

**UNIX Kerberos and LDAP Direct Active Directory Authentication**

# Document Control

## Version History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Status | Update Description | Completed by |
| 1.0 | 08/09/2010 | Draft | Draft | Simon Borthwick |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Document References

|  |  |
| --- | --- |
| Title | Document Location |
| UNIX Kerberos and LDAP Direct Active Directory Authentication | http://sharepoint/C17/C6/Direct%20Active%20Directory%20Authen |
|  |  |
|  |  |

## Document Review

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Name | Department/Function |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

This document will be reviewed annually.

## Document Approval

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Name of Approver | Department/Function |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Contents

[1. Document Control 2](#_Toc277159115)

[1.1. Version History 2](#_Toc277159116)

[1.2. Document References 2](#_Toc277159117)

[1.3. Document Review 2](#_Toc277159118)

[1.4. Document Approval 2](#_Toc277159119)

[2. Introduction 5](#_Toc277159120)

[2.1. Purpose of this Document 5](#_Toc277159121)

[2.2. Scope 5](#_Toc277159122)

[3. Overview of the authentication methodology 6](#_Toc277159123)

[3.1. Overview 6](#_Toc277159124)

[3.2. Access restrictions 6](#_Toc277159125)

[3.3. Limitations 6](#_Toc277159126)

[4. Active Directory Users, Groups & Computers 7](#_Toc277159127)

[4.1. Computer objects 7](#_Toc277159128)

[4.2. Users 7](#_Toc277159129)

[4.3. Bind account 7](#_Toc277159130)

[4.4. UNIX groups 7](#_Toc277159131)

[4.5. Server Access Groups 8](#_Toc277159132)

[5. Kerberos 9](#_Toc277159133)

[5.1. Kerberos keytab 9](#_Toc277159134)

[6. LDAP 10](#_Toc277159135)

[6.1. Attribute mapping 10](#_Toc277159136)

[6.2. User locations 10](#_Toc277159137)

[6.2.1. Restrict to users in specified server access group 10](#_Toc277159138)

[7. PAM 11](#_Toc277159139)

[8. Home Directories 12](#_Toc277159140)

[8.1. Port for mountd 12](#_Toc277159141)

[9. Firewall rules 13](#_Toc277159142)

[9.1. AD/LDAP/Kerberos 13](#_Toc277159143)

[9.2. Automounted home directories 13](#_Toc277159144)

[10. Implementation 14](#_Toc277159145)

[11. Active Directory 15](#_Toc277159146)

[11.1. Launching Active Directory Users & Computers snap-in as a different user 15](#_Toc277159147)

[11.2. Users and UNIX groups within Active Directory 15](#_Toc277159148)

[11.3. Computer and Server Access Group objects within Active Directory 16](#_Toc277159149)

[11.3.1. Create the Kerberos key for the new computer object 17](#_Toc277159150)

[12. DNS 19](#_Toc277159151)

[13. UNIX/Linux - Scripted 20](#_Toc277159152)

[14. UNIX/Linux - Manual 21](#_Toc277159153)

[14.1. Kerberos & LDAP configuration 21](#_Toc277159154)

[14.1.1. Solaris 10 21](#_Toc277159155)

[14.1.2. Solaris 9 23](#_Toc277159156)

[14.1.3. Solaris 8 23](#_Toc277159157)

[14.1.4. Red Hat 4 25](#_Toc277159158)

[14.1.5. Red Hat 5 27](#_Toc277159159)

[14.2. UNIX/Linux Server automounter configuration 29](#_Toc277159160)

[14.2.1. Red Hat 4 30](#_Toc277159161)

[14.2.2. Red Hat 5 30](#_Toc277159162)

# Introduction

## Purpose of this Document

This document summarises the proposed design and implementation steps for implementing direct active directory authentication from the Solaris and Red Hat hosts within the estate managed by TSG UNIX & Storage.

## Scope

The scope of this document is to describe the design by which a user within active directory can be permissioned to have command line login access to a UNIX host. The document will describe the active directory group layout and the UNIX configuration to allow this authentication.

Password changing for a user will still occur from within Windows and is out of scope for this proposal.

The document will assume that the required UNIX schema extensions have already been applied to the directory.

# Overview of the authentication methodology

## Overview

The authentication from UNIX to active directory will involve the use of both Kerberos and LDAP.

Kerberos will be used to perform the password exchange and authentication between the UNIX host and the active directory domain controller.

LDAP will be used to retrieve both user and group information from the directory.

## Access restrictions

Access will be restricted to a specified set of users through the use of server access groups. A group will be created in active directory per UNIX server, this group will contain all the user accounts which are allowed to login.

The LDAP configuration will specify that only users in the specified group have accounts on the server.

Using PAM to ensure the user must have a valid account before login is granted will ensure that the access is restricted.

## Limitations

Solaris 9 hosts cannot be authenticated directly to Active Directory. This is due to the Kerberos implantation in Solaris 9 being incompatible with the Kerberos key type used by Active Directory.

# Active Directory Users, Groups & Computers

## Computer objects

Each UNIX server will require a computer object to be created for it within Active Directory. These objects will be named to match the hostname of the UNIX server and will be placed in the following Organisational Unit:

uk.icap.com/Servers/Unix

## Users

In line with the Windows server logins, any user who requires access to a UNIX server will be allocated an admin account within Active Directory (distinguished by a –a at the end of the username). This username will be in lowercase only.

Each user account will be allocated a unique UID through the ‘Unix Attributes’ tab. These will be allocated sequentially starting at UID 8500.

## Bind account

LDAP requires that an account exists with Active Directory that it can use to bind to it. This account is created with Domain Guest access. The account used for this is:

uk.icap.com/Admin/User Administrative Accounts/Unix/unixbind

## UNIX groups

UNIX groups will be created within the Active Directory. These groups will be allocated a unique GID through the ‘Unix Attributes’ tab. These will be allocated sequentially starting at GID 4000.

A Unix\_Users group will be created with GID 4000. All users with access to a UNIX server will be a member of this group and this group will be allocated as their primary group through the ‘Unix Attributes’ tab of the user.

Additional groups of Unix\_Admins (for members of LDN UNIX & Storage) and Unix\_Ops (for members of LDN ASD Operations) will be created.

A unique Unix\_<application> group will be created for each application (ETC, GUIBOS etc) hosted on a UNIX server.

In addition to the Unix\_Users group a user will be allocated to at least one other Unix\_ group as a secondary group.

Adding a secondary group to a user will be performed by editing the group and adding the user to the default members list (‘Members’ tab) and also to the members list within the ‘Unix attributes’ tab.

The UNIX groups will be created within the following Organisational Unit

uk.icap.com/Admin/Unix Server Access Groups

## Server Access Groups

Each UNIX host will have a corresponding access group created for it. The naming convention will be LU\_<servername> (where LU stands for Local User)

These groups will be created within the following Organisational Unit:

uk.icap.com/ICAP Servers/Groups

Individual users will not be added to these groups. The Unix\_<xxx> groups will be added into these access groups and user membership will be controlled through their membership of an appropriate Unix\_<xxx> group.

# Kerberos

## Kerberos keytab

In order for the UNIX host to connect to Active Directory using Kerberos to perform authentication a Kerberos key needs to have been set up between the two.

The key will be created by running the ktpass command from one of the LDN BIT management servers:

uk0winfapp01p

uk0winfapp02p

uk0winfapp03p

The command to create the key is:

ktpass -out c:\<*HOST*>.out /rndpass -princ host/<*FQDN*>@UK.ICAP.COM -mapuser <*HOST*>$@UK.ICAP.COM -ptype KRB5\_NT\_SRV\_HST

Where:

HOST = Short name for host

FQDN = Fully qualified name for host

# LDAP

## Attribute mapping

LDAP will be configured to map UNIX user and group attributes onto the appropriate attributes within the Active Directory schema.

The mappings in use are:

group:userpasswprd=userPassword

group:memberuid=memberUid

group:gidnumber=gidNumber

passwd:gecos=cn

passwd:gidnumber=gidNumber

passwd:uidnumber=uidNumber

passwd:uid=sAMAccountName

passwd:homedirectory=unixHomeDirectory

passwd:loginshell=loginShell

shadow:shadowflag=shadowFlag

shadow:userpassword=userPassword

shadow:uid=sAMAccountName

## User locations

LDAP will be configured to locate users within the following Active Directory Organisation Unit:

uk.icap.com/Department

### Restrict to users in specified server access group

The restriction will be performed by using the memberOf attribute. The attribute will be set to only allow users access who belong to a group:

uk.icap.com/ICAP Servers/Groups/LU\_<servername>

Additionally OID 1.2.840.113556.1.4.1941 will be used with the memberOf attribute. This enables a recursive group search within the Active Directory, this allows the use of nested groups.

# PAM

Additional entries will be added to PAM to enable Kerberos as the login and auth provider and LDAP as the account provider.

Ordering of the entries within PAM is significant. The Kerberos and LDAP options will be placed after the local account entries. This will allow local accounts to be used if the active directory is not available.

# Home Directories

User home directories will continue to be hosts from the UNIX infrastructure servers uk0linfapp01p and uk1linfapp01p.

For each active directory user with UNIX access (therefore a member of the Unix\_Users group) they will have a home directory of /export/home/<username>

These home areas are NFS exported.

A comment auto\_home configuration for the automounter will be managed by Puppet and will mount the /export/home share onto /home on a local server.

Therefore within the active directory ‘Unix attributes’ tab for a user their home directory will be specified as /home/<username>

## Port for mountd

In order to allow the TCP port for mountd to be opened through firewalls the NFS configuration on the two management servers (uk0linfapp01p/uk1linfapp01p) has been updated. The MOUNTD\_PORT option has been set to 892 within /etc/sysconfig/nfs

# Firewall rules

In order for any DMZ hosts to be able to authenticate via AD and automount user’s home directories the following firewall rules are required. In all cases the source is the DMZ host

## AD/LDAP/Kerberos

TCP/389, TCP/636, TCP/88 to all domain controllers

## Automounted home directories

TCP/2049, TCP/892 to admin servers

# Implementation

The following sections describe the full procedure for attaching a new host to Active Directory.

Sections 10 & 11 must be completed

Either section 12 or section 13 needs to be completed.

# Active Directory

This section details the exact steps required to configure the different versions of Solaris and Red Hat.

## Launching Active Directory Users & Computers snap-in as a different user

From an XP workstation the Active Directory Users & Computers snap-in can be launched as a different user by running the following from a command prompt:

runas /user:*username*@uk.icap.com "mmc dsa.msc"

## Users and UNIX groups within Active Directory

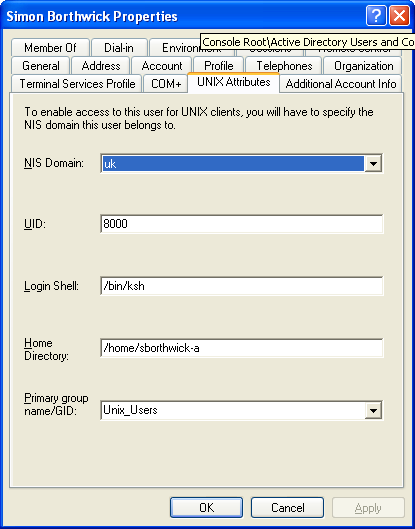
This section covers provisioning UNIX access to user accounts

For user and group IDs to use the ‘AD User and Group IDs’ Excel spreadsheet must be consulted and updated.

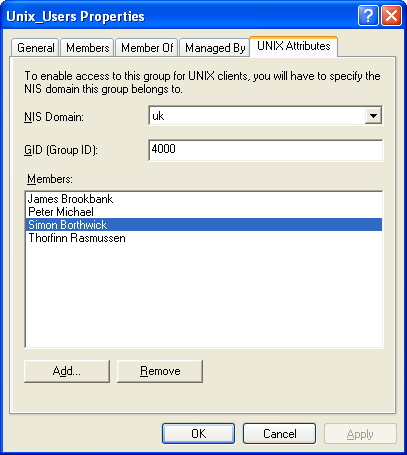
1. Create admin accounts (-a) for each user that will need to connect – Note: the account name must be in lower case
2. For each –a account edit its properties and ensure the values are completed within the ‘UNIX Attributes’ tab:

* NIS Domain – *uk*
* UID – *Next in list from spreadsheet*
* Login Shell - */bin/bash*
* Home Directory - */adhome/<userid>*
* Primary Group name/GID: *Unix\_Users*

(Note: All user’s primary group must be set to Unix\_Users any other required Unix groups will be added as secondary groups)



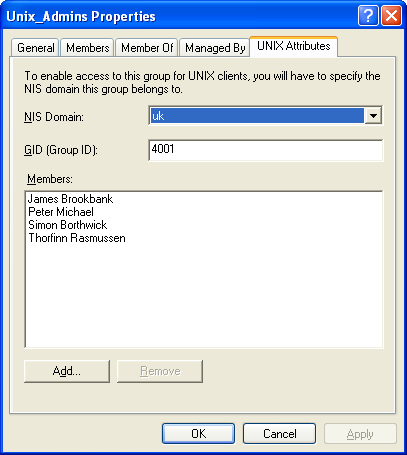
1. Edit the properties of uk.icap.com/Admin/Unix Server Access Groups/Unix\_Users
   1. Add the new user to the group ‘Members’
   2. In the UNIX Attributes tab add the user to the ‘Members’ list



1. If not already present, create the relevant application Unix group (Unix\_<application>) within the uk.icap.com/Admin/Unix Server Access Groups OU.
   1. Edit the properties of the new group and in the ‘UNIX attributes’ tab set:

* NIS Domain – *uk*
* GID (Group ID) – *Next in list from spreadsheet*

1. Edit the properties of the relevant Unix application group (the one created in step 4 if it is not already present).
   1. Add the new user to the group ‘Members’
   2. In the UNIX Attributes tab add the user to the ‘Members’ list

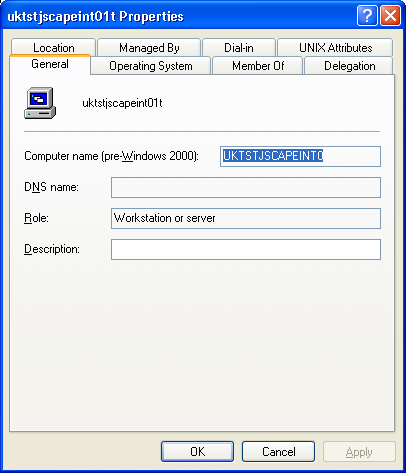


## Computer and Server Access Group objects within Active Directory

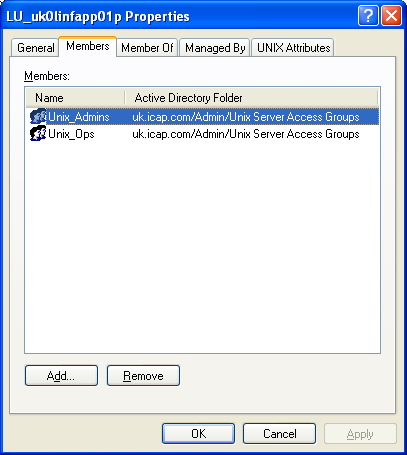
This section covers the provisioning of the required objects to attach a UNIX server into Active Directory

1. Create a computer object (with the same name as the UNIX host) in the uk.icap.com/Servers/Unix OU

NOTE: If the computer name is more than 15 characters in length – Create the computer account using the full length name however take a note of the ‘Computer name (pre-Windows 2000)’ value which will be needed when using ktpass



1. Create a new group (to be used as the server access group). The name must be LU\_<servername> and the objects must be created in the uk.icap.com/ICAP Server/Groups OU.
   1. Add Unix\_Admins and Unix\_Ops to the list of members
   2. Add any other Unix\_<xxx> groups to the members list which will require access



### Create the Kerberos key for the new computer object

1. Log into the BIT management server uk0winfapp02p
2. Open PowerShell
3. Change directory to C:\Unix
4. Run:

.\Unix\_ktpass.ps1 <servername>

NOTE: If the servername is more than 15 characters in length then the ‘Pre-Windows 2000’ name noted in 10.3 will need to be used instead of the full name

1. This will generate Kerberos key C:\Unix\<servername>.out
2. Use C:\Unix\pscp.exe to copy the Kerberos key to a temporary location on the UNIX admin server (uk0linfapp01p)

# DNS

Ensure that the server is in DNS for both forward and reverse lookups.

# UNIX/Linux - Scripted

This section uses a script to attach the host to Active Directory. To perform the connection manually refer to section 9.4 (UNIX/Linux – Manual)

Note: Step 1 & 2 should already be configured if the server is running puppet

**WARNING:** If the automatic configuration fails it may leave the server in a state where you are unable to login a new session. Therefore open a session on the server and leave this open while running the attach script from a different session.

**NOTE:** Due to the potential time for AD to replicate between all DCs, this stage should only be performed 30 minutes or more after the objects have been created in AD.

1. Ensure NTP is configured and running (a time difference between client and DC will stop Kerberos authentication from functioning)
2. Configure /etc/resolv.conf
3. Ensure the Kerberos key file generated in 9.1.3.1 is located on uk0linfapp01p
4. On uk0linfapp01p run:

/admin/AD/bin/configure\_ad.sh <host> <path\_to\_keytab\_file>

1. Test SSH connectivity to the host using an AD user.

# UNIX/Linux - Manual

This method performs all of the steps manually to attach a server to Active Directory. This section does not need to be completed if section 9.3 (UNIX/Linux – Scripted) has been performed.

## Kerberos & LDAP configuration

### Solaris 10

1. Ensure NTP is configured and running (a time difference between client and DC will stop Kerberos authentication from functioning)
2. Edit /etc/krb5/krb5.conf

[libdefaults]

default\_realm = UK.ICAP.COM

dns\_lookup\_realm = false

dns\_lookup\_kdc = false

default\_tkt\_enctypes = des-cbc-md5 des-cbc-crc

default\_tgs\_enctypes = des-cbc-md5 des-cbc-crc

[realms]

UK.ICAP.COM = {

kdc = uk.icap.com:88

admin\_server = uk.icap.com:749

kpasswd\_server = uk.icap.com:464

kpasswd\_protocol = SET\_CHANGE

default\_domain = uk.icap.com

}

[domain\_realm]

\*.uk.icap.com = UK.ICAP.COM

.uk.icap.com = UK.ICAP.COM

[logging]

default = FILE:/var/krb5/kdc.log

kdc = FILE:/var/krb5/kdc.log

kdc\_rotate = {

period = 1d

versions = 10

}

[appdefaults]

kinit = {

renewable = true

forwardable= true

}

1. Copy Kerberos key file to /etc/krb5/krb5.keytab
2. Change owner of keytab file to root and permissions 600
3. Update /etc/nsswitch.ldap and /etc/nsswitch.conf
   1. Change hosts and ipnodes lines to read files dns
4. Configure /etc/resolv.conf
5. Ensure the ktkt\_warn service is enabled
6. Test Kerberos
   1. Run kinit <user> (using a user that exists in AD)
   2. Run klist –k to list keys
7. Start DNS client
8. Ldapclient – Use either option a or b
   1. Copy from uk0linfapp01p /admin/scripts/ldap/ ldap\_add\_sol910.sh to the server then run using:

ldap\_add\_sol89.sh <servername>

* 1. Run the following:

ldapclient manual \

-a credentialLevel=proxy \

-a authenticationMethod=simple \

-a “proxyDN=cn=unixbind,ou=Unix,ou=User Administrative Accounts,ou=Admin,dc=uk,dc=icap,dc=com” \

-a proxyPassword=<TSGone> \

-a defaultSearchBase=dc=uk,dc=icap,dc=com \

-a domainName=uk.icap.com \

-a "defaultServerList=uk.icap.com" \

-a defaultSearchScope=sub \

-a attributeMap=group:userpasswprd=userPassword \

-a attributeMap=group:memberuid=memberUid \

-a attributeMap=group:gidnumber=gidNumber \

-a attributeMap=passwd:gecos=cn \

-a attributeMap=passwd:gidnumber=gidNumber \

-a attributeMap=passwd:uidnumber=uidNumber \

-a attributeMap=passwd:uid=sAMAccountName \

-a attributeMap=passwd:homedirectory=unixHomeDirectory \

-a attributeMap=passwd:loginshell=loginShell \

-a attributeMap=shadow:shadowflag=shadowFlag \

-a attributeMap=shadow:userpassword=userPassword \

-a attributeMap=shadow:uid=sAMAccountName \

-a objectClassMap=group:posixGroup=group \

-a objectClassMap=passwd:posixAccount=user \

-a objectClassMap=shadow:shadowAccount=user \

-a “serviceSearchDescriptor=passwd: dc=uk,dc=icap,dc=com?sub?memberOf:1.2.840.113556.1.4.1941:= cn=LU\_<servername>,ou=Groups,ou=ICAP Server,dc=uk,dc=icap,dc=com” \

-a “serviceSearchDescriptor=shadow:dc=uk,dc=icap,dc=com?sub?memberOf:1.2.840.113556.1.4.1941:=cn=LU\_<servername>,ou=Groups,ou=ICAP Server,dc=uk,dc=icap,dc=com” \

-a “serviceSearchDescriptor=group:ou=Unix Server Access Groups,ou=Admin, dc=uk,dc=icap,dc=com?sub”

1. Enable LDAP client
2. Update pam.conf sections as follows:

login auth requisite pam\_authtok\_get.so.1

login auth required pam\_dhkeys.so.1

login auth required pam\_unix\_cred.so.1

login auth sufficient pam\_unix\_auth.so.1

login auth sufficient pam\_krb5.so

login auth required pam\_dial\_auth.so.1

other auth requisite pam\_authtok\_get.so.1

other auth required pam\_dhkeys.so.1

other auth required pam\_unix\_cred.so.1

other auth sufficient pam\_unix\_auth.so.1

other auth sufficient pam\_krb5.so.1

other account requisite pam\_roles.so.1

other account sufficient pam\_unix\_account.so.1

other account required pam\_ldap.so.1

### Solaris 9

Solaris 9 cannot be authenticated directly to Active Directory. This is due to Solaris 9 not being compatible with the Kerberos key type generated by Active Directory.

### Solaris 8

1. Ensure NTP is configured and running (a time difference between client and DC will stop Kerberos authentication from functioning)
2. Edit /etc/krb5/krb5.conf

[libdefaults]

default\_realm = UK.ICAP.COM

dns\_lookup\_realm = false

dns\_lookup\_kdc = false

default\_tkt\_enctypes = des-cbc-md5 des-cbc-crc

default\_tgs\_enctypes = des-cbc-md5 des-cbc-crc

[realms]

UK.ICAP.COM = {

kdc = uk.icap.com:88

admin\_server = uk.icap.com:749

kpasswd\_server = uk.icap.com:464

kpasswd\_protocol = SET\_CHANGE

default\_domain = uk.icap.com

}

[domain\_realm]

\*.uk.icap.com = UK.ICAP.COM

.uk.icap.com = UK.ICAP.COM

[logging]

default = FILE:/var/krb5/kdc.log

kdc = FILE:/var/krb5/kdc.log

kdc\_rotate = {

period = 1d

versions = 10

}

[appdefaults]

kinit = {

renewable = true

forwardable= true

}

1. Copy Kerberos key file to /etc/krb5/krb5.keytab
2. Change owner of keytab file to root and permissions 600
3. Update /etc/nsswitch.ldap and /etc/nsswitch.conf
   1. Change hosts and ipnodes lines to read files dns
4. Configure /etc/resolv.conf
5. Ensure that the following entry is present in /etc/inetd.conf

100134/1 tli rpc/ticotsord wait root /usr/lib/krb5/ktkt\_warnd ktkt\_warnd

1. Test Kerberos
   1. Run kinit <user> (using a user that exists in AD)
   2. Run klist –k to list keys
2. Ldapclient – Use either option a or b
   1. Copy from uk0linfapp01p /admin/scripts/ldap/ ldap\_add\_sol8.sh to the server then run using:

ldap\_add\_sol89.sh <servername>

* 1. Run the following:

ldapclient -i \

-v proxy \

-a simple \

-D “cn=unixbind,ou=Unix,ou=User Administrative Accounts,ou=Admin,dc=uk,dc=icap,dc=com” \

-w <TSGone> \

-b dc=uk,dc=icap,dc=com \

-d uk.icap.com \

-s sub \

-R group:userpasswprd=userPassword \

-R group:memberuid=memberUid \

-R group:gidnumber=gidNumber \

-R passwd:gecos=cn \

-R passwd:gidnumber=gidNumber \

-R passwd:uidnumber=uidNumber \

-R passwd:uid=sAMAccountName \

-R passwd:homedirectory=unixHomeDirectory \

-R passwd:loginshell=loginShell \

-R shadow:shadowflag=shadowFlag \

-R shadow:userpassword=userPassword \

-R shadow:uid=sAMAccountName \

-M group:posixGroup=group \

-M passwd:posixAccount=user \

-M shadow:shadowAccount=user \

-S \ “passwd:ou=dc=uk,dc=icap,dc=com?sub?memberOf:1.2.840.113556.1.4.1941:= cn=LU\_<servername>,ou=Groups,ou=ICAP Server,dc=uk,dc=icap,dc=com” \

-S \ “shadow:ou=dc=uk,dc=icap,dc=com?sub?memberOf:1.2.840.113556.1.4.1941:= cn=LU\_<servername>,ou=Groups,ou=ICAP Server,dc=uk,dc=icap,dc=com” \

-S “group:ou=ou=Unix Server Access Groups,ou=Admin,dc=uk,dc=icap,dc=com?sub” \

uk.icap.com

1. Update pam.conf sections as follows:

login auth requisite pam\_authtok\_get.so.1

login auth required pam\_dhkeys.so.1

login auth sufficient pam\_unix\_auth.so.1

login auth sufficient pam\_krb5.so

login auth required pam\_dial\_auth.so.1

other auth requisite pam\_authtok\_get.so.1

other auth required pam\_dhkeys.so.1

other auth sufficient pam\_unix\_auth.so.1

other auth sufficient pam\_krb5.so.1

other account requisite pam\_roles.so.1

other account sufficient pam\_unix\_account.so.1

other account required pam\_ldap.so.1

### Red Hat 4

1. Ensure NTP is configured and running (a time difference between client and DC will stop Kerberos authentication from functioning)
2. Ensure client is configured in DNS (including reverse lookup)
3. Configure /etc/resolv.conf
4. Edit /etc/krb5.conf

[logging]

default = FILE:/var/log/krb5libs.log

kdc = FILE:/var/log/krb5kdc.log

admin\_server = FILE:/var/log/kadmind.log

[libdefaults]

default\_realm = UK.ICAP.COM

dns\_lookup\_realm = false

dns\_lookup\_kdc = false

default\_tkt\_enctypes = des-cbc-md5 des-cbc-crc

default\_tgs\_enctypes = des-cbc-md5 des-cbc-crc

[realms]

UK.ICAP.COM = {

kdc = uk.icap.com:88

admin\_server = uk.icap.com:749

kpasswd\_server = uk.icap.com:464

kpasswd\_protocol = SET\_CHANGE

default\_domain = uk.icap.com

}

[domain\_realm]

\*.uk.icap.com = UK.ICAP.COM

.uk.icap.com = UK.ICAP.COM

1. Create new computer object in AD
2. Create new Kerberos key using ktpass
3. Copy newly create key file to the Linux host called /etc/krb5.keytab
4. Change owner of keytab file to root and permissions 600
5. Test Kerberos
   1. Run kinit <user> (using a user that exists in AD)
   2. Run klist –k to list keys
6. Update /etc/nsswitch.conf
   1. Change hosts line to read files dns
   2. Change passwd and group lines to read files ldap [TRYAGAIN=continue]
7. Set /etc/ldap.conf to the following:

host uk.icap.com

base dc=uk,dc=icap,dc=com

uri ldap://uk.icap.com/

binddn cn=unixbind,ou=Unix,ou=User Administrative Accounts,ou=Admin,dc=uk,dc=icap,dc=com

bindpw <TSGone>

scope sub

pam\_filter objectclass=user

pam\_login\_attribute sAMAccountName

pam\_member\_attribute memberOf

pam\_password ad

nss\_base\_passwd dc=uk,dc=icap,dc=com?sub?memberOf:1.2.840.113556.1.4.1941:=cn=LU\_<servername>,ou=Groups,ou=ICAP Server,dc=uk,dc=icap,dc=com

nss\_base\_shadow dc=uk,dc=icap,dc=com?sub?memberOf:1.2.840.113556.1.4.1941:=cn=LU\_<servername>,ou=Groups,ou=ICAP Server,dc=uk,dc=icap,dc=com

nss\_base\_group ou=Unix Server Access Groups,ou=Admin,dc=uk,dc=icap,dc=com?sub

nss\_initgroups\_ignoreusers \ root,ldap,named,avahi,haldaemon,dbus,radvd,tomcat,radiusd,news,mailman,nscd,gdm

nss\_map\_objectclass posixAccount user

nss\_map\_objectclass shadowAccount user

nss\_map\_attribute uid sAMAccountName

nss\_map\_attribute uidNumber uidNumber

nss\_map\_attribute gidNumber gidNumber

nss\_map\_attribute homeDirectory unixHomeDirectory

nss\_map\_attribute loginShell loginShell

nss\_map\_attribute uniqueMember posixMember

nss\_map\_attribute memberUid memberUid

nss\_map\_objectclass posixGroup Group

1. If nscd is in use
   1. update /etc/nscd.conf

enable-cache passwd yes

positive-time-to-live passwd 10

negative-time-to-live passwd 10

enable-cache group yes

positive-time-to-live group 10

negative-time-to-live group 10

enable-cache hosts yes

positive-time-to-live hosts 10

negative-time-to-live hosts 10

1. Update /etc/pam.d/system-auth sections as follows:

auth required /lib/security/$ISA/pam\_env.so

auth sufficient /lib/security/$ISA/pam\_unix.so likeauth nullok

auth sufficient /lib/security/$ISA/pam\_krb5.so

auth required /lib/security/$ISA/pam\_deny.so

account sufficient /lib/security/$ISA/pam\_ldap.so

account required /lib/security/$ISA/pam\_unix.so

account sufficient /lib/security/$ISA/pam\_succeed\_if.so uid < 100 quiet

account required /lib/security/$ISA/pam\_permit.so

password requisite /lib/security/$ISA/pam\_cracklib.so retry=3

password sufficient /lib/security/$ISA/pam\_unix.so nullok use\_authtok md5 shadow

password required /lib/security/$ISA/pam\_deny.so

session required /lib/security/$ISA/pam\_limits.so

session required /lib/security/$ISA/pam\_unix.so

### Red Hat 5

1. Ensure NTP is configured and running (a time difference between client and DC will stop Kerberos authentication from functioning)
2. Ensure client is configured in DNS (including reverse lookup)
3. Configure /etc/resolv.conf
4. Edit /etc/krb5.conf

[logging]

default = FILE:/var/log/krb5libs.log

kdc = FILE:/var/log/krb5kdc.log

admin\_server = FILE:/var/log/kadmind.log

[libdefaults]

default\_realm = UK.ICAP.COM

dns\_lookup\_realm = false

dns\_lookup\_kdc = false

default\_tkt\_enctypes = des-cbc-md5 des-cbc-crc

default\_tgs\_enctypes = des-cbc-md5 des-cbc-crc

[realms]

UK.ICAP.COM = {

kdc = uk.icap.com:88

admin\_server = uk.icap.com:749

kpasswd\_server = uk.icap.com:464

kpasswd\_protocol = SET\_CHANGE

default\_domain = uk.icap.com

}

[domain\_realm]

\*.uk.icap.com = UK.ICAP.COM

.uk.icap.com = UK.ICAP.COM

1. Create new computer object in AD
2. Create new Kerberos key using ktpass
3. Copy newly create key file to the Linux host called /etc/krb5.keytab
4. Change owner of keytab file to root and permissions 600
5. Test Kerberos
   1. Run kinit <user> (using a user that exists in AD)
   2. Run klist –k to list keys
6. Update /etc/nsswitch.conf
   1. Change hosts line to read files dns
   2. Change passwd and group lines to read files ldap [TRYAGAIN=continue]
7. Set /etc/ldap.conf to the following:

host uk.icap.com

base dc=uk,dc=icap,dc=com

uri ldap://uk.icap.com/

binddn cn=unixbind,ou=Unix,ou=User Administrative Accounts,ou=Admin,dc=uk,dc=icap,dc=com

bindpw <TSGone>

scope sub

pam\_filter objectclass=user

pam\_login\_attribute sAMAccountName

pam\_member\_attribute memberOf

pam\_password ad

nss\_base\_passwd dc=uk,dc=icap,dc=com?sub?memberOf:1.2.840.113556.1.4.1941:=cn=LU\_<servername>,ou=Groups,ou=ICAP Server,dc=uk,dc=icap,dc=com

nss\_base\_shadow dc=uk,dc=icap,dc=com?sub?memberOf:1.2.840.113556.1.4.1941:=cn=LU\_<servername>,ou=Groups,ou=ICAP Server,dc=uk,dc=icap,dc=com

nss\_base\_group ou=Unix Server Access Groups,ou=Admin,dc=uk,dc=icap,dc=com?sub

nss\_initgroups\_ignoreusers \ root,ldap,named,avahi,haldaemon,dbus,radvd,tomcat,radiusd,news,mailman,nscd,gdm

nss\_map\_objectclass posixAccount user

nss\_map\_objectclass shadowAccount user

nss\_map\_attribute uid sAMAccountName

nss\_map\_attribute uidNumber uidNumber

nss\_map\_attribute gidNumber gidNumber

nss\_map\_attribute homeDirectory unixHomeDirectory

nss\_map\_attribute loginShell loginShell

nss\_map\_attribute uniqueMember posixMember

nss\_map\_attribute memberUid memberUid

nss\_map\_objectclass posixGroup Group

1. If nscd is in use
   1. update /etc/nscd.conf

enable-cache passwd yes

positive-time-to-live passwd 10

negative-time-to-live passwd 10

enable-cache group yes

positive-time-to-live group 10

negative-time-to-live group 10

enable-cache hosts yes

positive-time-to-live hosts 10

negative-time-to-live hosts 10

1. Update /etc/pam.d/system-auth sections as follows:

auth required pam\_env.so

auth sufficient pam\_unix.so nullok try\_first\_pass

auth sufficient pam\_krb5.so

auth required pam\_succeed\_if.so uid >= 500 quiet

auth required pam\_deny.so

account required pam\_unix.so

account sufficient pam\_localuser.so

account required pam\_ldap.so

account sufficient pam\_succeed\_if.so uid < 500 quiet

account required pam\_permit.so

password requisite pam\_cracklib.so minlen=8 lcredit=-1 ucredit=-1 dcredit=-1 ocredit=-1 retry=3 type=

password sufficient pam\_unix.so md5 shadow nis nullok try\_first\_pass use\_authtok

password required pam\_deny.so

session optional pam\_keyinit.so revoke

session required pam\_limits.so

session [success=1 default=ignore] pam\_succeed\_if.so service in crond quiet use\_uid

session required pam\_unix.so

## UNIX/Linux Server automounter configuration

The automounter needs to be configured to ensure that the user’s home directories will be mounted under /home

1. Edit /etc/auto\_master. Ensure that the following line is present:

/home /etc/auto\_home -nobrowse

1. Edit /etc/auto.master and ensure it contains the following:

+auto\_master

1. Edit /etc/auto\_home and ensure it contains:

\* ukadmin:/export/home/&

### Red Hat 4

Check that the UNDERSCORETODOT value is set to 0 in /etc/sysconfig/autofs

### Red Hat 5

Check that the DEFAULT\_MASTER\_MAP\_NAME in /etc/sysconfig/autofs is set to auto\_master

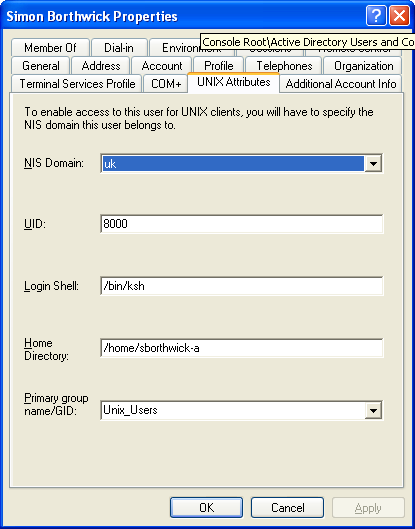
# Adding a new user to existing groups

If a new team member joins an existing (in terms of AD group) team, the following steps need to be followed to add the user:

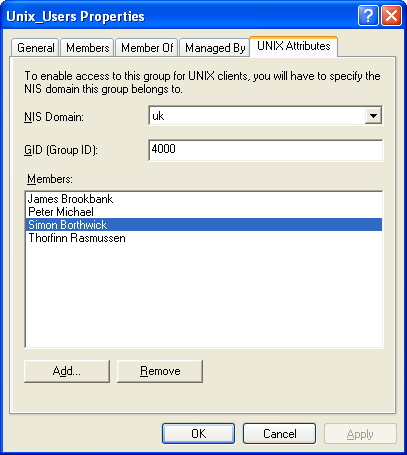
1. Create admin accounts (-a) for the new user – Note: the account name must be in lower case
2. Edit the properties of the new –a account and ensure the values are completed within the ‘UNIX Attributes’ tab:

* NIS Domain – *uk*
* UID – *Next in list from spreadsheet*
* Login Shell - */bin/bash*
* Home Directory - */adhome/<userid>*
* Primary Group name/GID: *Unix\_Users*

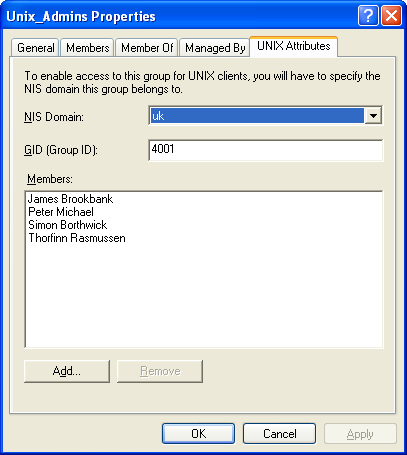
(Note: All user’s primary group must be set to Unix\_Users any other required Unix groups will be added as secondary groups)



1. Edit the properties of uk.icap.com/Admin/Unix Server Access Groups/Unix\_Users
   1. Add the new user to the group ‘Members’
   2. In the UNIX Attributes tab add the user to the ‘Members’ list



1. Edit the properties of the relevant Unix application group
   1. Add the new user to the group ‘Members’
   2. In the UNIX Attributes tab add the user to the ‘Members’ list



# Removing a UNIX AD user

In the case where a user needs to be removed the following steps must be followed:

1. Edit the properties of all Unix application groups (Unix\_<app>) that the user belongs to
   1. In the Members tab remove the user
   2. In the UNIX Attributes tab remove the user from the ‘Members’ list