Riconnettere una macchina al SMS dopo un HW replacement o un restore di VM

Rev 1 - 02/03/2021



Introduzione

Questa TN descrive come riconnettere al System Management Server (SMS) una macchina dopo che è stata rimpiazzata (hardware replacement) oppure se è stata rimpiazzata la VM dopo un suo malfunzionamento (VM restore).

Il System Management Server (SMS) è un componente degli ASB Runtime che abilita la comunicazione crittografata tra platform e che, grazie al supporto del TLS 1.2, cripta la comunicazione anche della parte Single Sign On (SSO) e gestione certificati. Ogni nodo di System Platform deve comunicare con il SMS e nel sistema quest'ultimo deve essere unico. Inoltre il SMS immagazzina i certificati di sicurezza condivisi e stabilisce tra le macchine una trust relationship.

Versioni

Quanto descritto in questa TN si applica alle versioni 2017 e successive. La procedura è stata verificata e testata su un sistema così composto:

- SMS: Windows Server 2019 con System Platform 2020
- Client: Windows Server 2016 con System Platform 2017 Update 3 SP1 P01
- •

Sintomi

Sono principalmente due i sintomi di una connessione rifiutata dal SMS. Il primo è che la macchina non riesce ad importare il certificato e quindi il Configurator restituisce un errore quando si tenta di connettere la nuova macchina al SMS. Il secondo è la presenza del seguente warning all'interno del log viewer nella System Management Console (SMC):

ArchestrA.CertificateManager: Please un-register the device <device name> from management server. Use the (Remove-AsbDevice) script to remove the device registration.

La causa di questo problema è dovuto al fatto che il SMS, per proteggere la sicurezza del sistema, identifica univocamente ogni macchina ad esso connesso. Quando un intruso tenta di ri-registrare una macchina con un nome già presente nel SMS (spoofing), quest'ultimo rifiuta la connessione proveniente dalla seconda macchina omonima (quindi dalla macchina dell'intruso).

Come risolvere il problema

Per risolvere, o prevenire il problema, esistono due azioni che si possono intraprendere:

 Prima di rimpiazzare la macchina e/o rimettere in piedi la VM, bisogna avviare il Configurator sulla macchina da rimpiazzare e disconnettersi dal SMS, ovvero bisogna configurare la macchina selezionando l'opzione "Nessun System Management Server configurato (SCELTA NON CONSIGLIATA)" in modo tale che il certificato importato sia cancellato dalla macchina e quest'ultima sia cancellata dal database del SMS.

ACor	nfigurator	– – ×
File H	Help	
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	VEVA Enterprise Licensing Platforr AVEVA Enterprise License Se ommon Platform System Management Server Touch Web Client Access entinel System Monitor Sentinel Manager Alert Email Server	Per poter utilizzare le comunicazioni crittografate, i computer su cui è in esecuzione il software AVEVA devono essere configurati in modo da riconoscersi reciprocamente attendibili. Per eseguire questa operazione, connetterili a System Management Server. Connettersi a un System Management Server. Questo computer è System Management Server. La topologia deve contenere un solo System Management Server per tutti i prodotti AVEVA. Tutti gli altri computer devono essere configurati per connettersi al System Management Server. Nessun System Management Server configurato. (SCELTA NON CONSIGLIATA) Questa opzione consente anche di rimuovere eventuali certificati esistenti gestiti dal System Management Server. È possibile connettersi a un System Management Server esistente o configurare uno nuovo selezionando rispettivamente una delle prime due opzioni. Facendo clic su Configura, saranno configurati un certificato e le porte Web da utilizzare per la comunicazione. Per modificare queste configurazione, fare clic su Avanzate.
	C F	Configuration Messages
		Certificates are configured. Fetching the universal solution configuration from the System Management Server 'https:// winsrv19wsp2020/identitymanager/'. The universal solution configuration is downloaded Registering the device. The device is registered. Device configuration completed.
	Refresh All Mes	sages Configure Close

- 2. Se la macchina "client" non è più disponibile per un qualsiasi motivo, bisogna seguire la procedura sottostante per rimuovere la connessione dal SMS manualmente:
 - a. Avviare la Windows PowerShell sul SMS utilizzando lo stesso utente che avvia il Configurator oppure come Amministratore

e 🗅 🔅		
Best match		
Windows PowerShell		
Desktop app	🕞 Run as administrator	
Apps	□ 🛱 Run as different user	
Windows PowerShell (x86)	D Open file location	
Windows PowerShell ISE	🔏 Unpin from Start	
Windows PowerShell ISE (x8	-⇔ Pin to taskbar	
Settings (7+)	l Uninstall	
	🗵 Run as Administrator	
	😫 Run ISE as Administrator	
	Windows PowerShell ISE	

b. Eseguire la linea di comando Get-AsbDevice così da avere la lista delle macchine registrate al SMS



- c. Eseguire la linea di comando Remove-AsbDevice specificando
 - i. DeviceID: il nome della macchina che si vuole eliminare (disponibile nella lista ritornata dall'esecuzione del comando Get-AsbDevice)
 - ii. ManagementServerAddress: il nome del SMS e deve essere nella forma https://nomemacchina:porta (di default è la porta 443)



d. Inserire le credenziali dell'utente Windows che ha la possibilità di avviare il Configurator o quelle dell'Amministratore



e. Eseguire nuovamente la linea di comando Get-AsbDevice per verificare che nella lista non ci sia più la macchina sostituita



f. Eseguire la configurazione del SMS spuntando la prima opzione del Configurator nella nuova macchina da inserire nel sistema

Tutta la PowerShell con gli script eseguiti si presenta così



Referenze

- o AVEVA TN 10373
- o System Platform Install Guide (presente nell'ISO di installazione della System Platform)

Autore: F. Pastore

Disclaimer

Il presente documento è fornito a scopo di esempio e non sostituisce la documentazione AVEVA L'applicazione di quanto contenuto, in un preciso ambito applicativo, deve essere sempre validata da un tecnico Wonderware. La documentazione rilasciata da AVEVA resta il riferimento tecnico ufficiale da seguire: <u>softwaresupport.aveva.com</u>. Wonderware Italia non si assume la responsabilità di un'applicazione scorretta di questo documento.