Full credit is given to the above companies including the OS that this PDF file was generated!

Red Hat Enterprise Linux Release 9.2 Manual Pages on 'sssd-ldap-attributes.5' command

$ man sssd-ldap-attributes.5

SSSD-LDAP-ATTRIBUT(5) File Formats and Conventions SSSD-LDAP-ATTRIBUT(5)

NAME

sssd-ldap-attributes - SSSD LDAP Provider: Mapping Attributes

DESCRIPTION

This manual page describes the mapping attributes of SSSD LDAP provider sssd-ldap(5). Refer to the sssd-ldap(5) manual page for full details about SSSD LDAP provider configuration options.

USER ATTRIBUTES

ldap_user_object_class (string)

The object class of a user entry in LDAP.

Default: posixAccount

ldap_user_name (string)

The LDAP attribute that corresponds to the user's login name.

Default: uid (rfc2307, rfc2307bis and IPA), sAMAccountName (AD)

ldap_user_uid_number (string)

The LDAP attribute that corresponds to the user's id.

Default: uidNumber

ldap_user_gid_number (string)

The LDAP attribute that corresponds to the user's primary group id.

Default: gidNumber

ldap_user_primary_group (string)

Active Directory primary group attribute for ID-mapping. Note that this attribute should only be set manually if you are running the

?ldap? provider with ID mapping.

Default: unset (LDAP), primaryGroupID (AD)

ldap_user_gecos (string)

The LDAP attribute that corresponds to the user's gecos field.

Default: gecos

ldap_user_home_directory (string)

The LDAP attribute that contains the name of the user's home directory.

Default: homeDirectory (LDAP and IPA), unixHomeDirectory (AD)

ldap_user_shell (string)

The LDAP attribute that contains the path to the user's default shell.

Default: loginShell

ldap_user_uuid (string)

The LDAP attribute that contains the UUID/GUID of an LDAP user object.

Default: not set in the general case, objectGUID for AD and ipaUniqueID for IPA

ldap_user_objectsid (string)

The LDAP attribute that contains the objectSID of an LDAP user object. This is usually only necessary for ActiveDirectory servers.

Default: objectSid for ActiveDirectory, not set for other servers.

ldap_user_modify_timestamp (string)

The LDAP attribute that contains timestamp of the last modification of the parent object.

Default: modifyTimestamp

ldap_user_shadow_last_change (string)

When using ldap_pwd_policy=shadow, this parameter contains the name of an LDAP attribute corresponding to its shadow(5) counterpart (date of the last password change).

Default: shadowLastChange

ldap_user_shadow_min (string)

When using ldap_pwd_policy=shadow, this parameter contains the name

of an LDAP attribute corresponding to its shadow(5) counterpart (minimum password age).

Default: shadowMin

ldap_user_shadow_max (string)

When using ldap_pwd_policy=shadow, this parameter contains the name of an LDAP attribute corresponding to its shadow(5) counterpart (maximum password age).

Default: shadowMax

ldap_user_shadow_warning (string)

When using ldap_pwd_policy=shadow, this parameter contains the name of an LDAP attribute corresponding to its shadow(5) counterpart (password warning period).

Default: shadowWarning

ldap_user_shadow_inactive (string)

When using ldap_pwd_policy=shadow, this parameter contains the name of an LDAP attribute corresponding to its shadow(5) counterpart (password inactivity period).

Default: shadowInactive

ldap_user_shadow_expire (string)

When using ldap_pwd_policy=shadow or ldap_account_expire_policy=shadow, this parameter contains the name of an LDAP attribute corresponding to its shadow(5) counterpart (account expiration date).

Default: shadowExpire

ldap_user_krb_last_pwd_change (string)

When using ldap_pwd_policy=mit_kerberos, this parameter contains the name of an LDAP attribute storing the date and time of last password change in kerberos.

Default: krbLastPwdChange

ldap_user_krb_password_expiration (string)

When using ldap_pwd_policy=mit_kerberos, this parameter contains the name of an LDAP attribute storing the date and time when current password expires.

Default: krbPasswordExpiration

ldap_user_ad_account_expires (string)

When using ldap_account_expire_policy=ad, this parameter contains the name of an LDAP attribute storing the expiration time of the account.

Default: accountExpires

ldap_user_ad_user_account_control (string)

When using ldap_account_expire_policy=ad, this parameter contains the name of an LDAP attribute storing the user account control bit field.

Default: userAccountControl

ldap_ns_account_lock (string)

When using ldap_account_expire_policy=rhds or equivalent, this parameter determines if access is allowed or not.

Default: nsAccountLock

ldap_user_nds_login_disabled (string)

When using ldap_account_expire_policy=nds, this attribute determines if access is allowed or not.

Default: loginDisabled

ldap_user_nds_login_expiration_time (string)

When using ldap_account_expire_policy=nds, this attribute determines until which date access is granted.

Default: loginDisabled

ldap_user_nds_login_allowed_time_map (string)

When using ldap_account_expire_policy=nds, this attribute determines the hours of a day in a week when access is granted.

Default: loginAllowedTimeMap

ldap_user_principal (string)

The LDAP attribute that contains the user's Kerberos User Principal Name (UPN).

Default: krbPrincipalName

ldap_user_extra_attrs (string)

Comma-separated list of LDAP attributes that SSSD would fetch along

with the usual set of user attributes.

The list can either contain LDAP attribute names only, or colon-separated tuples of SSSD cache attribute name and LDAP attribute name. In case only LDAP attribute name is specified, the attribute is saved to the cache verbatim. Using a custom SSSD attribute name might be required by environments that configure several SSSD domains with different LDAP schemas.

Please note that several attribute names are reserved by SSSD, notably the ?name? attribute. SSSD would report an error if any of the reserved attribute names is used as an extra attribute name.

Examples:

ldap_user_extra_attrs = telephoneNumber

Save the ?telephoneNumber? attribute from LDAP as ?telephoneNumber? to the cache.

ldap_user_extra_attrs = phone:telephoneNumber

Save the ?telephoneNumber? attribute from LDAP as ?phone? to the cache.

Default: not set

ldap_user_ssh_public_key (string)

The LDAP attribute that contains the user's SSH public keys.

Default: sshPublicKey

ldap_user_fullname (string)

The LDAP attribute that corresponds to the user's full name.

Default: cn

ldap_user_member_of (string)

The LDAP attribute that lists the user's group memberships.

Default: memberOf

ldap_user_authorized_service (string)

If access_provider=ldap and ldap_access_order=authorized_service, SSSD will use the presence of the authorizedService attribute in the user's LDAP entry to determine access privilege.

An explicit deny (!svc) is resolved first. Second, SSSD searches for explicit allow (svc) and finally for allow_all (*).

Please note that the ldap_access_order configuration option must include ?authorized_service? in order for the ldap_user_authorized_service option to work.

Some distributions (such as Fedora-29+ or RHEL-8) always include the ?systemd-user? PAM service as part of the login process. Therefore when using service-based access control, the ?systemd-user? service might need to be added to the list of allowed services.

Default: authorizedService

ldap_user_authorized_host (string)

If access_provider=ldap and ldap_access_order=host, SSSD will use the presence of the host attribute in the user's LDAP entry to determine access privilege.

An explicit deny (!host) is resolved first. Second, SSSD searches for explicit allow (host) and finally for allow_all (*).

Please note that the ldap_access_order configuration option must include ?host? in order for the ldap_user_authorized_host option to work.

Default: host

ldap_user_authorized_rhost (string)

If access_provider=ldap and ldap_access_order=rhost, SSSD will use the presence of the rhost attribute in the user's LDAP entry to determine access privilege. Similarly to host verification process.

An explicit deny (!rhost) is resolved first. Second, SSSD searches for explicit allow (rhost) and finally for allow_all (*).

Please note that the ldap_access_order configuration option must include ?rhost? in order for the ldap_user_authorized_rhost option to work.

Default: rhost

ldap_user_certificate (string)

Name of the LDAP attribute containing the X509 certificate of the user.

Default: userCertificate;binary

ldap_user_email (string)

Name of the LDAP attribute containing the email address of the user.

Note: If an email address of a user conflicts with an email address or fully qualified name of another user, then SSSD will not be able to serve those users properly. If for some reason several users need to share the same email address then set this option to a nonexistent attribute name in order to disable user lookup/login by email.

Default: mail

GROUP ATTRIBUTES

ldap_group_object_class (string)

The object class of a group entry in LDAP.

Default: posixGroup

ldap_group_name (string)

The LDAP attribute that corresponds to the group name.

Default: cn (rfc2307, rfc2307bis and IPA), sAMAccountName (AD)

ldap_group_gid_number (string)

The LDAP attribute that corresponds to the group's id.

Default: gidNumber

ldap_group_member (string)

The LDAP attribute that contains the names of the group's members.

Default: memberuid (rfc2307) / member (rfc2307bis)

ldap_group_uuid (string)

The LDAP attribute that contains the UUID/GUID of an LDAP group object.

Default: not set in the general case, objectGUID for AD and ipaUniqueID for IPA

ldap_group_objectsid (string)

The LDAP attribute that contains the objectSID of an LDAP group object. This is usually only necessary for ActiveDirectory servers.

Default: objectSid for ActiveDirectory, not set for other servers.

ldap_group_modify_timestamp (string)

The LDAP attribute that contains timestamp of the last modification of the parent object.

Default: modifyTimestamp

ldap_group_type (string)

The LDAP attribute that contains an integer value indicating the type of the group and maybe other flags.

This attribute is currently only used by the AD provider to determine if a group is a domain local groups and has to be filtered out for trusted domains.

Default: groupType in the AD provider, otherwise not set

ldap_group_external_member (string)

The LDAP attribute that references group members that are defined in an external domain. At the moment, only IPA's external members are supported.

Default: ipaExternalMember in the IPA provider, otherwise unset.

NETGROUP ATTRIBUTES

ldap_netgroup_object_class (string)

The object class of a netgroup entry in LDAP.

In IPA provider, ipa_netgroup_object_class should be used instead.

Default: nisNetgroup

ldap_netgroup_name (string)

The LDAP attribute that corresponds to the netgroup name.

In IPA provider, ipa_netgroup_name should be used instead.

Default: cn

ldap_netgroup_member (string)

The LDAP attribute that contains the names of the netgroup's members.

In IPA provider, ipa_netgroup_member should be used instead.

Default: memberNisNetgroup

ldap_netgroup_triple (string)

The LDAP attribute that contains the (host, user, domain) netgroup triples.

This option is not available in IPA provider.

Default: nisNetgroupTriple

ldap_netgroup_modify_timestamp (string)

The LDAP attribute that contains timestamp of the last modification of the parent object.

This option is not available in IPA provider.

Default: modifyTimestamp

HOST ATTRIBUTES

ldap_host_object_class (string)

The object class of a host entry in LDAP.

Default: ipService

ldap_host_name (string)

The LDAP attribute that corresponds to the host's name.

Default: cn

ldap_host_fqdn (string)

The LDAP attribute that corresponds to the host's fully-qualified domain name.

Default: fqdn

ldap_host_serverhostname (string)

The LDAP attribute that corresponds to the host's name.

Default: serverHostname

ldap_host_member_of (string)

The LDAP attribute that lists the host's group memberships.

Default: memberOf

ldap_host_ssh_public_key (string)

The LDAP attribute that contains the host's SSH public keys.

Default: sshPublicKey

ldap_host_uuid (string)

The LDAP attribute that contains the UUID/GUID of an LDAP host object.

Default: not set

SERVICE ATTRIBUTES

ldap_service_object_class (string)

The object class of a service entry in LDAP.

Default: ipService

ldap_service_name (string)

The LDAP attribute that contains the name of service attributes and their aliases.

Default: cn

ldap_service_port (string)

The LDAP attribute that contains the port managed by this service.

Default: ipServicePort

ldap_service_proto (string)

The LDAP attribute that contains the protocols understood by this service.

Default: ipServiceProtocol

SUDO ATTRIBUTES

ldap_sudorule_object_class (string)

The object class of a sudo rule entry in LDAP.

Default: sudoRole

ldap_sudorule_name (string)

The LDAP attribute that corresponds to the sudo rule name.

Default: cn

ldap_sudorule_command (string)

The LDAP attribute that corresponds to the command name.

Default: sudoCommand

ldap_sudorule_host (string)

The LDAP attribute that corresponds to the host name (or host IP address, host IP network, or host netgroup)

Default: sudoHost

ldap_sudorule_user (string)

The LDAP attribute that corresponds to the user name (or UID, group name or user's netgroup)

Default: sudoUser

ldap_sudorule_option (string)

The LDAP attribute that corresponds to the sudo options.

Default: sudoOption

ldap_sudorule_runasuser (string)

The LDAP attribute that corresponds to the user name that commands may be run as.

Default: sudoRunAsUser

ldap_sudorule_runasgroup (string)

The LDAP attribute that corresponds to the group name or group GID that commands may be run as.

Default: sudoRunAsGroup

ldap_sudorule_notbefore (string)

The LDAP attribute that corresponds to the start date/time for when the sudo rule is valid.

Default: sudoNotBefore

ldap_sudorule_notafter (string)

The LDAP attribute that corresponds to the expiration date/time, after which the sudo rule will no longer be valid.

Default: sudoNotAfter

ldap_sudorule_order (string)

The LDAP attribute that corresponds to the ordering index of the rule.

Default: sudoOrder

AUTOFS ATTRIBUTES

ldap_autofs_map_object_class (string)

The object class of an automount map entry in LDAP.

Default: nisMap (rfc2307, autofs_provider=ad), otherwise automountMap

ldap_autofs_map_name (string)

The name of an automount map entry in LDAP.

Default: nisMapName (rfc2307, autofs_provider=ad), otherwise automountMapName

ldap_autofs_entry_object_class (string)

The object class of an automount entry in LDAP. The entry usually corresponds to a mount point.

Default: nisObject (rfc2307, autofs_provider=ad), otherwise

automount

ldap_autofs_entry_key (string)

The key of an automount entry in LDAP. The entry usually corresponds to a mount point.

Default: cn (rfc2307, autofs_provider=ad), otherwise automountKey

ldap_autofs_entry_value (string)

The key of an automount entry in LDAP. The entry usually corresponds to a mount point.

Default: nisMapEntry (rfc2307, autofs_provider=ad), otherwise automountInformation

IP HOST ATTRIBUTES

ldap_iphost_object_class (string)

The object class of an iphost entry in LDAP.

Default: ipHost

ldap_iphost_name (string)

The LDAP attribute that contains the name of the IP host attributes and their aliases.

Default: cn

ldap_iphost_number (string)

The LDAP attribute that contains the IP host address.

Default: ipHostNumber

IP NETWORK ATTRIBUTES

ldap_ipnetwork_object_class (string)

The object class of an ipnetwork entry in LDAP.

Default: ipNetwork

ldap_ipnetwork_name (string)

The LDAP attribute that contains the name of the IP network attributes and their aliases.

Default: cn

ldap_ipnetwork_number (string)

The LDAP attribute that contains the IP network address.

Default: ipNetworkNumber

SEE ALSO

sssd(8), sssd.conf(5), sssd-ldap(5), sssd-ldap-attributes(5), sssd-krb5(5), sssd-simple(5), sssd-ipa(5), sssd-ad(5), sssd-files(5), sssd-sudo(5), sssd-session-recording(5), sss_cache(8), sss_debuglevel(8), sss_obfuscate(8), sss_seed(8), sssd_krb5_locator_plugin(8), sss_ssh_authorizedkeys(8), sss_ssh_knownhostsproxy(8), sssd-ifp(5), pam_sss(8). sss_rpcidmapd(5) sssd-systemtap(5)

AUTHORS

The SSSD upstream - https://github.com/SSSD/sssd/

SSSD 07/10/2023 SSSD-LDAP-ATTRIBUT(5)