

SECONDA EDIZIONE

SIMONE PICCARDI

**INTEGRAZIONE
SISTEMISTICA
CON LDAP**



Integrazione Sistemistica con LDAP

Seconda edizione

Simone Piccardi

Integrazione Sistemistica con LDAP – Seconda edizione

Copyright © 2002-2019 by Simone Piccardi and Truelite S.r.l.

This work is licensed under the Creative Commons Attribution-ShareAlike 4.0 International License. To view a copy of this license, visit <https://creativecommons.org/licenses/by-sa/4.0/> or send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.

Quest'opera è distribuita con *Licenza Creative Commons Attribuzione - Condividi allo stesso modo 4.0 Internazionale*. Per una copia di questa licenza visitare <https://creativecommons.org/licenses/by-sa/4.0/>. La licenza completa è disponibile in formato testo all'indirizzo <https://creativecommons.org/licenses/by-sa/4.0/legalcode>.

Progetto grafico a cura di Fabio Venni

Questa documentazione libera è stata realizzata a supporto delle attività formative effettuate da Truelite S.r.l. La stesura di parte del materiale è stata finanziata insieme alla realizzazione di alcuni corsi erogati dall'azienda e lo stesso viene messo a disposizione di tutti sotto licenza CC-BY-SA.

Questo significa che potete distribuirlo, estenderlo e migliorarlo, a condizione che venga resa adeguata attribuzione (riportando esplicitamente anche il collegamento indicato nel paragrafo successivo) e che venga mantenuta la stessa licenza.

Questo testo viene distribuito su Internet all'indirizzo:

<https://www.truelite.it/Integrazione-Sistemistica-con-LDAP/>

dove saranno pubblicate tutte le informazioni su nuove versioni ed aggiornamenti.



Società italiana specializzata nella fornitura di servizi, consulenza e formazione esclusivamente su GNU/Linux e software libero.

Per informazioni:

Truelite S.r.l.

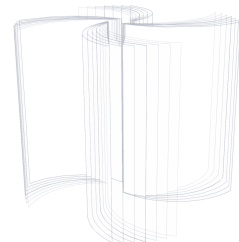
Via Monferrato 6,

50142 Firenze.

Tel: 055-7879597

e-mail: info@truelite.it

web: <http://www.truelite.it>



Indice

1	Introduzione a LDAP	1
1.1	Il protocollo LDAP	1
1.1.1	Una visione di insieme	1
1.1.2	La strutturazione dei dati di LDAP	2
1.1.3	Il formato LDIF	9
1.1.4	L'architettura delle interrogazioni su LDAP	11
1.2	L'uso del servizio LDAP e la gestione dei dati	14
1.2.1	La configurazione generica per l'accesso client	14
1.2.2	Interrogazioni e ricerche su LDAP	17
1.2.3	La gestione dei dati su LDAP	24
2	Il server di <i>OpenLDAP</i>	31
2.1	Installazione e configurazione del server	31
2.1.1	Installazione ed avvio del servizio	31
2.1.2	La configurazione tradizionale del server	36
2.1.3	La configurazione dinamica via LDAP	45
2.1.4	Creazione e manutenzione di un database LDAP	51
2.2	Configurazioni avanzate	55
2.2.1	I meccanismi di autenticazione	55
2.2.2	Il controllo degli accessi	64
2.2.3	La configurazione per l'uso di SSL/TLS	72
2.2.4	L'estensione delle funzionalità del server e gli <i>overlay</i>	76
2.3	La replicazione	79
2.3.1	Il meccanismo della replicazione	79
2.3.2	La replicazione con <i>slurpd</i>	81
2.3.3	La replicazione con <i>syncrepl</i>	84
2.3.4	Utilizzo avanzato di <i>syncrepl</i>	91
3	L'integrazione con LDAP	101
3.1	La gestione centralizzata di utenti e gruppi	101
3.1.1	Utenti e gruppi su LDAP	101
3.1.2	La configurazione del <i>Name Service Switch</i> su LDAP	108
3.1.3	La configurazione di PAM per l'autenticazione su LDAP	114

3.1.4	Gestione centralizzata di utenti e gruppi con sssd	119
3.2	L'integrazione dell'autenticazione su LDAP	127
3.2.1	Apache e LDAP	127
3.2.2	Squid e LDAP	131
3.2.3	Dovecot e LDAP	135
3.3	La centralizzazione delle informazioni su LDAP	140
3.3.1	La gestione dell'indirizzario	140
3.3.2	Postfix e LDAP	142
3.3.3	Domain controller classici con Samba e LDAP	145

Presentazione

Integrazione Sistemistica con LDAP è un testo che affronta e analizza tutti gli aspetti dell'uso del Lightweight Directory Access Protocol, uno standard per l'interrogazione e la modifica dei dati mantenuti su un servizio centralizzato organizzato in maniera gerarchica come un indirizzario o una rubrica telefonica.

L'obiettivo del libro è quello di fornire le basi per installare, configurare e utilizzare LDAP come fonte di informazione da parte di altri servizi di rete.

La prima parte del testo è dedicata all'introduzione dei concetti, della terminologia ed del funzionamento di LDAP e fornisce le basi per la comprensione sia del protocollo che della strutturazione dei dati.

Viene poi spiegata nel dettaglio la configurazione del servizio, sia lato client sia lato server facendo riferimento al progetto OpenLDAP, una implementazione libera del servizio LDAP e delle librerie di gestione.

Infine viene illustrata l'integrazione su LDAP di vari servizi di rete e di sistema.

Integrazione Sistemistica con LDAP si rivolge a sistemisti che abbiano già una conoscenza di base sia delle problematiche dell'amministrazione di sistema su sistemi Unix-like, sia del funzionamento di reti e servizi. Per l'approfondimento di questi temi si consiglia la lettura di "Amministrare GNU/Linux".

Restando fedele alla filosofia di sviluppo del software libero il testo è pubblicato con licenza libera.

Indice analitico

Apache

direttiva

- AuthLDAPBindDN, 130
- AuthLDAPBindPassword, 130
- AuthLDAPCompareDNOnServer, 130
- AuthLDAPGroupAttributeIsDN, 130
- AuthLDAPGroupAttribute, 130
- AuthLDAPURL, 130

attributi operativi, 9

attributi virtuali, 9

autenticazione semplice, 55

Base-64, 10

change record, 24–27

Change Sequence Number (CSN), 85

comando

- basic_ldap_auth, 132
- cpu, 107
- ext_ldap_group_acl, 134
- ldapadd, 24
- ldapdelete, 25
- ldapmodify, 24
- ldapmodrdn, 27
- ldappasswd, 59
- ldapsearch, 17
- ldapvi, 27
- slapacl, 70
- slapadd, 52
- slapcat, 52
- slapindex, 54
- slappasswd, 56
- slaptest, 45
- smbldap-groupadd, 156
- smbldap-groupdel, 156
- smbldap-groupmod, 157

smbldap-passwd, 156

smbldap-populate, 153

smbldap-useradd, 155

smbldap-userdel, 155

smbldap-usermod, 155

configurazione

.ldaprc, 16

.ldapvi, 28

/etc/cpu/cpu.conf, 107

/etc/dovecot/conf.d/, 135

/etc/dovecot/dovecot.conf, 136

/etc/dovecot/local.conf, 136

/etc/ldap/ldap.conf, 15

/etc/ldap/sasl/slapd.conf, 62

/etc/ldap/slapd.conf, 36

/etc/ldap/slapd.d, 45

/etc/ldapvi.conf, 28

/etc/libnss-ldap.conf, 109

/etc/migrationtools/migrate_common.ph, 103

/etc/nslcd.conf, 111

/etc/pam_ldap.conf, 114

/etc/smbldap/smbldap.conf, 151

/etc/smbldap/smbldap_bind.conf, 151

/etc/sss/conf.d/, 121

/etc/sss/sss.conf, 121

Data Information Tree (DIT), 2

delete phase, 86

delta replication, 95–97

demone

nslcd, 111

slapd, 34

slurpd, 81

sss, 119

Distinguished Name (DN), 3

Extensible Match Search Filter, 22

- filtri di ricerca, 20–22
- giornale di replicazione, 82
- ISO X.500, 1
- LDAP Content Synchronization Protocol*, 84
- LDAP Data Interchange Format (LDIF)*, 9
- LDAP Password Modify Extended Operations*, 40, 58
- Name Service Switch (NSS)*, 108
- objectclass*, 6–9
 - dcObject, 6
 - groupOfNames, 129
 - inetLocalMailRecipient, 143
 - inetOrgPerson, 8, 9
 - olcBackendConfig, 48
 - olcDatabaseConfig, 48
 - olcGlobal, 46
 - olcHdbConfig, 48
 - olcMdbConfig, 48
 - olcModuleList, 47
 - olcOverlayConfig, 50
 - olcSchemaConfig, 48
 - organizationalPerson, 21
 - organizationalUnit, 7
 - person, 21
 - posixAccount, 101
 - posixGroup, 101
 - sambaGroupMapping, 148
 - sambaSamAccount, 148
 - shadowAccount, 101
 - top, 6
- Object ID (OID)*, 6
- OpenLDAP
 - backend
 - bdb, 41
 - hdb, 41
 - ldap, 92
 - mdb, 42
 - monitor, 78
 - direttiva client
 - BASE, 16
 - BINDDN, 15
 - BINDPW, 15
 - DEREF, 15
 - HOST, 16
 - PORT, 16
 - REFERRAL, 15
 - SASL_AUTHCID, 60
 - SASL_AUTHZID, 60
 - SASL_MECH, 60
 - SASL_REALM, 60
 - SCOPE, 15
 - SIZELIMIT, 15
 - TIMELIMIT, 15
 - TLS_CACERT, 75
 - TLS_CERT, 75
 - TLS_CIPHER_SUITE, 75
 - TLS_KEY, 75
 - TLS_REQCERT, 75
 - URI, 16
 - debug, 15
 - rootbinddn, 15
 - scope, 15
 - direttiva server
 - TLSCACertificateFile, 73
 - TLSCertificateFile, 73
 - TLSCertificateKeyFile, 73
 - TLSCipherSuite, 73
 - TLSVerifyClient, 73
 - access, 64
 - acl-bind, 92
 - argsfile, 40
 - auditlog, 79
 - authz-regexp, 61
 - backend, 37
 - cachesize, 41
 - checkpoint, 41
 - database, 37
 - dbconfig, 41
 - dbnosync, 42
 - directory, 44
 - hidden, 43
 - idletimeout, 40
 - include, 39
 - index, 43
 - lastmod, 43
 - limits, 72

- logdb, 95
- loglevel, 40
- logops, 95
- logpurge, 95
- logsuccess, 95
- maxsize, 42
- mirrormode, 99
- mode, 41
- moduleload, 40
- modulepath, 40
- overlay, 77
- password-crypt-salt-format, 58
- password-hash, 40, 58
- pidfile, 40
- readonly, 43
- referral, 40
- replicationinterval, 82
- replica, 82
- repllogfile, 82
- restrict, 43
- rootdn, 56
- rootpw, 56
- sasl-auxprops, 63
- serverID, 99
- sizelimit, 39
- suffix, 44
- syncprov-checkpoint, 86
- syncprov-nopresent, 86
- syncprov-reloadhint, 86
- syncprov-sessionlog, 86
- syncrepl, 88
- timelimit, 40
- updatedn, 83
- updateref, 83
- uri, 92
- overlay
 - accesslog, 95
 - auditlog, 79
 - smbk5pwd, 150
 - syncprov, 86
- operational attributes*, 9

- present phase*, 86
- proxy replication*, 91–95

- referral*, 13–14
- Relative Distinguished Name (RDN)*, 3
- Root DSE*, 22

- Security ID (SID)*, 146
- Security Strength Factor (SSF)*, 68
- simple authentication*, 55–56
- Simple Authentication and Security Layer (SASL)*, 59
- suffisso, 4–6
- suffisso base, 4–6
- System Security Services Daemon*, 119

Bibliografia

- [AGL] Simone Piccardi. *Amministrare GNU/Linux*. Truelite S.r.l., 5th edition, 2018. <https://www.truelite.it/amministrare-gnu-linux>.
- [GaPiL] Simone Piccardi. *Guida alla Programmazione in Linux*. Simone Piccardi, 2012. <https://gopil.gnulinix.it>.
- [RegExp] Jeffrey E. F. Friedl. *Mastering regular expression*. O'Reilly, 1997.
- [SGL] Simone Piccardi. *La sicurezza con GNU/Linux*. Truelite S.r.l., 2003. <https://labs.truelite.it>.
- [WebServ] Simone Piccardi. *I servizi web*. Truelite S.r.l., 2003. <https://labs.truelite.it>.