Kerberos V

Introduction

These package allows you to access Kerberos V administration servers. You can create, modify, and delete Kerberos V principals and policies.

More information about Kerberos can be found at » http://web.mit.edu/kerberos/www/.

Documentation for Kerberos and KADM5 can be found at
» http://web.mit.edu/kerberos/www/krb5-1.2/krb5-1.2.8/doc/admin_toc.html.

Installing/Configuring

Requirements

No external libraries are needed to build this extension.

Installation

There is no installation needed to use these functions; they are part of the PHP core.

Runtime Configuration

This extension has no configuration directives defined in *php.ini*.

Resource Types

This extension defines a KADM5 handle returned by kadm5_init_with_password().

Predefined Constants

The constants below are defined by this extension, and will only be available when the extension has either been compiled into PHP or dynamically loaded at runtime.

Constants for Attribute Flags

The functions kadm5_create_principal(), kadm5_modify_principal(), and kadm5_modify_principal() allow to specify special attributes using a bitfield. The symbols are defined below:

Attributes for use by the KDC

constant
KRB5_KDB_DISALLOW_POSTDATED
KRB5_KDB_DISALLOW_FORWARDABLE
KRB5_KDB_DISALLOW_TGT_BASED
KRB5_KDB_DISALLOW_RENEWABLE
KRB5_KDB_DISALLOW_PROXIABLE
KRB5_KDB_DISALLOW_DUP_SKEY
KRB5_KDB_DISALLOW_ALL_TIX
KRB5_KDB_REQUIRES_PRE_AUTH
KRB5_KDB_REQUIRES_HW_AUTH
KRB5_KDB_REQUIRES_PWCHANGE
KRB5_KDB_DISALLOW_SVR
KRB5_KDB_PWCHANGE_SERVER
KRB5_KDB_SUPPORT_DESMD5
KRB5_KDB_NEW_PRINC

Constants for Options

The functions kadm5_create_principal(), kadm5_modify_principal(), and kadm5_get_principal() allow to specify or return principal's options as an associative array. The keys for the associative array are defined as string constants below:

Options for creating/modifying/retrieving principals

constant	funcdef	description
KADM5_PRINCIPAL	long	The expire time of the princial as a Kerberos timestamp.
KADM5_PRINC_EXPIRE_TIME	long	The expire time of the princial as a Kerberos timestamp.
KADM5_LAST_PW_CHANGE	long	The time this principal's password was last changed.
KADM5_PW_EXPIRATION	long	The expire time of the principal's current password, as a Kerberos timestamp.
KADM5_MAX_LIFE	long	The maximum lifetime of any Kerberos ticket issued to this principal.
KADM5_MAX_RLIFE	long	The maximum renewable lifetime of any Kerberos ticket issued to or for this principal.
KADM5_MOD_NAME	string	The name of the Kerberos principal that most recently modified this principal.
KADM5_MOD_TIME	long	The time this principal was last modified, as a Kerberos timestamp.
KADM5_KVNO	long	The version of the principal's current key.
KADM5_POLICY	string	The name of the policy controlling this principal.
KADM5_CLEARPOLICY	long	Standard procedure is to assign the 'default' policy to new principals. KADM5_CLEARPOLICY suppresses this behaviour.

KADM5_LAST_SUCCESS	long	The KDC time of the last successfull AS_REQ.
KADM5_LAST_FAILED	long	The KDC time of the last failed AS_REQ.
KADM5_FAIL_AUTH_COUNT	long	The number of consecutive failed AS_REQs.
KADM5_RANDKEY	long	Generates a random password for the principal. The parameter *password* will be ignored.
KADM5_ATTRIBUTES	long	A bitfield of attributes for use by the KDC.

Examples

This simple example shows how to connect, query, print resulting principals and disconnect from a KADM5 database.

Example #1 - KADM5 extension overview example

```
<?php

 $handle = kadm5_init_with_password("afs-1", "GONICUS.LOCAL", "admin/admin",
"password");

 print "<h1>get_principals</h1>\n";
 $principals = kadm5_get_principals($handle);
 for( $i=0; $i<count($principals); $i++)
     print "$principals[$i]<br>\n";

 print "<h1>get_policies</h1>\n";
 $policies = kadm5_get_policies($handle);
 for( $i=0; $i<count($policies); $i++)
     print "$policies[$i]<br>\n";

 print "<h1>get_principal burbach@GONICUS.LOCAL</h1>\n";

 $options = kadm5_get_principal($handle, "burbach@GONICUS.LOCAL" );
 $keys = array_keys($options);
 for( $i=0; $i<count($keys); $i++) {
   $value = $options[$keys[$i]];
   print "$keys[$i]: $value<br>\n";
 }

 $options = array(KADM5_PRINC_EXPIRE_TIME => 0);
 kadm5_modify_principal($handle, "burbach@GONICUS.LOCAL", $options);

 kadm5_destroy($handle);
?>
```

KADM5 Functions

kadm5_chpass_principal

kadm5_chpass_principal -- Changes the principal's password

Description

bool **kadm5_chpass_principal** (resource `$handle`, string `$principal`, string `$password`)

kadm5_chpass_principal() sets the new password *`password`* for the *`principal`*.

Parameters

`handle`
A KADM5 handle.

`principal`
The principal.

`password`
The new password.

Return Values

Returns **TRUE** on success or **FALSE** on failure.

Examples

Example #2 - Example of changing principal's password

```
<?php

$handle = kadm5_init_with_password("afs-1", "GONICUS.LOCAL", "admin/admin",
"password");

kadm5_chpass_principal($handle, "burbach@GONICUS.LOCAL", "newpassword");

kadm5_destroy($handle);
?>
```

kadm5_create_principal

kadm5_create_principal -- Creates a kerberos principal with the given parameters

Description

bool **kadm5_create_principal** (resource `$handle`, string `$principal` [, string `$password` [, array `$options`]])

Creates a *`principal`* with the given *`password`*.

Parameters

`handle`
A KADM5 handle.

`principal`
The principal.

`password`
If *`password`* is omitted or is **NULL**, a random key will be generated.

`options`
It is possible to specify several optional parameters within the array *`options`*. Allowed are the following options: **KADM5_PRINC_EXPIRE_TIME**, **KADM5_PW_EXPIRATION**, **KADM5_ATTRIBUTES**, **KADM5_MAX_LIFE**, **KADM5_KVNO**, **KADM5_POLICY**, **KADM5_CLEARPOLICY**, **KADM5_MAX_RLIFE**.

Return Values

Returns **TRUE** on success or **FALSE** on failure.

Examples

Example #3 - Example of principal's creation

```
<?php

$handle = kadm5_init_with_password("afs-1", "GONICUS.LOCAL", "admin/admin",
"password");

$attributes = KRB5_KDB_REQUIRES_PRE_AUTH | KRB5_KDB_DISALLOW_PROXIABLE;
$options = array(KADM5_PRINC_EXPIRE_TIME => 0,
                 KADM5_POLICY => "default",
                 KADM5_ATTRIBUTES => $attributes);
```

```
kadm5_create_principal($handle, "burbach@GONICUS.LOCAL", "password",
$options);

kadm5_destroy($handle);
?>
```

See Also

- kadm5_modify_principal()
- kadm5_delete_principal()

kadm5_delete_principal

kadm5_delete_principal -- Deletes a kerberos principal

Description

bool **kadm5_delete_principal** (resource `$handle`, string `$principal`)

Removes the *`principal`* from the Kerberos database.

Parameters

`handle`
A KADM5 handle.

`principal`
The removed principal.

Return Values

Returns **TRUE** on success or **FALSE** on failure.

Examples

Example #4 - kadm5_delete_principal() example

```
<?php

$handle = kadm5_init_with_password("afs-1", "GONICUS.LOCAL", "admin/admin",
"password");

kadm5_delete_principal($handle, "burbach@GONICUS.LOCAL");

kadm5_destroy($handle);
?>
```

See Also

- kadm5_modify_principal()
- kadm5_create_principal()

kadm5_destroy

kadm5_destroy -- Closes the connection to the admin server and releases all related resources

Description

bool **kadm5_destroy** (resource `$handle`)

Closes the connection to the admin server and releases all related resources.

Parameters

`handle`
A KADM5 handle.

Return Values

Returns **TRUE** on success or **FALSE** on failure.

See Also

- kadm5_init_with_password()

kadm5_flush

kadm5_flush -- Flush all changes to the Kerberos database

Description

bool **kadm5_flush** (resource `$handle`)

Flush all changes to the Kerberos database, leaving the connection to the Kerberos admin server open.

Parameters

`handle`
A KADM5 handle.

Return Values

Returns **TRUE** on success or **FALSE** on failure.

kadm5_get_policies

kadm5_get_policies -- Gets all policies from the Kerberos database

Description

array **kadm5_get_policies** (resource `$handle`)

Gets an array containing the policies's names.

Parameters

`handle`
A KADM5 handle.

Return Values

Returns array of policies on success, or **FALSE** on failure.

Examples

Example #5 - kadm5_get_policies() example

```
<?php
$handle = kadm5_init_with_password("afs-1", "GONICUS.LOCAL", "admin/admin",
"password");

print "<h1>get_policies</h1>\n";
foreach (kadm5_get_policies($handle) as $policy) {
   echo "$policy<br />\n";
}

kadm5_destroy($handle);
?>
```

kadm5_get_principal

kadm5_get_principal -- Gets the principal's entries from the Kerberos database

Description

array **kadm5_get_principal** (resource `$handle`, string `$principal`)

Gets the principal's entries from the Kerberos database.

Parameters

`handle`
A KADM5 handle.

`principal`
The principal.

Return Values

Returns array of options containing the following keys: KADM5_PRINCIPAL, KADM5_PRINC_EXPIRE_TIME, KADM5_PW_EXPIRATION, KADM5_ATTRIBUTES, KADM5_MAX_LIFE, KADM5_MOD_NAME, KADM5_MOD_TIME, KADM5_KVNO, KADM5_POLICY, KADM5_MAX_RLIFE, KADM5_LAST_SUCCESS, KADM5_LAST_FAILED, KADM5_FAIL_AUTH_COUNT on success, or **FALSE** on failure.

Examples

Example #6 - kadm5_get_principal() **example**

```
<?php
$handle = kadm5_init_with_password("afs-1", "GONICUS.LOCAL", "admin/admin",
"password");

print "<h1>get_principal burbach@GONICUS.LOCAL</h1>\n";

$options = kadm5_get_principal($handle, "burbach@GONICUS.LOCAL" );

foreach ($options as $key => $value) {
   echo "$key: $value<br />\n";
}

kadm5_destroy($handle);
?>
```

See Also

- kadm5_get_principals()

kadm5_get_principals

kadm5_get_principals -- Gets all principals from the Kerberos database

Description

array **kadm5_get_principals** (resource `$handle`)

kadm5_get_principals() returns an array containing the principals's names.

Parameters

`handle`
A KADM5 handle.

Return Values

Returns array of principals on success, or **FALSE** on failure.

Examples

Example #7 - kadm5_get_principals() example

```
<?php
$handle = kadm5_init_with_password("afs-1", "GONICUS.LOCAL", "admin/admin",
"password");

print "<h1>get_principals</h1>\n";
foreach (kadm5_get_principals($handle) as $principal) {
   echo "$principal<br />\n";
}

kadm5_destroy($handle);
?>
```

See Also

- kadm5_get_principal()

kadm5_init_with_password

kadm5_init_with_password -- Opens a connection to the KADM5 library

Description

resource **kadm5_init_with_password** (string `$admin_server`, string `$realm`, string `$principal`, string `$password`)

Opens a connection with the KADM5 library using the *`principal`* and the given *`password`* to obtain initial credentials from the *`admin_server`*.

Parameters

`admin_server`
: The server.

`realm`
: Defines the authentication domain for the connection.

`principal`
: The principal.

`password`
: If *`password`* is omitted or is **NULL**, a random key will be generated.

Return Values

Returns a KADM5 handle on success, or **FALSE** on failure.

Examples

Example #8 - KADM5 initialization example

```
<?php

$handle = kadm5_init_with_password("afs-1", "GONICUS.LOCAL", "admin/admin",
"password");

$attributes = KRB5_KDB_REQUIRES_PRE_AUTH | KRB5_KDB_DISALLOW_PROXIABLE;
$options = array(KADM5_PRINC_EXPIRE_TIME => 0,
                 KADM5_POLICY => "default",
                 KADM5_ATTRIBUTES => $attributes);

kadm5_create_principal($handle, "burbach@GONICUS.LOCAL", "password",
$options);
```

```
kadm5_destroy($handle);
?>
```

Notes

Note
Connection should be closed after use with kadm5_destroy().

See Also

- kadm5_destroy()

kadm5_modify_principal

kadm5_modify_principal -- Modifies a kerberos principal with the given parameters

Description

bool **kadm5_modify_principal** (resource `$handle`, string `$principal`, array `$options`)

Modifies a *`principal`* according to the given *`options`*.

Parameters

`handle`
A KADM5 handle.

`principal`
The principal.

`options`
It is possible to specify several optional parameters within the array *`options`*. Allowed are the following options: **KADM5_PRINC_EXPIRE_TIME**, **KADM5_PW_EXPIRATION**, **KADM5_ATTRIBUTES**, **KADM5_MAX_LIFE**, **KADM5_KVNO**, **KADM5_POLICY**, **KADM5_CLEARPOLICY**, **KADM5_MAX_RLIFE**. **KADM5_FAIL_AUTH_COUNT**.

Return Values

Returns **TRUE** on success or **FALSE** on failure.

Examples

Example #9 - Example of modifying principal

```
<?php

$handle = kadm5_init_with_password("afs-1", "GONICUS.LOCAL", "admin/admin",
"password");

$attributes = KRB5_KDB_REQUIRES_PRE_AUTH;
$options = array(KADM5_PRINC_EXPIRE_TIME => 3451234,
                 KADM5_POLICY => "gonicus",
                 KADM5_ATTRIBUTES => $attributes);

kadm5_modify_principal($handle, "burbach@GONICUS.LOCAL", $options);

kadm5_destroy($handle);
```

```
?>
```

See Also

- kadm5_create_principal()
- kadm5_delete_principal()