Document number	Revision
DOCU12211	1

Active Directory (Ldap) usergroup and user replication

Active Directory

Active directory (newer versions) allows groups to contain groups (sub-groups). Highstage eliminates recursive groups (Active directory weakness?). Recursion will occur if a sub-group refers to a parent group. Highstage will maintain a strict hierarchy, child group references to parent group(s) will be ignored. Active Directory primary group property will also be handled.

TS parameters

These are the TS parameters relevant for ActiveDirectory (Ldap) replication. Parameters may be checked/set from this page.

Name	Type	Values	Description
Domain	Text	Free text	Default domain name for Ldap lookup etc. If blank then the domain of the IIS process identity will be used.
LdapUserId	Text	Free text	User name for ActiveDirectory (LDAP server) authentication.
LdapPassword	Text	Free text	Password for ActiveDirectory (LDAP server) authentication.
			Ideally this be will just one group containing all groups and users. But experience say that different responsibilities exists for Active Directory (LDAP) maintenance and Highstage parameter maintenance. So the administration burden is most often delegated to Highstage administrators due to finance/IT department decisions.

Name	Type	Values	Description
LdapUserGroups	Text	Semicolon delimited list of user groups	In a single domain this parameter will just be a list of semicolon separated user groups. In multi-domain environment the group names may be specified as <domain name><user group> or <server name><user group> The group specifier will be converted to the LDAP path for group lookup: `LPAD://<domain name>` or `LDAP://<server name>` If no group path is specified then the following path will be used: `LDAP://<domain>` *(See the domain parameter)*

Trouble shooting users with no permission to web site

The following reasons may cause a user from not having access to web site:

1. The user is not included in LdapUserGroups.
2. The user has a different Ldap ObjectGUID. This typically happens if user is deleted from Active Directory and then recreated. The user now has a different ObjectGuid. TS keeps track of ObjectGuid to prevent that a new user from getting full access to data belonging to old user with same userID. This ObjectGuid mismatch can be resolved in one of two ways, depending on collision cause, see below.

Resolving that ObjectGuid mismatch which is due to account has been administrative deleted and recreated by IT personal, but the user is the same physical person:

1. Clear the user ObjectGuid from this page, you must be running as AdminWrite to be able to clear ObjectGuid.
2. Run Ldap replication.

Resolving that ObjectGuid mismatch which is due to old employee has left company and new employee with same userID has joined the company:

1. Rename old employees UserID from this page.
2. Run Ldap replication.