Internet Draft
<draft-bannister-dbis-policy-03.txt>
Category: Informational
Expires September 12, 2014

M. R. Bannister
Prose Consulting Ltd.

March 11, 2014

Directory-Based Information Services: Password Policies

Status of this Memo

Distribution of this memo is unlimited.

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on September 12, 2014.

Copyright Notice

Abstract

This document extends Directory-Based Information Services (DBIS) described in [draft-bannister-dbis-mapping-00] to support the shadow databases.

The shadow database schema SHALL be backwards compatible with the Network Information Service [NIS] but stored within [X.500] entries so that it may be resolved with the Lightweight Directory Access Protocol [RFC4510].

A shadow database extends user login accounts with credential policy data.

This document represents shadow database entries as an extended set of attributes that may be applied to both passwd and group database entries for the management of consistent password policies.

This document describes configuration maps [draft-bannister-dbis-mapping-00] for shadow databases, and database entries referenced by those maps.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED" and "MAY" in this document are to be interpreted as described in [RFC2119].

Table of Contents

1. Database

1.1. passwd

1.1.1. Definition

DBIS shadow database entries are defined in attributes that are added to a posixUserAccount or posixGroupAccount object [draft-bannister-dbis-passwd-00] by assigning the posixPwdPolicy auxiliary class. Configuration maps [draft-bannister-dbis-mapping-00] are not required for shadow database entries.

A DBIS passwd entry may also contain the fields from the shadow database:

- Date when password was last modified.

- Minimum number of days required between password changes, or -1 to disable password aging.

- Maximum number of days the password is valid, or -1 to disable password aging.

- Number of days before password expires that user is warned, or -1 to disable password aging.

- Number of days of inactivity permitted before account is locked.

- Date when user account expires.

- Failed login count.

The shadow database represents dates as the number of days since 1 January 1970. The DBIS schema represents dates in generalizedTime

format [RFC4517]. The DUA SHALL translate between the two formats to maintain backwards compatibility with NIS.

DBIS also adds the following information:

- Number of days grace allowed for user to change their password after it has reached its maximum age and before the account is locked.

- Date when user account was last used.

The information that makes up a database entry is obtained from the attributes described in the following sections.

It is RECOMMENDED that password policies are managed using native features in the LDAP Directory Server if available, or using Pluggable Authentication Modules [PAM] to provide consistency of security and centralised administration. Whether or not the shadow attributes are used by the policy will vary between implementations.

1.1.2. Object Classes

1.1.2.1. Introduction

A passwd entry MAY have the posixPwdPolicy class assigned if password policies are to be managed using these attributes. A DUA SHALL support password policies on passwd accounts via this class.

1.1.2.2. dbisShadowCompat

For compatibility, the pwdLastChange and pwdExpire attributes described in this document that take dates in Generalized Time format (1.3.6.1.4.1.1466.115.121.1.24) may alternatively be remapped with dbisMapAttr to attributes that use Integer format instead (1.3.6.1.4.1.1466.115.121.1.27).

This is intended to support existing configurations only and SHOULD NOT be used for new entries, which should use Generalized Time. A DUA MUST support both formats.

The dbisShadowCompat class MAY be associated with a dbisPasswdConfig entry to enable this compatibility setting, and is defined as follows:

```
objectclass ( 1.3.6.1.4.1.23780.219.1.36 NAME 'dbisShadowCompat'
  DESC 'DBIS shadow map time format compatibility'
  SUP top ABSTRACT )
```

This only applies to pwdLastChange and pwdExpire. It does not affect the pwdLastUsed attribute.

1.1.2.3. posixPwdPolicy

The posixPwdPolicy class is defined as follows:

```
objectclass ( 1.3.6.1.4.1.23780.219.1.10 NAME 'posixPwdPolicy'
  DESC 'POSIX-style password policy attributes'
  SUP top AUXILIARY
  MAY ( pwdLastChange $ pwdAgeMin $ pwdAgeMax $ pwdAgeWarning $
        pwdAgeGrace $ pwdLastUsed $ pwdInactivity $
        pwdExpire $ pwdFailCount ) )
```

1.1.3. Attributes

1.1.3.1. pwdLastChange

The date identifying when the account's password was last modified is stored in the shadowLastChange attribute that MAY be assigned to a posixPwdPolicy entry:

```
attributetype ( 1.3.6.1.4.1.23780.219.2.17 NAME 'pwdLastChange'
  DESC 'Date when password last changed'
  EQUALITY generalizedTimeMatch
  ORDERING generalizedTimeOrderingMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.24 SINGLE-VALUE )
```

If it exists, this attribute SHALL be updated by the DUA whenever the account's password is changed.

If the attribute is missing, it must be assumed that the password has never been changed. For the purposes of password aging, the password will be considered to have reached its maximum age.

1.1.3.2. pwdAgeMin

The minimum number of days between password changes is stored in the pwdAgeMin attribute that MAY be assigned to a posixPwdPolicy entry:

```
attributetype ( 1.3.6.1.4.1.23780.219.2.18 NAME 'pwdAgeMin'
  DESC 'Minimum number of days between password changes'
  EQUALITY integerMatch
  ORDERING integerOrderingMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )
```

The DUA SHALL NOT permit the password to be changed unless the pwdLastChange attribute indicates that the present password is at

least as old as indicated by pwdAgeMin.

If the attribute is missing or set to -1, the password aging policy is disabled. If set to 0, passwords have no minimum age.

1.1.3.3. pwdAgeMax

The maximum number of days a password is valid is stored in the pwdAgeMax attribute that MAY be assigned to a posixPwdPolicy entry:

```
attributetype ( 1.3.6.1.4.1.23780.219.2.19 NAME 'pwdAgeMax'
  DESC 'Maximum number of days a password is valid'
  EQUALITY integerMatch
  ORDERING integerOrderingMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )
```

The DUA SHOULD prompt the account owner to change their password if it has reached the maximum age configured in the password policy and is not older than the sum of pwdAgeMax and pwdAgeGrace, except when there is no interactive process available to obtain input. The DUA SHALL NOT successfully authenticate an account under these conditions unless it has been able to prompt the owner to supply their old and new passwords and the pwdLastChange attribute has been updated.

If the password is older than the sum of pwdAgeMax and pwdAgeGrace, then the DUA SHALL NOT prompt the owner to change their password and MUST lock the account by deleting all authPassword attributes associated with the account.

If the attribute is missing or set to -1, the password aging policy is disabled. If set to 0, the password must be changed on every use.

1.1.3.4. pwdAgeWarning

The number of days before a password expires that the user is warned is stored in the pwdAgeWarning attribute that MAY be assigned to a posixPwdPolicy entry:

```
attributetype ( 1.3.6.1.4.1.23780.219.2.20 NAME 'pwdAgeWarning'
  DESC 'Number of days prior to password expiry a user is warned'
  EQUALITY integerMatch
  ORDERING integerOrderingMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )
```

If this attribute is set, the DSA SHALL examine the pwdAgeMax and pwdExpire attributes and warn the user when the password is due to expire, except when there is no method available for communicating with the user. The DSA MAY also warn the user after pwdAgeMax has

been reached but before the end of the grace period defined in pwdAgeGrace. In this context "DSA" MAY represent a separate agent running on the DSA or on another system elected to issue password age warnings.

If the attribute is missing or set to -1, warnings are disabled. If set to 0, a password expiration warning is issued each time the password is used.

1.1.3.5. pwdAgeGrace

The number of days grace allowed for the account owner to change their password after it has reached its maximum age and before the account is locked is stored in the pwdAgeGrace attribute that MAY be assigned to a posixPwdPolicy entry:

```
attributetype ( 1.3.6.1.4.1.23780.219.2.21 NAME 'pwdAgeGrace'
  DESC 'Days allowed to change password after max age reached'
  EQUALITY integerMatch
  ORDERING integerOrderingMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )
```

If this attribute is set, the DUA SHALL modify its behaviour when password maximum age has been reached or exceeded. This modified behaviour is discussed in section 1.1.3.1.

If the attribute is missing or set to -1, the grace period is disabled.

1.1.3.6. pwdLastUsed

The date when the account was last used is stored in the 'pwdLastUsed' attribute that MAY be assigned to a posixPwdPolicy entry:

```
attributetype ( 1.3.6.1.4.1.23780.219.2.22 NAME 'pwdLastUsed'
  DESC 'Date when account was last used'
  EQUALITY generalizedTimeMatch
  ORDERING generalizedTimeOrderingMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.24 SINGLE-VALUE )
```

If this attribute exists, the DUA SHALL update it upon successfully authenticating an account. Note that this attribute will only track when an account is authenticated, and will not provide information on accounts used by long-running system processes.

If this attribute is missing then account lock-out due to inactivity will be disabled.

1.1.3.7. pwdInactivity

The number of days of inactivity permitted before the account is locked is stored in the 'pwdInactivity' attribute that MAY be assigned to a posixPwdPolicy entry:

```
attributetype ( 1.3.6.1.4.1.23780.219.2.23 NAME 'pwdInactivity'
  DESC 'Days of inactivity permitted before account is locked'
  EQUALITY integerMatch
  ORDERING integerOrderingMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )
```

If this attribute exists, the DUA SHALL verify when the account is authenticated that the date stored in the pwdLastUsed attribute is no older than the number of days stored in this attribute. If it is then the authentication SHALL NOT succeed.

If this attribute is missing or set to -1 then account lock-out due to inactivity will be disabled.

1.1.3.8. pwdExpire

The date when the account expires is stored in the 'pwdExpire' attribute that MAY be assigned to a posixPwdPolicy entry:

```
attributetype ( 1.3.6.1.4.1.23780.219.2.24 NAME 'pwdExpire'
  DESC 'Date when account expires'
  EQUALITY generalizedTimeMatch
  ORDERING generalizedTimeOrderingMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.24 SINGLE-VALUE )
```

If this attribute exists, the DUA SHALL verify when the account is authenticated that today's date is earlier than the date stored in this attribute. If it is not, then the authentication SHALL NOT succeed.

If this attribute is missing then password expiry is disabled.

1.1.3.9. pwdFailCount

The number of failed authentication attempts is stored in the 'pwdFailCount' attribute that MAY be assigned to a posixPwdPolicy entry:

```
attributetype ( 1.3.6.1.4.1.23780.219.2.25 NAME 'pwdFailCount'
  DESC 'Number of password failures'
  EQUALITY integerMatch
  ORDERING integerOrderingMatch
```

```
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )
```

The DUA SHALL increment this attribute for each failed login attempt if the attribute exists and is greater than -1.

If this attribute is missing or set to -1 then no password failure count is maintained.

Note that this is the total number of password failures since the account was created and is not reset upon successful authentication.

1.1.4. Example Passwd Entry

The following is an example of a posixUserAccount and posixPwdPolicy entry in LDIF format [RFC2849]. As posixUserAccount is an auxiliary class, it has in this example been attached to an instance of inetOrgPerson [RFC2798]:

```
dn: en=mark,ou=passwd,ou=sales,o=infra
objectClass: top
objectClass: inetOrgPerson
objectClass: posixUserAccount
objectClass: posixPwdPolicy
cn: Mark
sn: Bannister
displayName: Bannister, Mark
en: mark
uidNumber: 101
exactPrimary: staff
homeDirectory: /home/mark
loginShell: /bin/bash
exactGroup: sales
exactGroup: dev
exactNetgroup: engineering
pwdLastChange: 201306100735Z
pwdAgeMin: 1
pwdAgeMax: 90
pwdAgeWarning: 5
pwdAgeGrace: 3
pwdLastUsed: 201306101706Z
pwdInactivity: 90
```

1.2. group

1.2.1. Definition

DBIS permits the posixPwdPolicy class to be assigned to a group entry bringing with it a superset of fields traditionally stored in the

shadow database. This allows the same password policies to be applied to group accounts as user accounts. Password policies SHOULD be used if group accounts are given passwords.

It is RECOMMENDED that password policies are managed using native features in the LDAP Directory Server if available, or using Pluggable Authentication Modules [PAM] to provide consistency of security and centralised administration. Whether or not the shadow attributes are used by the policy will vary between implementations.

1.2.2. Object Classes

A group entry MAY have the posixPwdPolicy class assigned if password policies are to be managed using these attributes. A DUA SHALL support password policies on group accounts via this class.

1.2.3. Attributes

Password policies can be applied to group account passwords. When the posixPwdPolicy class is associated with a group database entry then the attributes from that class may be added to the group account. The meaning of these attributes when associated with a posixGroupAccount entry is as described in section 1.1.3 of this document, except that they apply to group accounts instead of user accounts.

1.2.4. Example Group Entry

The following is an example of a posixGroupAccount and posixPwdPolicy entry in LDIF format [RFC2849]:

```
dn: en=finance,ou=group,ou=sales,o=infra
objectClass: top
objectClass: posixGroupAccount
objectClass: posixPwdPolicy
en: finance
gidNumber: 152
exactUser: mark
exactUser: julie
exactUser: stephen
exactUser: nathan
pwdLastChange: 201306100735Z
pwdAgeMin: 1
pwdAgeMax: 90
pwdAgeWarning: 5
pwdAgeGrace: 3
pwdLastUsed: 201306170714Z
pwdInactivity: 90
```

2. Attribute Syntax

The following syntaxes are used by the attributes defined in this document:

Syntax OID	Value	Reference
1.3.6.1.4.1.1466.115.121.1.24	Generalized Time	[RFC4517]
1.3.6.1.4.1.1466.115.121.1.27	Integer	[RFC4517]

3. Implementation Notes

3.1. NIS Compatible Field Mapping

3.1.1. Introduction

All fields that are required to generate NIS-compatible colon-separated shadow database formats exist in this schema and can be mapped to attribute types using common ABNF productions described in [draft-bannister-dbis-netgroup-00], section 1.2.

The NIS-compatible shadow database fields are mapped as follows:

```
user     = en
password = authPassword   ; implementation-specific, see below
lastchg  = pwdLastChange  ; date conversion required, see below
min      = pwdAgeMin
max      = pwdAgeMax
warn     = pwdAgeWarning
inactive = pwdInactivity
expire   = pwdExpire      ; date conversion required, see below
flag     = pwdFailCount   ; low 4-bits only, see below

shadow-entry = user COLON password COLON lastchg COLON
                    min COLON max COLON warn COLON
                    inactive COLON expire COLON flag
```

In the shadow mappings above:

- password is implementation-specific. See notes for password field in [draft-bannister-dbis-passwd-00] section 5.1.2.

- lastchg and expire date formats do not match the format required in a NIS-compatible entry, but rather use an LDAP-specific standard. When producing a colon-separated shadow database entry, the DUA SHALL convert the date to the number of days since 1 January 1970.

This conversion will not be necessary if the dbisShadowCompat class is assigned to the dbisPasswdConfig entry, see section 1.1.2.2.

- flag has the password failure count in the lowest four bits, while NIS reserves the remaining bits for future use. Therefore, if pwdFailCount is greater than 15, the DUA SHALL return 15 in the flag field.

- pwdAgeGrace and pwdLastUsed have no corresponding NIS fields. The DUA SHALL provide an alternative means for a user to query the values of these fields.

The posixPwdPolicy attributes when assigned to group database entries have no corresponding NIS fields. The DUA SHALL provide an alternative means for a user to query the values of these fields.

4. Security Considerations

The security considerations discussed in [draft-bannister-dbis-passwd-00] apply equally to this document.

5. References

5.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2798] Smith, M., "Definition of the inetOrgPerson LDAP Object Class", RFC 2798, April 2000.

[RFC2849] Good, G., "The LDAP Data Interchange Format (LDIF) - Technical Specification", RFC 2849, June 2000.

[RFC4510] Zeilenga, K., Ed., "Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map", RFC 4510, June 2006.

[RFC4517] Legg, S., Ed., "Lightweight Directory Access Protocol (LDAP): Syntaxes and Matching Rules", RFC 4517, June 2006.

[draft-bannister-dbis-mapping-00] Bannister, M. R., "Directory-Based Information Services: Mapping Objects", draft-bannister-dbis-mapping-00.txt, August 2013.

[draft-bannister-dbis-netgroup-00] Bannister, M. R., "Directory-Based Information Services: Netgroups and Netservices", draft-bannister-dbis-netgroups-00.txt, August 2013.

[draft-bannister-dbis-passwd-00] Bannister, M. R., "Directory-Based Information Services: Users and Groups", draft-bannister-dbis-netgroups-00.txt, August 2013.

5.2. Informative References

[X.500] Weider, C. and J. Reynolds, "Executive Introduction to Directory Services Using the X.500 Protocol", FYI 13, RFC 1308, March 1992.

[NIS] Wikipedia, "Network Information Service", <http://en.wikipedia.org/wiki/Network_Information_Service>.

[PAM] Wikipedia, "Pluggable authentication module", <http://en.wikipedia.org/wiki/Pluggable_Authentication_Modules>.

Author's Address

Mark R. Bannister
Prose Consulting Ltd.
73 Claygate Lane
Esher, Surrey, KT10 0BQ
United Kingdom

Tel: +44 7764 604316
EMail: dbis@proseconsulting.co.uk