FortiGate FSSO 配置手册

作者	版本	时间	修订
李飞（初稿）	1.0	2019 年 1 月	/
屈剑峰	1.1	2021 年 2 月	第四、五、六章节
杜和乐	2.1	2021 年 10 月	修改原始章节内容
使用版本	Fortios 6.2.9-VM AD ： 2xWindows 2016 FSSO： 1xWindows 2016 Client： 1xWindows 10		

目 录

一. 简介

单点登录(SSO)是允许被识别用户访问多个应用的一种方法，识别的用户不提示提供认证凭证，即可进行访问，FSSO 软件识别用户的源 IP 地址，FortiGate 基于用户的 IP 地址允许访问 (基于身份的策略)。

每种 FSSO 使用不同的方法把登录事件发送给 FortiGate，目前我们常用的是两种目录服务：Windows Active Directory (AD)或 Novell eDirectory

本文重点介绍 Windows AD

二. FSSO 模式介绍

2.1. Microsoft Active Directory 有三种模式

(1)、域控制器代理(DC agent)模式

(2)、查询(polling)模式：

a、基于agent的Collector（安装）

b、无agent

2.2. DC Agent 模式

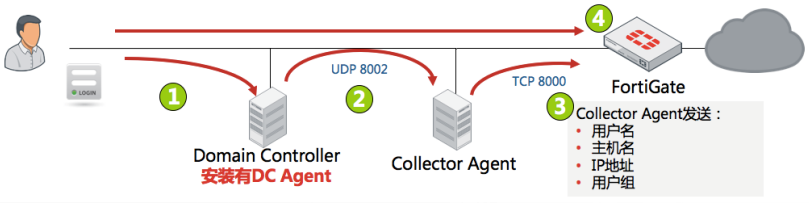
DC Agent 模式是 FSSO 标准模式，需要在每一个域控制器上 DC Agent 在 Windows\system32 目录中安装 dcagent.dll,用于监视用户登录事件并处理 DNS 查找(默认)

除此以外一个或更多的 collector agent 安装在 Windows server 上，负责组验证、客户机检查、在 FortiGate 上更新登录记录、发送域本地安全组、Organizational Units (OU)和全局安全组信息到 FortiGate。

DC Agent 模式不需要额外在 AD 上开启审计事件。

DC Agent 认证流程见下图

1. 用户在Windows DC上认证
2. DC agent看到登录事件并转发给collector agent
3. Collector agent从DC agent上收到事件并转发给FortiGate.
4. FortiGate基于用户IP地址确信用户，用户不需要再次认证



2.2.1. 相应流程

1、DC 检测 Logon User（包含用户名和 IP 地址），发送给 CA

2、CA 检测 DNS 看客户端 IP 地址是否改变（IP address change verify interval 60s）

3、CA 工作站检测，是否 Logoff，通过 Check HKEY_USERS (Workstation verify Interval 5m)

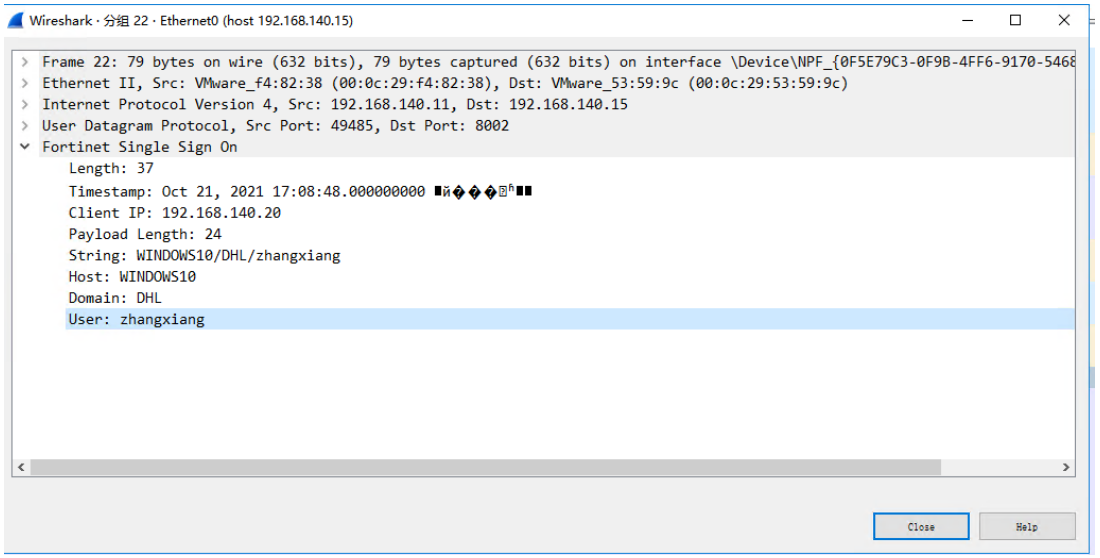
4、如果工作站存活检测未检测成功，480 分钟后用户条目删除（Dead entry timeout 480m）

5、CA 进行用户的组成员查找：通过目录访问或者 API 验证组信息

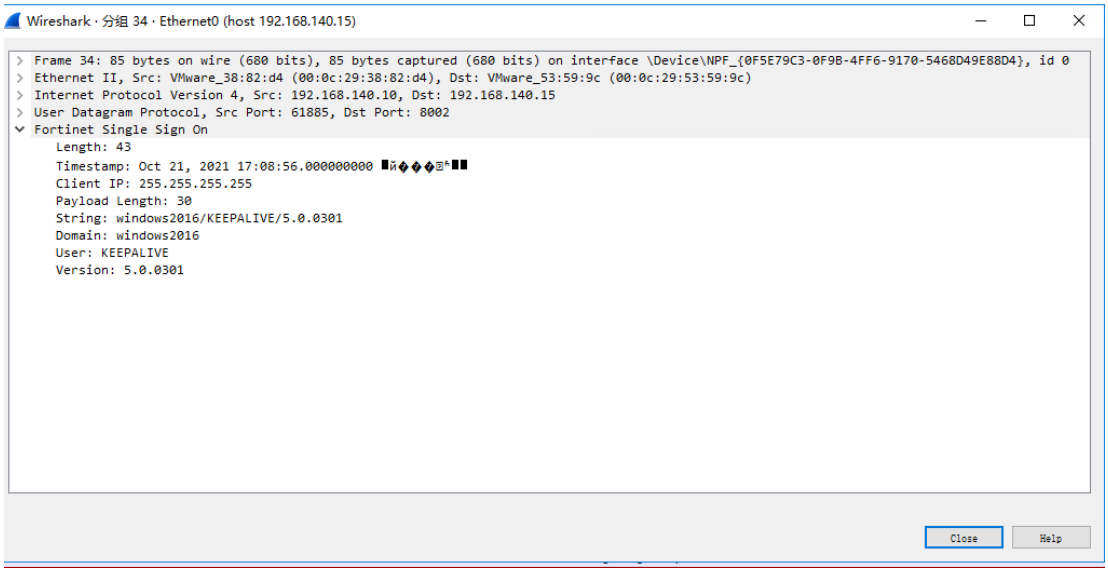
6、发送信息给 Fortigate

2.2.2. 报文格式

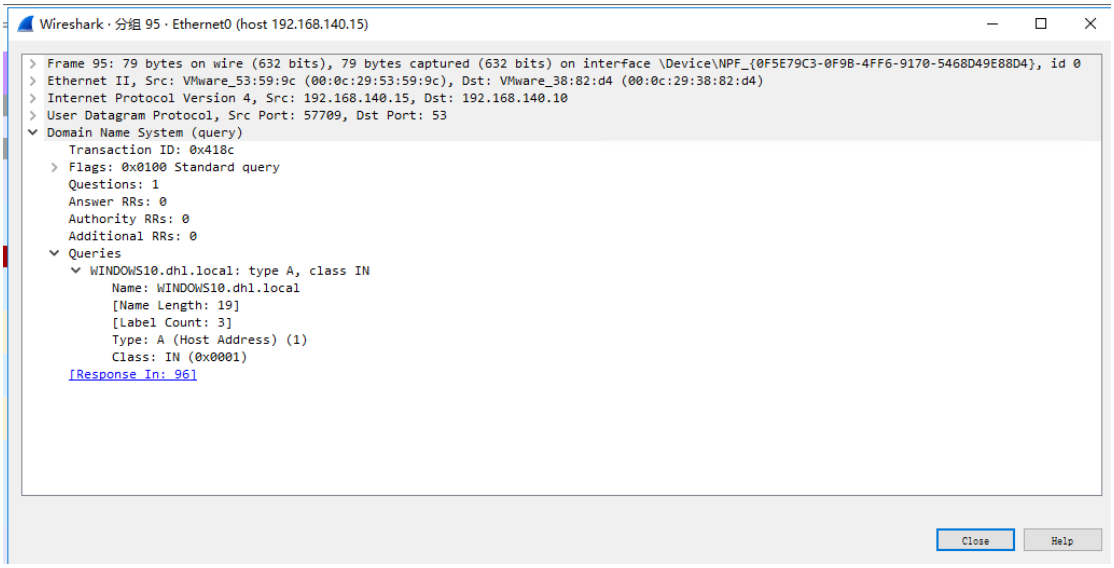
DC Agent User 信息发送报文格式



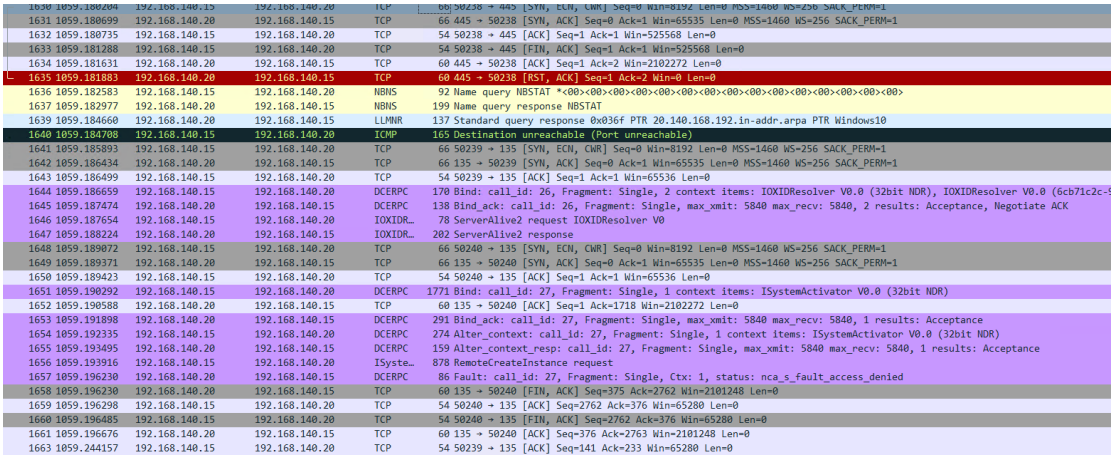
DC Agent 与 Collector Agent 保活报文格式：



Collector Agent 进行客户端 DNS 验证报文格式：

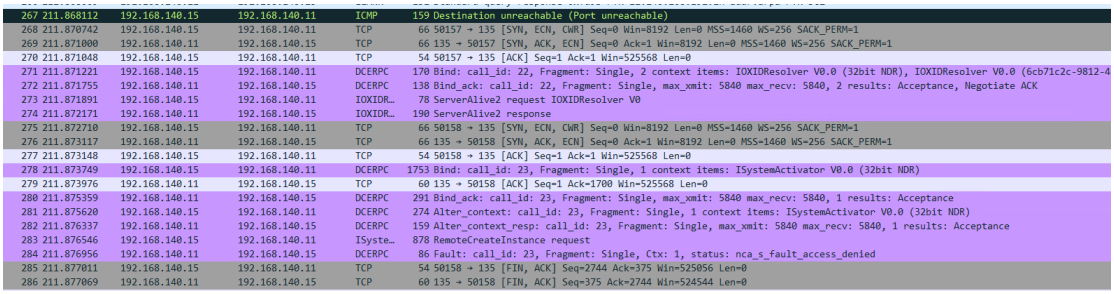


Collector Agent 验证 Workstation Logoff 报文格式：



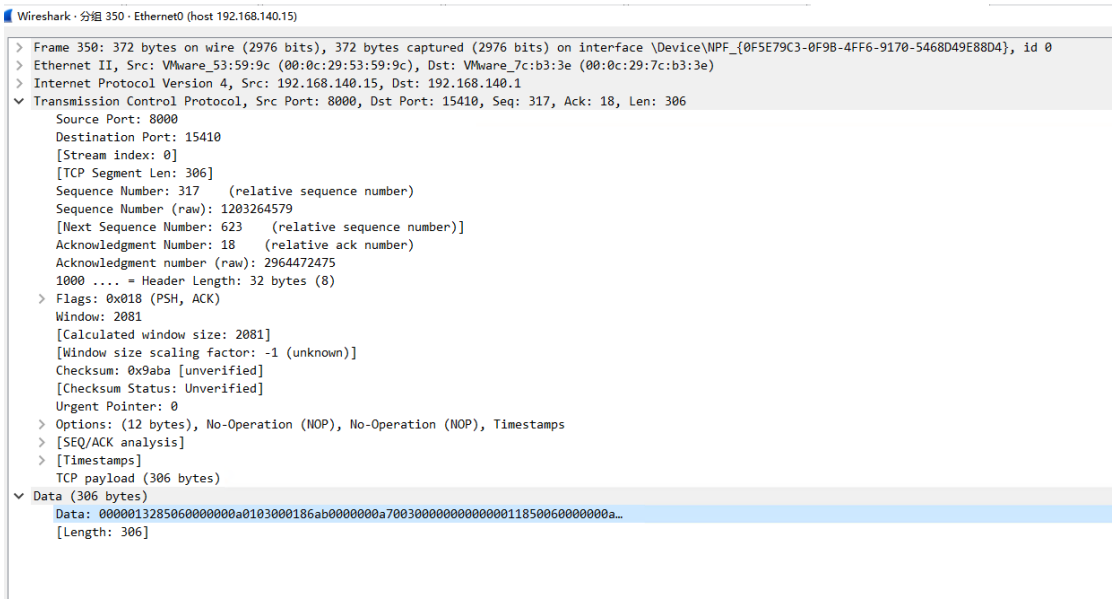
1631 1059.180699	192.168.140.20	192.168.140.15	TCP	66 445 → 50238 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
1632 1059.180735	192.168.140.15	192.168.140.20	TCP	54 50238 → 445 [ACK] Seq=1 Ack=1 Win=525568 Len=0
1633 1059.181288	192.168.140.15	192.168.140.20	TCP	54 50238 → 445 [FIN, ACK] Seq=1 Ack=1 Win=525568 Len=0
1634 1059.181631	192.168.140.20	192.168.140.15	TCP	60 445 → 50238 [ACK] Seq=1 Ack=2 Win=2102272 Len=0
1635 1059.181883	192.168.140.20	192.168.140.15	TCP	60 445 → 50238 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
1636 1059.182583	192.168.140.15	192.168.140.20	NBNS	92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
1637 1059.182977	192.168.140.20	192.168.140.15	NBNS	199 Name query response NBSTAT
1639 1059.184660	192.168.140.20	192.168.140.15	LLMNR	137 Standard query response 0x036f PTR 20.140.168.192.in-addr.arpa PTR Windows10
1640 1059.184708	192.168.140.15	192.168.140.20	ICMP	165 Destination unreachable (Port unreachable)
1641 1059.185893	192.168.140.15	192.168.140.20	TCP	66 50239 → 135 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1642 1059.186434	192.168.140.20	192.168.140.15	TCP	66 135 → 50239 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
1643 1059.186499	192.168.140.15	192.168.140.20	TCP	54 50239 → 135 [ACK] Seq=1 Ack=1 Win=65536 Len=0
1644 1059.186659	192.168.140.15	192.168.140.20	DCERPC	170 Bind: call_id: 26, Fragment: Single, 2 context items: IOXIDResolver V0.0 (32bit NDR), IOXIDResolver V0.0 (6cb71c2c-9
1645 1059.187474	192.168.140.20	192.168.140.15	DCERPC	138 Bind_ack: call_id: 26, Fragment: Single, max_xmit: 5840 max_recv: 5840, 2 results: Acceptance, Negotiate ACK
1646 1059.187654	192.168.140.15	192.168.140.20	IOXIDR…	78 ServerAlive2 request IOXIDResolver V0
1647 1059.188224	192.168.140.20	192.168.140.15	IOXIDR…	202 ServerAlive2 response
1648 1059.189072	192.168.140.15	192.168.140.20	TCP	66 50240 → 135 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
1649 1059.189371	192.168.140.20	192.168.140.15	TCP	66 135 → 50240 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
1650 1059.189423	192.168.140.15	192.168.140.20	TCP	54 50240 → 135 [ACK] Seq=1 Ack=1 Win=65536 Len=0
1651 1059.190292	192.168.140.15	192.168.140.20	DCERPC	1771 Bind: call_id: 27, Fragment: Single, 1 context items: ISystemActivator V0.0 (32bit NDR)
1652 1059.190588	192.168.140.20	192.168.140.15	TCP	60 135 → 50240 [ACK] Seq=1 Ack=1718 Win=2102272 Len=0
1653 1059.191898	192.168.140.20	192.168.140.15	DCERPC	291 Bind_ack: call_id: 27, Fragment: Single, max_xmit: 5840 max_recv: 5840, 1 results: Acceptance
1654 1059.192335	192.168.140.15	192.168.140.20	DCERPC	274 Alter_context: call_id: 27, Fragment: Single, 1 context items: ISystemActivator V0.0 (32bit NDR)
1655 1059.193495	192.168.140.20	192.168.140.15	DCERPC	159 Alter_context_resp: call_id: 27, Fragment: Single, max_xmit: 5840 max_recv: 5840, 1 results: Acceptance
1656 1059.193916	192.168.140.15	192.168.140.20	ISyste…	878 RemoteCreateInstance request
1657 1059.196230	192.168.140.20	192.168.140.15	DCERPC	86 Fault: call_id: 27, Fragment: Single, Ctx: 1, status: nca_s_fault_access_denied
1658 1059.196230	192.168.140.20	192.168.140.15	TCP	60 135 → 50240 [FIN, ACK] Seq=375 Ack=2762 Win=2101248 Len=0
1659 1059.196298	192.168.140.15	192.168.140.20	TCP	54 50240 → 135 [ACK] Seq=2762 Ack=376 Win=65280 Len=0
1660 1059.196485	192.168.140.15	192.168.140.20	TCP	54 50240 → 135 [FIN, ACK] Seq=2762 Ack=376 Win=65280 Len=0
1661 1059.196676	192.168.140.20	192.168.140.15	TCP	60 135 → 50240 [ACK] Seq=376 Ack=2763 Win=2101248 Len=0
1663 1059.244157	192.168.140.15	192.168.140.20	TCP	54 50239 → 135 [ACK] Seq=141 Ack=233 Win=65280 Len=0

Collector Agent 验证用户组关系报文格式：



267 211.868112	192.168.140.15	192.168.140.11	ICMP	159 Destination unreachable (Port unreachable)
268 211.870742	192.168.140.15	192.168.140.11	TCP	66 50157 → 135 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
269 211.871000	192.168.140.11	192.168.140.15	TCP	66 135 → 50157 [SYN, ACK, ECN] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
270 211.871048	192.168.140.15	192.168.140.11	TCP	54 50157 → 135 [ACK] Seq=1 Ack=1 Win=525568 Len=0
271 211.871221	192.168.140.15	192.168.140.11	DCERPC	170 Bind: call_id: 22, Fragment: Single, 2 context items: IOXIDResolver V0.0 (32bit NDR), IOXIDResolver V0.0 (6cb71c2c-9812-4
272 211.871755	192.168.140.11	192.168.140.15	DCERPC	138 Bind_ack: call_id: 22, Fragment: Single, max_xmit: 5840 max_recv: 5840, 2 results: Acceptance, Negotiate ACK
273 211.871891	192.168.140.15	192.168.140.11	IOXIDR…	78 ServerAlive2 request IOXIDResolver V0
274 211.872171	192.168.140.11	192.168.140.15	IOXIDR…	190 ServerAlive2 response
275 211.872710	192.168.140.15	192.168.140.11	TCP	66 50158 → 135 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
276 211.873117	192.168.140.11	192.168.140.15	TCP	66 135 → 50158 [SYN, ACK, ECN] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
277 211.873148	192.168.140.15	192.168.140.11	TCP	54 50158 → 135 [ACK] Seq=1 Ack=1 Win=525568 Len=0
278 211.873749	192.168.140.15	192.168.140.11	DCERPC	1753 Bind: call_id: 23, Fragment: Single, 1 context items: ISystemActivator V0.0 (32bit NDR)
279 211.873976	192.168.140.11	192.168.140.15	TCP	60 135 → 50158 [ACK] Seq=1 Ack=1700 Win=525568 Len=0
280 211.875359	192.168.140.11	192.168.140.15	DCERPC	291 Bind_ack: call_id: 23, Fragment: Single, max_xmit: 5840 max_recv: 5840, 1 results: Acceptance
281 211.875620	192.168.140.15	192.168.140.11	DCERPC	274 Alter_context: call_id: 23, Fragment: Single, 1 context items: ISystemActivator V0.0 (32bit NDR)
282 211.876337	192.168.140.11	192.168.140.15	DCERPC	159 Alter_context_resp: call_id: 23, Fragment: Single, max_xmit: 5840 max_recv: 5840, 1 results: Acceptance
283 211.876546	192.168.140.15	192.168.140.11	ISyste…	878 RemoteCreateInstance request
284 211.876956	192.168.140.11	192.168.140.15	DCERPC	86 Fault: call_id: 23, Fragment: Single, Ctx: 1, status: nca_s_fault_access_denied
285 211.877011	192.168.140.15	192.168.140.11	TCP	54 50158 → 135 [FIN, ACK] Seq=2744 Ack=375 Win=525056 Len=0
286 211.877069	192.168.140.11	192.168.140.15	TCP	60 135 → 50158 [FIN, ACK] Seq=375 Ack=2744 Win=524544 Len=0

Fortigate 与 Collector Agent 报文格式



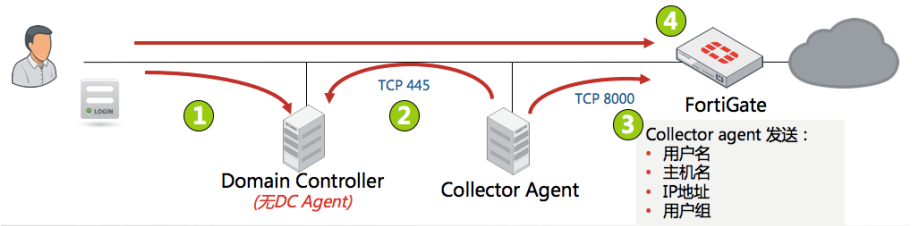
2.3. 基于 Agent 的 Collector Polling 模式

只在 Windows server 上安装 collector agent，不需要 FSSO DC agent，Collector agent 每隔几秒查询每一个 DC 的用户登录事件，默认使用 TCP 445 端口和 TCP 135 端口, TCP 139 和 UDP 137 做备用，在 DC 上必须开启事件日志，降低安装复杂性，减少日常维护。

三种模式中 NetAPI 可以不开启审计事件，WinSecLog 和 WMI 均需开启审计事件，只是查询方式不一样

基于 Agent 的 Collector Polling 模式认证流程见下图

1. 用户在域控制器 (DC)上认证
2. Collector agent频繁的查询DC，获取用户登录事件
3. Collector agent转发登录信息给FortiGate.
4. 用户不需要再次认证



基于 Agent 的 Collector Polling 模式可以有以下三种方式获取事件日志

*****在我们日常使用中采用 winSecLog 的方式居多

2.3.1. 相应流程

1、CA 通过 SMB2 查询 Event Log（port 445）、CA 通过 NETAPI 查询用户登录信息、CA 通过 WMI 查询用户登录信息，CA 同时需要验证客户端 IP，因为发送的 Log 只有用户名和主机名

2、CA 检测 DNS 看客户端 IP 地址是否改变（IP address change verify interval 60s）

3、CA 工作站检测，是否 Logoff，通过 Check HKEY_USERS (Workstation verify Interval 5m)

4、如果工作站存活检测未检测成功，480 分钟后用户条目（Dead entry timeout 480m）

5、CA 进行用户的组成员查找：通过目录访问或者 API 验证组信息

6、发送信息给 Fortigate

2.3.2. Winlog 报文格式

与 2.2.2 报文格式的唯一区别是 CA 通过 SMB2 查询 Event Log 的报文

229	3.027697	192.168.140.15	192.168.140.11	TCP	54	49812 → 445 [ACK] Seq=1231 Ack=32605 Win=2053 Len=0
230	3.031039	192.168.140.15	192.168.140.10	SMB2	194	Create Request File: EVENTLOG
231	3.031758	192.168.140.10	192.168.140.15	SMB2	210	Create Response File: EVENTLOG
232	3.031940	192.168.140.15	192.168.140.10	DCERPC	330	Bind: call_id: 2, Fragment: Single, 3 context items: EVENTLOG V0.0 (32bit NDR), EVENT
233	3.032351	192.168.140.10	192.168.140.15	SMB2	138	Write Response
234	3.032474	192.168.140.15	192.168.140.10	SMB2	171	Read Request Len:1024 Off:0 File: EVENTLOG
235	3.032728	192.168.140.10	192.168.140.15	DCERPC	258	Bind_ack: call_id: 2, Fragment: Single, max_xmit: 4280 max_recv: 4280, 3 results: Pro
236	3.032861	192.168.140.15	192.168.140.10	DCERPC	298	Request: call_id: 2, Fragment: Single, opnum: 7, Ctx: 1
237	3.033511	192.168.140.10	192.168.140.15	DCERPC	202	Fault: call_id: 2, Fragment: Single, Ctx: 1, status: nca_s_fault_access_denied
238	3.033679	192.168.140.15	192.168.140.10	SMB2	146	Close Request File: EVENTLOG
239	3.033929	192.168.140.10	192.168.140.15	SMB2	182	Close Response
240	3.034704	192.168.140.15	192.168.140.10	SMB2	194	Create Request File: EVENTLOG
241	3.035103	192.168.140.10	192.168.140.15	SMB2	210	Create Response File: EVENTLOG
242	3.035267	192.168.140.15	192.168.140.10	DCERPC	330	Bind: call_id: 2, Fragment: Single, 3 context items: EVENTLOG V0.0 (32bit NDR), EVENT
243	3.035529	192.168.140.10	192.168.140.15	SMB2	138	Write Response
244	3.035629	192.168.140.15	192.168.140.10	SMB2	171	Read Request Len:1024 Off:0 File: EVENTLOG
245	3.035926	192.168.140.10	192.168.140.15	DCERPC	258	Bind_ack: call_id: 2, Fragment: Single, max_xmit: 4280 max_recv: 4280, 3 results: Pro
246	3.036086	192.168.140.15	192.168.140.10	DCERPC	298	Request: call_id: 2, Fragment: Single, opnum: 7, Ctx: 1
247	3.036556	192.168.140.10	192.168.140.15	DCERPC	202	Fault: call_id: 2, Fragment: Single, Ctx: 1, status: nca_s_fault_access_denied
248	3.037532	192.168.140.15	192.168.140.10	SMB2	146	Close Request File: EVENTLOG
249	3.037925	192.168.140.10	192.168.140.15	SMB2	182	Close Response

2.3.3. NETAPI 报文格式

与 2.2.2 报文格式的唯一区别是 CA 通过 NETAPI 查询用户信息

11	5.513120	192.168.140.15	192.168.140.11	SMB2	190	Create Request File: srvsvc
12	5.513832	192.168.140.11	192.168.140.15	SMB2	210	Create Response File: srvsvc
13	5.514083	192.168.140.15	192.168.140.11	DCERPC	330	Bind: call_id: 2, Fragment: Single, 3 context items: SRVSVC V3.0 (32bit
14	5.514521	192.168.140.11	192.168.140.15	SMB2	138	Write Response
15	5.514697	192.168.140.11	192.168.140.15	SMB2	171	Read Request Len:1024 Off:0 File: srvsvc
16	5.515004	192.168.140.11	192.168.140.15	DCERPC	254	Bind_ack: call_id: 2, Fragment: Single, max_xmit: 4280 max_recv: 4280, 3
17	5.515228	192.168.140.15	192.168.140.11	DCERPC	342	Request: call_id: 2, Fragment: Single, opnum: 12, Ctx: 1
18	5.515760	192.168.140.11	192.168.140.15	DCERPC	386	Response: call_id: 2, Fragment: Single, Ctx: 1
19	5.515918	192.168.140.15	192.168.140.11	SMB2	146	Close Request File: srvsvc
20	5.516120	192.168.140.11	192.168.140.15	SMB2	182	Close Response
21	5.528336	192.168.140.15	192.168.140.11	TCP	54	49801 → 445 [ACK] Seq=277 Ack=85 Win=2049 Len=0
22	5.528424	192.168.140.15	192.168.140.11	TCP	54	49813 → 445 [ACK] Seq=229 Ack=285 Win=2049 Len=0
23	5.528584	192.168.140.15	192.168.140.10	SMB2	190	Create Request File: srvsvc
24	5.529342	192.168.140.10	192.168.140.15	SMB2	210	Create Response File: srvsvc
25	5.529486	192.168.140.15	192.168.140.10	DCERPC	330	Bind: call_id: 2, Fragment: Single, 3 context items: SRVSVC V3.0 (32bit
26	5.529797	192.168.140.10	192.168.140.15	SMB2	138	Write Response
27	5.529977	192.168.140.15	192.168.140.10	SMB2	171	Read Request Len:1024 Off:0 File: srvsvc
28	5.530307	192.168.140.10	192.168.140.15	DCERPC	254	Bind_ack: call_id: 2, Fragment: Single, max_xmit: 4280 max_recv: 4280, 3
29	5.530499	192.168.140.15	192.168.140.10	DCERPC	358	Request: call_id: 2, Fragment: Single, opnum: 12, Ctx: 1
30	5.531351	192.168.140.10	192.168.140.15	DCERPC	530	Response: call_id: 2, Fragment: Single, Ctx: 1
31	5.531571	192.168.140.15	192.168.140.10	SMB2	146	Close Request File: srvsvc
32	5.531891	192.168.140.10	192.168.140.15	SMB2	182	Close Response

2.3.4. WMI 报文格式

与 2.2.2 报文格式的唯一区别是 CA 通过 WMI 查询用户信息

135	0.055425	192.168.140.15	192.168.140.10	TCP	66	49921 → 49666 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
136	0.055678	192.168.140.10	192.168.140.15	TCP	66	49666 → 49921 [SYN, ACK, ECN] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
137	0.055713	192.168.140.15	192.168.140.10	TCP	54	49921 → 49666 [ACK] Seq=1 Ack=1 Win=525568 Len=0
149	0.058090	192.168.140.15	192.168.140.10	DCERPC	1918	Bind: call_id: 2, Fragment: Single, 3 context items: IRemUnknown2 V0.0 (32bit NDR), IRemUnknown2 V0.0 (64bit NDR), IRemUnk…
150	0.058196	192.168.140.10	192.168.140.15	TCP	60	49666 → 49921 [ACK] Seq=1 Ack=1865 Win=525568 Len=0
151	0.058739	192.168.140.10	192.168.140.15	DCERPC	339	Bind_ack: call_id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 3 results: Acceptance, Provider rejection, Negotiat…
152	0.058921	192.168.140.15	192.168.140.10	DCERPC	274	Alter_context: call_id: 2, Fragment: Single, 1 context items: IRemUnknown2 V0.0 (32bit NDR)
153	0.059285	192.168.140.10	192.168.140.15	DCERPC	159	Alter_context_resp: call_id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 1 results: Acceptance
154	0.059478	192.168.140.15	192.168.140.10	IRemUn…	210	RemQueryInterface request IID[1]=IWbemLoginClientID
155	0.059794	192.168.140.10	192.168.140.15	IRemUn…	194	RemQueryInterface response S_OK[1] -> S_OK
156	0.060059	192.168.140.15	192.168.140.10	DCERPC	126	Alter_context: call_id: 3, Fragment: Single, 1 context items: IWbemLoginClientID V0.0 (32bit NDR)
157	0.060230	192.168.140.10	192.168.140.15	DCERPC	110	Alter_context_resp: call_id: 3, Fragment: Single, max_xmit: 5840 max_recv: 5840, 1 results: Acceptance
158	0.060293	192.168.140.15	192.168.140.10	DCERPC	210	Request: call_id: 3, Fragment: Single, opnum: 3, Ctx: 2 IWbemLoginClientID V0
159	0.060469	192.168.140.10	192.168.140.15	DCERPC	130	Response: call_id: 3, Fragment: Single, Ctx: 2 IWbemLoginClientID V0
160	0.060544	192.168.140.15	192.168.140.10	DCERPC	126	Alter_context: call_id: 4, Fragment: Single, 1 context items: IWbemLevel1Login V0.0 (32bit NDR)
161	0.060645	192.168.140.10	192.168.140.15	DCERPC	110	Alter_context_resp: call_id: 4, Fragment: Single, max_xmit: 5840 max_recv: 5840, 1 results: Acceptance
162	0.060703	192.168.140.15	192.168.140.10	DCERPC	178	Request: call_id: 4, Fragment: Single, opnum: 3, Ctx: 3 IWbemLevel1Login V0
163	0.060859	192.168.140.10	192.168.140.15	DCERPC	130	Response: call_id: 4, Fragment: Single, Ctx: 3 IWbemLevel1Login V0
164	0.061039	192.168.140.15	192.168.140.10	DCERPC	338	Request: call_id: 5, Fragment: Single, opnum: 6, Ctx: 3 IWbemLevel1Login V0
165	0.061615	192.168.140.10	192.168.140.15	DCERPC	322	Response: call_id: 5, Fragment: Single, Ctx: 3 IWbemLevel1Login V0
166	0.062619	192.168.140.15	192.168.140.10	IRemUn…	226	RemRelease request Cnt=2 Refs=5-0,5-0
167	0.062885	192.168.140.10	192.168.140.15	IRemUn…	130	RemRelease response -> S_OK
168	0.063175	192.168.140.15	192.168.140.10	DCERPC	181	Alter_context: call_id: 7, Fragment: Single, 1 context items: IWbemServices V0.0 (32bit NDR), NTLMSSP_NEGOTIATE
169	0.063467	192.168.140.10	192.168.140.15	DCERPC	322	Alter_context_resp: call_id: 7, Fragment: Single, max_xmit: 5840 max_recv: 5840, 1 results: Acceptance, NTLMSSP_CHALLENGE
170	0.063870	192.168.140.15	192.168.140.10	DCERPC	508	AUTH3: call_id: 7, Fragment: Single, NTLMSSP_AUTH, User: DHL\SSO
171	0.063970	192.168.140.15	192.168.140.10	DCERPC	982	Request: call_id: 7, Fragment: Single, opnum: 22, Ctx: 4 IWbemServices V0
172	0.064055	192.168.140.10	192.168.140.15	TCP	60	49666 → 49921 [ACK] Seq=1407 Ack=4630 Win=525568 Len=0
180	0.085631	192.168.140.10	192.168.140.15	DCERPC	310	Response: call_id: 7, Fragment: Single, Ctx: 4 IWbemServices V0
181	0.086111	192.168.140.15	192.168.140.10	IRemUn…	210	RemQueryInterface request IID[1]=IWbemFetchSmartEnum
182	0.086408	192.168.140.10	192.168.140.15	IRemUn…	194	RemQueryInterface response S_OK[1] -> S_OK
183	0.086579	192.168.140.15	192.168.140.10	DCERPC	126	Alter_context: call_id: 9, Fragment: Single, 1 context items: IWbemFetchSmartEnum V0.0 (32bit NDR)
184	0.086742	192.168.140.10	192.168.140.15	DCERPC	110	Alter_context_resp: call_id: 9, Fragment: Single, max_xmit: 5840 max_recv: 5840, 1 results: Acceptance
185	0.086796	192.168.140.15	192.168.140.10	DCERPC	162	Request: call_id: 9, Fragment: Single, opnum: 3, Ctx: 5 IWbemFetchSmartEnum V0
186	0.087040	192.168.140.10	192.168.140.15	DCERPC	322	Response: call_id: 9, Fragment: Single, Ctx: 5 IWbemFetchSmartEnum V0
187	0.087168	192.168.140.15	192.168.140.10	DCERPC	126	Alter_context: call_id: 10, Fragment: Single, 1 context items: IWbemWCOSmartEnum V0.0 (32bit NDR)
188	0.087325	192.168.140.10	192.168.140.15	DCERPC	110	Alter_context_resp: call_id: 10, Fragment: Single, max_xmit: 5840 max_recv: 5840, 1 results: Acceptance

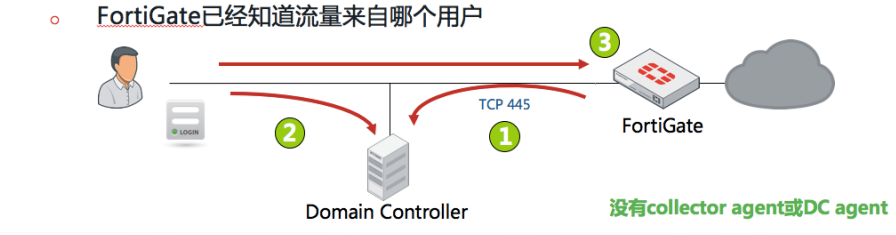
2.4. 无 Agent polling 模式

类似基于 agent polling，不过是使用 FortiGate 查询，不需要外部的 DC agent 或 collector agent，FortiGate 直接收集数据，必须在 DC 上开启事件日志，需要占用更多的 FortiGate 的 CPU 和 RAM，只支持 polling 选项 WinSecLog，FortiGate 使用 SMB 协议读取事件查看器日志，相比基于 agent 的 collector polling 模式，可用功能少。

相对来说此模式用的非常少，不多做介绍。

无 Agent polling 认证流程见下图

1. FortiGate频繁的查询DC，获取用户登录事件
2. 用户通过domain controller (DC)认证
   - FortiGate将在下一次查询中发现登录事件
3. 用户不需要再次认证
   - FortiGate已经知道流量来自哪个用户



使用防火墙查询同样需要开启 AD 的审计事件

2.5. 模式对比

	DC agent模式	Polling模式
安全	*复杂*— 多次安装(每DC一个)，需要重启	*简单* — 一次或零安装，不需要重启
DC agent 需求	Yes	No
资源	与DC agent共享	使用自身资源
可扩展性	更高	更低
冗余性	Yes	No
可信级别	捕获所有登录	可能丢失(NetAPI)，或有延迟(WinSecLog)

三. 前置配置

3.1. 域控制器日志开启

3.1.1. 关于 Microsoft Active Directory 日志 ID 介绍

FortiGate 的 FSSO Agent 目前支持微软的日志 ID 有 4768, 4769, 4776, 4624, 4770，这些日志 ID 可以被识别。

4624 位于组策略中“计算机配置---Windows 设置---安全设置---本地策略---审核策略---审核登录事件（audit Logon Events）”

4768, 4769, 4776, 4770 位于组策略中“计算机配置---Windows 设置---安全设置---本地策略---审核策略---审核登录事件（audit Account Logon Events）”同时需要开启 Kerberos 的审计，位于“计算机配置---Windows 设置---安全设置---高级审核策略配置---审核策略---账户登录”

Audit Logon Events

Event ID	Description
4624	An account was successfully logged on
4625	An account failed to log on
4648	A logon was attempted using explicit credentials
4634	An account was logged off
4647	User initiated logoff
4672	Special privileges assigned to new logon
4778	A session was reconnected to a Window Station

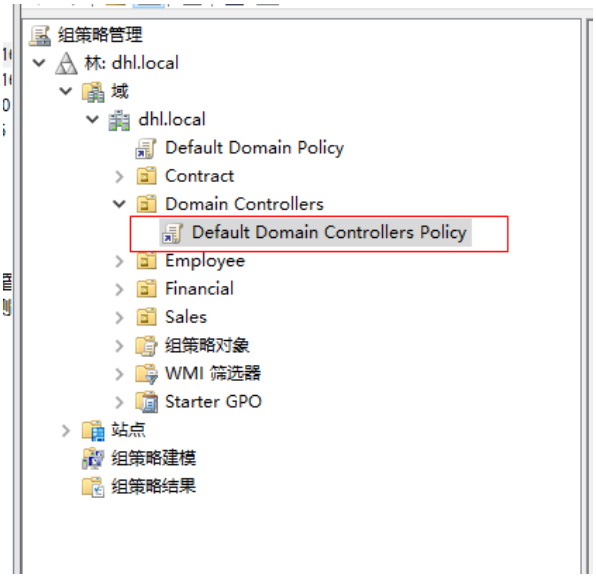
Audit Account Logon Events

Event ID	Description
4768	A Kerberos authentication ticket (TGT) was requested
4769	A Kerberos service ticket was requested
4770	A Kerberos service ticket was renewed
4771	Kerberos pre-authentication failed
4774	An account was mapped for logon
4776	The domain controller attempted to validate the credentials for an account

3.1.2. Windows Active Directory 2008/2012 开启日志 ID

目前支持的日志 ID，4770，4776，4768，4769 为 Kerberos 日志，必须确定 Windows server 上启用了 Kerberos 日志，否则 FSSO 默认将不能解析。

在 AD 里利用组策略管理新建组策略关联至 DC 或者使用默认的 Domain Controller Default Policy



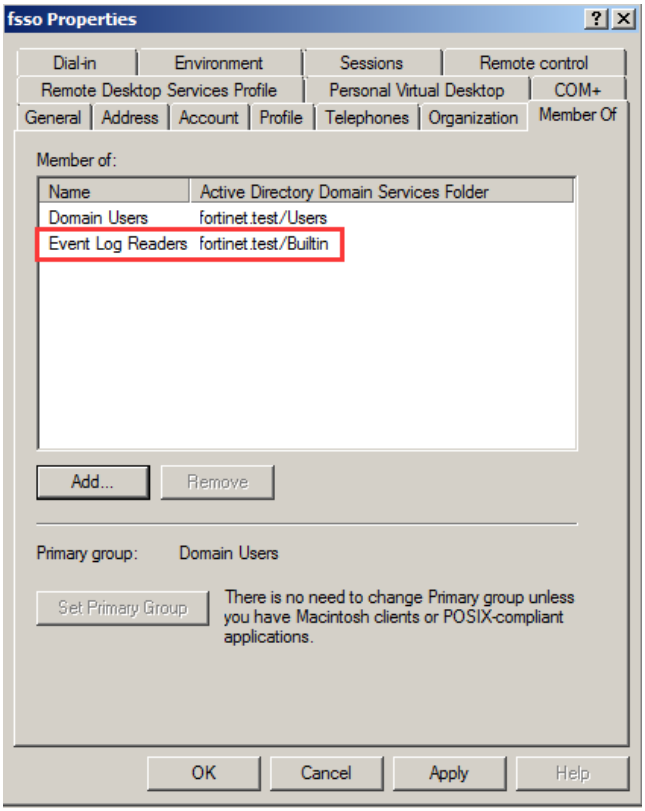
再在此策略汇中修改相应日志

设置完组策略后使用 gpupdate /force 刷新组策略

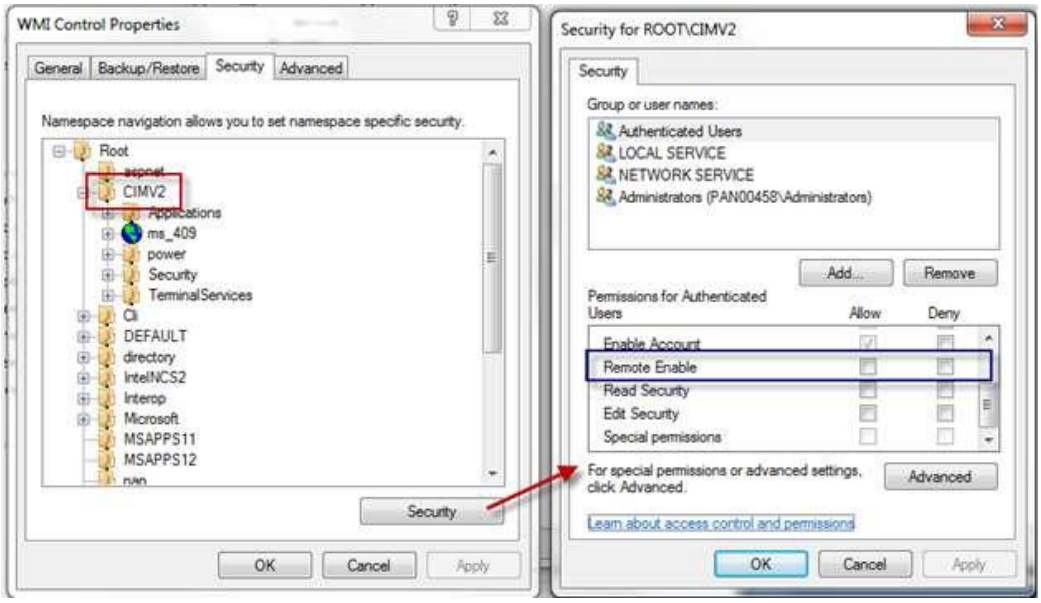
验证高级审计策略状态使用：Auditpol.exe /get /category:*

3.2. 创建服务账户

在 AD 域控服务器上面新建一个域账户 sso，将 sso 用户帐号添加到 Event Log Readers 组中，在系统服务中手工指定读取日志的域用户，操作步骤如下图所示



把这个账号添加到 WMI 功能里面：运行 wmimgmt.msc，执行 WMI 控件，右键属性，安全，root，CIMV2，设置，添加这个用户，同时 enable account、remote enable、read security 开启 allow。（非 WMI 查询可不要）



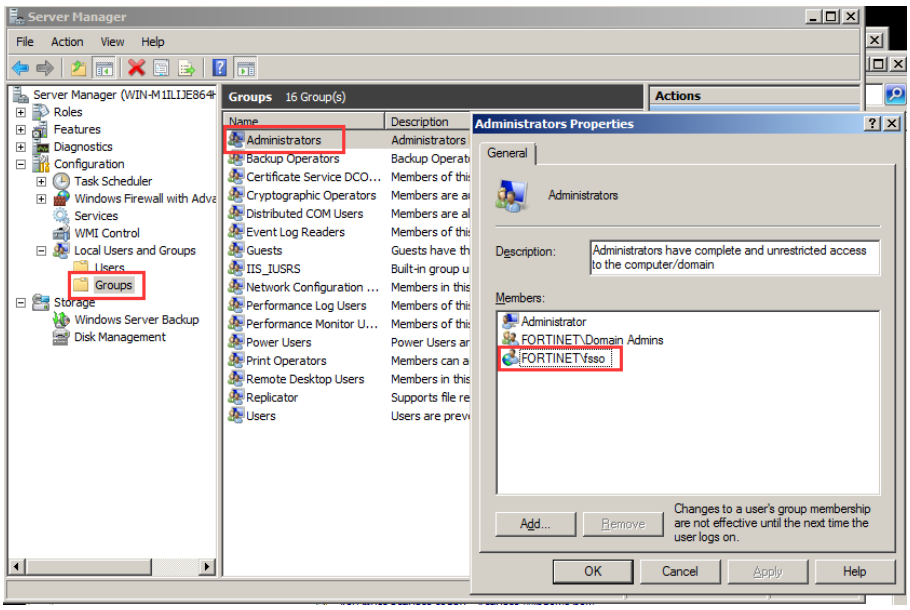
3.3. 创建 FSSO Agent 的服务器

创建一台 Windows Server 2008 或者 2012（以下简称域内主机），并加入到相应域内，硬件资源需求：4 个虚拟 CPU，8G 内存，硬盘无限制。

用本地 administrator 管理账号登录这台域内主机，将 3.2 创建的域用户 sso 加入到本地

administrators 组里面，然后切换用账号 Domian/sso 登陆。

sso 加入到本地 administrator 组里面操作如下：

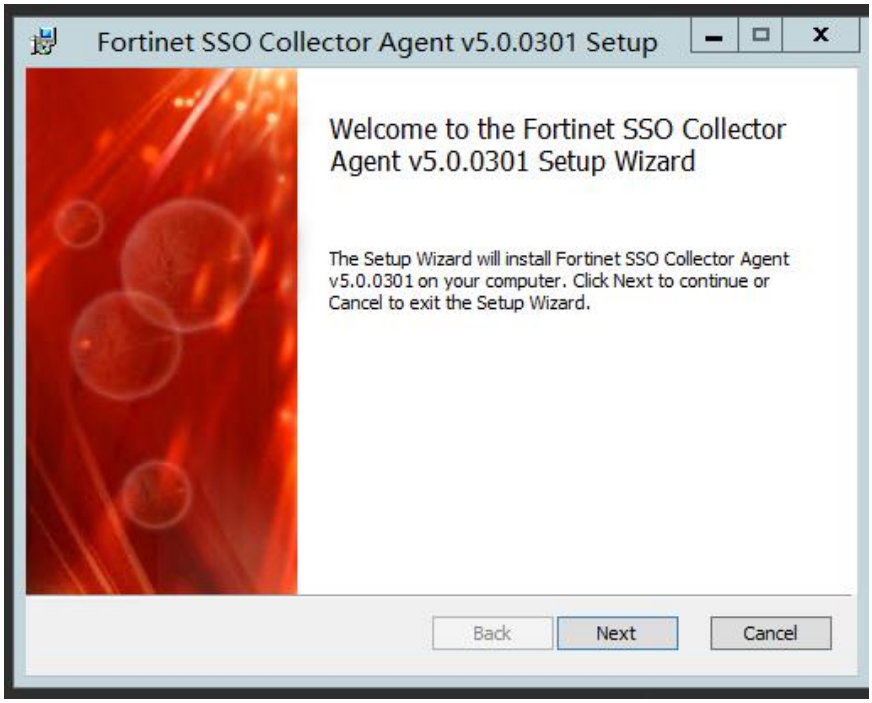


四. FSSO Agent 通用配置

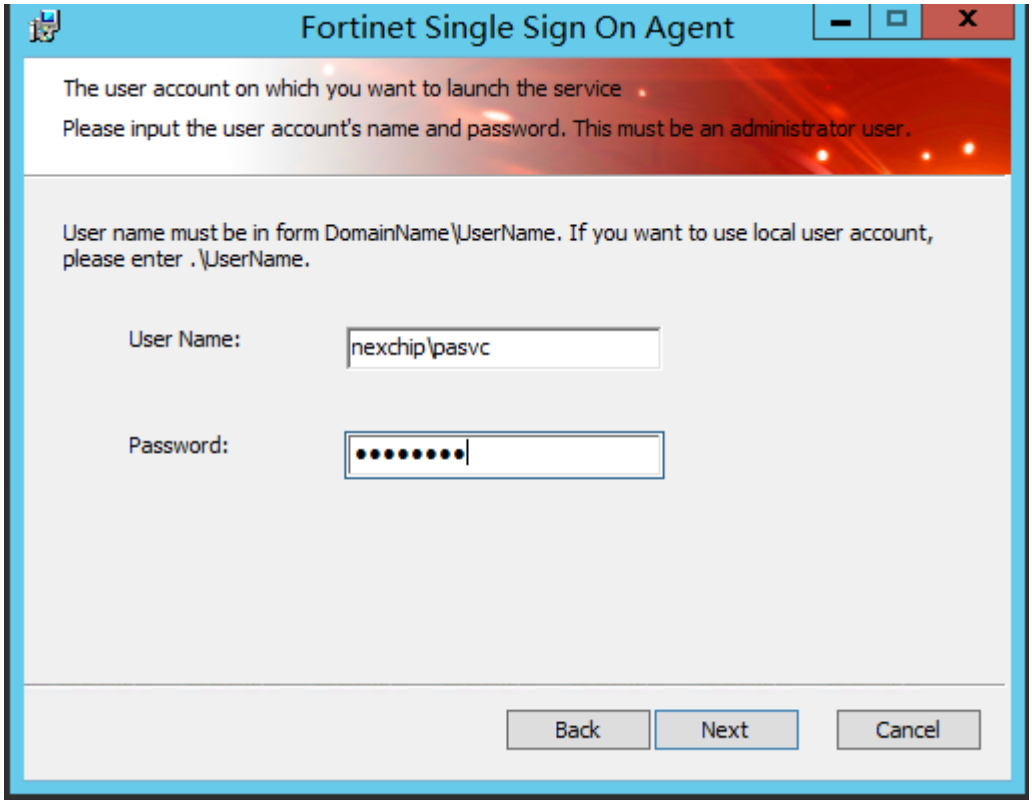
4.1. 安装程序

客户端程序：

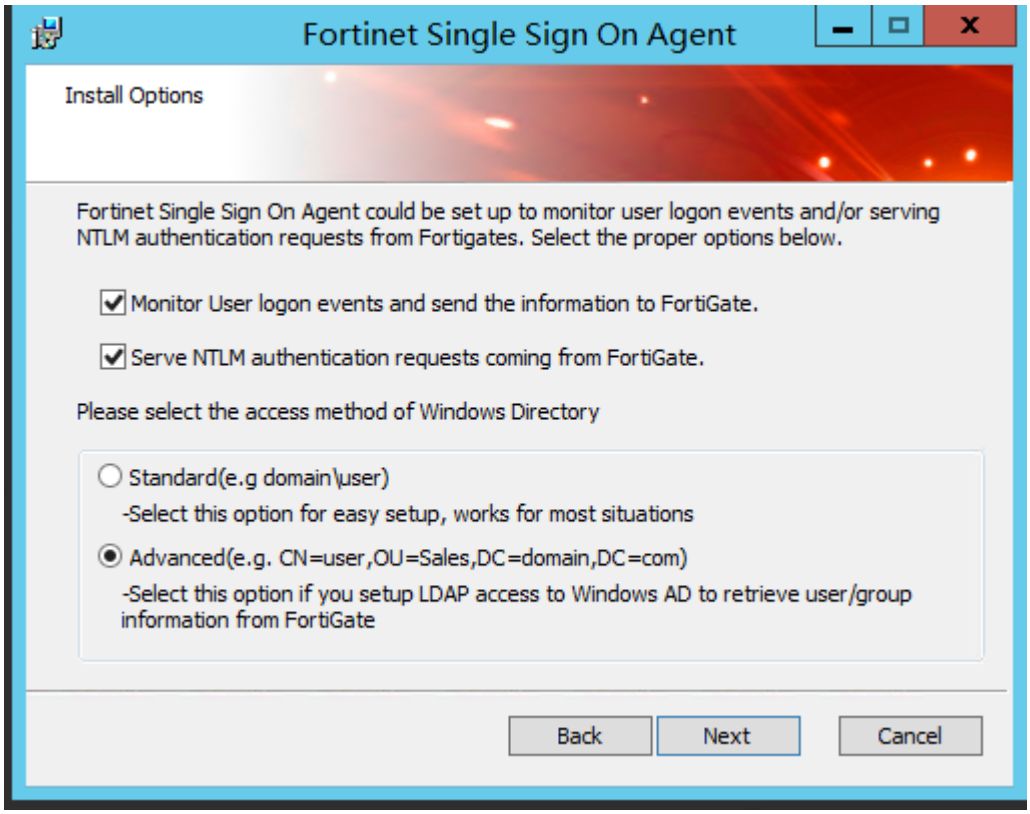
FSSO_Setup_5.0.0301_x64.exe



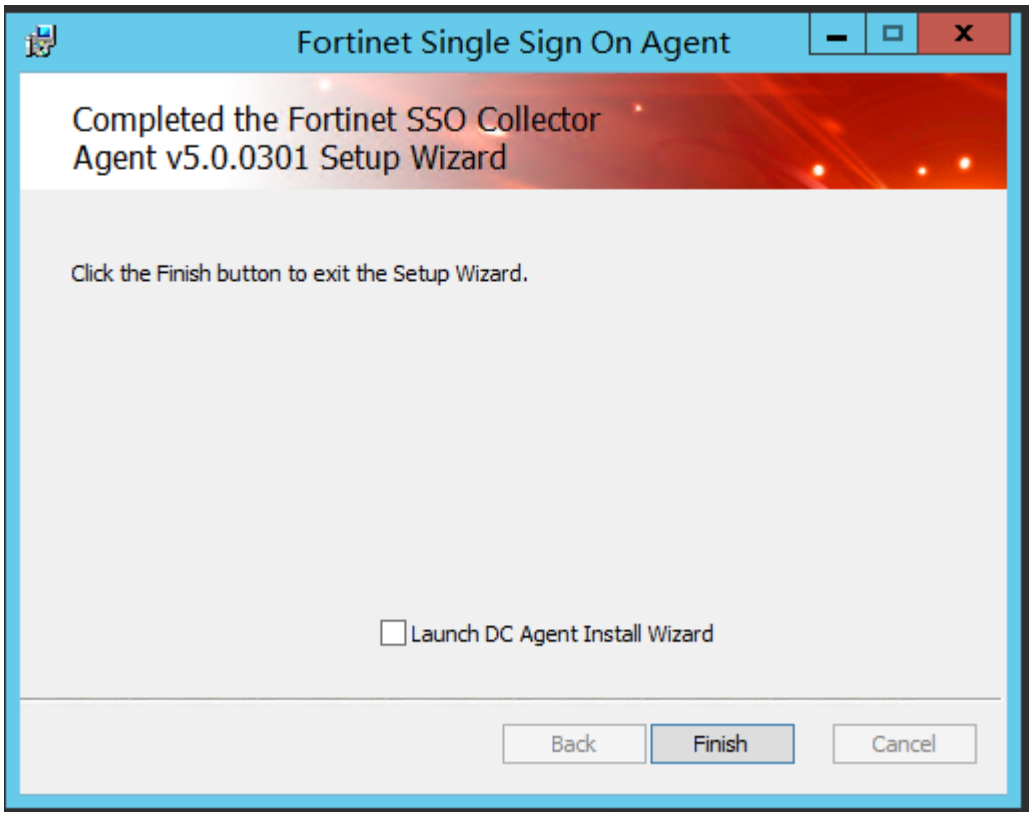
安装账户选择 domain\SSO，密码填入相应密码（该账户之前已经加入本机管理员组中）



Access mode 选择 Advanced



取消安装 DC Agent

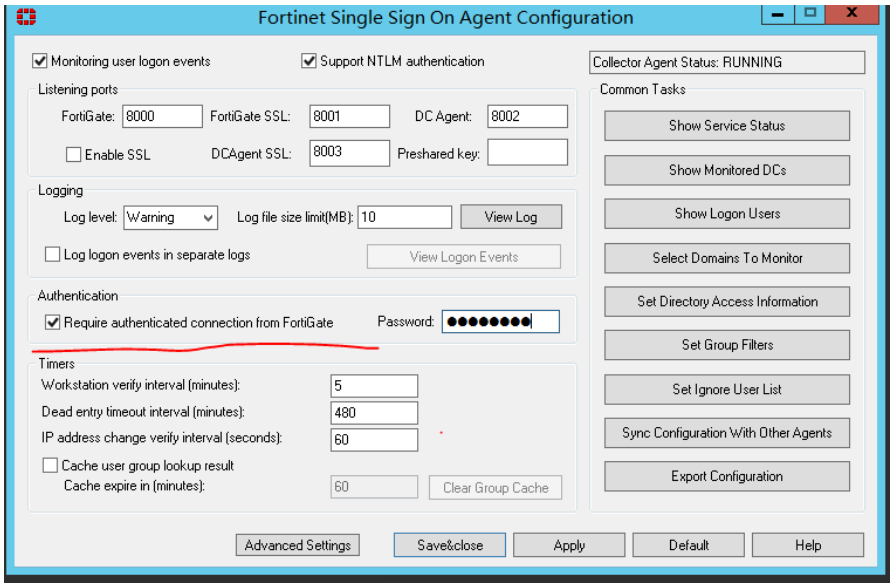


安装完毕后，

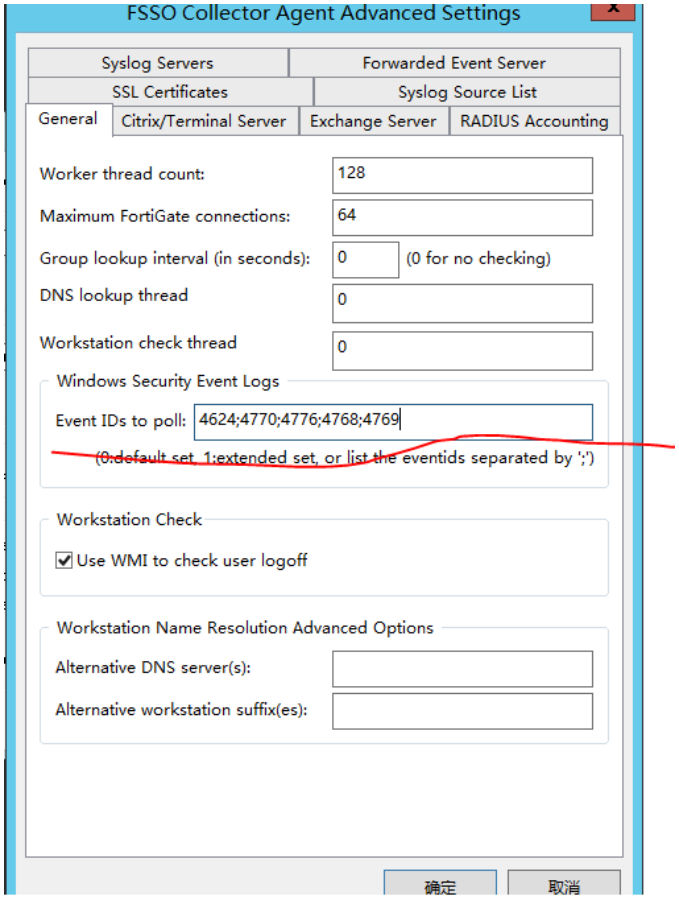
4.2. 配置 Collector Agent

选择开始菜单，下拉至 Configure Collector Agent

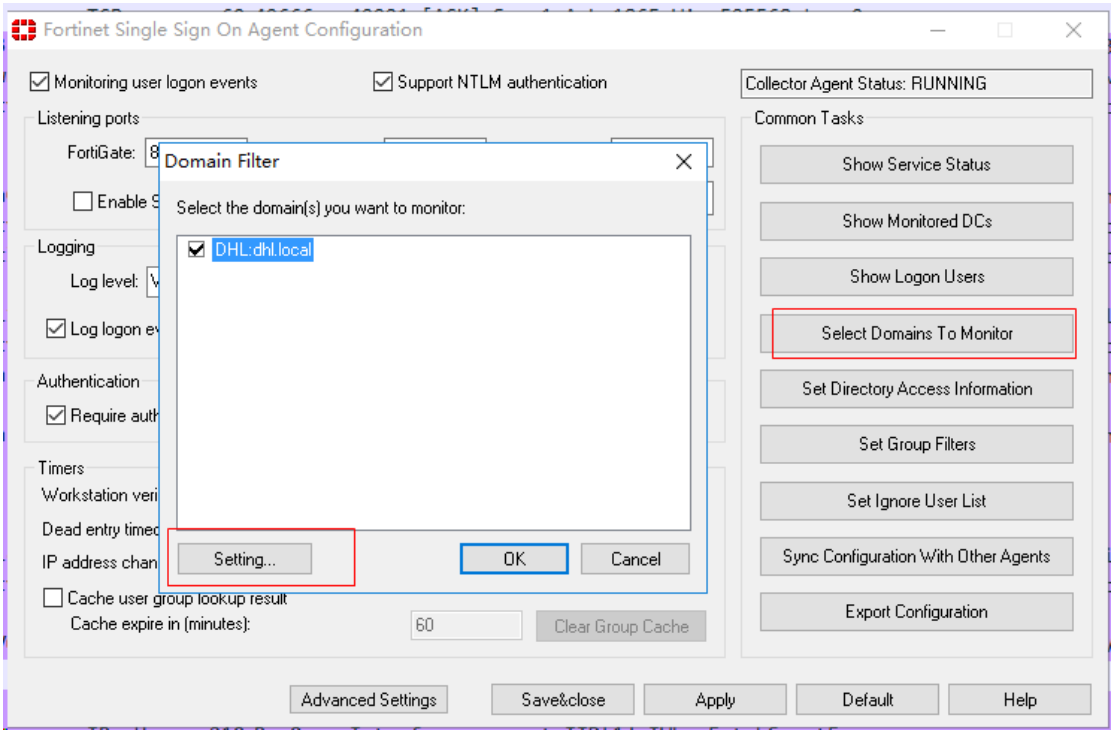
设置与 Fortinet 对接的密码（本次设置为 fortinet）



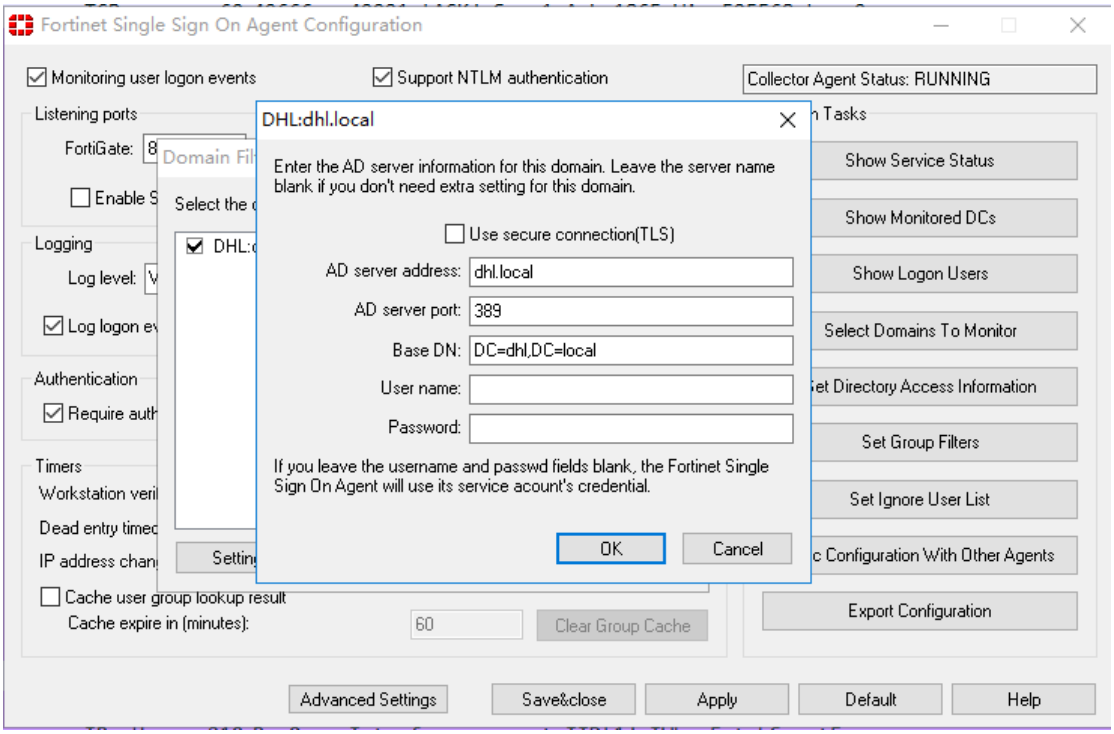
点击 advanced，选择要接受的日志 ID 后，点击确定



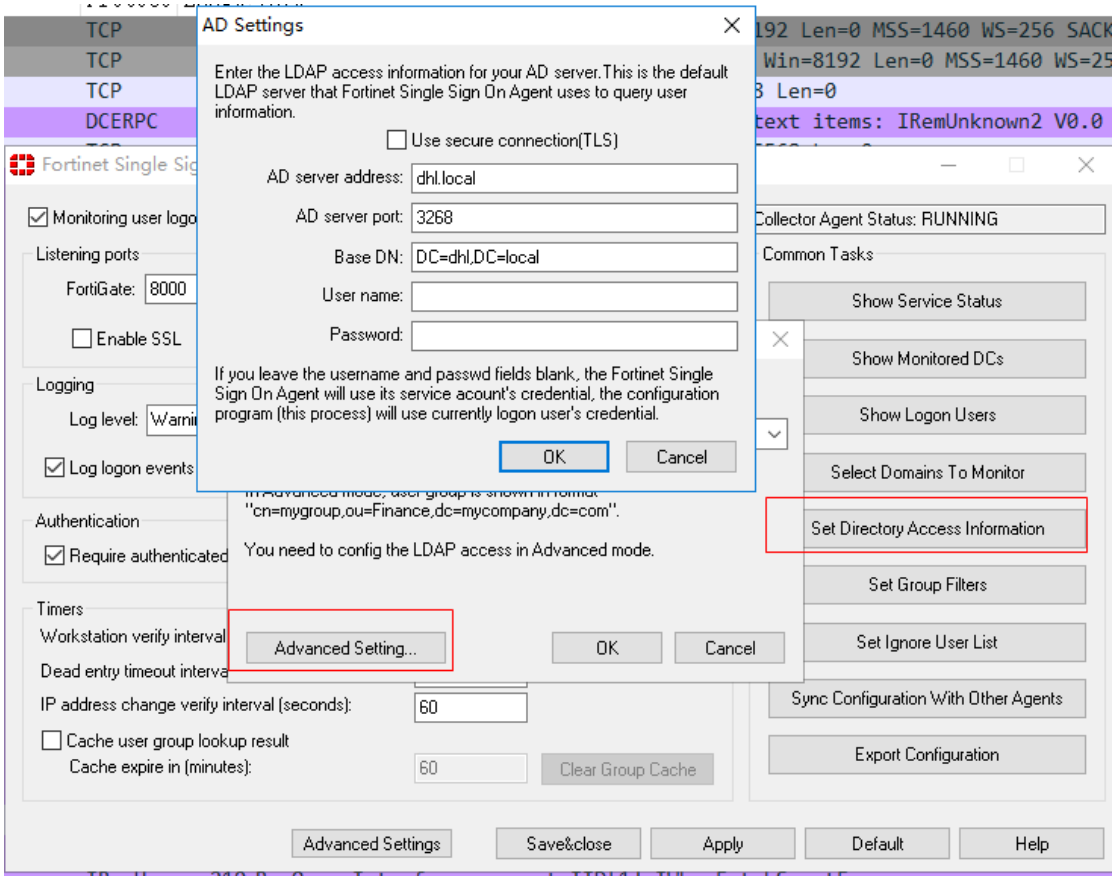
点击 Set Domain to monitor，去掉不需要监控的 Domain，针对选中的 domain 选择 Settings



AD Server Address 选择域名，通过 DNS 检索出所有的 DC，在用户名和密码中填入相应信息，也可以不填用户名和密码，利用安装账户去检索（不需要携带域名，他会从 base DN 中补充），完成后点击确定



点击 Set Directory Access Information-----advanced settings----输入访问活动目录的账户和密码，AD Server Address 用域名即可，用户名不需要携带域信息，也可以不填用户名，系统会用安装账户去检索，点击 OK。



以上步骤完成设置。

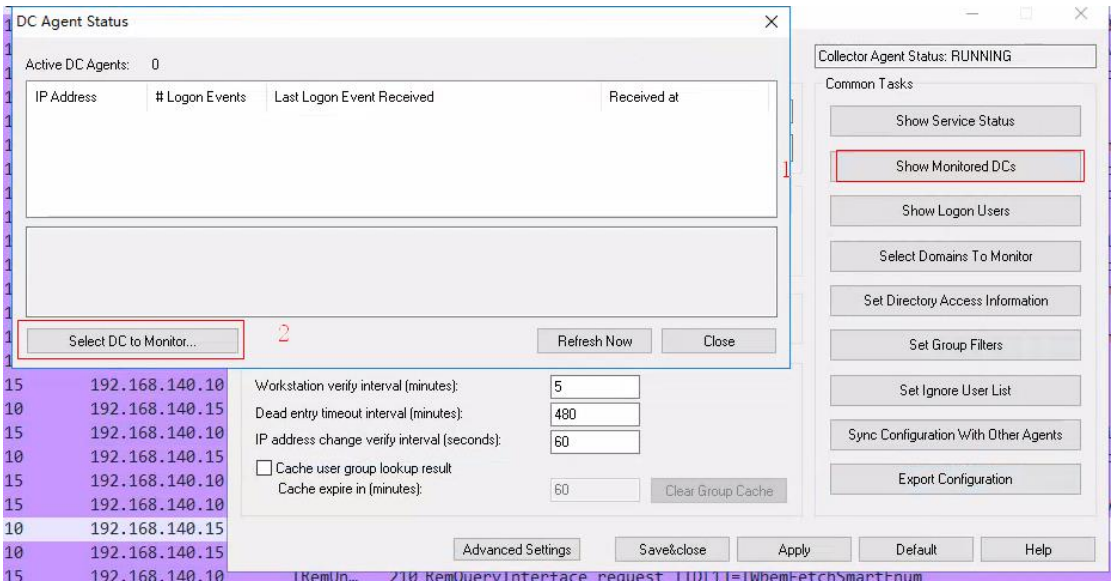
五. DC Agent 配置

关于 DC Agent 的安装有 2 种方式，一种是在 FSSO Agent 侧推送安装，另外一种是在 AD 服务器上主动安装，更推荐在 AD 服务器上主动安装，因为客户如果有多台 DC（Domain Controller），可以按照不同顺序安装，实现冗余。

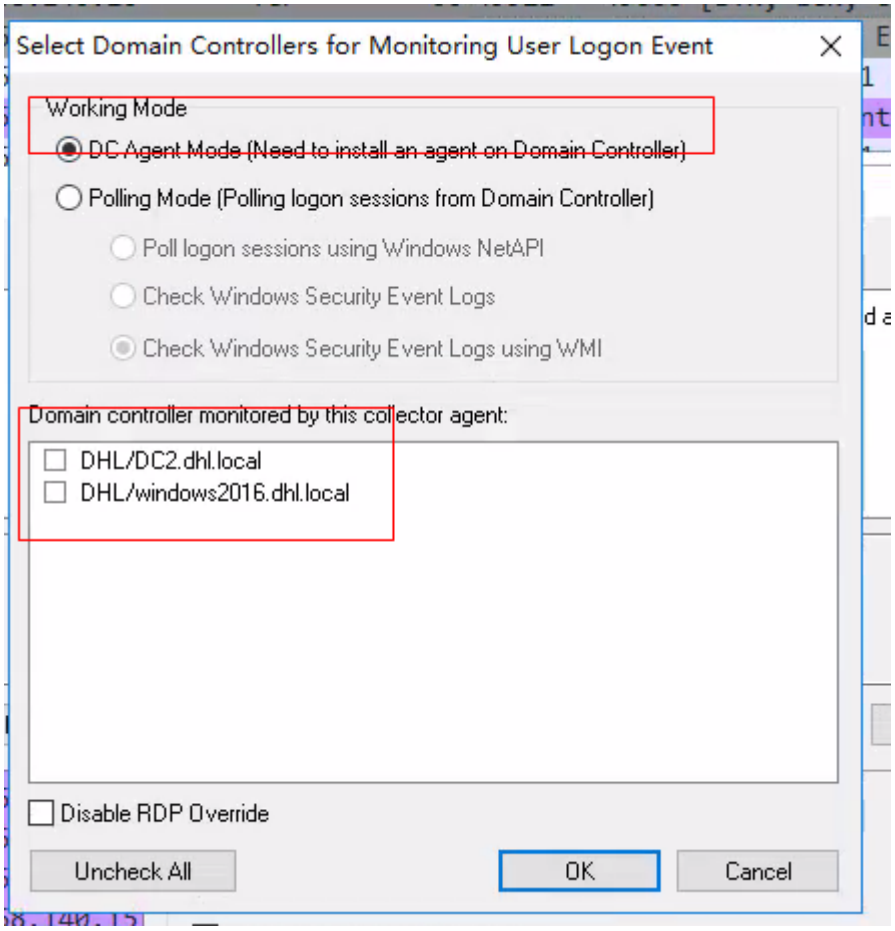
5.1. AD 服务器主动安装

5.1.1. 设置 FSSO Agent

点击 show monitored DC---select DC to monitor



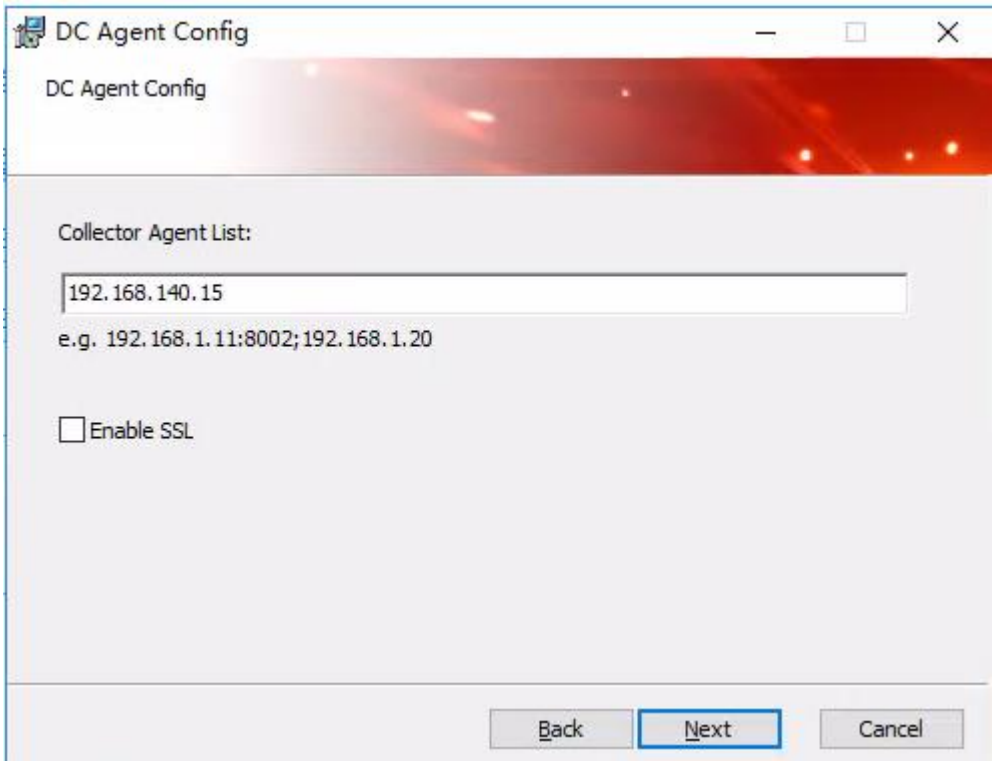
选择 DC Agent 模式，取消 DC 服务器的勾选选项，点击确定



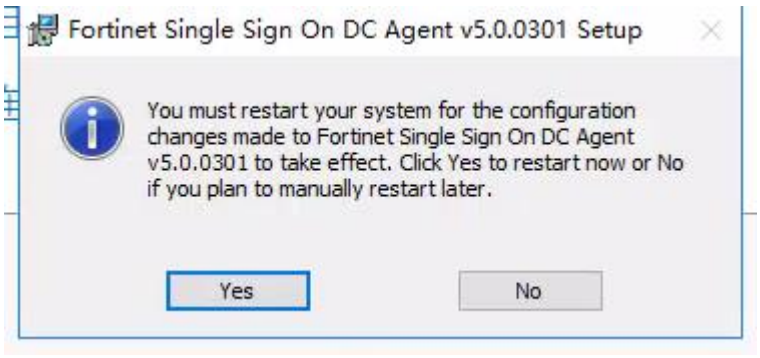
5.1.2. 安装 DC Agent

在 DC 服务器上安装 DC Agent

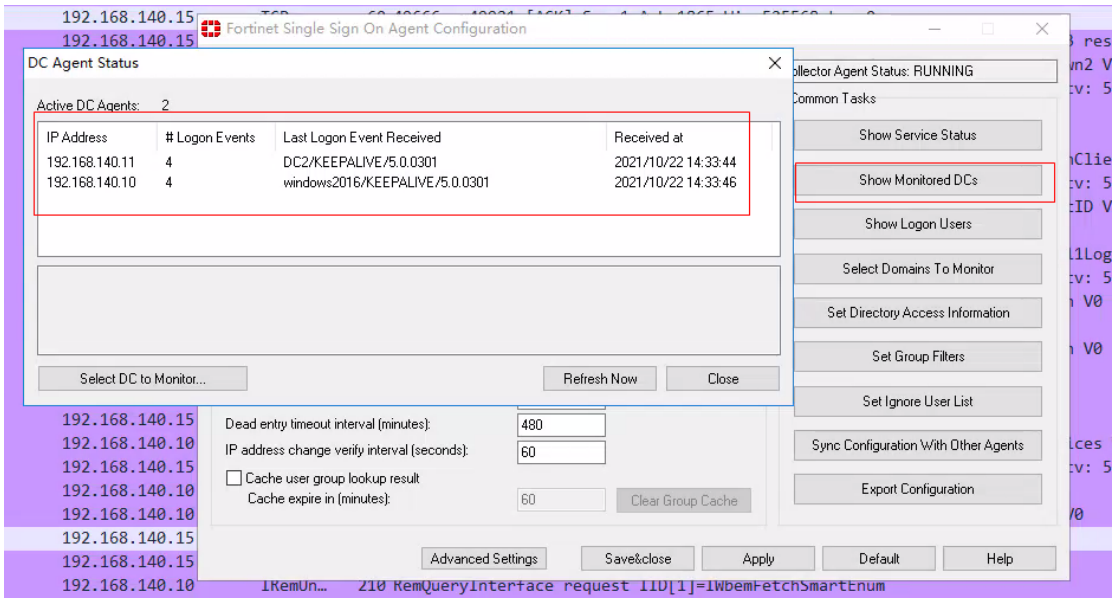
输入 collector Agent 地址，支持冗余，使用;进行分隔



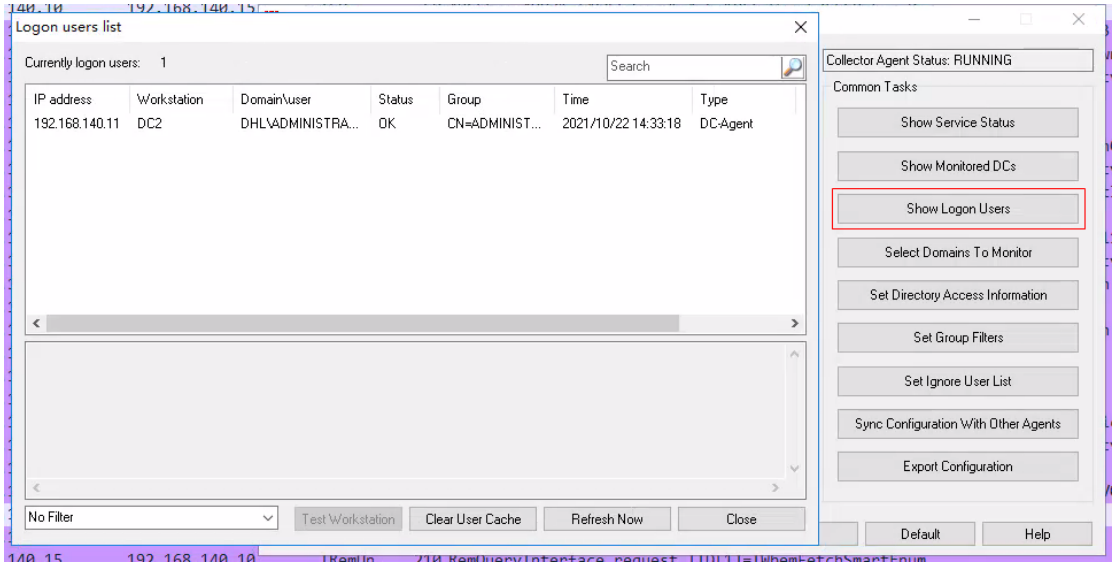
重启 DC 完成安装



验证：从 FSSO Agent 上可以看见 DC Agent 推送的消息

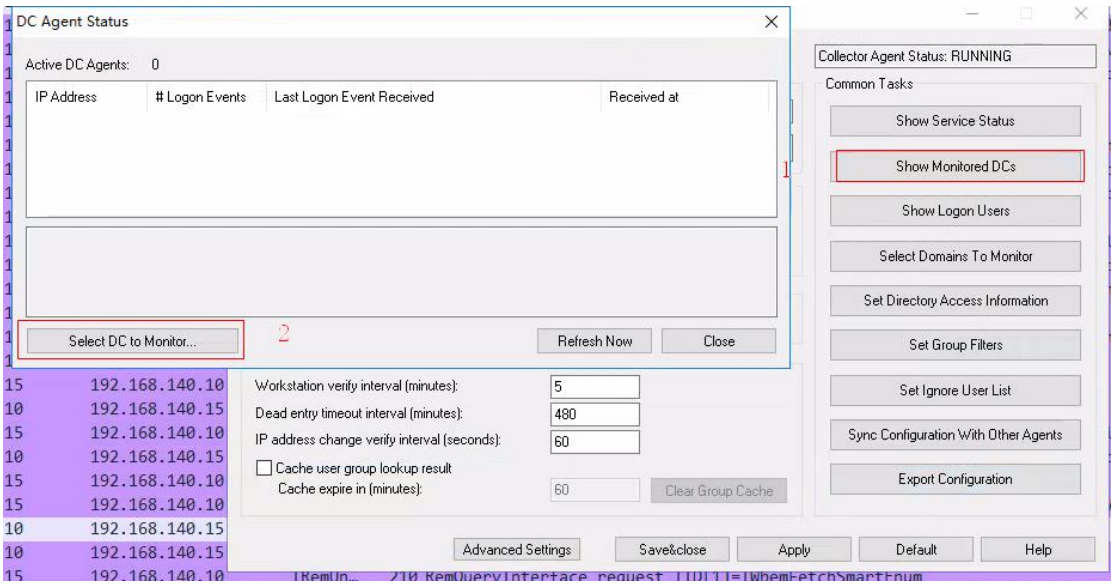


也可以看见用户的登录信息

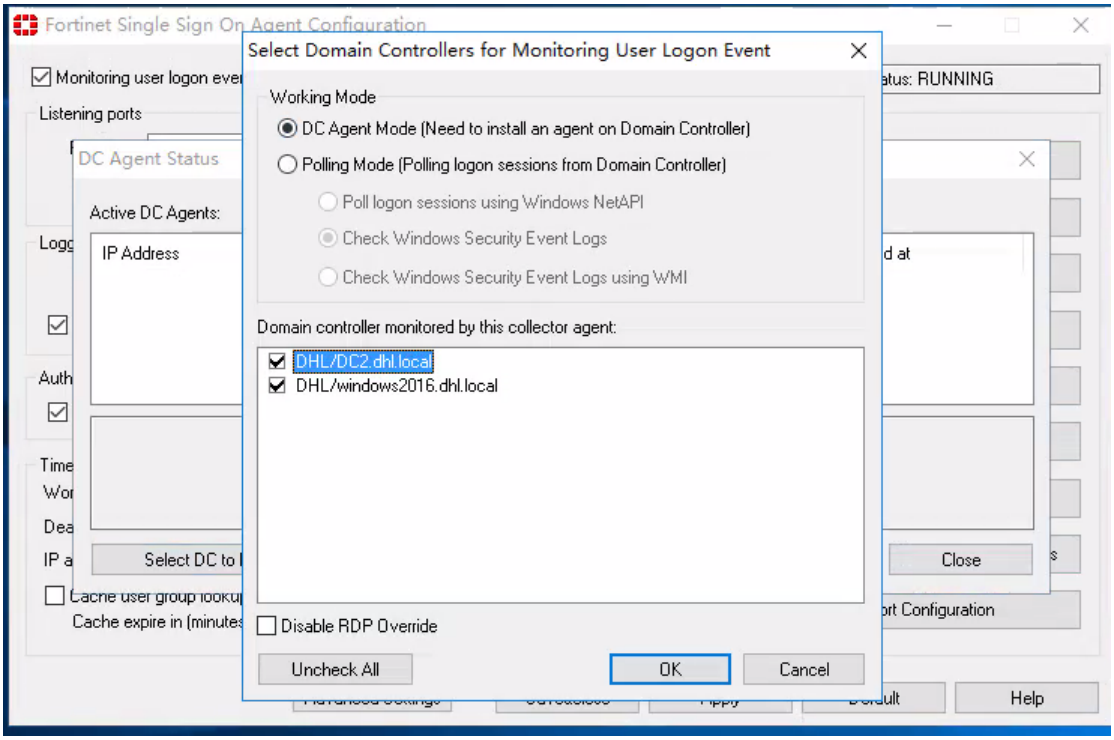


5.2. FSSO 主动推送

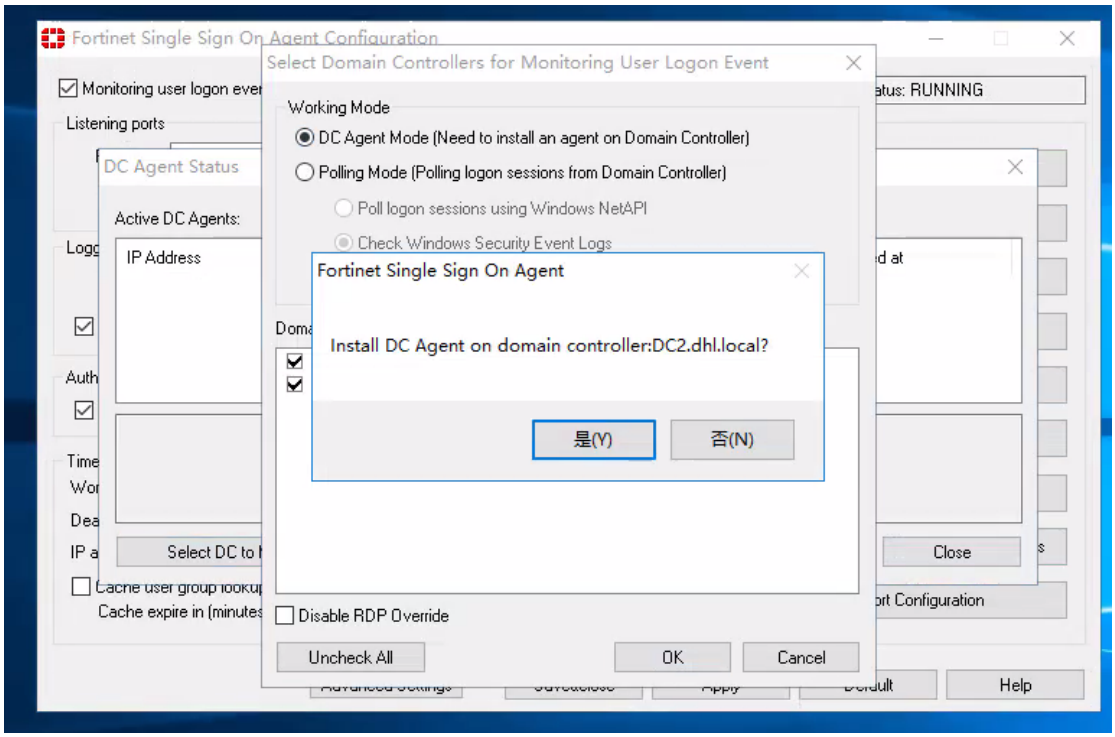
FSSO 主动推送安装比较方便，点击 show monitored DC---select DC to monitor



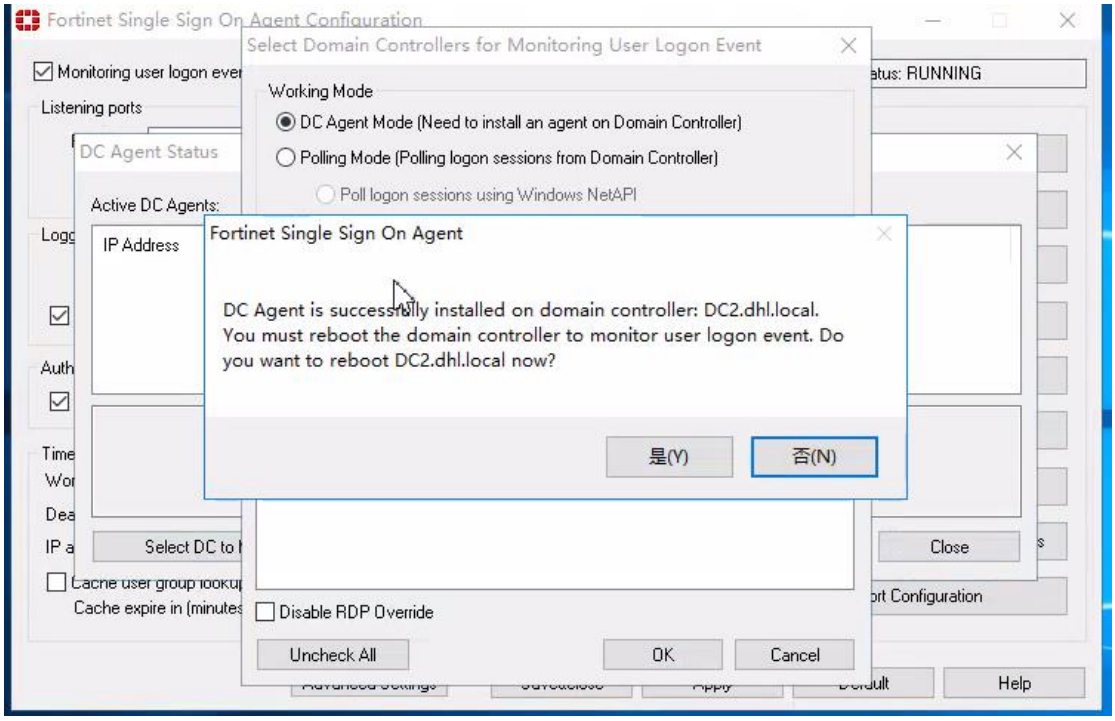
选择 DC Agent 模式，勾选 DC 服务器的选项，点击确定，FSSO Agent 会主动推送安装，安装完会自动重启，需要重启安装账户的权限。



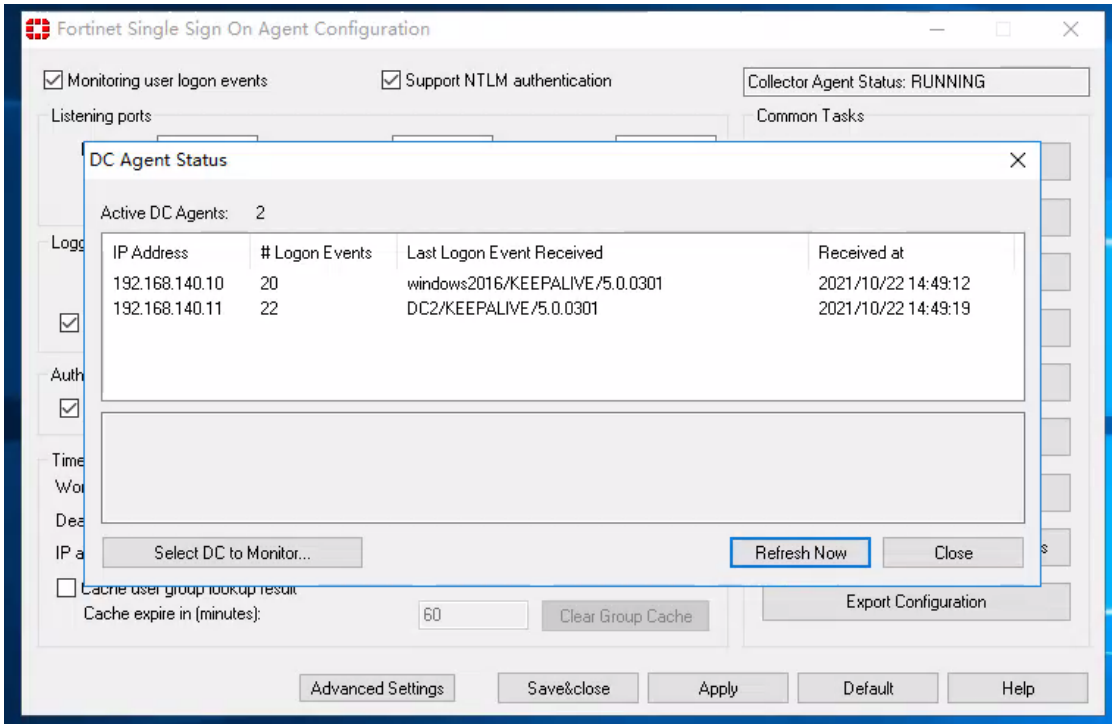
安装时会提示安装至相应的服务器



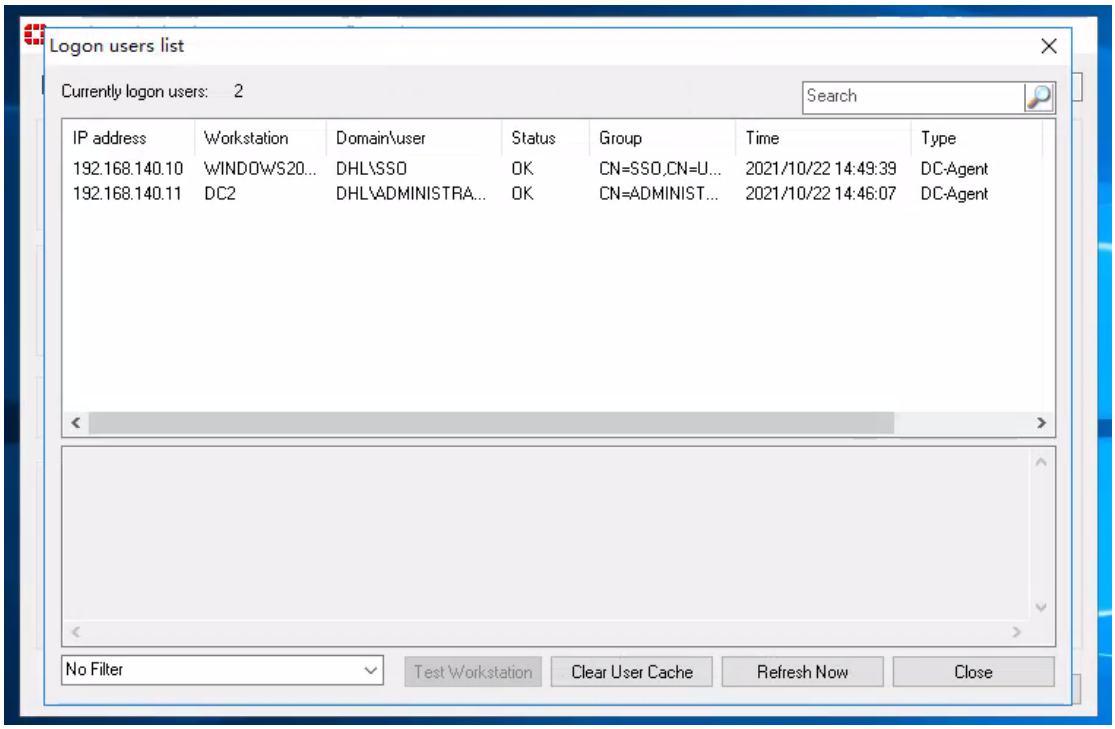
安装完成后会提示你重启，点击确定



安装完成后从看见 DC 推送的消息

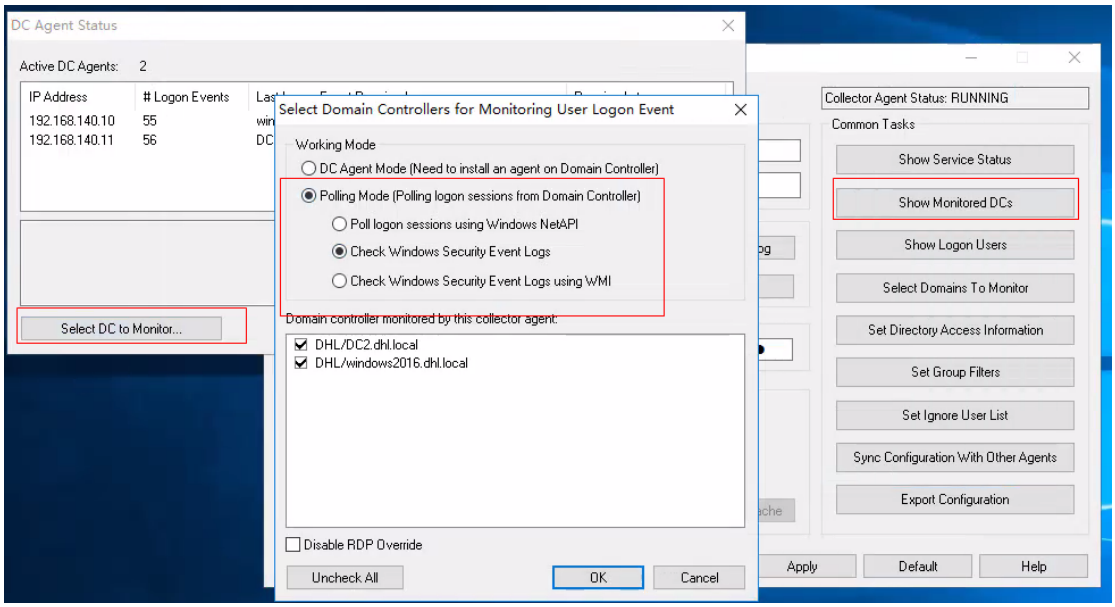

Fortinet Single Sign On Agent Configuration
Monitoring user logon events
Support NTLM authentication
Collector Agent Status: RUNNING
Listening ports
Common Tasks
DC Agent Status
Active DC Agents: 2
IP Address
Logon Events
Last Logon Event Received
Received at
192.168.140.10
20
windows2016/KEEPALIVE/5.0.0301
2021/10/22 14:49:12
192.168.140.11
22
DC2/KEEPALIVE/5.0.0301
2021/10/22 14:49:19
Select DC to Monitor...
Refresh Now
Close
Cache expire in (minutes):
60
Clear Group Cache
Export Configuration
Advanced Settings
Save&close
Apply
Default
Help

能看见用户登录信息


Logon users list
Currently logon users: 2
Search
IP address
Workstation
Domain\user
Status
Group
Time
Type
192.168.140.10
WINDOWS20...
DHL\SSO
OK
CN=SSO,CN=U...
2021/10/22 14:49:39
DC-Agent
192.168.140.11
DC2
DHL\ADMINISTRA...
OK
CN=ADMINIST...
2021/10/22 14:46:07
DC-Agent
No Filter
Test Workstation
Clear User Cache
Refresh Now
Close

六. Agent Polling 配置

Agent Polling 模式只需要在 Show Monitored DC 中，选择 Select DC to Monitor，然后选择相应协议即可，如下图所示：



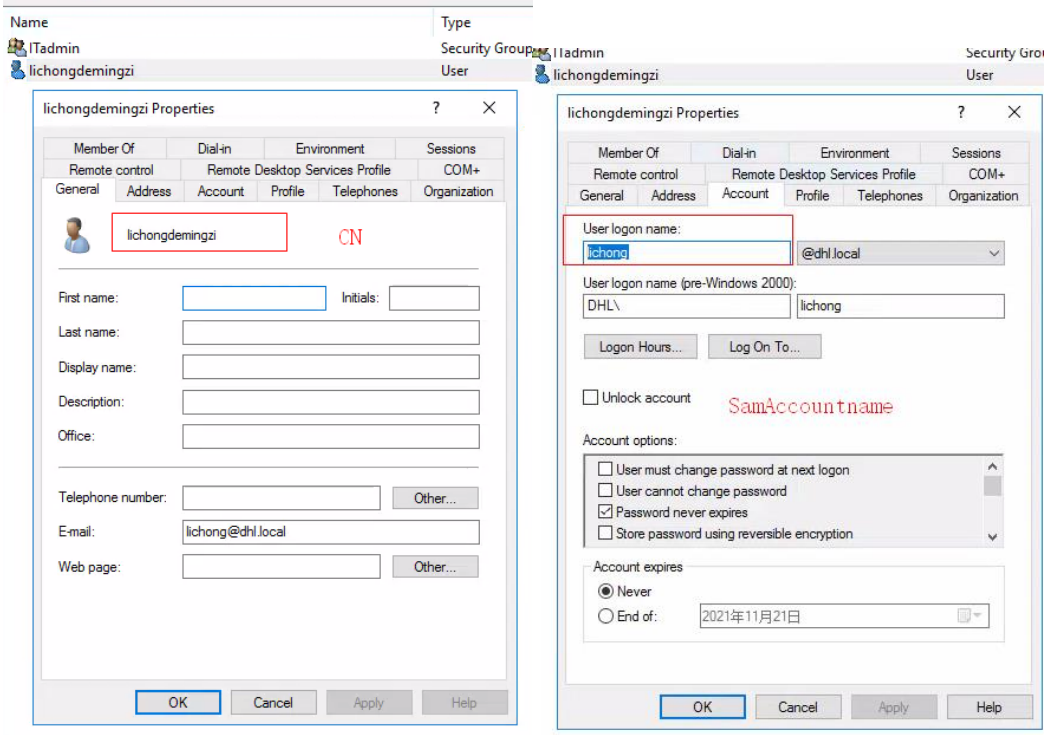
七. 防火墙相关配置

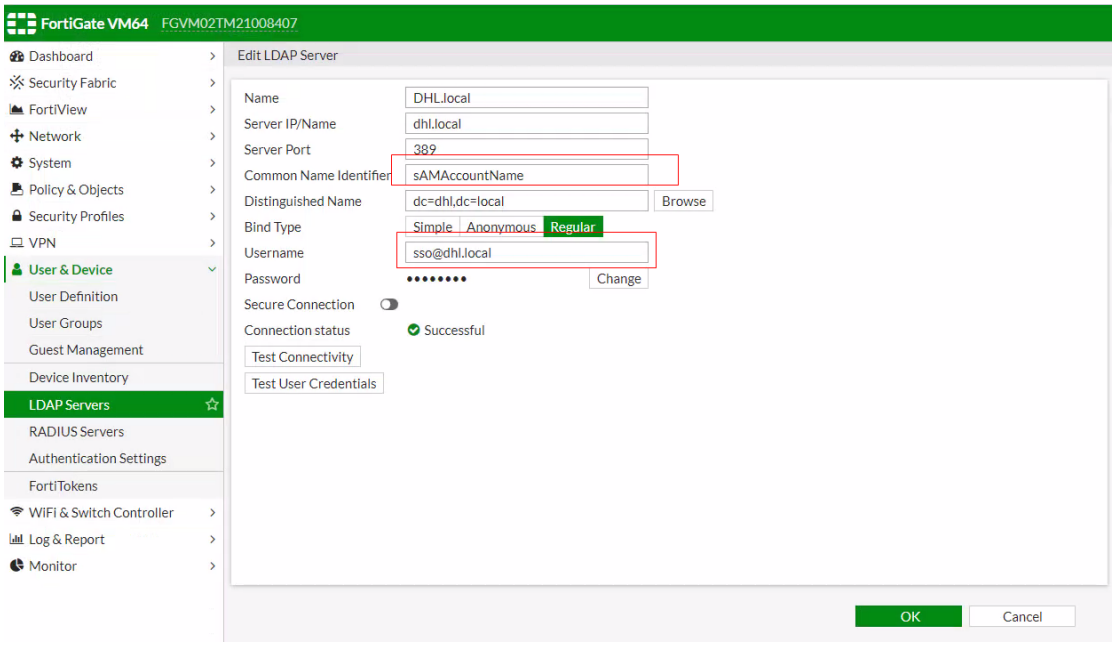
防火墙需要与 AD 和 FSSO Agent 进行通信，且通信方式采用带内通信，所以 HA 环境中 Reverse 的 Mgmt 是无法使用的，需要额外使用一个带内接口，配置 IP 后进行通信。

7.1. 配置 LDAP Server 相关信息

设置 Fortigate 使用内部 DNS，可以解析本地主机和本地 DC 的，Server 地址可以直接使用域名，**Common identify name** 有 2 个选项，CN 和 Samaccountname，CN 相当于是 AD 用户中的显示名称，SamAccountname 是登录名称，根据用户 AD 的情况选择不同的识别方式，多数用户 CN 和 SamAccountName 是一致的，所以可以二选一，设置完成后点击 Test 进行相应测试。

CN 与 SamAccountname 的区别





7.2. 配置 Fabric 连接器，选择【Fortinet 单点登陆代理】

主 FSSO agent IP 是指安装 FSSO collector agent 服务器 IP，密码与 CA agent 上输入的密码一致，这里为 Fortinet；

User Group Source 推荐使用本地 LDAP 获取，因为这样获取可以做过滤并且更方便；

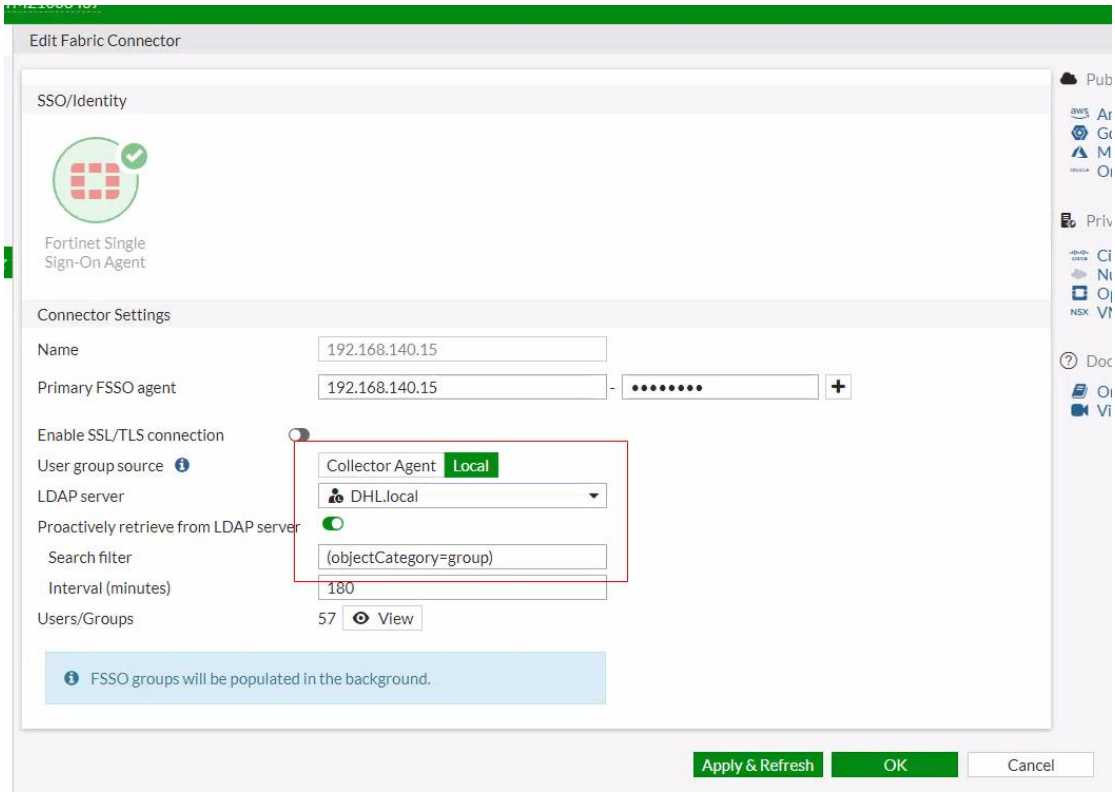
Proactively Retrieve from LDAP Server 勾选，可以预先读取 LDAP 上的组或用户信息；

Search Filter 这里可以对 LDAP 服务器的查询进行过滤，像默认的过滤 LDAP 上所有的组(ObjectCategory=group)，想过滤出所有的用户可以使用(ObjectCategory=person)，一些简单的过滤语法如下：

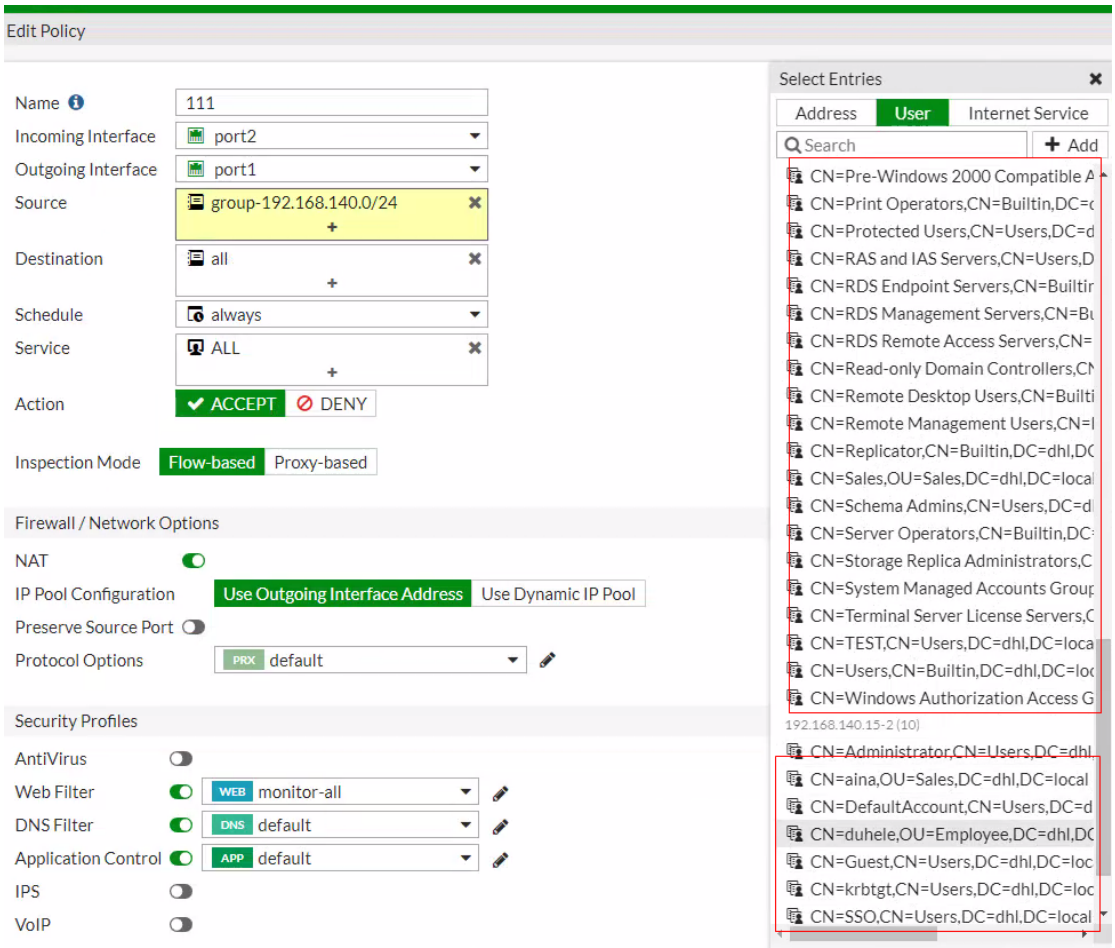
过滤某个组的用户：

(&(objectcategory=person)(memberof=CN=sales,ou=sales,DC=dhl,DC=local))，标红的为某个 Group 的 DN，需要写全

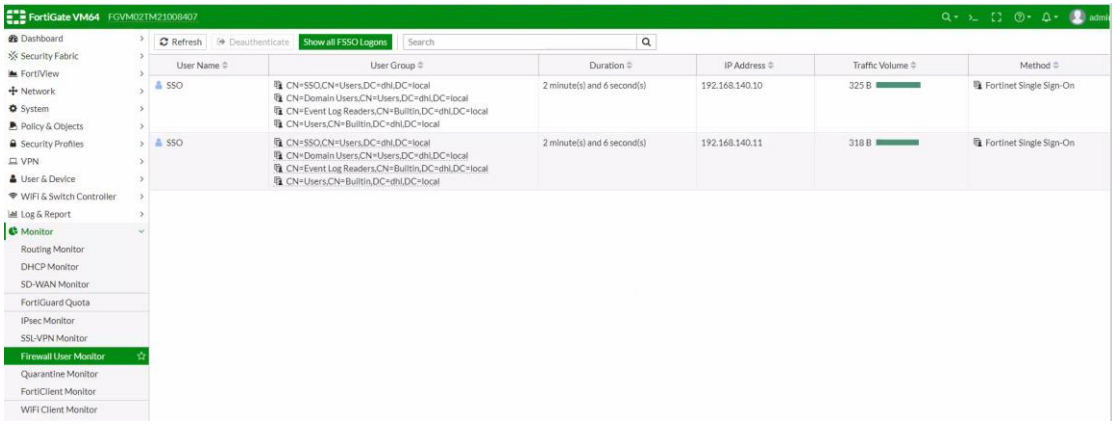
过滤某个组：(&(objectcategory=group)(cn=sales))，标红的为组名，可以使用通配符


Edit Fabric Connector
SSO/Identity
Fortinet Single Sign-On Agent
Connector Settings
Name
192.168.140.15
Primary FSSO agent
192.168.140.15
Enable SSL/TLS connection
User group source
Collector Agent
Local
LDAP server
DHL.local
Proactively retrieve from LDAP server
Search filter
(objectCategory=group)
Interval (minutes)
180
Users/Groups
57
View
FSSO groups will be populated in the background.
Apply & Refresh
OK
Cancel

7.3. 在策略里面调用相关 FSSO 用户组或用户进行 IPv4 过滤



7.4. 在防火墙上面查看 FSSO 登录相关信息



八.额外注意事项

防火墙的系统时间、时区保持正确

防火墙和域内主机的 DNS 必须是内部 DNS

Collect agent 必须能查询到客户机，通知是否用户仍在登录，在 collector agent/FortiGate 和所有主机间必须打开 TCP 139 和 445，每个客户端上必须运行远程注册服务

九.参考 Link 和文档

TAC Training

FSSO_training_2015.pdf

Technical Tip : Alternative LDAP settings for FSSO Collector Agent

来自 <https://kb.fortinet.com/kb/viewContent.do?externalId=FD49702&sliceId=1>

Technical Tip: FSSO Collector agent redundancy with two Windows AD and two Fortinet DC Agents

来自 <https://kb.fortinet.com/kb/viewContent.do?externalId=FD39911&sliceId=1>

Technical Tip: Excluding IP addresses from FSSO logon events

来自 <https://kb.fortinet.com/kb/viewContent.do?externalId=FD45566&sliceId=1>

Active Directory: LDAP Syntax Filters

来自 <https://social.technet.microsoft.com/wiki/contents/articles/5392.active-directory-ldap-syntax-filters.aspx>

Use active directory objects directly in policies

来自 <https://docs.fortinet.com/document/fortigate/6.2.9/cookbook/795593/use-active-directory-objects-directly-in-policies>

Technical Note: Unset the DNS resolution of the FSSO DCAgent

来自 <https://kb.fortinet.com/kb/viewContent.do?externalId=FD37705&sliceId=1>

Technical Note : FSAE Troubleshooting Guide

来自 <https://kb.fortinet.com/kb/viewContent.do?externalId=FD31819&sliceId=1>

Technical Tip: How to set source IP address for FSSO and LDAP

来自 <https://kb.fortinet.com/kb/viewContent.do?externalId=FD38942&sliceId=1>

Technical Tip: FSSO Group Filter configured on Collector Agent

来自 <https://kb.fortinet.com/kb/viewContent.do?externalId=FD52383&sliceId=1>

Technical Tip: FSSO Windows Directory Access Methods - Standard versus Advanced Mode

来自 <https://kb.fortinet.com/kb/viewContent.do?externalId=FD30964&sliceId=1>

Technical Note: FSSO collector agent failover configuration

来自 <https://kb.fortinet.com/kb/viewContent.do?externalId=FD36603&sliceId=1>

Technical Note : Details about 'FSSO Guest Users'

来自 <https://kb.fortinet.com/kb/viewContent.do?externalId=FD31780&sliceId=1>

Technical Tip: FSSO local poller (fssod) limitations compared to FSSO collector agent

来自 <https://kb.fortinet.com/kb/viewContent.do?externalId=FD38897&sliceId=1>