

## Verifiche per installazione di System Platform 2023 R2

### Introduzione

Questa TN descrive alcune operazioni suggerite da effettuare per una corretta installazione System Platform.

Per i paragrafi segnati con asterischi:

\* Consultare la [TN007 – Deploy: Best Practices e Troubleshooting](#)

### Versioni

Quanto descritto in questa TN è stato verificato sulle seguenti versioni:

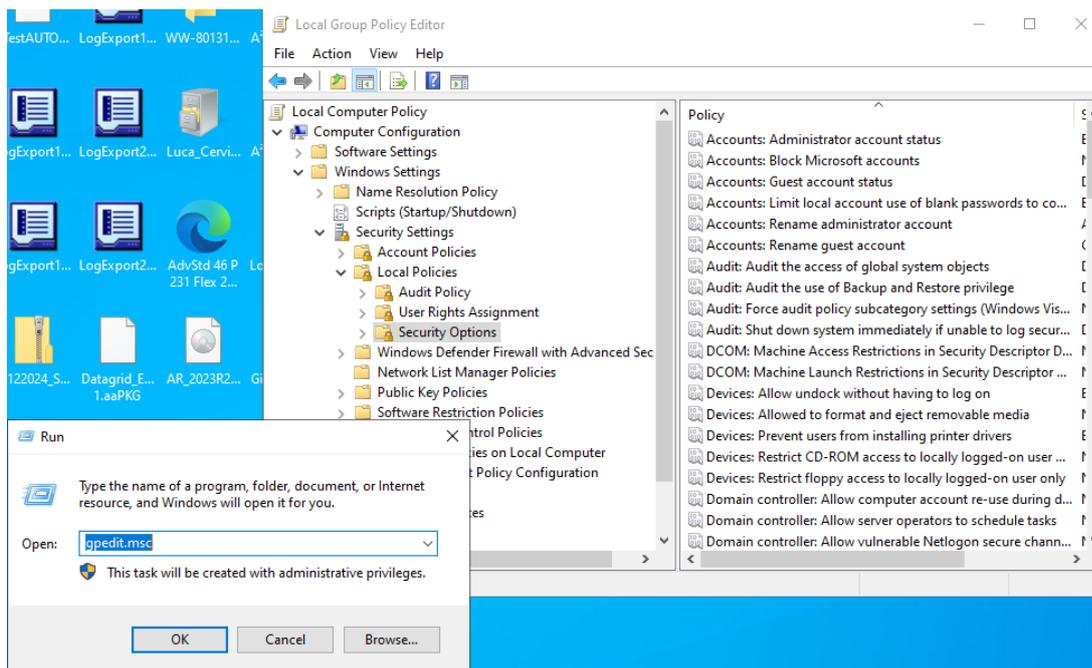
- SP 2023 R2 in avanti

Prima dell'installazione della System Platform, effettuare i seguenti controlli:

- + **Non è possibile** installare la System Platform su un Domain Controller.
- + Il Nome macchina non deve contenere caratteri speciali né underscore (ad eccezione del carattere "-" e deve avere lunghezza massima di 15 caratteri\*
- + disinstallare eventuali utilities di terze parti (HP, Acer, etc) se macchina fisica.
- + **disattivare temporaneamente il firewall di Windows.\***
- + **disattivare temporaneamente Windows Defender da impostazioni di windows, servizi e da policies.**
- + disattivare e stoppare servizio Intel Command Center Service (se presente nei servizi).
- + disattivare Windows Updates (da Group Policies, registro e servizi).
- + disattivare Tamper Control Antivirus Defender.
- + disattivare temporaneamente eventuali antivirus diversi da windows defender.
- + Inserire eventuale account di dominio con cui si esegue l'installazione nel gruppo Administrators locale. \*
- + Compilare file hosts di Windows con indirizzo IP e Nome macchina di tutte le macchine presenti nell'infrastruttura (in particolare in ambiente non di dominio). \*
- + Disattivare IPV6 dalle schede di rete se non utilizzato per altri scopi.
- + Se presenti più schede di rete, settare metrica non su automatico ma con priorità sulla scheda di comunicazione tra le platform (quindi più bassa, per esempio 10) e le altre meno prioritarie (per esempio 20); \*

Abilitare policy di sicurezza da Group Policy Editor:

Da Start di Windows -> Run -> gpedit.msc -> Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options:



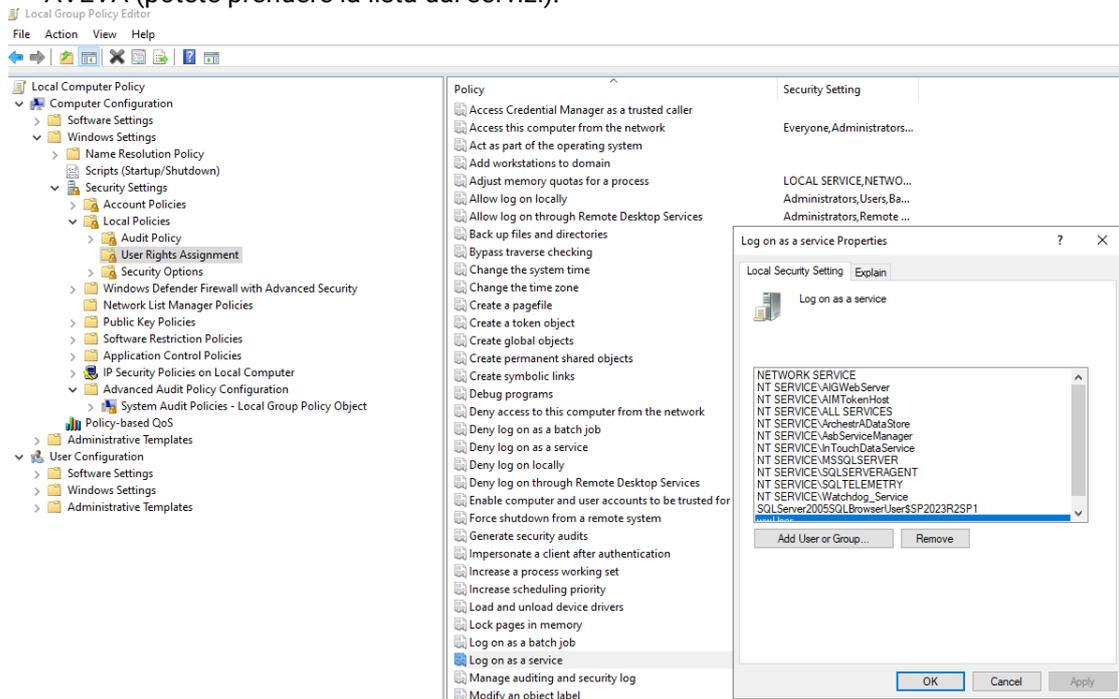
1. Accounts: Administrator account status;
2. Network access: Allow anonymous SID/Name Translation
3. Network access: Let Everyone permission apply to anonymous users

Installazione System Platform:

- **Prima dell'installazione controllare che l'ISO di installazione sia sbloccata (tasto destro->proprietà->unlock-> Apply-> Ok) e lanciare come amministratore.**
- Nel Network Account non inserire caratteri speciali né punti.
- Configurare tutte le sezioni del Configurator, facendo attenzione ad eventuali tempi morti dovuti alla procedura d'installazione e aspettare eventuale popup di restart macchina e riavviare macchina.

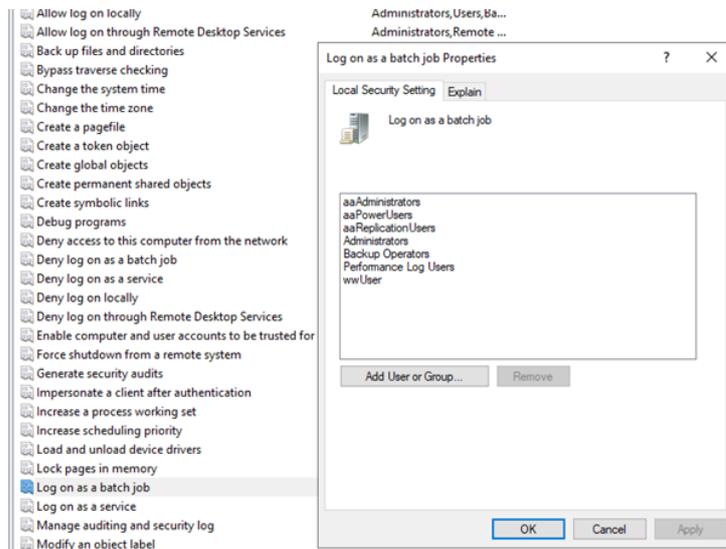
Fine installazione:

- ✚ Sempre da Group Policy Editor, Assicurarsi che l'installazione abbia inserito in *Log on as a service*, oltre al Network Account, anche tutti gli NT SERVICE[...] che gestiscono i servizi AVEVA (potete prendere la lista dai servizi):



✚ E in *Log on as a batch job*:

- > Account Policies
- > Local Policies
- > Audit Policy
- > User Rights Assignment
- > Security Options
- > Windows Defender Firewall with Advanced Security
- > Network List Manager Policies
- > Public Key Policies
- > Software Restriction Policies
- > Application Control Policies
- > IP Security Policies on Local Computer
- > Advanced Audit Policy Configuration
- > System Audit Policies - Local Group Policy Object
- > Policy-based QoS
- > Administrative Templates
- > User Configuration
- > Software Settings
- > Windows Settings
- > Administrative Templates



- applicare le Antivirus Exclusions prima di riattivare l'antivirus (vedi Referenze infondo 000032662);
- Controllare che le Porte Firewall utilizzate dalla system platform siano aperte e non abbiano alcuna restrizione (vedi Referenze in fondo 000048918).

### **N.B. Licensing:**

E' vivamente consigliato l'upgrade del licensing alla versione **4.2.1** nella sua versione standalone (non contenuto nel file di installazione della System Platform) scaricabile al seguente link:

<https://softwaresupportsp.aveva.com/en-US/downloads/products/details/9b7e3ca7-0408-4d61-9cdc-93373eee5900>

- al download del file .zip, come per l'ISO System Platform, è necessario **sbloccare il file (tasto destro->proprietà->unblock-> Apply-> Ok)**
- Lanciare il file setup.exe come amministratore e eseguire l'upgrade seguendo il setup guidato;
- Configurare tutte le sezioni del Configurator, facendo attenzione ad eventuali tempi morti dovuti alla procedura d'installazione e aspettare eventuale popup di restart macchina e riavviare macchina.

Abilitare la sicurezza TLS 1.2 da chiavi di registro

- Estrarre il contenuto del file TLSConfiguration.zip (scaricabile [QUI](#))
- Rinominare ConfigTLS.txt in ConfigTLS.bat
- Eseguire come amministratore nel prompt dei comandi
- Premere "y" in modo che il file batch continui
- Dopo il completamento, **verrà riavviata** la macchina

### Referenze

- [TN10567 \(000032662\) - AVEVA System Platform 2020 to 2023 R2 - Anti-virus Exclusions](#)
- [Support Article 000048918 Ports used by System Platform products](#)
- [TN007 – Deploy: Best Practices e Troubleshooting](#)