Il servizio del database Cisco Firepower User Agent non si riavvia dopo un arresto

Sommario

Introduzione

Un agente utente Cisco può monitorare il server Microsoft Active Directory (AD) e segnalare le attività di accesso e disconnessione autenticate da un server LDAP. Un centro di gestione Firepower (FMC) integra queste attività con gli eventi di sicurezza che raccoglie da un dispositivo gestito Firepower. Questo documento fornisce una soluzione a un problema quando l'agente utente non viene avviato dopo l'arresto del servizio.

Sintomi

È possibile utilizzare la soluzione in questo documento se si notano i seguenti sintomi con il servizio Agente utente:

- Nell'interfaccia Agente utente il servizio viene visualizzato come Non in esecuzione.
- In Console servizi Windows, services.msc, lo stato di Cisco User Agent è vuoto e non è possibile avviare il servizio.
  - Nel registro eventi di Windows viene visualizzato un errore simile a "Relazione di trust non riuscita tra il dominio primario e il dominio trusted"
  - Un file UserEncryptionBytes.bin viene creato in C:\ con dimensioni pari a zero byte.
- La modalità di debug di un client agente utente visualizza i seguenti messaggi di errore nella scheda Log dell'agente utente:

```
,"debug","[0102] - An error occured while fetching encryption bytes from
'C:\UserAgentEncryptionBytes.bin':
The trust relationship between the primary domain and the trusted domain failed.."

 ,"error","[0102] - An error occured while fetching encryption bytes from
'C:\UserAgentEncryptionBytes.bin':
Specified key is not a valid size for this algorithm.."

 ,"error","[0002] - Error connecting to 10.85.3.122: System.UnauthorizedAccessException:
Access is denied. (Exception from HRESULT: 0x80070005 (E_ACCESSDENIED))
```
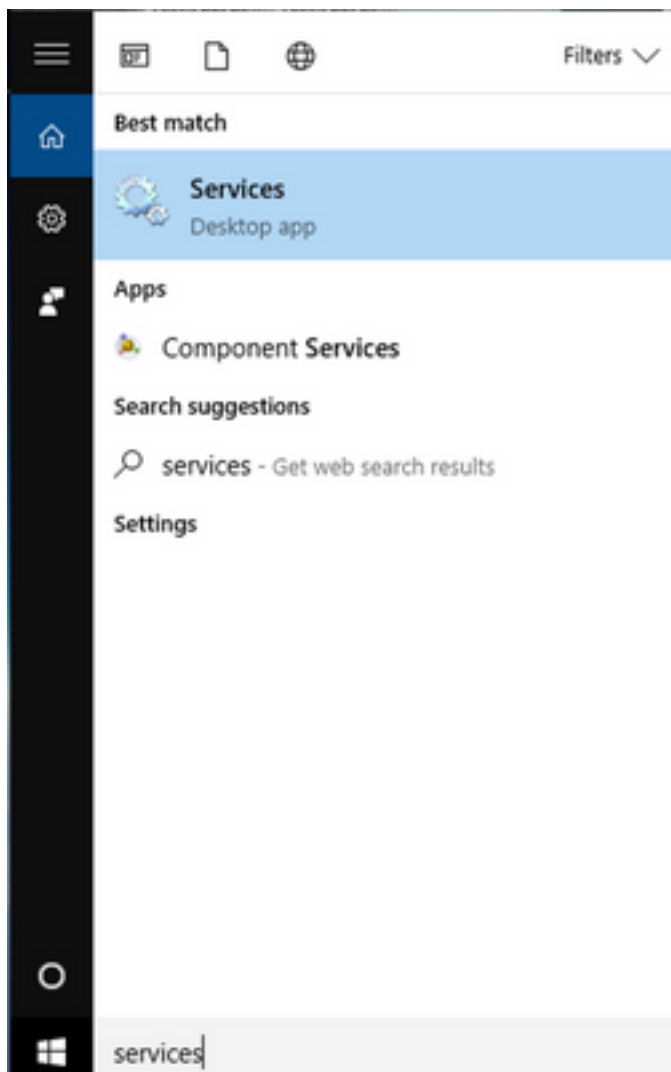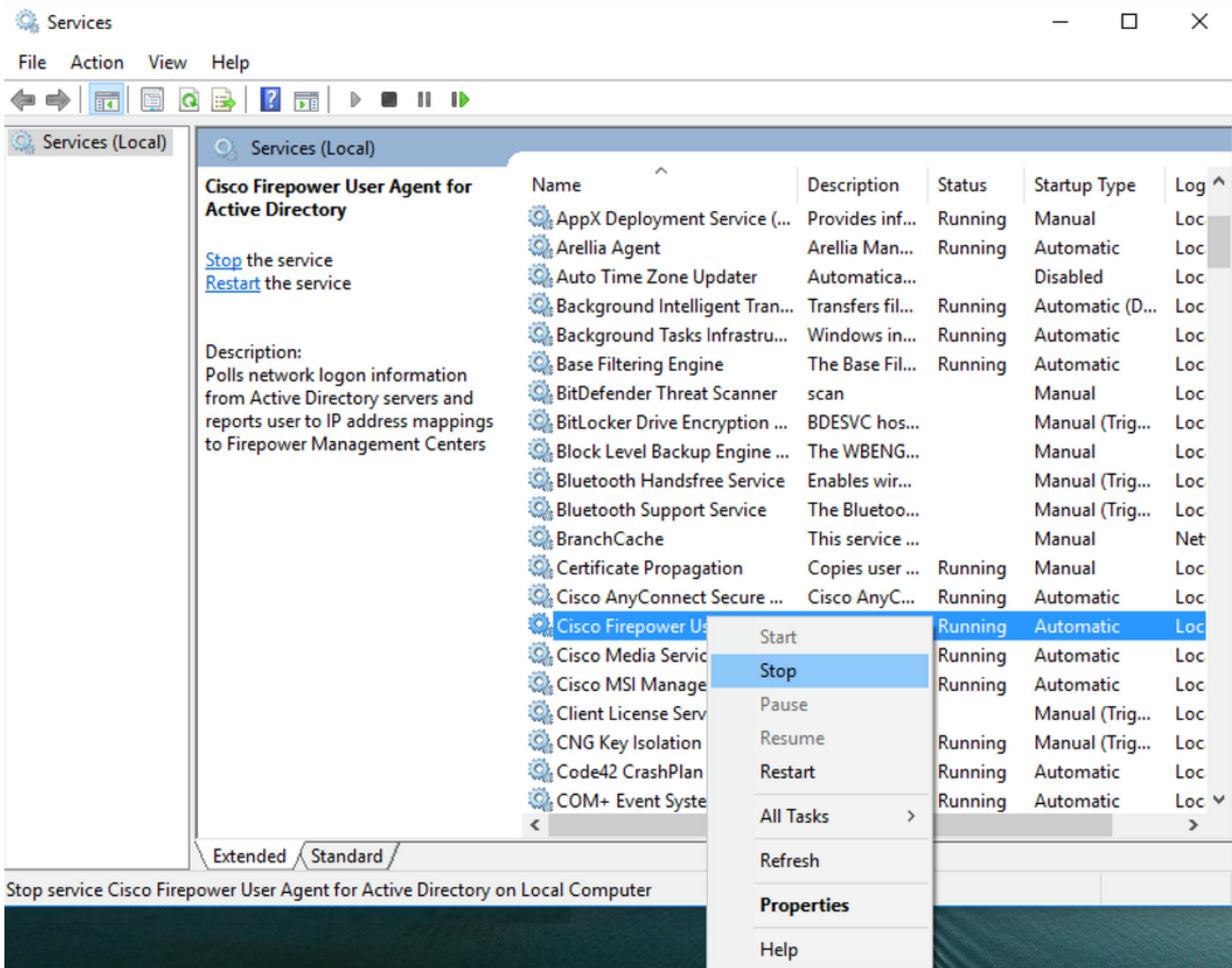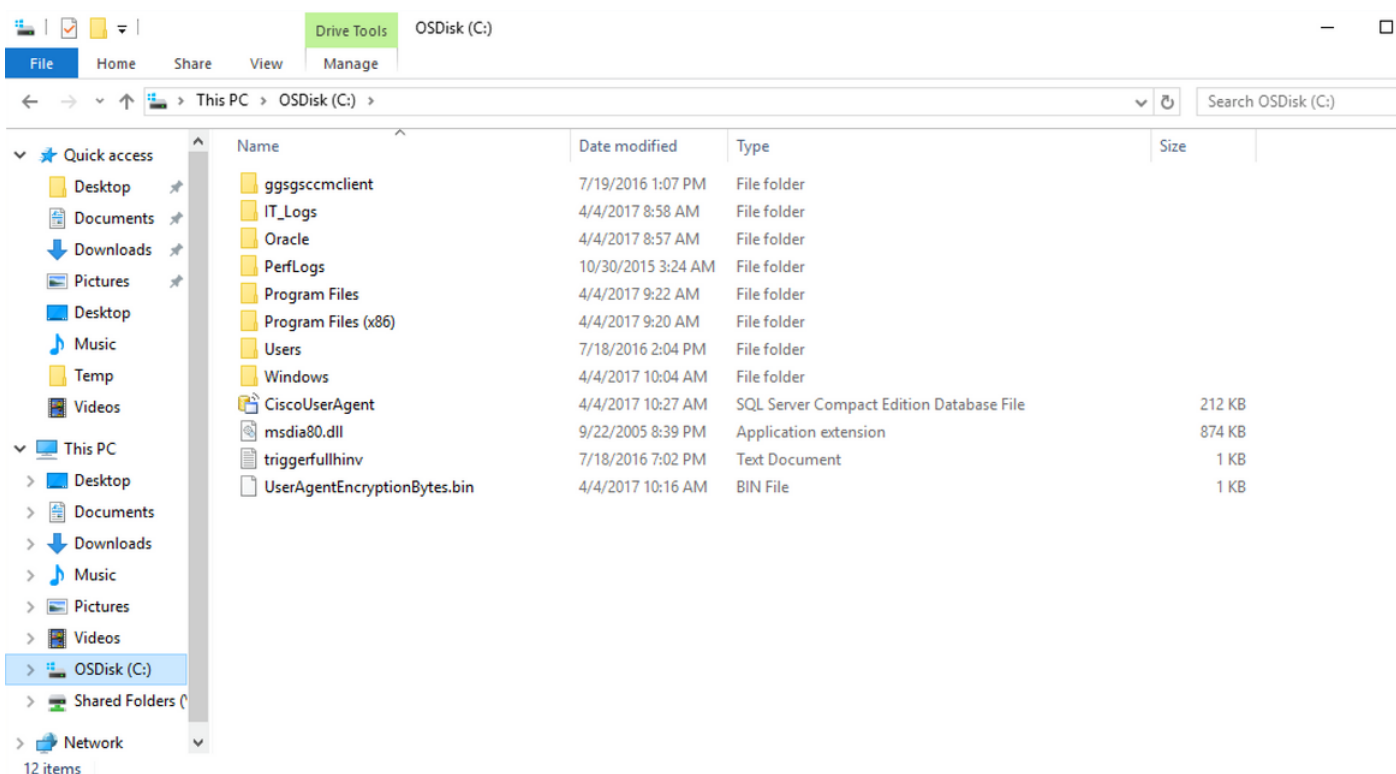
Soluzione

Passaggio 1: Eseguire Microsoft Windows Services Console, services.msc. Consente di disabilitare o abilitare un servizio Windows.
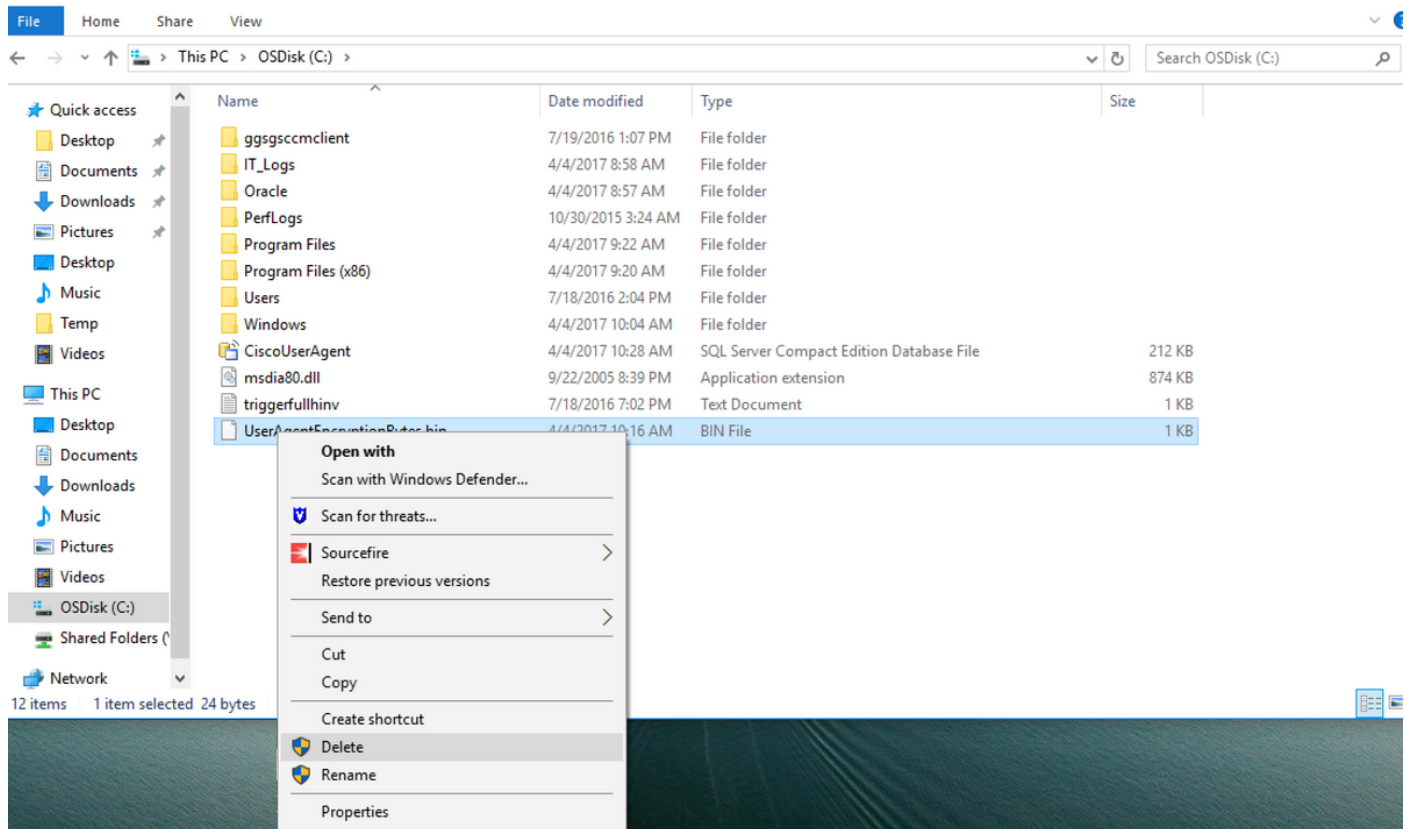
Passaggio 2: Fare clic con il pulsante destro del mouse sul servizio Cisco User Agent e selezionare **Stop** (Arresta) per arrestare il servizio.
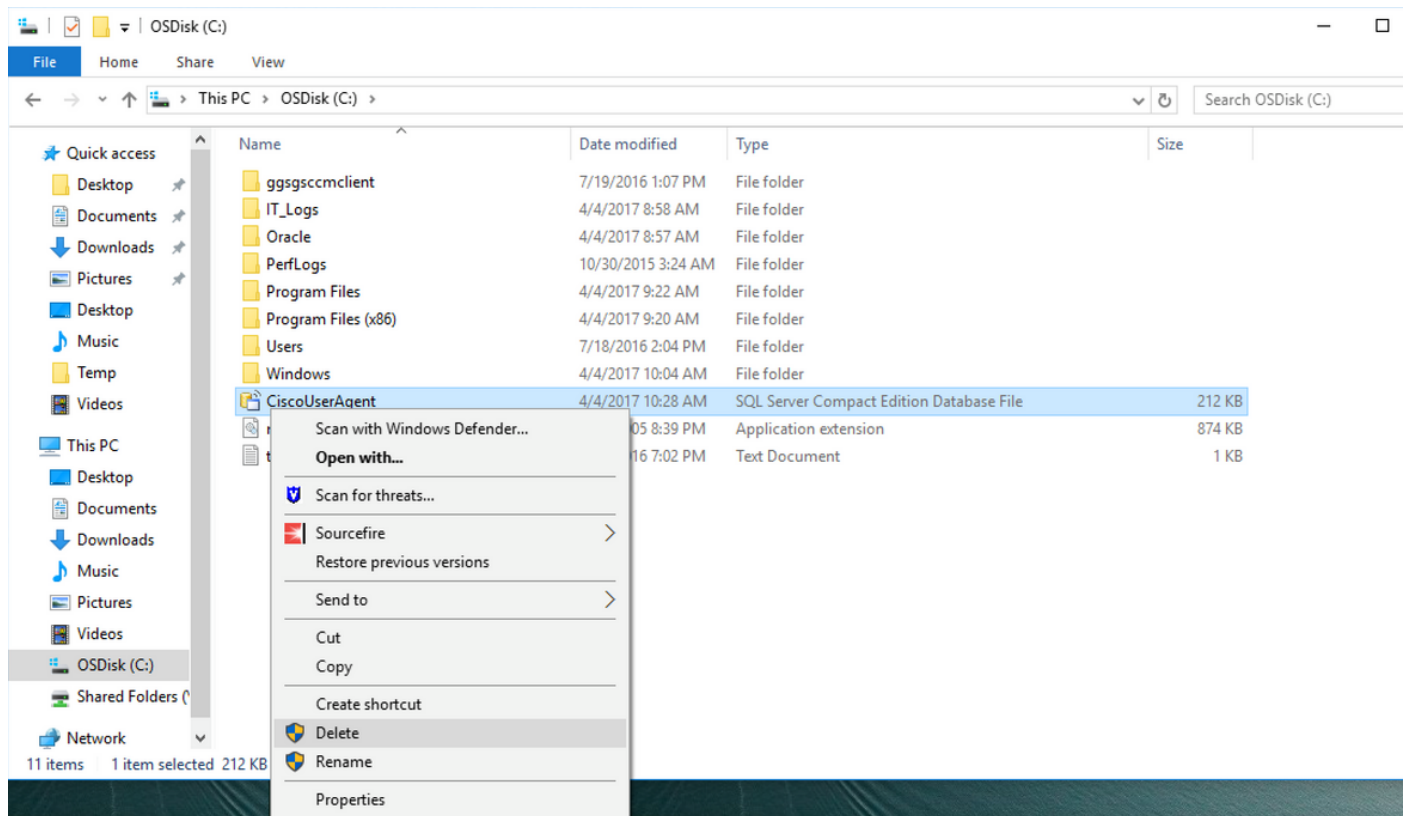
Passaggio 3: Passare alla scheda C: unità.

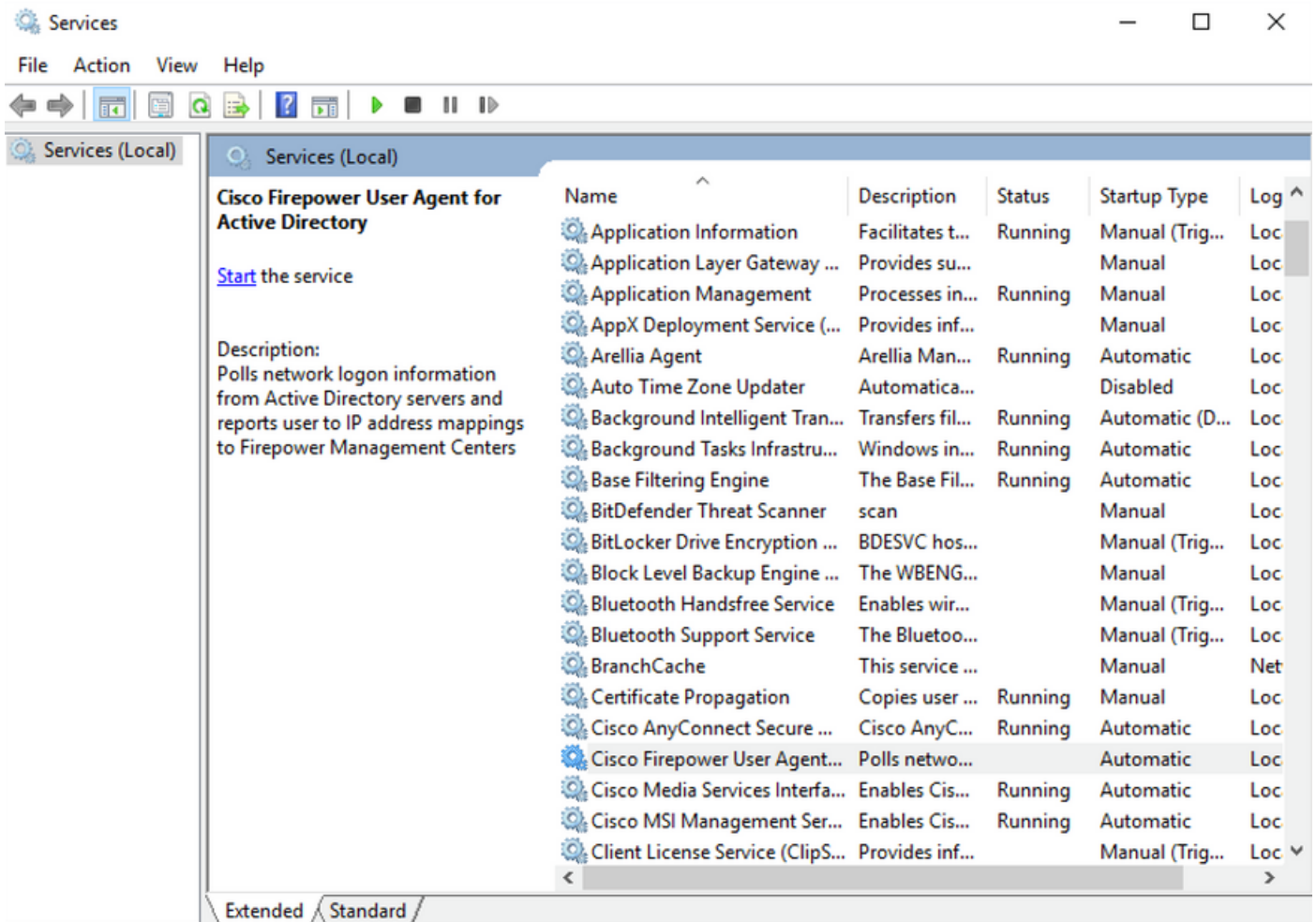**Passaggio 4:** Eliminare il file UserAgentEncryptionBytes.bin.

Passaggio 5: Eliminare il file CiscoUserAgent, che è un file di database di SQL Server Compact Edition.


Passaggio 6: Tornare a services.msc. Fare clic con il pulsante destro del mouse sul servizio Cisco User Agent, selezionare **Proprietà**, quindi selezionare **Log On** tab (Accedi) e configurare un utente come accesso utente AD. Al termine, fare clic su **Apply** (Applica).
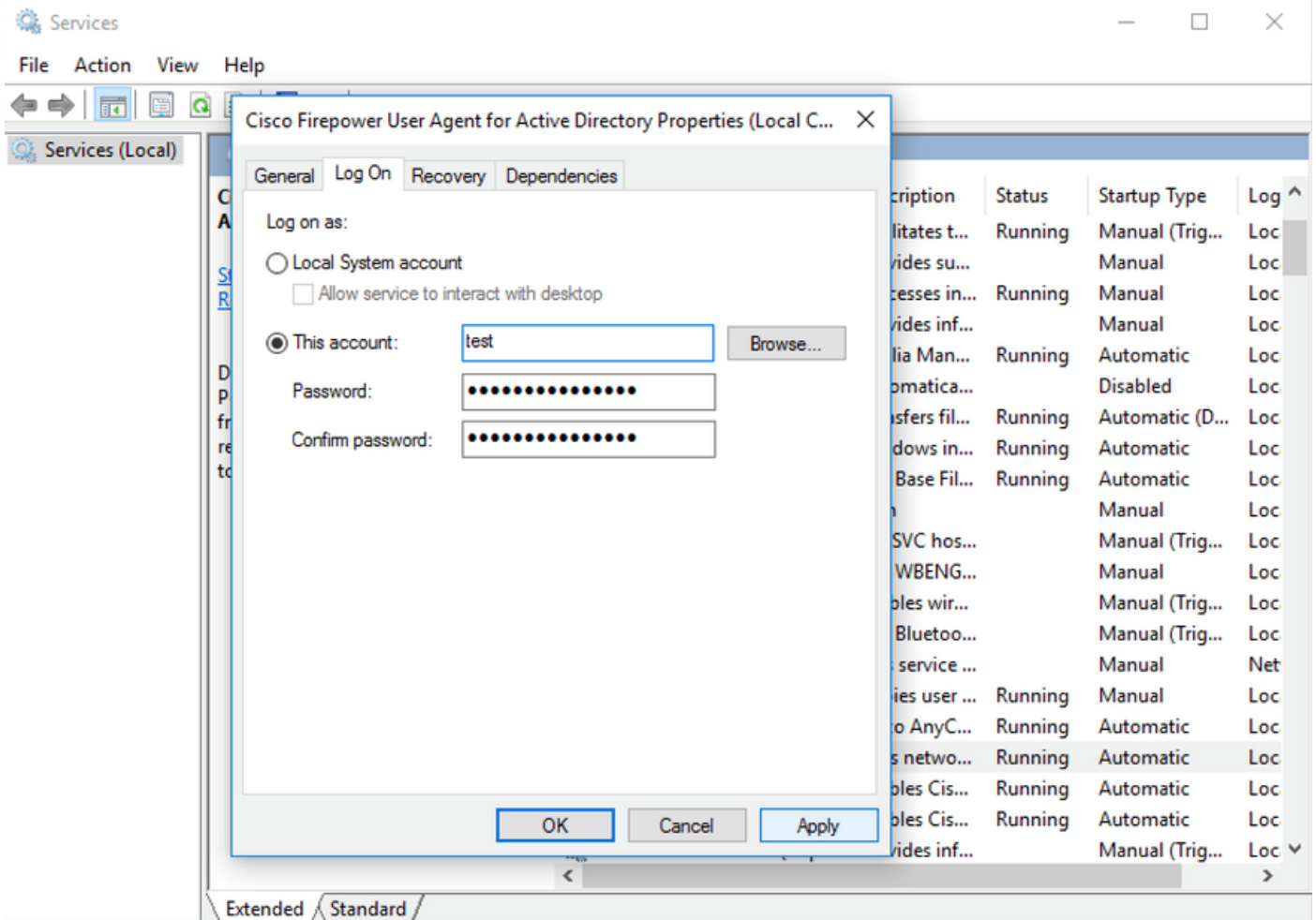
Passaggio 7: Nel file services.msc fare clic su **Start** per il **servizio Cisco Firepower User Agent** per Active Directory.

Passaggio 8: Verificare le dimensioni del file UserAgentEncryptionBytes.bin. Non deve essere 0 KB.
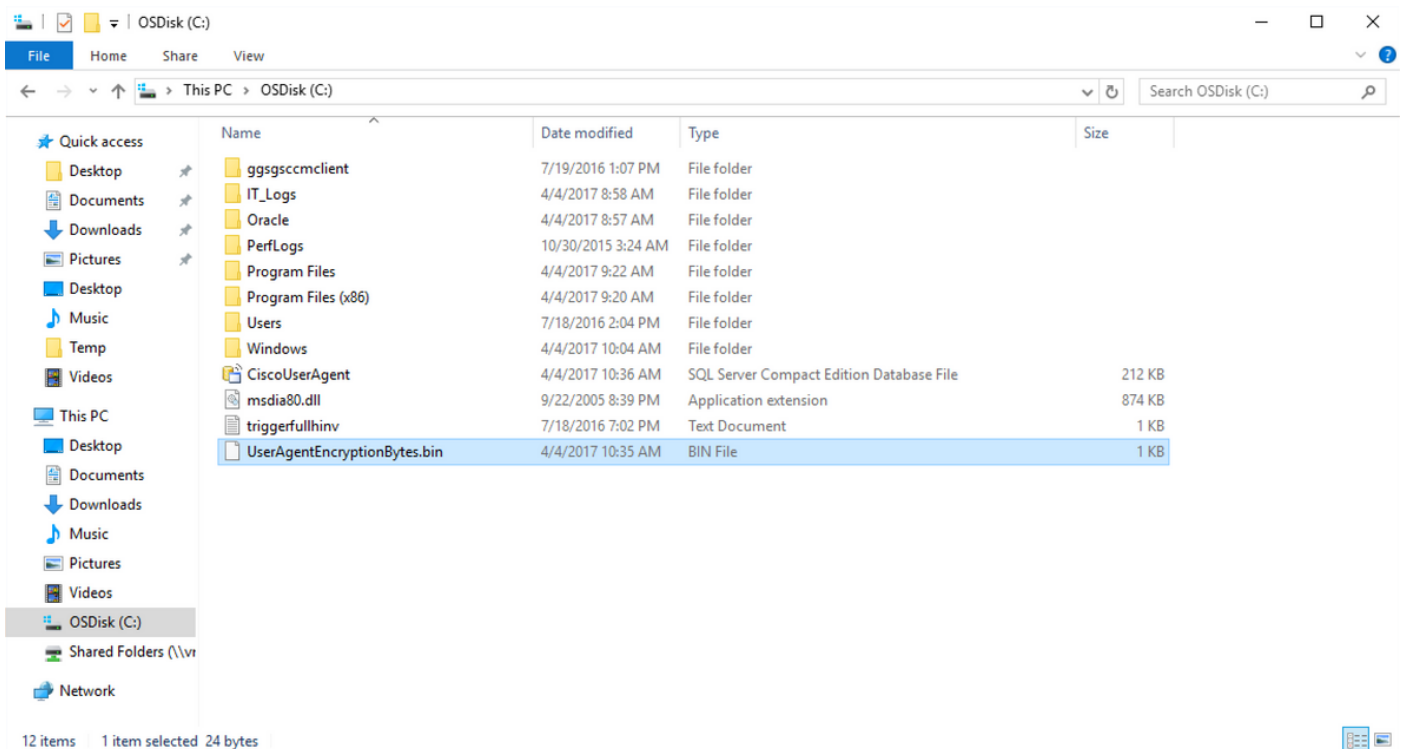
Passaggio 9: Aggiungere i controller di dominio e Firepower Management Center al client agente utente. Accertarsi di aggiungere i controller di dominio/l'host locale prima di aggiungere Firepower Management Center all'agente utente.
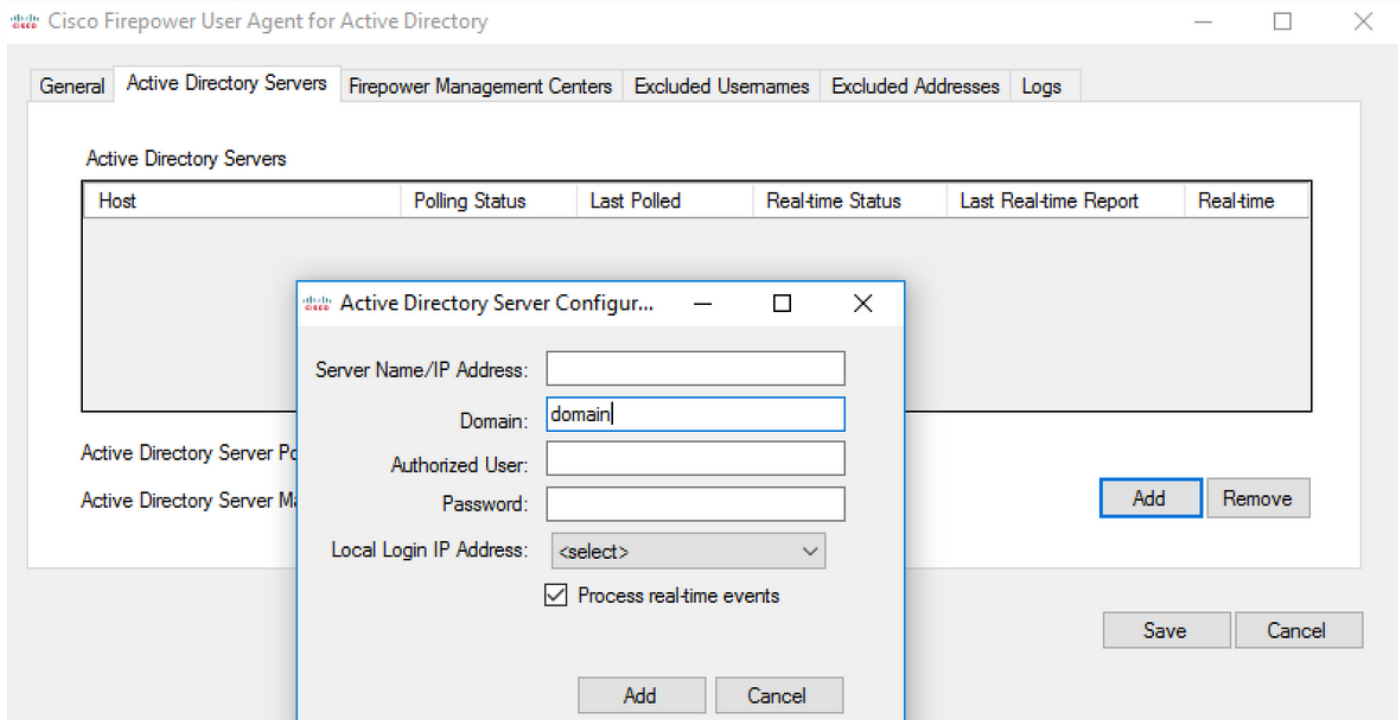
Riferimenti

- [Guida alla configurazione di Firepower User Agent, 2.3](#)
- [L'Agente Utente interrompe la derivazione se non è in grado di convertire l'account del servizio in SecurityIdentifier (CSCuw20184)](#)
- [Concedere autorizzazioni minime a un account utente di Active Directory utilizzato dall'agente utente Sourcefire](#)