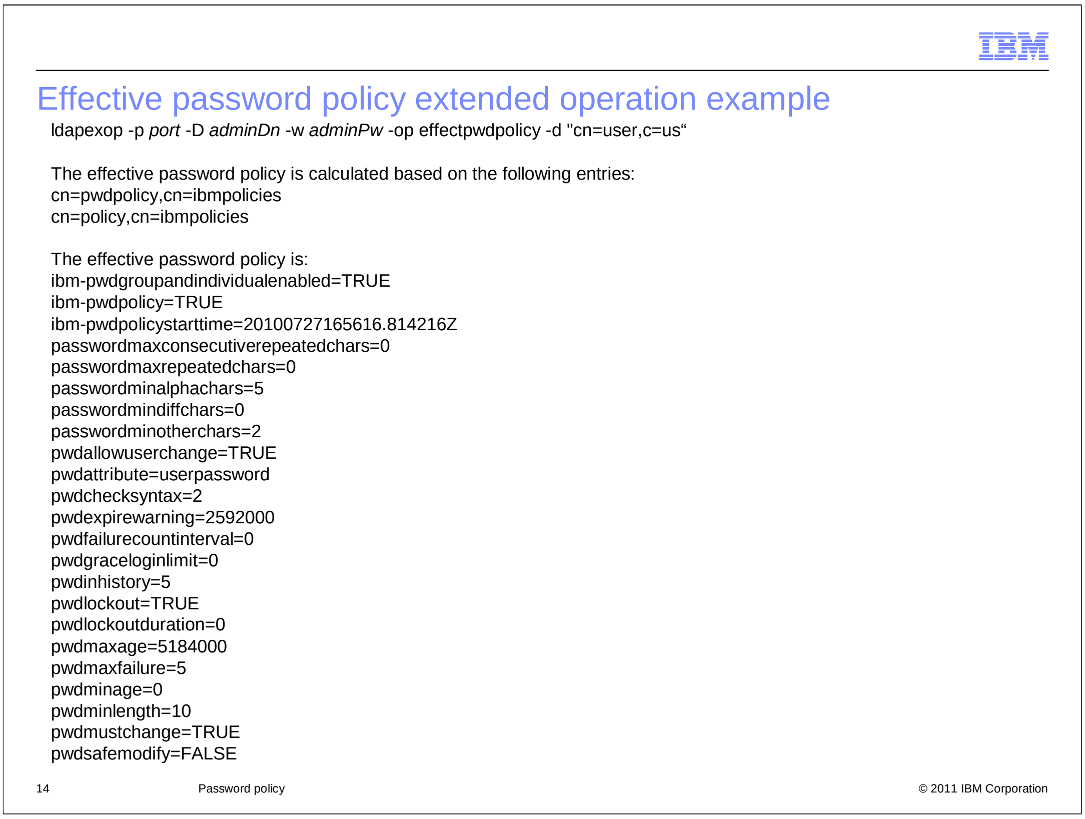


Account status extended operation example

```
▪ ldapexop -p port -D adminDn -w adminPw -op acctstatus -d “cn=user,c=us”
  acctstatus_extended_op: Account is locked.
```

13 Password policy © 2011 IBM Corporation

This slide shows an example of using the **ldapexop** utility to query the current account status of the cn=user,c=us entry. In this case, the cn=user,c=us entry is locked.



Effective password policy extended operation example

ldapexop -p *port* -D *adminDn* -w *adminPw* -op effectpwdpolicy -d "cn=user,c=us“

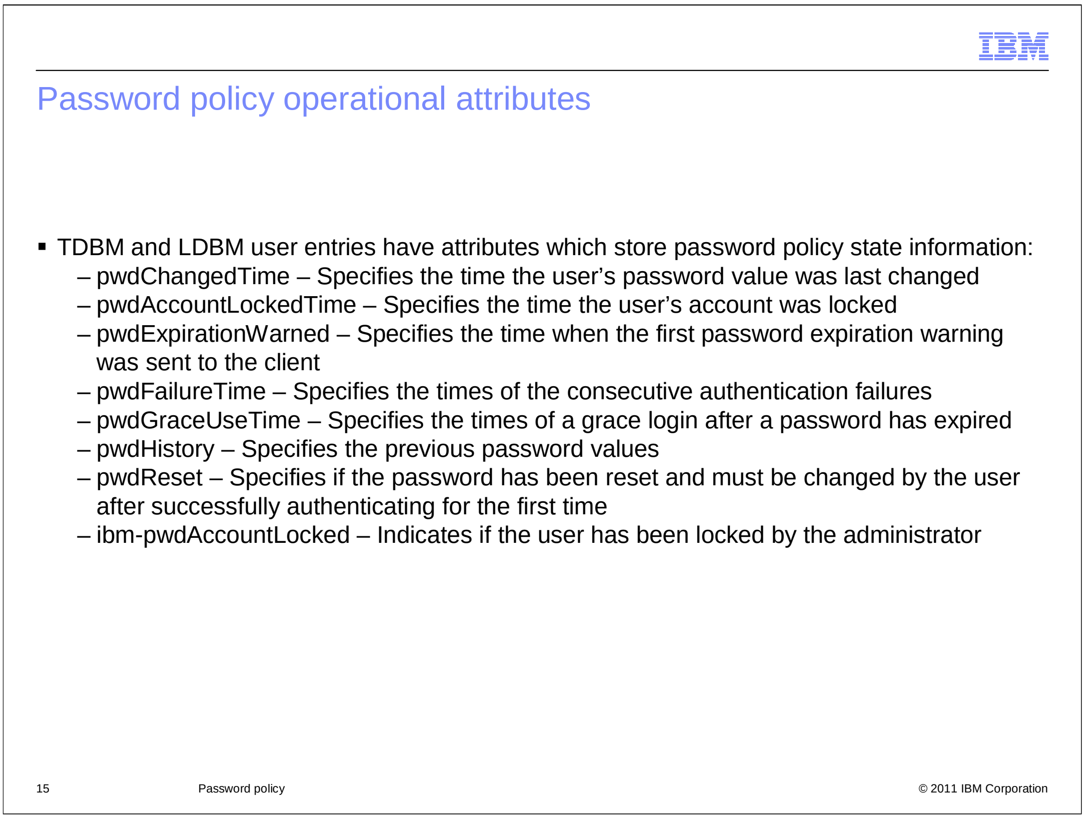
```
The effective password policy is calculated based on the following entries:
cn=pwdpolicy,cn=ibmpolicies
cn=policy,cn=ibmpolicies

The effective password policy is:
ibm-pwdgroupandindividualenabled=TRUE
ibm-pwdpolicy=TRUE
ibm-pwdpolicystarttime=20100727165616.814216Z
passwordmaxconsecutiverepeatedchars=0
passwordmaxrepeatedchars=0
passwordminalphachars=5
passwordmindiffchars=0
passwordminotherchars=2
pwdallowuserchange=TRUE
pwdattribute=userpassword
pwdchecksyntax=2
pwdexpirewarning=2592000
pwdfailurecountinterval=0
pwdgraceloginlimit=0
pwdinhistory=5
pwdlockout=TRUE
pwdlockoutduration=0
pwdmaxage=5184000
pwdmaxfailure=5
pwdminage=0
pwdminlength=10
pwdmustchange=TRUE
pwdsafemodify=FALSE
```

14 Password policy © 2011 IBM Corporation

This slide shows an example of using the **ldapexop** utility to query the effective password policy for the cn=user,c=us entry. Note that a few slides ago, we updated cn=user,c=us to use an individual password policy of cn=policy,cn=ibmpolicies. Therefore the effective password policy for cn=user,c=us takes into account both the global and individual password policies.

As illustrated earlier, when creating additional password policies it is not necessary to set every attribute in a policy. When calculating the effective password policy of a user or group, there is a hierarchy of where the attributes in the effective password policy are obtained from. The attributes in the individual policy are looked at first, then any group policies, and finally the global policy. For more information about how the effective password policy is determined, see the “IBM Tivoli Directory Server Administration and Use for z/OS” manual.

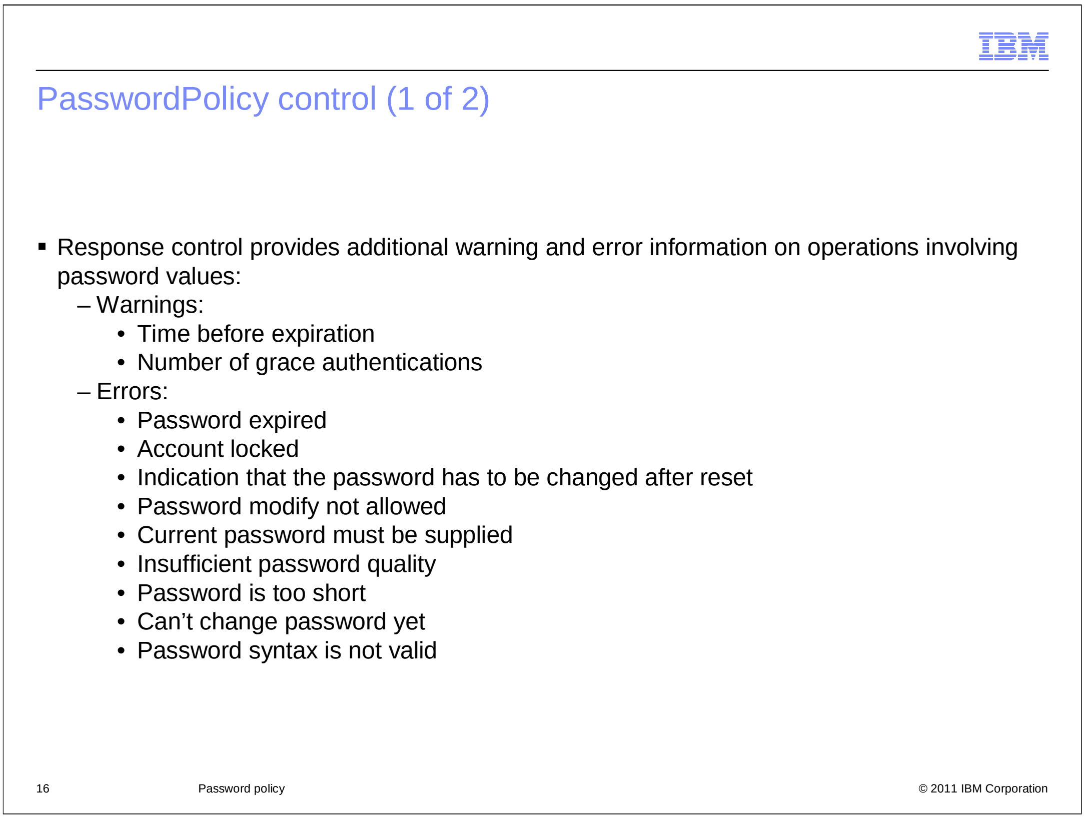


Password policy operational attributes

- TDBM and LDBM user entries have attributes which store password policy state information:
  - pwdChangedTime – Specifies the time the user’s password value was last changed
  - pwdAccountLockedTime – Specifies the time the user’s account was locked
  - pwdExpirationWarned – Specifies the time when the first password expiration warning was sent to the client
  - pwdFailureTime – Specifies the times of the consecutive authentication failures
  - pwdGraceUseTime – Specifies the times of a grace login after a password has expired
  - pwdHistory – Specifies the previous password values
  - pwdReset – Specifies if the password has been reset and must be changed by the user after successfully authenticating for the first time
  - ibm-pwdAccountLocked – Indicates if the user has been locked by the administrator

15 Password policy © 2011 IBM Corporation

There are a number of operational attributes that are stored in a user’s entry when certain password policy features are active in the LDAP server. Since these are operational attribute types, an LDAP administrator or someone with sufficient authority must specify them on the search request or the ‘+’ (plus sign) can be specified to return all operational attributes on a search request. These operational attributes can be queried to determine the status of a user’s entry when password policy is active in the LDAP server.

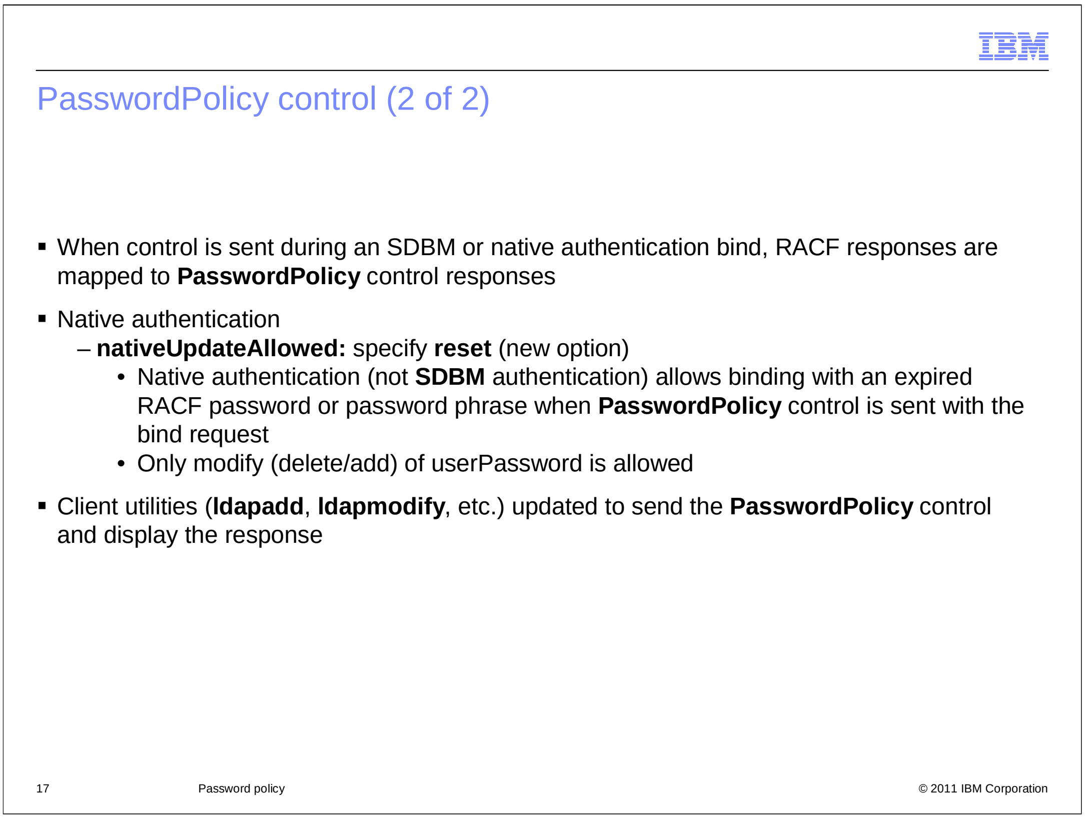


PasswordPolicy control (1 of 2)

- Response control provides additional warning and error information on operations involving password values:
  - Warnings:
    - Time before expiration
    - Number of grace authentications
  - Errors:
    - Password expired
    - Account locked
    - Indication that the password has to be changed after reset
    - Password modify not allowed
    - Current password must be supplied
    - Insufficient password quality
    - Password is too short
    - Can’t change password yet
    - Password syntax is not valid

16 Password policy © 2011 IBM Corporation

The **PasswordPolicy** server control is specified on a client request to solicit additional warning and error information related to password policy enforcement, which the server returns in the **PasswordPolicy** response control. For example, during authentication, the **PasswordPolicy** response control can notify the user that the password must be changed, is about to expire, or there are only a few grace logins available before the user's password expires. For add requests, the **PasswordPolicy** response control provides additional error information about the password value syntax. For modify requests, the **PasswordPolicy** response control provides additional error information about the password value syntax, the new password value exists in the password history, or the current password must be specified when changing the password value.



PasswordPolicy control (2 of 2)

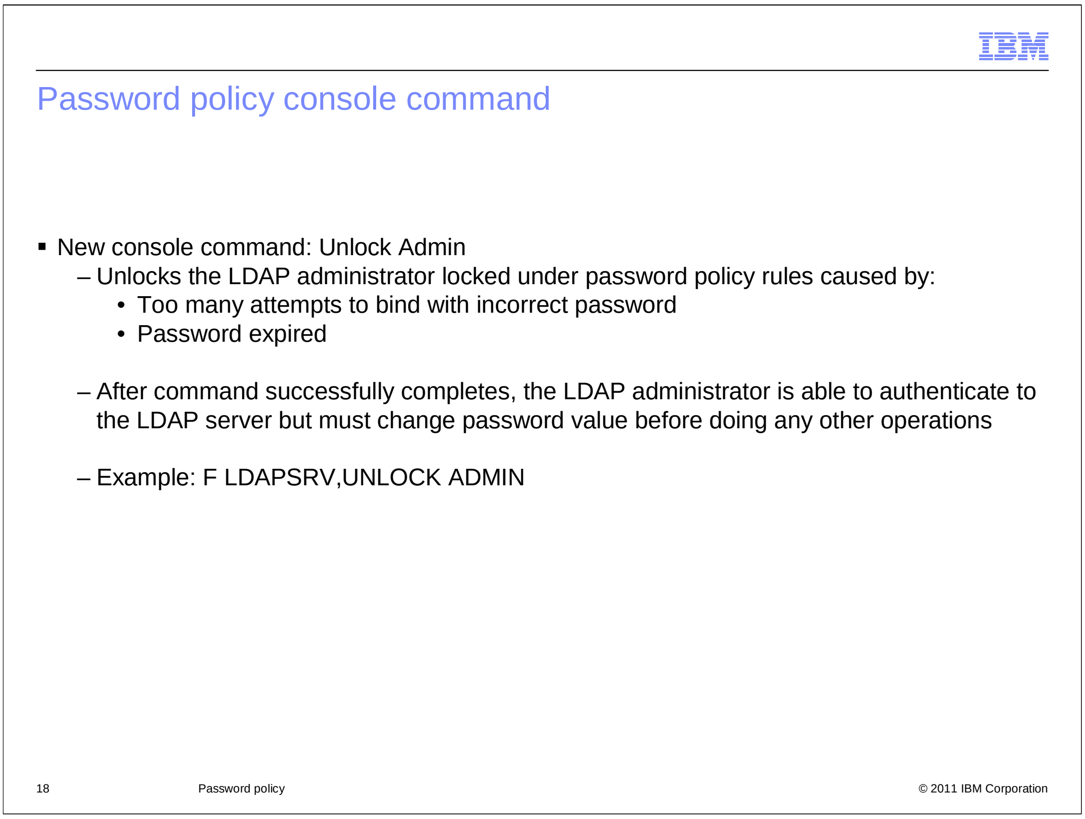
- When control is sent during an SDBM or native authentication bind, RACF responses are mapped to **PasswordPolicy** control responses
- Native authentication
  - **nativeUpdateAllowed:** specify **reset** (new option)
    - Native authentication (not **SDBM** authentication) allows binding with an expired RACF password or password phrase when **PasswordPolicy** control is sent with the bind request
    - Only modify (delete/add) of userPassword is allowed
- Client utilities (**ldapadd**, **ldapmodify**, etc.) updated to send the **PasswordPolicy** control and display the response

17 Password policy © 2011 IBM Corporation

If the **PasswordPolicy** control is sent during an SDBM or native authentication bind, RACF responses are mapped to **PasswordPolicy** control responses. Based on information returned from RACF during an SDBM bind, the **PasswordPolicy** response control can return: **accountLocked, passwordExpired, mustSupplyOldPassword,** and **invalidPasswordSyntax.** In addition native authentication binds allow the return of the **passwordModNotAllow** return code. The **timeBeforeExpiration, passwordTooShort, passwordTooYoung, passwordInHistory,** and **changeAfterReset** are never returned as RACF only returns invalid password for these cases. Lastly, **graceLoginsRemaining** is never returned because it is not supported by RACF or returned by the underlying interface to the z/OS Security Manager.

The native authentication configuration option, **nativeUpdateAllowed**, has been updated with a **reset** option which when specified allows binding with an expired RACF password or password phrase. In this case, the native authentication bind succeeds (LDAP server return code is 0) and **changeAfterReset** is returned in the **PasswordPolicy** control response. The only operation that the bound user can perform is a modify containing the special delete/add combination of the **userPassword** attribute to change the expired native password or password phrase. After the password is modified, the client can then perform other LDAP operations. The expired password and password phrase support is only enabled when the **PasswordPolicy** control is included on the bind request.

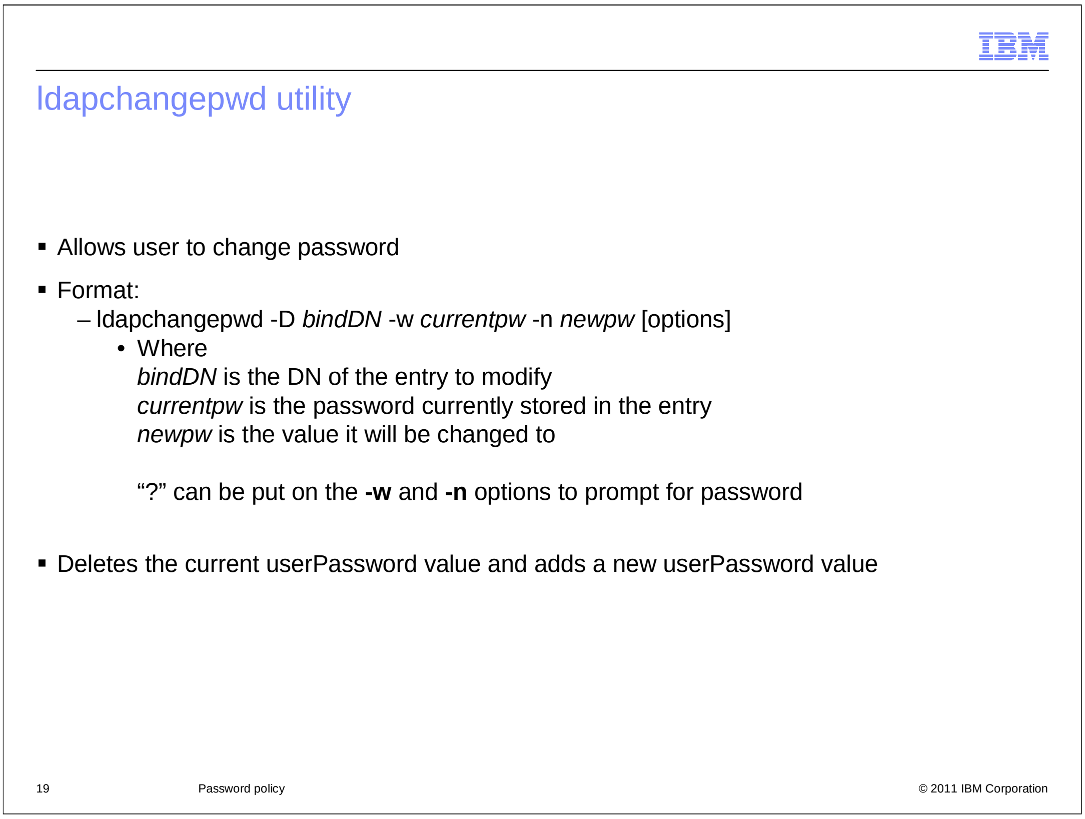
In z/OS V1.12, all z/OS LDAP client utilities have all been updated to send the **PasswordPolicy** control and to display the response on bind requests. The **ldapadd**, **ldapmodify**, and **ldapcompare** utilities have also been updated to send the **PasswordPolicy** control and display the response on add, modify, and compare requests.



Password policy console command

- New console command: Unlock Admin
  - Unlocks the LDAP administrator locked under password policy rules caused by:
    - Too many attempts to bind with incorrect password
    - Password expired
  - After command successfully completes, the LDAP administrator is able to authenticate to the LDAP server but must change password value before doing any other operations
  - Example: F LDAPSRV,UNLOCK ADMIN

If the LDAP administrator’s entry is subject to password policy on the LDAP server, it is possible for the account to get locked under password policy rules because of too many failed authentication attempts or the password has expired. When this occurs, the LDAP administrator is unable to access the directory to perform any administrative functions. To allow the LDAP administrator to authenticate to the LDAP server in these situations, the UNLOCK ADMIN console command has been added to allow for unlocking the administrator’s account. If the UNLOCK ADMIN console command successfully completes, the administrator is able to authenticate to the LDAP server but must change the password value before being allowed to perform any other LDAP operations.



ldapchangepwd utility

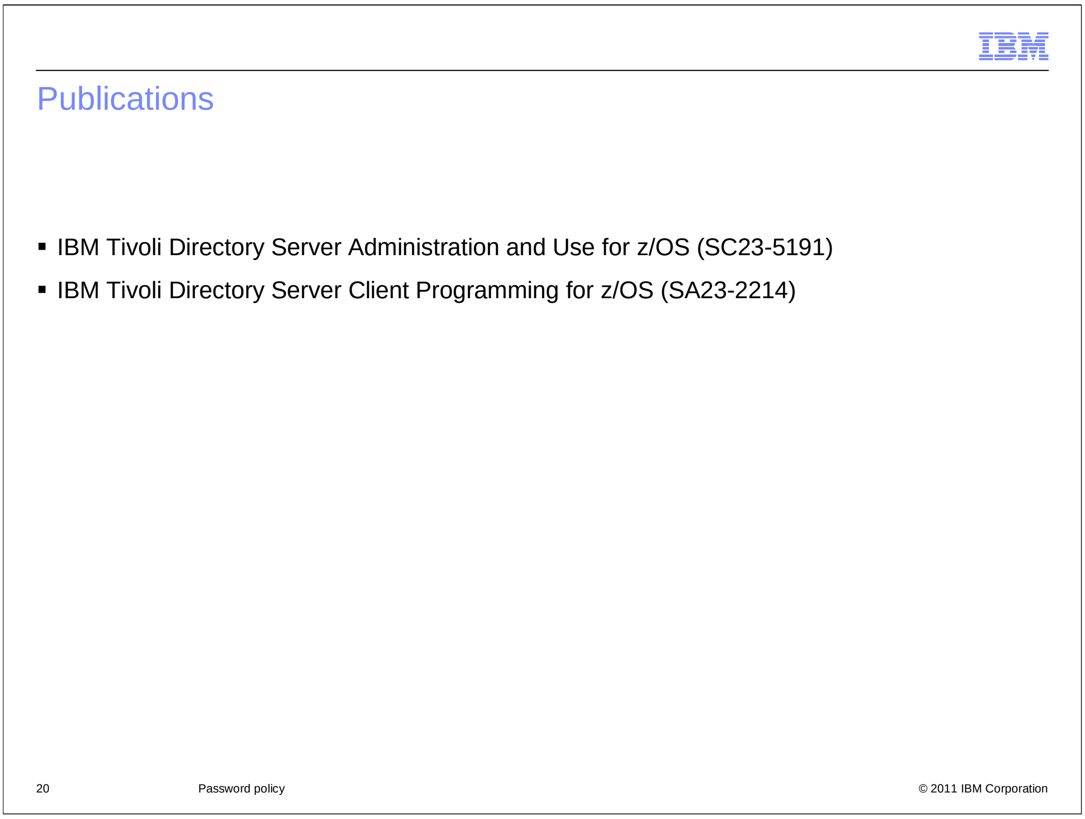
- Allows user to change password
- Format:
  - ldapchangepwd -D *bindDN* -w *currentpw* -n *newpw* [options]
    - Where
      bindDN is the DN of the entry to modify
      currentpw is the password currently stored in the entry
      newpw is the value it will be changed to

      "?" can be put on the **-w** and **-n** options to prompt for password
- Deletes the current userPassword value and adds a new userPassword value

19 Password policy © 2011 IBM Corporation

In z/OS V1.12, the **ldapchangepwd** utility was added to simplify changing password values instead of using the **ldapmodify** utility. The **ldapchangepwd** utility allows a user to specify the current password and a new password value on the command line. This eliminates the need to create an LDIF input file for password modify requests. If the **ldapchangepwd** utility is run from OMVS, an "?" can be used on the –w and –n options to prompt for the password value. However, "?" is not currently supported to prompt for a password value when running the **ldapchangepwd** utility from TSO or JCL. The syntax of the **ldapchangepwd** utility is very similar to the other z/OS LDAP client utilities such as **ldapmodify**.

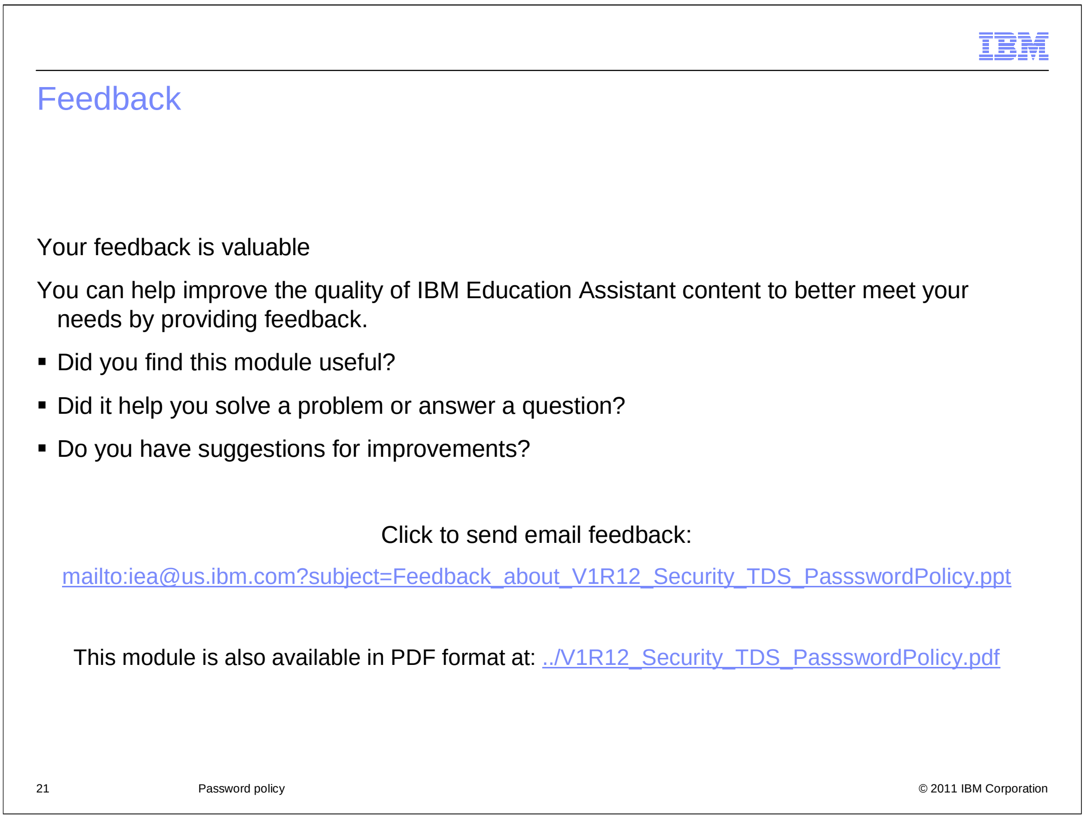
If password policy is active for the user whose password is being changed and the new password value does not meet the minimum password quality requirements (for example, the new password is not long enough), the effective password policy attributes related to password syntax are displayed after running the **ldapchangepwd** utility. This helps the end user select a password that adheres to the organization's password requirements.



Publications

- IBM Tivoli Directory Server Administration and Use for z/OS (SC23-5191)
- IBM Tivoli Directory Server Client Programming for z/OS (SA23-2214)

For additional information refer to the IBM Tivoli Directory Server Administration and Use for z/OS (SC23-5191) and IBM Tivoli Directory Server Client Programming for z/OS (SA23-2214) manuals.



Feedback

Your feedback is valuable

You can help improve the quality of IBM Education Assistant content to better meet your needs by providing feedback.

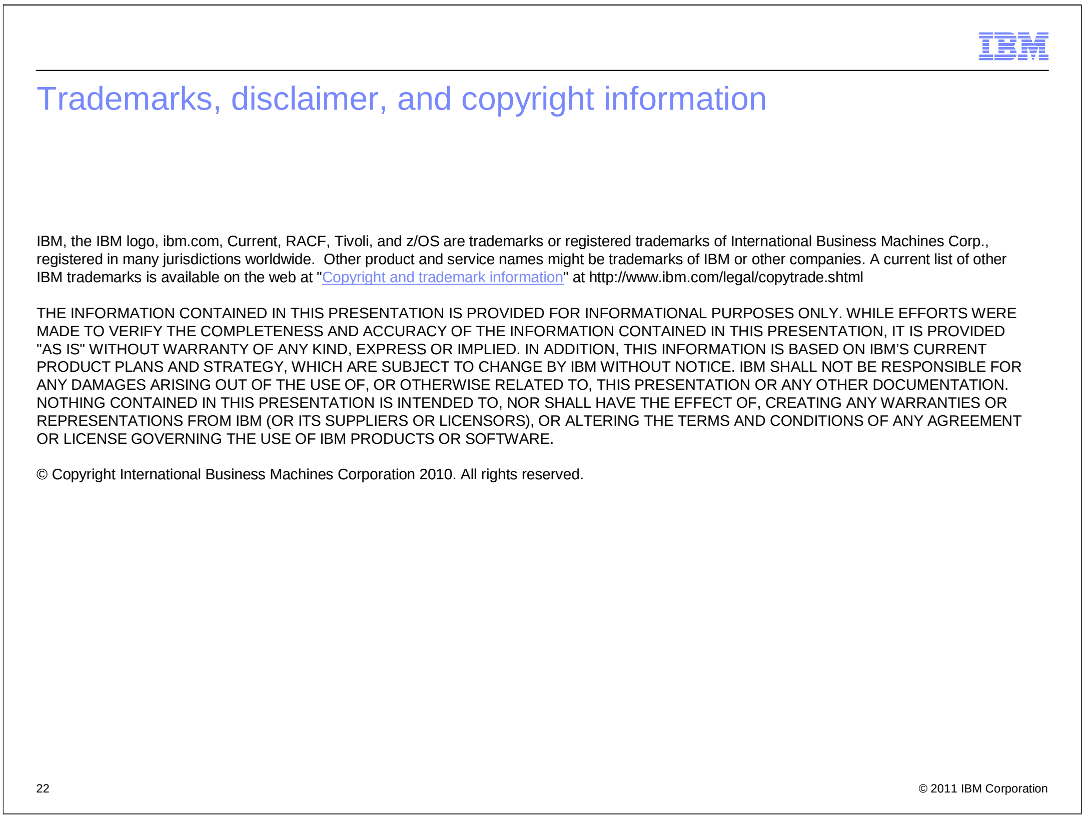
- Did you find this module useful?
- Did it help you solve a problem or answer a question?
- Do you have suggestions for improvements?

Click to send email feedback:

mailto:iea@us.ibm.com?subject=Feedback_about_V1R12_Security_TDS_PassswordPolicy.ppt

This module is also available in PDF format at: ../V1R12_Security_TDS_PassswordPolicy.pdf

You can help improve the quality of IBM Education Assistant content by providing feedback.



Trademarks, disclaimer, and copyright information

IBM, the IBM logo, ibm.com, Current, RACF, Tivoli, and z/OS are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of other IBM trademarks is available on the web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS OR SOFTWARE.