

Join di una workstation GNU Linux in un dominio WS08-R2 ADDS

Introduzione

Lo scopo di quest'articolo è di dimostrare come sia possibile effettuare l'operazione di *join* di una workstation con Sistema Operativo GNU Linux in un dominio Active Directory (AD) basato su Windows Server 2008 R2.

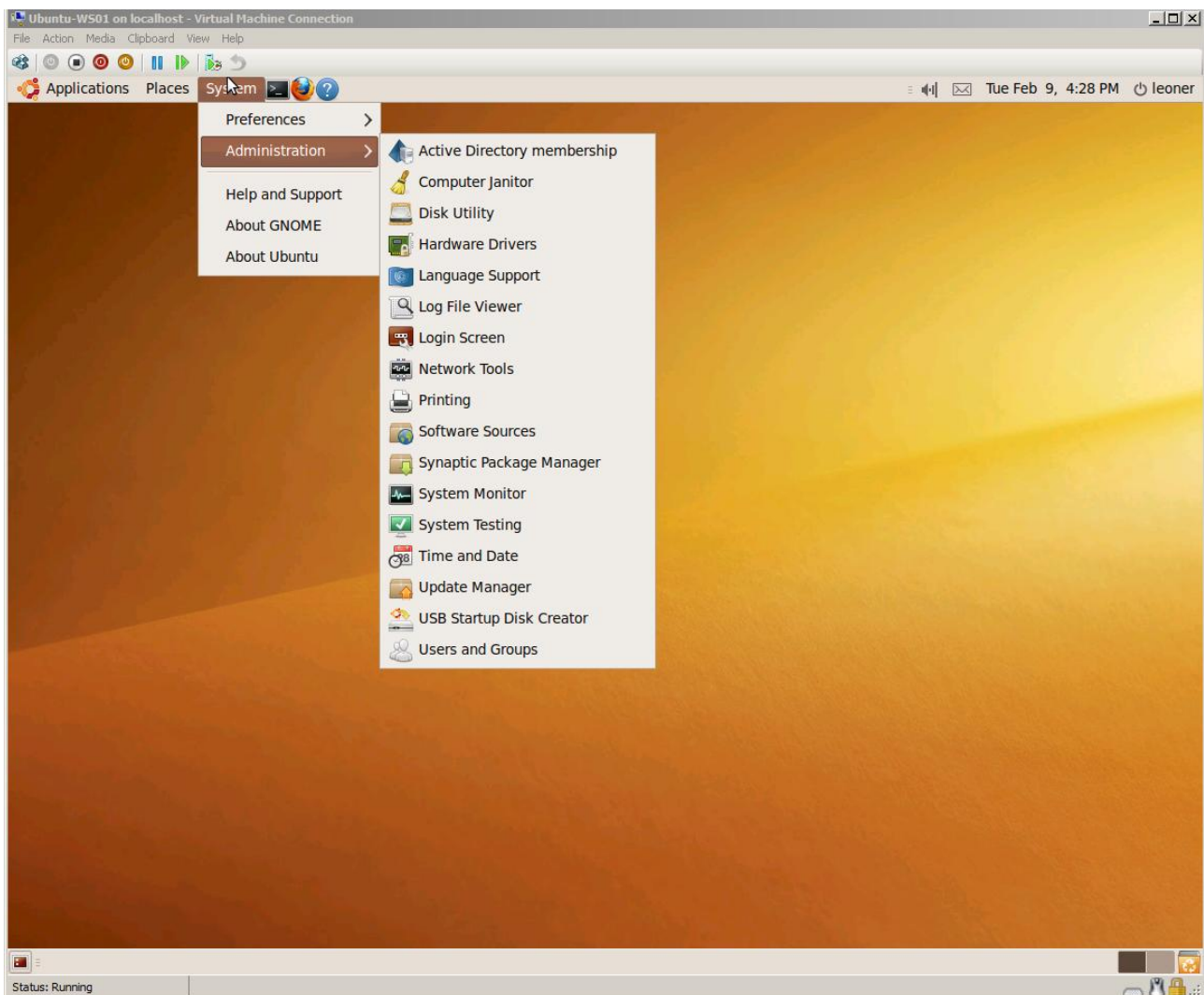
Per questa demo è stata utilizzata una macchina virtuale Linux Ubuntu 9.10 creata con Hyper-V 2.0.

Installare il package “Likewise AD Settings”

```
sudo apt-get install likewise-open5-gui
```

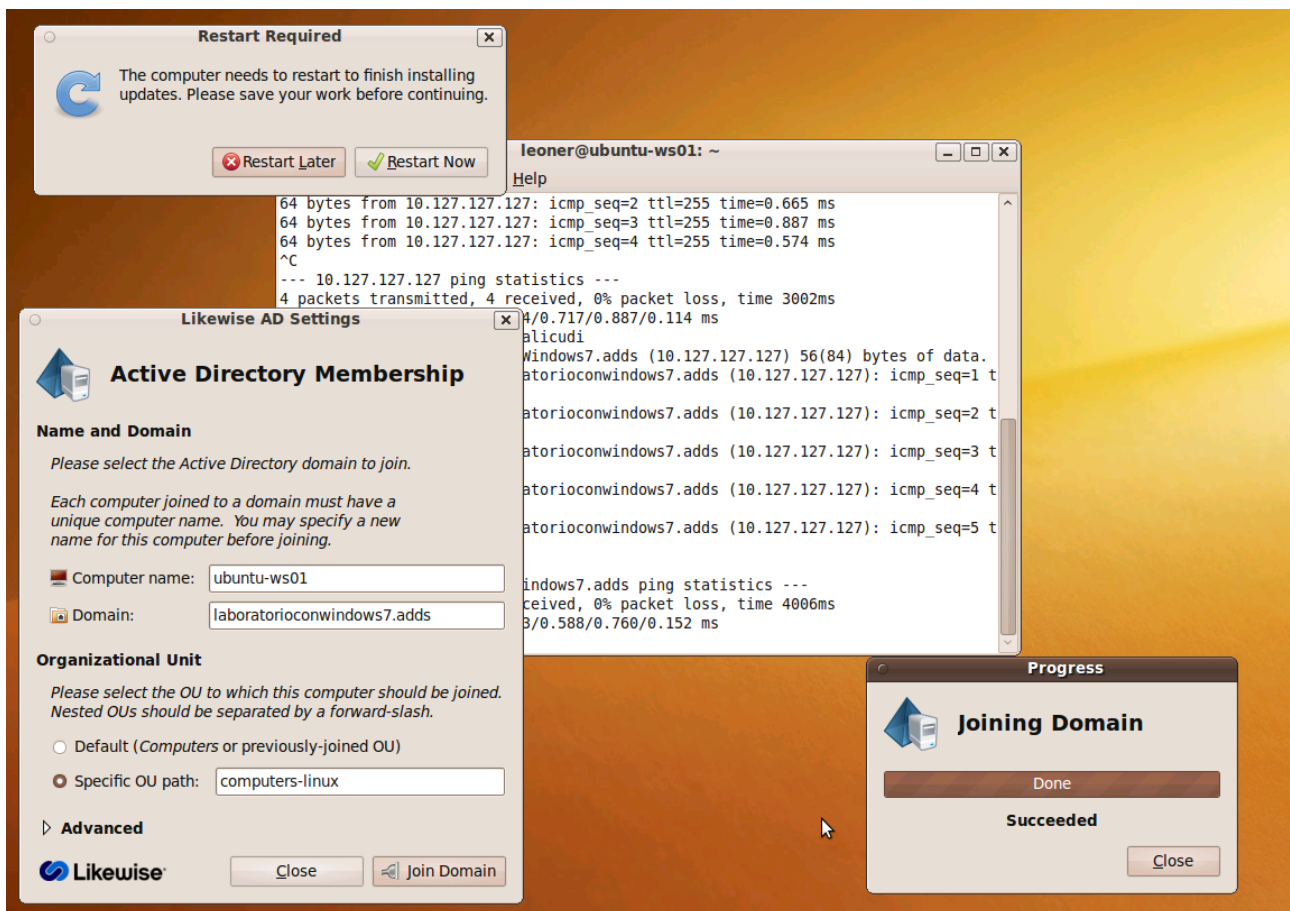
Eseguire la join della workstation Linux nel dominio AD

Invocare l'applicazione “Active Directory Membership”:

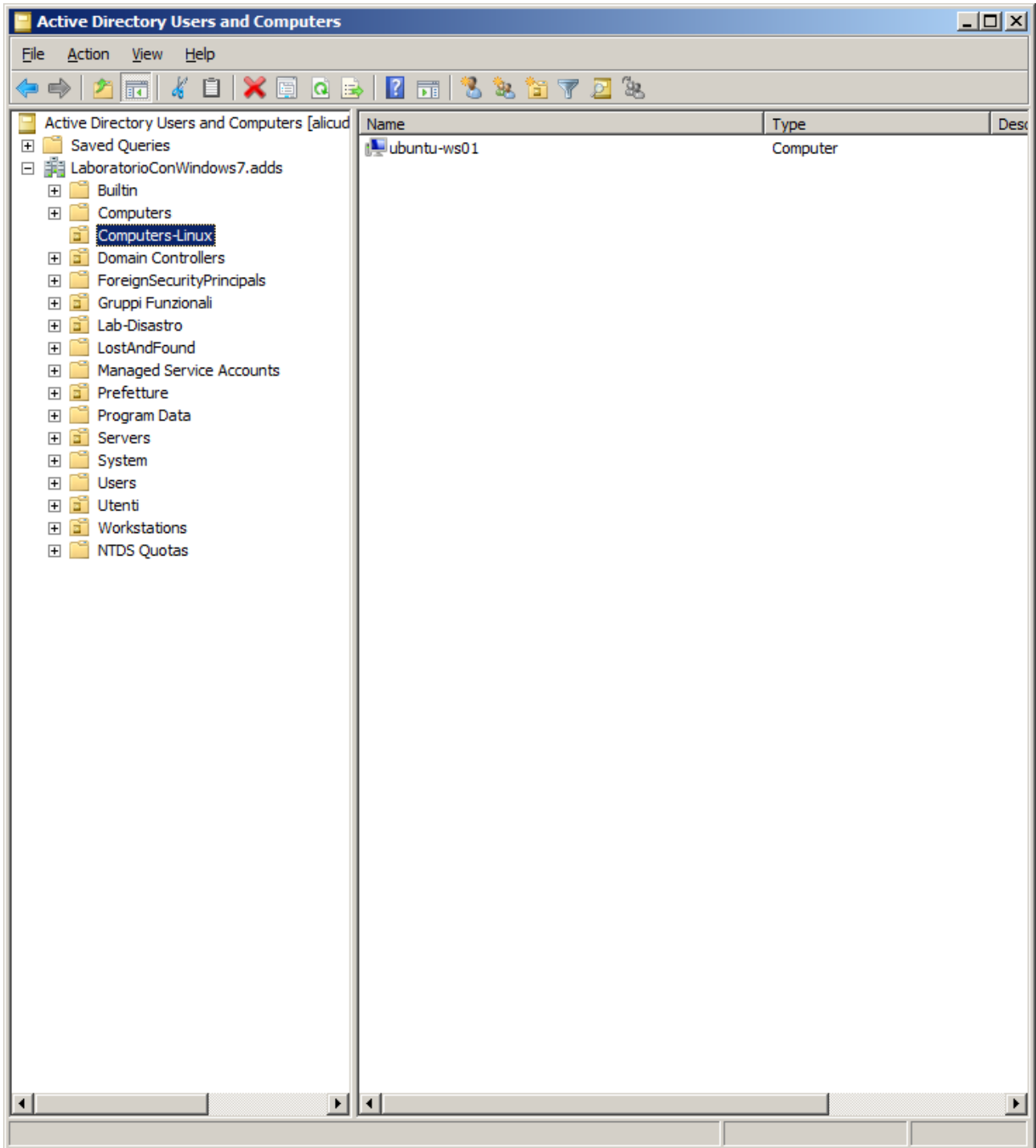


ed inserire le coordinate per portare a termine la join nel dominio AD desiderato:

- ComputerName (Hostname)
- FQDN del dominio AD
- Volendo pubblicare l'oggetto LDAP Computer in un contenitore diverso dallo standard Computers, è possibile inserire il nome della OU (in caso di OU di secondo livello è necessario separare le OU con il carattere slash (/)):
 - Nota di Leone rivolta agli sviluppatori: perchè non utilizzare l'attributo standard LDAP "DistinguishedName" per indicare la OU ?




Verificare la creazione dell'oggetto Computer in AD



ubuntu-ws01 Properties [?] [X]

Location	Managed By	Object	Security	Dial-in	Attribute Editor
General	Operating System	Member Of	Delegation	Password Replication	

 ubuntu-ws01

Computer name (pre-Windows 2000):

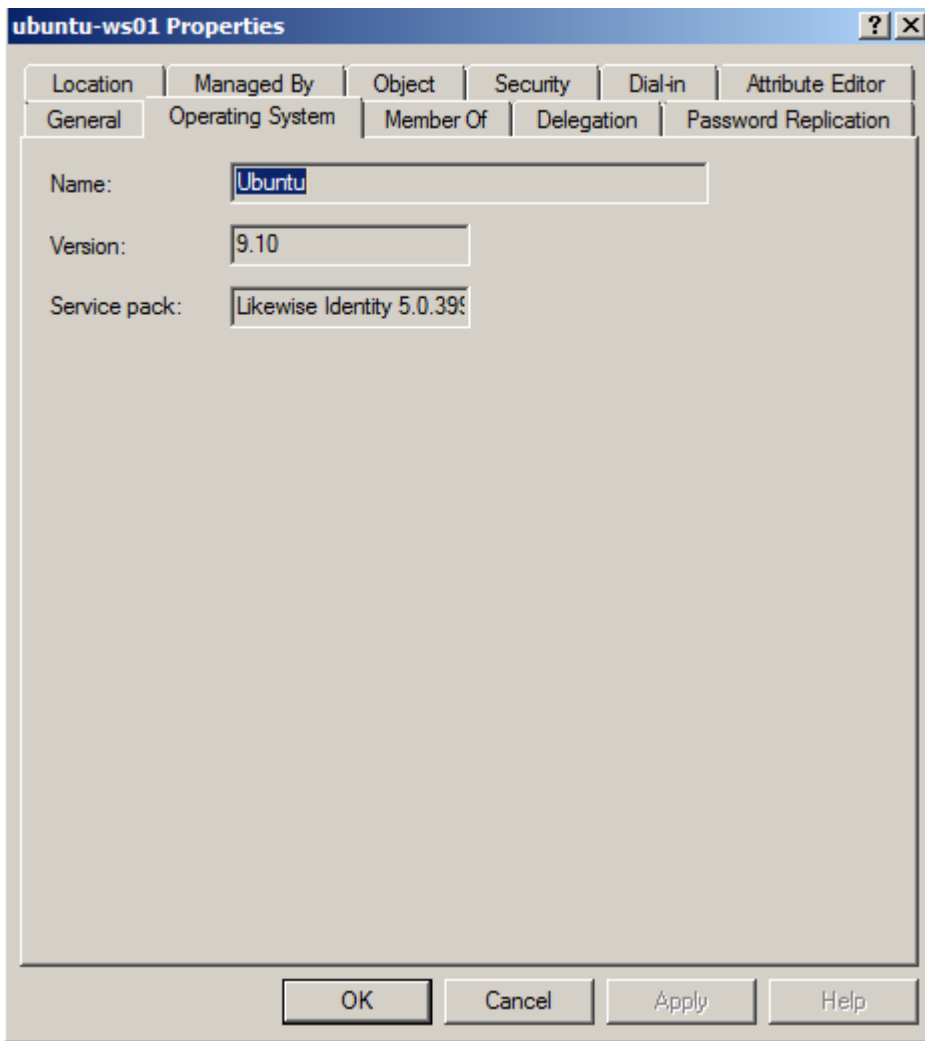
DNS name:

DC Type:

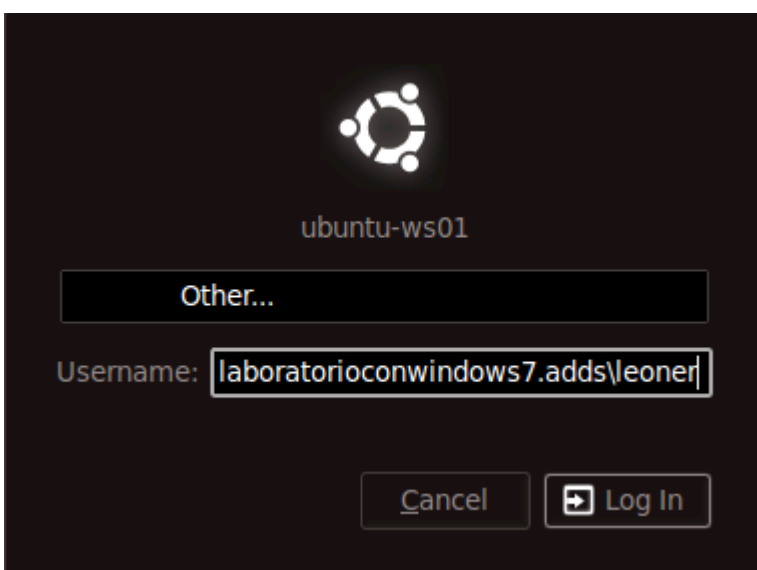
Site:

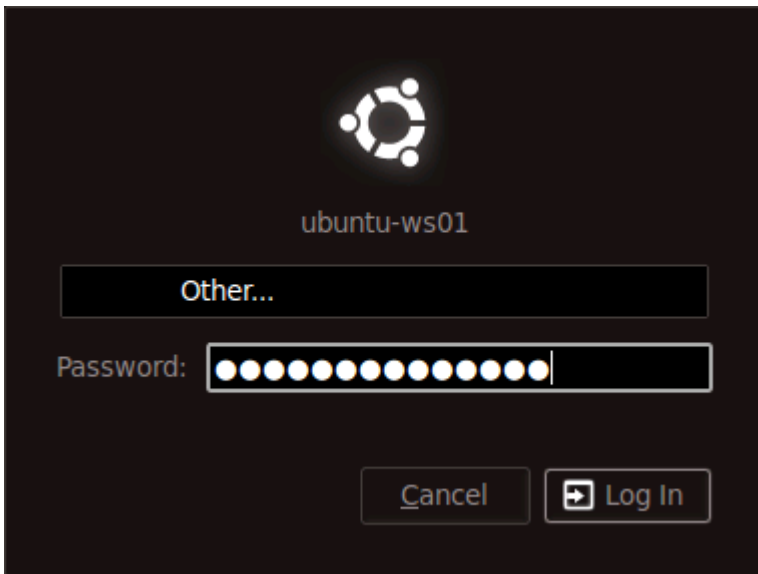
Description:

OK Cancel Apply Help



Eseguire Login sulla workstation Linux Ubuntu con le credenziali di un utente AD





Rilevazione del traffico LDAP e Kerberos scatenato dall'autenticazione dell'utente in AD

Microsoft Corporation: Capturing - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No. -	Time	Source	Destination	Protocol	Info
39	6.521238	10.1.7.100	10.127.127.127	DNS	Standard query SRV_kerberos-master._udp.LABORATORIOCONWINDOWS7.ADDS
40	6.521497	10.127.127.127	10.1.7.100	DNS	Standard query response, No such name
41	6.522532	10.1.7.100	10.127.127.127	KRB5	AS-REQ
42	6.523714	10.127.127.127	10.1.7.100	KRB5	KRB Error: KRB5KRB_ERR_RESPONSE_TOO_BIG
43	6.524264	10.1.7.100	10.127.127.127	DNS	Standard query SRV_kerberos-master._udp.LABORATORIOCONWINDOWS7.ADDS
44	6.524874	10.127.127.127	10.1.7.100	DNS	Standard query response, No such name
45	6.525026	10.1.7.100	10.127.127.127	TCP	59090 > kerberos [SYN] Seq=0 win=5840 Len=0 MSS=1460 TSV=819716 TSER=0 WS=5
46	6.525108	10.127.127.127	10.1.7.100	TCP	kerberos > 59090 [SYN, ACK] Seq=0 Ack=1 win=8192 [TCP CHECKSUM INCORRECT] Len=0 MSS=
47	6.525511	10.1.7.100	10.127.127.127	TCP	59090 > kerberos [ACK] Seq=1 Ack=1 win=5856 Len=0 TSV=819716 TSER=2643735
48	6.525959	10.1.7.100	10.127.127.127	KRB5	AS-REQ
49	6.526815	10.127.127.127	10.1.7.100	KRB5	AS-REP
50	6.527309	10.1.7.100	10.127.127.127	TCP	59090 > kerberos [ACK] Seq=277 Ack=1449 win=8736 Len=0 TSV=819717 TSER=2643735
51	6.527976	10.1.7.100	10.127.127.127	TCP	59090 > kerberos [ACK] Seq=277 Ack=1553 win=8736 Len=0 TSV=819717 TSER=2643735
52	6.528051	10.1.7.100	10.127.127.127	TCP	59090 > kerberos [FIN, ACK] Seq=277 Ack=1553 win=8736 Len=0 TSV=819717 TSER=2643735
53	6.528077	10.127.127.127	10.1.7.100	TCP	kerberos > 59090 [ACK] Seq=1553 Ack=278 win=131584 [TCP CHECKSUM INCORRECT] Len=0 TS
54	6.528169	10.127.127.127	10.1.7.100	TCP	kerberos > 59090 [RST, ACK] Seq=1553 Ack=278 win=0 [TCP CHECKSUM INCORRECT] Len=0 TS
55	6.532099	10.1.7.100	10.127.127.127	DNS	Standard query SRV_kerberos-master._tcp.LABORATORIOCONWINDOWS7.ADDS
56	6.532229	10.127.127.127	10.1.7.100	DNS	Standard query response, No such name
57	6.534457	10.1.7.100	10.127.127.127	TCP	59091 > kerberos [SYN] Seq=0 win=5840 Len=0 MSS=1460 TSV=819719 TSER=0 WS=5
58	6.534508	10.127.127.127	10.1.7.100	TCP	kerberos > 59091 [SYN, ACK] Seq=0 Ack=1 win=8192 [TCP CHECKSUM INCORRECT] Len=0 MSS=
59	6.534930	10.1.7.100	10.127.127.127	TCP	59091 > kerberos [ACK] Seq=1 Ack=1 win=5856 Len=0 TSV=819719 TSER=2643736
60	6.535379	10.1.7.100	10.127.127.127	TCP	[TCP segment of a reassembled PDU]
61	6.535774	10.1.7.100	10.127.127.127	KRB5	TGS-REQ
62	6.535795	10.127.127.127	10.1.7.100	TCP	kerberos > 59091 [ACK] Seq=1 Ack=1547 win=131584 [TCP CHECKSUM INCORRECT] Len=0 TSV=
63	6.549703	10.127.127.127	10.1.7.100	KRB5	TGS-REP
64	6.550091	10.1.7.100	10.127.127.127	TCP	59091 > kerberos [ACK] Seq=1547 Ack=1449 win=8736 Len=0 TSV=819722 TSER=2643737
65	6.550341	10.1.7.100	10.127.127.127	TCP	59091 > kerberos [ACK] Seq=1547 Ack=1737 win=11648 Len=0 TSV=819723 TSER=2643737
66	6.550622	10.1.7.100	10.127.127.127	TCP	59091 > kerberos [FIN, ACK] Seq=1547 Ack=1737 win=11648 Len=0 TSV=819723 TSER=264373
67	6.550677	10.127.127.127	10.1.7.100	TCP	kerberos > 59091 [ACK] Seq=1737 Ack=1548 win=131584 [TCP CHECKSUM INCORRECT] Len=0 TS
68	6.550674	10.127.127.127	10.1.7.100	TCP	kerberos > 59091 [RST, ACK] Seq=1737 Ack=1548 win=0 [TCP CHECKSUM INCORRECT] Len=0 TS
69	6.551154	10.1.7.100	10.127.127.127	DNS	standard query SRV_kerberos-master._tcp.LABORATORIOCONWINDOWS7.ADDS
70	6.551255	10.127.127.127	10.1.7.100	DNS	Standard query response, No such name
71	6.555376	10.1.7.100	10.127.127.127	TCP	59098 > ldap [SYN] Seq=0 win=5840 Len=0 MSS=1460 TSV=819724 TSER=0 WS=5
72	6.555436	10.127.127.127	10.1.7.100	TCP	ldap > 59098 [SYN, ACK] Seq=0 Ack=1 win=8192 [TCP CHECKSUM INCORRECT] Len=0 MSS=1460
73	6.556049	10.1.7.100	10.127.127.127	TCP	59098 > ldap [ACK] Seq=1 Ack=1 win=5856 Len=0 TSV=819724 TSER=2643738
74	6.557492	10.1.7.100	10.127.127.127	TCP	[TCP segment of a reassembled PDU]
75	6.557785	10.1.7.100	10.127.127.127	LDAP	bindRequest(1) ["root", "sas"]
76	6.557815	10.127.127.127	10.1.7.100	TCP	ldap > 59098 [ACK] Seq=1 Ack=1463 win=131584 [TCP CHECKSUM INCORRECT] Len=0 TSV=2643
77	6.558440	10.127.127.127	10.1.7.100	LDAP	bindResponse(1) success
78	6.559090	10.1.7.100	10.127.127.127	TCP	59098 > ldap [ACK] Seq=1463 Ack=161 win=6912 Len=0 TSV=819725 TSER=2643738
79	6.559892	10.1.7.100	10.127.127.127	LDAP	searchRequest(2) ["CN=Leone Randazzo,CN=Users,DC=Laboratorioconwindows7,DC=adds", "base
80	6.560381	10.127.127.127	10.1.7.100	LDAP	searchResEntry(2) ["<GUID=cba09ce2488311409c603ea0d8b0d942>;<SID=0105000000000001500
81	6.560701	10.1.7.100	10.127.127.127	TCP	59098 > ldap [ACK] Seq=1604 Ack=1738 win=12704 Len=0 TSV=819725 TSER=2643738