


```

print "\n";
exit;
}

# print_dttm() function - argument is a Unix-time-in-seconds integer value.
# If no argument is given, we will use the current time.
sub print_dttm {
    if ($_[0] ne "") {
        $TIME_ARG=$_[0];
    } else {
        # Because of how getopt works, this will probably
        # never be reached.
        $TIME_ARG=time;
    }
    # strftime() formats the data in the list returned by
    # localtime() based on the format string given.
    print strftime("$FMT_STR\n",localtime($TIME_ARG));
    return 0;
}

# print_utis() function - argument passed is a date/time string.
# Currently supported format is "WDAY MONTH DAY TIME YEAR"
# i.e. Sun Mar 2 19:52:46 2003
sub print_utis {
    my($time_str)=@_;
    if (! defined($time_str)) {
        # Return utis for current time.
        $UTIS_STR=time;
    } else {
        my($weekday,$month,$mday,$time,$year) = split(/ /,$time_str);
        # We need to parse time time string sent in.

        # Here are some arrays of conversion stuff.
        # week day conversion:
        my(%WDAY)=( "Sun",0,
                    "Mon",1,
                    "Tue",2,
                    "Wed",3,
                    "Thu",4,
                    "Fri",5,
                    "Sat",6);

        my(%MON)=(
                    "Jan",0,
                    "Feb",1,
                    "Mar",2,
                    "Apr",3,
                    "May",4,
                    "Jun",5,
                    "Jul",6,
                    "Aug",7,

```

NOTES



```

        "Sep",8,
        "Oct",9,
        "Nov",10,
        "Dec",11);

# Set the week day and month numbers based on the above hash.
my($wday)=$WDAY{$weekday};
my($mon)=$MON{$month};

# split up the time into hour, min, and sec.
my($hour,$min,$sec)=split(/:/,$time);

# Make the real year:)
$year-=1900;

# See what happens:P
$UTIS_STR=mktime($sec,$min,$hour,$mday,$mon,$year);
}
print "$UTIS_STR\n";
}

##### MAIN #####
# Process command-line args.
# perl 5.001 doesn't understand hashes yet:P
#getopts('?hd:t:g', \%opts);
getopts('hd:t:g');

# check if we want help.
if ($opt_h) {
    usage_exit "";
}

# Parse the rest of ARGV in case a format is specified.
$arg="@ARGV";
if ($arg =~ /^^(.*)/) {
    $FMT_STR="$1";
}

# only one of -d or -t are allowed, and -f isn't allowed for -t...
if ($opt_d && $opt_t) {
    usage_exit "-d and -t options cannot be used together.";
}

if (! $opt_d && ! $opt_t) {
    print_utis;
} elsif ( $opt_d ) {
    print_dttm $opt_d;
} elsif ( $opt_t ) {
    print_utis $opt_t;
}

```

NOTES



Stratégie de verrouillage du compte

La stratégie de verrouillage du compte permet de désactiver un compte d'utilisateur si un mot de passe est incorrectement entré un certain nombre de fois durant une période donnée. Ces paramètres de stratégie contribuent à empêcher les agresseurs potentiels de deviner les mots de passe des utilisateurs et réduisent ainsi l'éventualité d'une attaque sur votre réseau.

Deux méthodes s'offrent à vous pour appliquer ce genre de stratégie. Passer directement par l'annuaire LDAP pour définir vos stratégies, ce que nous vous recommandons ou encore les définir sous Samba à l'aide de l'outil *pdbedit*.

L'application de la stratégie de verrouillage du compte de votre domaine vous permettra d'appliquer les éléments suivants:

- Définir le temps de verrouillage d'un compte,
- Définir le nombre de tentative d'essai d'un mot de passe avant le verrouillage,
- La réinitialisation du nombre de tentatives,
- Temps de déconnexion,
- Date d'expiration du compte utilisateur.

Stratégie de verrouillage du compte globale.

Voici les attributs vous permettant de définir votre stratégie de verrouillage du compte de façon globale.

- `sambaForceLogoff`
- `sambaLockoutDuration`
- `sambaLockoutObservationWindows`
- `sambaLockoutThreshold`

NOTES



sambaForceLogoff

Définit l'obligation de déconnexion de l'utilisateur qui est en dehors de la plage horaire autorisée. Par défaut la valeur de ce paramètre est de -1. Cet attribut nécessite l'ajout de l'attribut LDAP *sambaLogonHours*.

-1	Désactivé
0	Activé

sambaLockoutDuration

Définit le temps de verrouillage en minutes. Par défaut la valeur est de 30 minutes. La valeur de -1 indique que le compte sera verrouillé pour toujours.

sambaLockoutObservationWindows

Définit le délai de temps en minutes avant la réinitialisation après un verrouillage. Par défaut cette valeur est de 30 minutes.

sambaLockoutThreshold

Nombre de tentative d'essai d'un mot de passe avant le verrouillage d'un compte utilisateur. Par défaut la valeur est de 0 tentative, soit désactivé.

Stratégie de verrouillage du compte spécifique.

Voici les attributs vous permettant de définir votre stratégie de verrouillage du compte pour un utilisateur spécifique.

Pour appliquer la stratégie de verrouillage du compte spécifique sous LDAP, vous devez ajouter les attributs suivants pour chacun des comptes nécessitant une stratégie de verrouillage du compte.

- sambaLogonTime
- sambaLogoffTime
- sambaKickoffTime
- sambaLogonHours

NOTES



sambaLogonTime

L'attribut *sambaLogonTime* indique la date de la dernière ouverture de session de l'utilisateur en format UNIX time. Cet attribut est simplement indicatif, mais nécessaire pour les stratégies de verrouillage du compte.

sambaLogoffTime

L'attribut *sambaLogoffTime* indique la date de la dernière fermeture de session de l'utilisateur en format UNIX time. Cet attribut est simplement indicatif, mais nécessaire pour les stratégies de verrouillage du compte.

sambaKickoffTime

L'attribut *sambaKickoffTime* indique la date lorsque le compte de l'utilisateur sera automatiquement verrouillé. Le format de cette valeur doit être inscrit en format UNIX time. Cet attribut est idéal pour les comptes temporaires.

Si vous prévoyez ne pas utiliser cette fonctionnalité, ajouter tout de même l'attribut, mais laisser une valeur vide dans son champ.

sambaLogonHours

L'attribut *sambaLogonHours* indique une plage horaire où l'utilisateur est autorisé à ouvrir une session sur les postes de travail du domaine.

Cet attribut représente un champ de bits de 168 bits, chaque bit représente une heure de la semaine. Le tout est sous 21 caractères hexadécimale ($21 \times 8 = 168$).

Pour les fuseaux horaires, le *sambaLogonHours* fonctionne avec l'heure GMT. Vous devez donc ajuster vous même la valeur selon votre fuseau horaire.

Le premier bit représente la plage de dimanche entre 0:00 et 0:59, le second bit représente la plage entre 1:00 et 1:59.

NOTES



L'exemple suivant représente la plage de 6:00 à 17:59, du lundi au vendredi

```
00000000F87F00F87F00F87F00F87F00F87F000000
```

La méthode sûrement la plus simple pour définir le `sambaLogonHours` est d'utiliser l'utilitaire `usrmgr.exe` de Microsoft. Cependant faites très attention. Il est très important d'utiliser la version 4.0.1371.1 de l'utilitaire. Avec la version 5.2.3790.1127, vous obtiendrez l'erreur:

*User Manager for Domains cannot be used to manage a Windows 2000 or higher domain.
Do you want to select another domain to administer?*

Vous pouvez télécharger la bonne version sur le site de Microsoft au:

<http://download.microsoft.com/download/winntwks40/utility/7/nt4/en-us/srvtools.exe>

Tableau comparatif

Voici un tableau comparatif entre les options sous Samba et ceux que l'on retrouve dans l'annuaire LDAP.

Samba (pdbedit)	Annuaire LDAP
Logon time	sambaLogonTime
Logoff time	sambaLogoffTime
Kickoff time	sambaKickoffTime
Logon hours	sambaLogonHours

NOTES



sambaMaxPwdAge

Défini le temps d'existence du mot de passe maximum en secondes. Par défaut la valeur est de -1 ce qui indique que le mot de passe n'expire jamais.

sambaMinPwdAge

Définie le temps d'existence du mot de passe minimum en secondes. Par défaut la valeur est de 0 ce qui autorise le changement immédiat du mot de passe.

sambaMinPwdLength

Défini la longueur minimale du mot de passe de l'utilisateur. Par défaut la valeur est de 5 caractères. Nous vous recommandons de mettre une valeur de 8 caractères au minimum.

sambaPwdHistoryLength

Défini le nombre d'entrées des mots de passe dans l'historique. Par défaut la valeur est de 0, soit désactivé. Nous vous recommandons de mettre une valeur de 12 mots de passe au minimum.

sambaRefuseMachinePwdChange

Autorise que le mot de passe des ordinateurs soient changés. Par défaut la valeur est de 0, soit désactivé.

Gestion d'une stratégie de mot de passe global.

- Ouvrez l'outil web phpLDAPAdmin.
- Dans le volet de gauche, naviguer jusqu'à l'entrée `sambaDomainName=CYBIOLAB`.
- Puis ajouter les attributs de stratégie de mot de passe désirés, à l'aide du lien Ajouter un nouvel attribut dans le volet de droit.
- Donner à votre attribut la valeur qui correspond à vos besoins.

NOTES



Stratégie de mot de passe spécifique.

Voici les attributs vous permettant de définir votre stratégie de mot de passe pour un utilisateur spécifique. La majorité des attributs qui suivent nécessite l'utilisation du script *amtime.pl* pour faire la conversion de votre valeur en format Unix time.

sambaPwdCanChange

L'attribut *sambaPwdCanChange* indique la date que l'utilisateur peut changer son mot de passe en format UNIX time.

sambaPwdLastSet

L'attribut *sambaPwdLastSet* indique la date du dernier changement de mot de passe (*sambaLMPassword* et *sambaNTPassword*) en format UNIX time.

sambaPwdMustChange

L'attribut *sambaPwdMustChange* indique la date que l'utilisateur doit changer son mot de passe en format UNIX time.

Les utilisateurs de poste sous Windows Professionnel auront un avertissement comme quoi leur mot de passe expirera dans X jour. Lors du changement de mot de passe les attributs LDAP, *sambaPwdCanChange*, *sambaPwdLastSet* et *sambaPwdMustChange* seront modifiés.

Pour définir cette valeur, il est pratique d'utiliser la commande `pdbedit`, surtout si vous avez des clients Linux sur votre domaine. Effectivement, un utilisateur du domaine sous Linux pourrait changer son mot de passe, mais l'attribut *sambaPwdMustChange* ne serait pas modifié pour autant. Il va de soit que cela vous occasionnera certain problème. Aussi aucun avertissement ne sera envoyé à l'utilisateur sous Linux.

Voici donc comment faire avec la commande `pdbedit`.

```
pdbedit --pwd-must-change-time="2006-01-31" --time-format="%Y-%m-%d" <nom_utilisateur>
```

NOTES



Renforcement de mot de passe (globale).

Voici un ajout intéressant pour Samba. Le *renforcement de mot de passe* s'assure de la complexité de ces derniers. Le mot de passe de l'utilisateur devra donc contenir des caractères, des chiffres ainsi que des caractères spéciaux. Aussi, ce mot de passe ne devra pas être un mot du dictionnaire (*anglais*).

Nous allons installer la librairie nécessaire à la vérification des mots de passe.

emerge cracklib

Faites la vérification que l'application fonctionne correctement.

cracklib-check

Saisissez le mot de passe `allo`.

```
allo
```

```
allo: it is too short
```

Application du renforcement de mot de passe

Éditer le fichier `smb.conf` et ajouter sous la ligne *encrypt passwords* le paramètre suivant:

```
check password script = /usr/sbin/cracklib-check
```

Et faites la vérification de votre modification.

testparm

NOTES



Autre gestion des utilisateurs

Pour appliquer d'autres options aux stratégies de groupes, vous devez ajouter les attributs suivant pour chacun des comptes.

- `sambaUserWorkstations`
- `sambaMungedDial`
- `sambaDomainName`

sambaUserWorkstations

L'attribut `sambaUserWorkstations` indique les ordinateurs sous lequel un utilisateur peut ouvrir une session.

sambaDomainName

L'attribut `sambaDomainName` indique le nom du domaine dans lequel l'utilisateur fait parti. Cet attribut est simplement indicatif.

sambaMungedDial

L'attribut `sambaMungedDial` donne les options d'appel suivantes.

- **Pas de rappel** (*No Call Back*): Le serveur RAS ne rappelle pas le client et l'utilisateur distant établit la communication. C'est la valeur par défaut.
- **Défini par l'appelant** (*Set by Caller*): L'utilisateur peut définir un numéro de téléphone que le service d'appel distant utilise pour appeler. C'est l'entreprise qui établit la communication.
- **Prédéfini au** (*Preset to*): L'administrateur fixe le numéro de téléphone qui sera utilisé lors de l'appel. Cela permet de renforcer la sécurité en forçant l'autorisation que d'un seul numéro entrant.

La méthode la plus simple pour définir le `sambaMungedDial` est d'utiliser l'utilitaire `usrmgr.exe` de Microsoft. Cependant faites attention de bien utiliser la version 4.0.1371.1 de l'utilitaire.

NOTES



