

13.7.2026

Windows Event Forwarding

מדריך להטמעת WEF בארגון.

יוצר המסמך: **ירון קינג**

ניתן לשתף מסמך זה ברבים, בליווי מתן קרדיט ליוצר. 😊

תוכן עניינים

3	1. מבוא
3	1.1. מה זה WEF?
3	1.2. יצירת מנגנון של WEF
4	2. דרישות קדם
4	2.1. הגדרות בתחנת המקור
6	2.2. הגדרות ב-GPO
9	2.3. הגדרות בשרת האיסוף
11	2.4. הגדרת Custom Logs
11	3. יצירת חוקים (Subscriptions)
14	4. נקודות נוספות
14	5. תקלות
14	5.1. Error Code 5004
17	5.2. בעיה ברישום תחנות בשרת האיסוף
17	5.3. הגדרות חסרות ב-GPO
18	5.4. לוגים לא מופיעים בשרת ה-WEC
18	5.4.1. אתחול ה-Windows Event Log
19	5.4.2. טיפול ב-Windows Event Collector בשרת ה-WEC
20	5.5. Event ID 111
21	5.6. חוסר רספונסיביות של ה-Event Viewer בעת צפיה ב-Subscriptions בשרת ה-WEC
21	6. נקודות נוספות

1. מבוא

1.1. מה זה WEF?

Windows Event Forwarding (להלן: WEF) הנו מנגנון מובנה של מייקרוסופט, המאפשר לשלוח לוגים (מסוג "Windows Event Logs") מתחנות-קצה ושרתים. לוגים אלו יכולים להוות "חיישן" נוסף המדווח על אירועים המתרחשים באותם מחשבים, אשר אותם ניתן להעביר ל-SIEM לצרכי התרעה בזמן-אמת או תחקור בדיעבד.

באופן כללי, התצורה של WEF מובנית לפי 3 רכיבים עיקריים:

א. תחנות הקצה והשרתים (מקור המידע).

ב. שרת איסוף מרכזי האוסף את הלוגים הנשלחים אליו ("Forwarded Events") מאותם מחשבים.

ג. SIEM אשר מתחבר לשרת האיסוף המרכזי ושואב ממנו את הלוגים.

❖ הערה חשובה: ניתן להעשיר את המידע המתקבל מה-Windows Event Logs ע"י התקנה וקסטומיזציה של הכלי Sysmon (מבית Microsoft \ Sysinternals) בתחנות קצה ושרתים, שכן הוא מספק מידע נוסף שאינו קיים בלוגים "הרגילים" של חלונות.

1.2. יצירת מנגנון של WEF

באופן כללי, מנגנון ה-WEF כולל את השלבים:

1. בניה של Policy ב-GPO (המוכל על מחשבים ספציפיים, OU מסויים או על כלל המחשבים בארגון) אשר בו מוגדר מיהו שרת האיסוף המרכזי שאליו המחשבים צריכים לשלוח את הלוגים.
2. הגדרה של חוקים ("Subscriptions") בשרת האיסוף המרכזי, הכוללים פרטים כגון:
 - אילו לוגים יש לשלוח לשרת האיסוף.
 - על מי מוכל ה-Subscription (מחשבים ספציפיים, OU מסויים וכן הלאה). כך ניתן להגדיר חוקים שונים למחשבים שונים, בהתאם לצורך.
3. הפעלת שירותים מסויימים במחשב המקור על מנת לאפשר שליחה של הלוגים לשרת האיסוף.

2. דרישות קדם

2.1. הגדרות בתחנת המקור

על מנת לאפשר תהליך של WEF עבור תחנה, יש לבצע בה מס' פעולות והגדרות –

א. הפעלת שירות WinRM

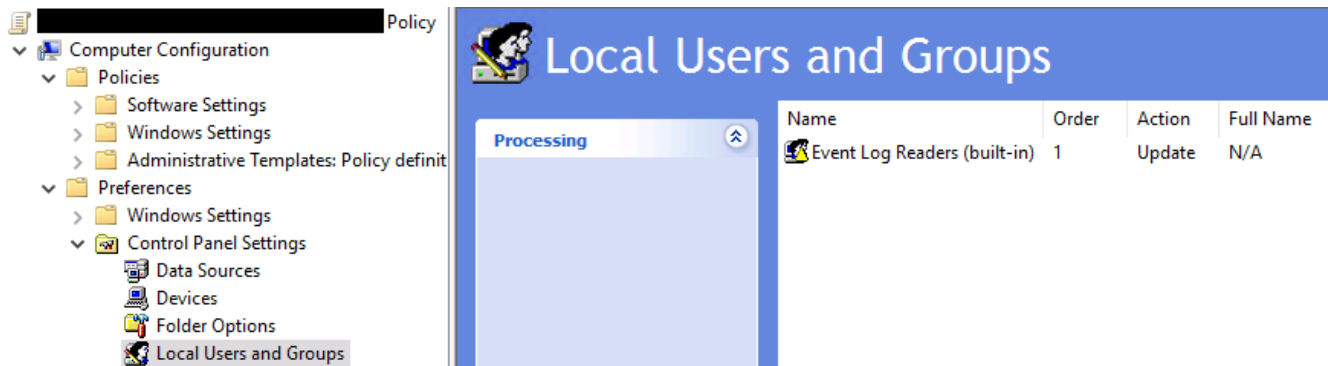
WinRM (= Windows Remote Management) הנו שירות (Service) מובנה בתחנה שאותו יש להפעיל.

Name	Status	Startup Type	Log On As
Windows Presentation Foundation Font Cache 3.0.0.0	Started	Manual	Local Service
Windows Remote Management (WS-Management)	Started	Automatic	Network Service
Themes	Started	Automatic	Local System

הפעלת שירות זה כוללת יותר פעולות מאשר רק איפוסור השירות עצמו (enabled, automatic), ולכן הדרך המהירה ביותר להפעילו היא באמצעות הרצת הפקודה הבאה:
winrm quickconfig -q

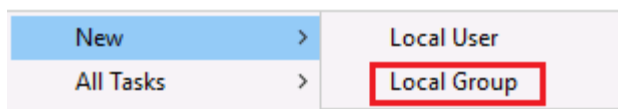
ב. הוספת היוזר המקומי "Network Service" לקבוצה המקומית "Event log Readers"

ניתן להוסיף יוזר זה באמצעות GPO באופן הבא –

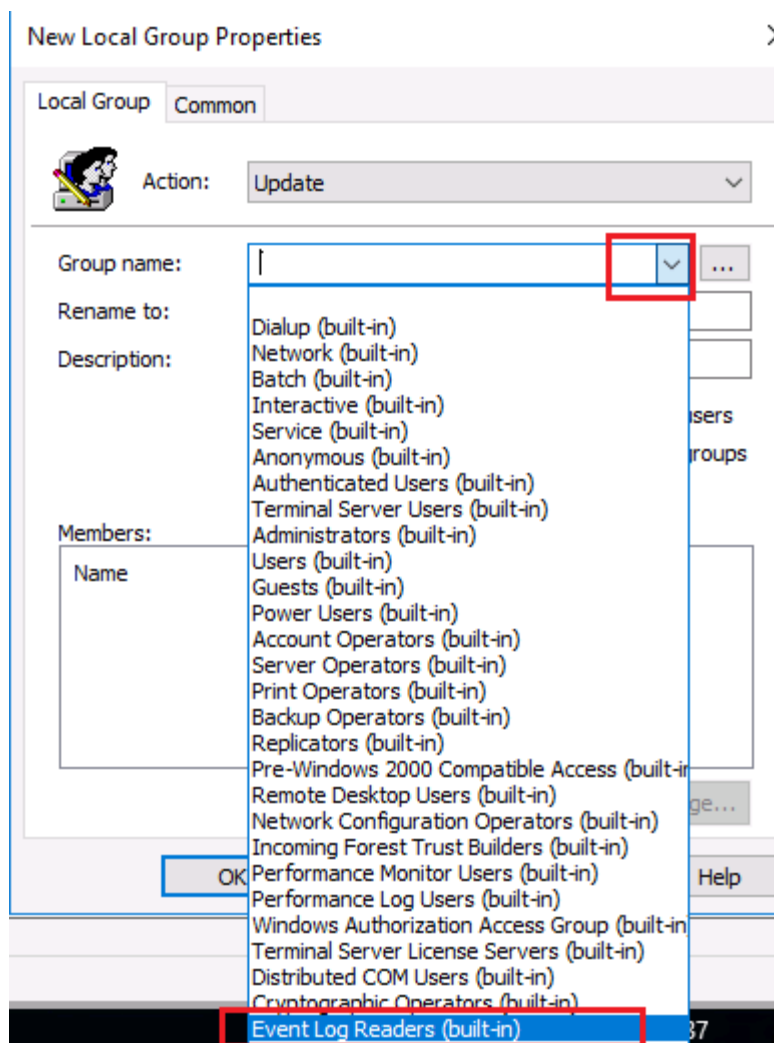


Computer Configuration\Preferences\Control Panel Settings\Local Users and Groups

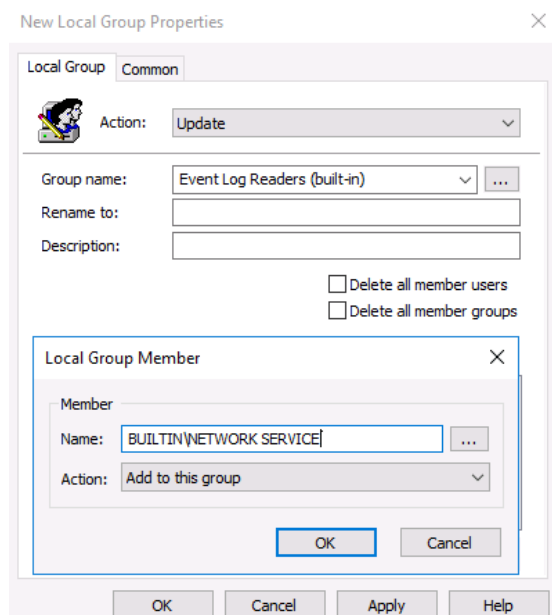
במידה והקבוצה אינה מופיעה שם, ניתן לבצע קליק-ימני ולבחור ב-New → Local Group



ואז לבחור בקבוצה זו מתוך תיבת הרשימה "Group Name".



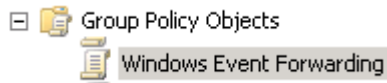
לאחר מכן, יש להקליק על הכפתור "Add" ולהכניס את השם המלא של היוזר המקומי המדובר:
 .BUILTIN\NETWORK SERVICE



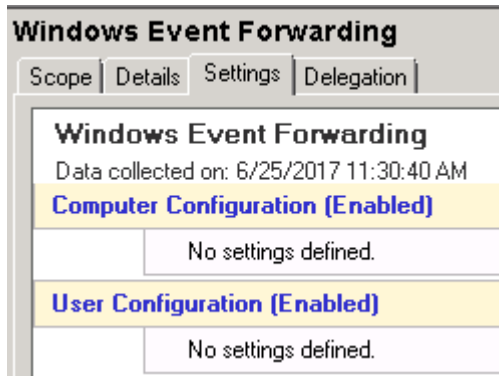
2.2. הגדרות ב-GPO

יש ליצור GPO שיכיל את ההגדרות הנחוצות שיכולו על תחנות-הקצה (בפרט: לאיזה שרת איסוף להעביר את הלוגים). לשם כך, יש לבצע את הפעולות הבאות:

א. יש להגדיר רשומת Policy ב-GPO. נניח שנקרא לה "Windows Event Forwarding".



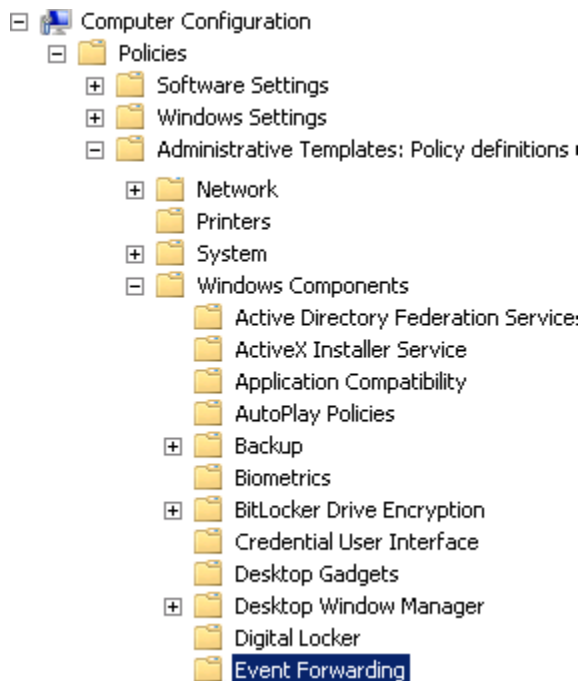
כמובן שמיד לאחר יצירתה, הרשומה לא תכיל פרטים או הגדרות כלשהם –



יש לבצע קליק-ימני על הרשומה, ולבחור באפשרות "Edit" על מנת לערוך אותה.

ב. יש לגשת אל הקונטיינר הבא –

Computer Configuration\Policies\Administrative Templates\Windows Components\Event Forwarding



ג. יש להקליק על הרשומה "Configure the server address, refresh interval..."

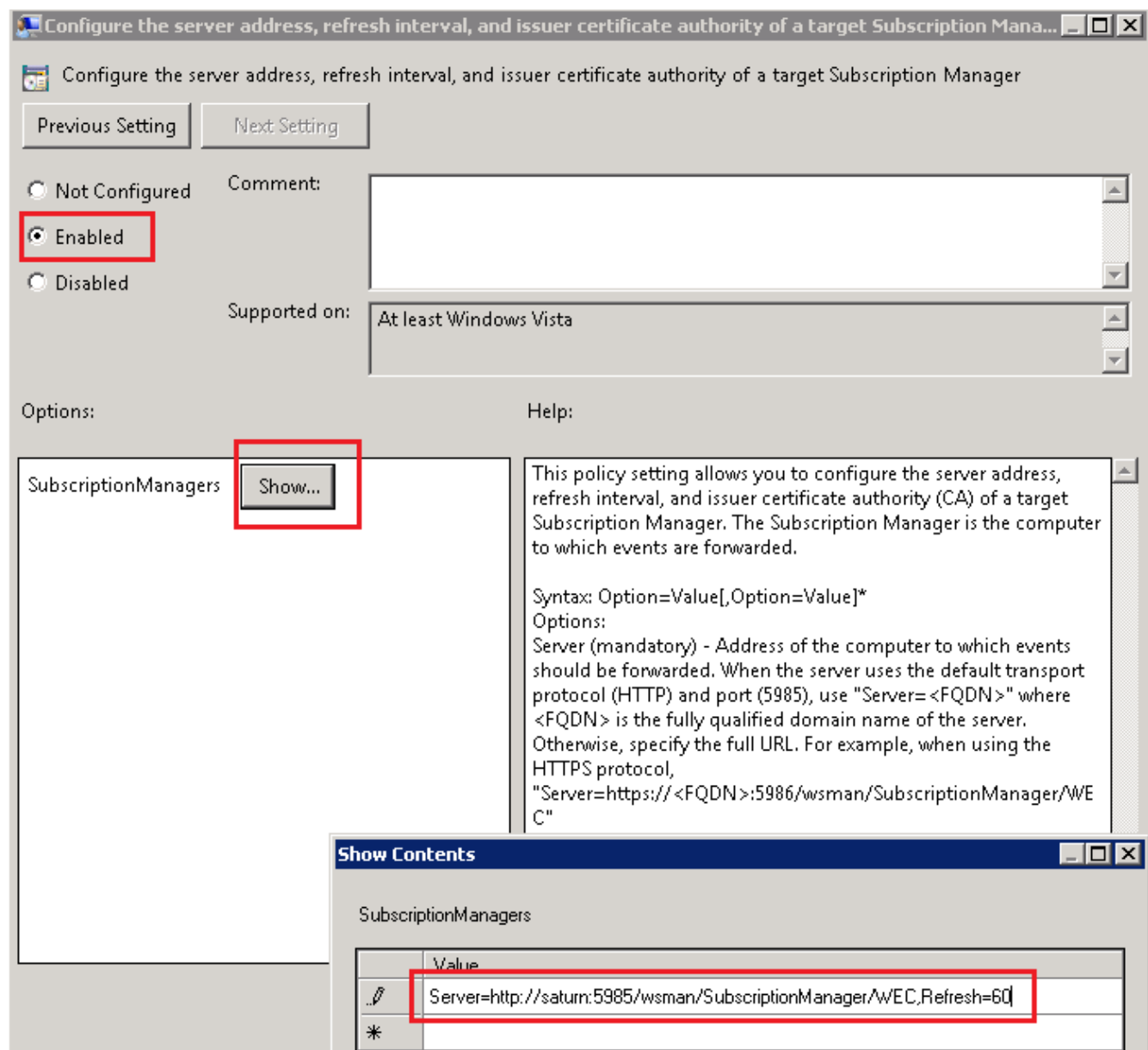
Setting	State
 ForwarderResourceUsage	Not configured
 Configure the server address, refresh interval, and issuer certificate authority of a target Subscription Manager	Not configured

בחלון שנפתח:

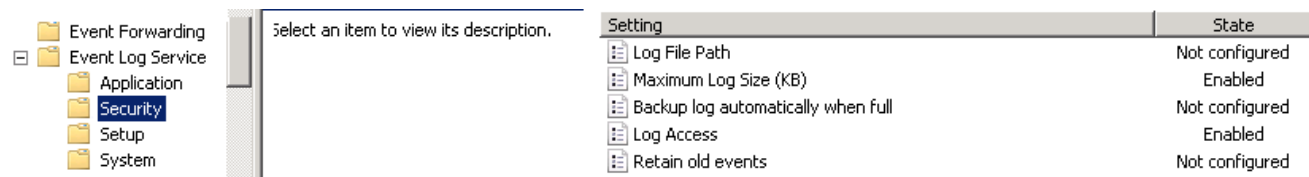
- יש לבחור באפשרות "Enabled".
- יש להקליק על הכפתור "Show" (שבסמוך ל-SubscriptionManagers). בתפריט החדש, יש להקליק על "Add" ולהכניס את הפרמטרים הדרושים; פרמטרים אלו כוללים את:
 - הכתובת של שרת האיסוף (ניתן להכניס כתובת IP, או את השם ה-DNS-י שלו, ה- FQDN [= Fully Qualified Domain Name])
 - ה-URL של ה-SubscriptionManager
 - תדירות האינטרוול (בשניות) שבו נשלחים הלוגים מהתחנה לשרת האיסוף.

לדוגמא:

Server=http://MyServer:5985/wsman/SubscriptionManager/WEC,**Refresh**=60



בנוסף, ניתן לגשת לקונטיינר "Event Log Service" ולהגדיר הגדרות שונות עבור הלוגים של Application, Security ו-System (הנוגעים לגודל הלוג, מי מורשי הגישה לקרוא אותו ושמירת לוגים ישנים).



❖ הערה: רצוי להגדיל את גודל הלוגים השונים בתחנות המקור על מנת לאסוף כמה שיותר מידע. למשל:

- הגדלת גודל לוגים של APPLICATION, SECURITY, SYSTEM ל-100 מגה (לפחות).
- הגדלת גודל לוג של SYSMON ל-100 מגה (לפחות).

2.3 הגדרות בשרת האיסוף

ייתכן המצב שבו כל הרשומות שנכנסות ל-"ForwardedEvents" (או לפחות חלקן) מופיעות עם מידע חלקי או מידע שאינו מוצג עם השדות שלו (כפי שהוא מופיע לפי פורמט הלוג בתחנה שממנו הרשומה הגיעה במקור). נחלק את הסעיף הזה להגדרות עבור רשומות של Windows Events ועבור רשומות של Sysmon:

▪ הגדרת רשומות של Windows Events מובנים

לדוגמא: אנו מקבלים הודעה בנוסח הבא –

"The description for event ID 4688 from source Microsoft-Windows-Security-Auditing cannot be found.

Level	Date and Time	Source	Ev...	Task Category	Log
Information	26/06/2017 14:27:40	Microsoft Windows security auditing.	4688	Process Creation	Security
Information	26/06/2017 14:27:23	Microsoft Windows security auditing.	4688	Process Creation	Security

Event 4688, Microsoft Windows security auditing.

General Details

The description for Event ID 4688 from source Microsoft-Windows-Security-Auditing cannot be found. Either the component on the local computer is missing or the component on the local computer is not the same as the component on the remote computer.

If the event originated on another computer, the display information had to be saved with the event.

The following information was included with the event:

על מנת לסדר את הרשומות, יש לפעול לפי הכתוב במדריך הבא:

<http://www.gorlani.com/portal/articles/windows-event-forwarding-and-missing-event-text>

The explanation is simple. The event log does not contain the full message text, but only a reference to a (usually) localized DLL. You must have the right DLLs on your system. This is not new, you can find this everywhere on the net, I would only clarify several things.

Where to find these DLLs? - Jump to this registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog, find the event source you need (**security** for the message I posted) and then the right subkey (you can read **Microsoft-Windows-Security-Auditing**) in the message.

The EventMessageFile contains %SystemRoot%\system32\adtschema.dll. That is the DLL we need on the collector. You can copy it from the original server and copy to your log collector, even changing the path if you feel. Then you need to setup the same keys in the registry to point to that DLL. The easiest way is to export the key from the original server and import on the collector, eventually changing the DLL paths.

Just a final reboot and... The same problem arises again. You have the DLLs, the registry settings, but events are not resolved to their text.

After deep searching and experimenting, I found the solution:

- List the subscriptions on your collector by issuing the following command:

```
wecutil enum-subscription
```

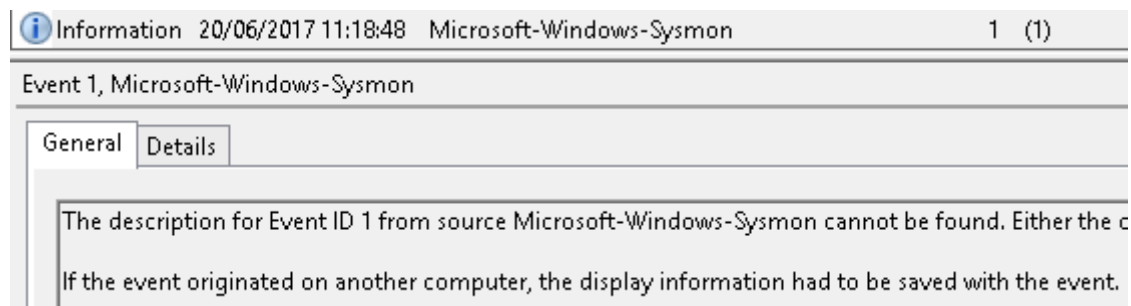
- Change the event format from RenderedText (default) to Events:

```
wecutil ss <sub_name_from_preceding_command> /cf:Events
```

▪ הגדרת רשומות של Sysmon

לדוגמא: אנו מקבלים הודעה בנוסח הבא –

"The description for event ID"...



הסיבה לכך שהמידע אינו מוצג בשרת האיסוף כפי שהוא מופיע בתחנה המקורית, היא שבתחנה המקורית – Sysmon התקין את ה-event-log manifest שלו, אשר "מסביר" ל-Event Viewer כיצד לקרוא את הרשומות ובפרט למפות שדות לערכים שלהם. על מנת לסדר את הרשומות, יש להעתיק את sysmon.exe לשרת האיסוף, ולהריץ שם את שורת הפקודה הבאה (כאדמיניסטרטור): **sysmon -m**. יש לבצע זאת פעם אחת בלבד, פר גרסא מותקנת של Sysmon בארגון.

אם אנו רואים הודעות בנוסח כזה בתחנת המקור שעליה התקנו את Sysmon, ייתכן שביצענו את ההתקנה או את הפקודה "sysmon -m" כאשר ה-Event Viewer היה פתוח. יש לסגור אותו, ואז להריץ את הפקודה שוב.

2.4. הגדרת Custom Logs

ניתן לקרוא כיצד ליצור WEF Logs נוספים (מעבר ל-"ForwardedLogs" הקיים) ולאכלס אותם בלוגים מסוגים ספציפיים כרצוננו, בקישור הבא:

<https://blogs.technet.microsoft.com/russellt/2016/05/18/creating-custom-windows-event-forwarding-logs/>

3. יצירת חוקים (Subscriptions)

יצירת חוקים ("Subscriptions") בעלי תוכן, כאלו אשר אינם "מפציצים" את אנליסט ה-SIEM ברעש רב מדי, אלא מספקים לו מידע ערכי שניתן לפעול לפיו, הוא נושא בפני עצמו אשר קצרה היריעה מלהכיל במסמך זה. לשם כך, יש להכיר לעומק את אירועי ה-Windows השונים שקיימים במערכת החלונות שבארגון, ולהבין כיצד פעילות של תוקף המתנהל ברשת באה לידי ביטוי באותם אירועים.

יחד עם זאת, תחת ההנחה של קסטומיזציה נבונה של Sysmon היא כזו המובנית לפי תרחישים – ניתן לברור מהלוגים שנוצרים על-ידו אירועים מסויימים שאותם נרצה להעביר לשרת האיסוף.

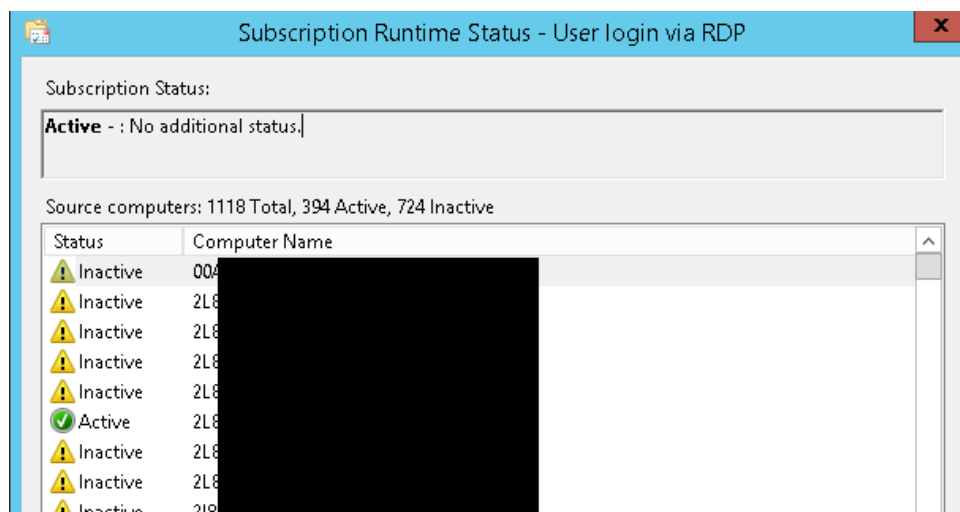
לדוגמא:

א. נגדיר עבור Sysmon לייצר רשומת לוג עבור כל תהליך שנגע בתהליך lsass.exe. מידע זה יישמר בקובץ הלוג של Sysmon בתחנת המקור.

ב. כעת נגדיר חוק בשרת האיסוף אשר ישלח את כל רשומות הלוג של אירועים שבהם נגע ב-lsass.exe תהליך שאינו אחד מהתהליכים "הלגיטימיים" הרצים בארגון (כגון: services.exe, wininit.exe, האנטי-וירוס, וכו'). כך נשמור בתחנת המקור את כלל המידע למקרה הצורך, אולם ל-SIEM יגיע מידע חלקי שכולל פחות רעש וממוקד יותר בתהליכים אשר יכולים להיחשד כזדוניים לפי פעילות זו שלהם.

Delete
Runtime Status
Properties
Disable
Retry

על מנת לראות אילו מכונות רשומות תחת Subscription מסויים, ניתן לבצע קליק-ימני על שם החוק, ואז לבחור באפשרות "Runtime Status" – כעת נוכל לצפות בחלון ברשימת המכונות ולראות את הסטטוס של כל אחד מהן ("Active" או "Inactive").



❖ הערה: רישום מכונה באמצעות Subscription לשרת האיסוף

ברגע שמכונה נרשמת בשרת האיסוף, רכיב ה-WEC (= Windows Event Collection) יוצר מפתח ברג'יסטרי עם מס' תתי-ערכים תחתיו עבור כל מכונה אשר שולחת אירועים של חוק נתון שאליו נרשמה.

אלא שהרישום הזה נשאר בשרת האיסוף לנצח; כלומר – גם אם יסירו את המכונה מהדומיין, שרת האיסוף לא ידע על כך. במילים אחרות:

“WEC never deletes these registry objects even after sources are no longer valid”.

אפשר לקבל מידע על הגדרות ה-Subscriptions, כמו גם ליצור או למחוק אותם, באמצעות הכלי המובנה wecutil. ניתן לקרוא עוד על אופן השימוש בו ויכולותיו בקישור הבא:

<https://docs.microsoft.com/en-us/windows/desktop/WEC/wecutil>

כיצד לבצע Export של Subscription לקובץ XML:

<http://godlessheathenmemoirs.blogspot.com/2013/05/windows-event-forwarding-export-and.html#>

- על מנת לצפות מחלון ה-clicli ברשימת ה-Subscriptions המוגדרים, יש להריץ את הפקודה הבאה:
wecutil es
- על מנת לייצא Subscription לקובץ XML (לבצע לו Export), ניתן להריץ את הפקודה באופן הבא:
wecutil gs MySubscriptionName /f:xml > MySubscriptionFile.xml

הנה סקריפט Batch פשוט לייצוא כל ה-Subscriptions:

```
:: Create a folder
mkdir c:\Temp

:: Save all subscription names to a file:
wecutil es > C:\\Temp\\subscriptions.txt

:: Enumerate list of subscriptions (from file) and save all to a directory:
for /f "usebackq delims=" %%i in (C:\\temp\\subscriptions.txt) do wecutil gs "%%i" /f:xml
>> "C:\\Temp\\%%i.xml"
```

■ על מנת לייבא Subscription מתוך קובץ XML (לבצע לו Import) לתוך שרת איסוף, ניתן להריץ את הפקודה באופן הבא:

wecutil cs filename.xml

אבל... קובץ שביצעתם לו Export לא ייטען ישירות באמצעות הפקודה. **למה?**

כי השורה הראשונה בקובץ מכילה הצהרת XML (XML Declaration) (מסומן פה באדום) –

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <Subscription xmlns="http://schemas.microsoft.com/...
```

זוהי מפריע לתהליך הייבוא של הקובץ לשרת האיסוף. אם ננסה לטעון קובץ כזה, נקבל הודעת שגיאה עם קוד שגיאה (Error=0x80070057). יש למחוק את השורה הראשונה, ורק אז לנסות לטעון את הקובץ.

❖ הערה חשובה:

ניתן להגדיר בשרת ה-WEC על אילו מחשבים יחול Subscription מסויים. **אולם** – האפשרות היחידה היא לבחור מחשבים או קבוצות AD, ולא ניתן לבחור ב-OU מסויים!

עקב כך, אם ברצוננו למשל להפריד בין Subscriptions המיועדים לתחנות-קצה ל-Subscriptions המיועדים לשרתים, אין לנו יכולת לעשות זאת (אלא אם כן אנו מתחזקים באופן עצמאי קבוצת AD דינאמית שדואגת להכיל את כל המחשבים שאנו רוצים להכיל עליהם Subscription מסויים).

הדרך האפשרית היחידה לבצע הפרדה כזו, היא באופן הבא:

1. להגדיר שני שרתי WEC נפרדים, כאשר כל Subscription בהם יוגדר להיות מוכל על קבוצת ה-AD ששמה "Domain Computers".

2. להגדיר שני אובייקטי GPO נפרדים של Windows Event Forwarding, שכל אחד מהם מוגדר Subscription Manager אחר (כלומר שרת WEC אחר), ואת כל אחד משני האובייקטים הנ"ל נקשר (בבצע Linking) ל-OU אחר (כגון OU של תחנות קצה ו-OU של שרתים).

ניתן לקרוא עוד על הנושא הזה בקישור שלהלן:

<https://support.logbinder.com/SuperchargerKB/50149/Controlling-Which-Computers-Subscribe-to-a-WEC-Subscription>

4. נקודות נוספות

■ השירות (Service) ששמו "Wecsvc" (או "Windows Event Collector") אחראי על ניהול ה- Windows Event Forwarding (WEF =) בצד שרת איסוף הלוגים; הוא גם אחראי גם לכתיבת לוגים בנתיב C:\Windows\System32\LogFiles\HTTPERR (תיקיה שבה למשל גם שרתי IIS כותבים לתוכה לוגים).

גם כאשר לתחנות אין רשומות לוג ספציפיות של WEF שהן צריכות לשלוח לשרת – עדיין מתקיים מנגנון Keep-Alive, שבו התחנות יוצרות סשן קצר מול השרת. אם השרת לא מקבל מידע נוסף מהן תוך אינטרוואל זמן קצר, הוא מנתק את הסשן.

תופעה זו מופיעה בלוג בתור רשומה הנראית כך: (האיזכור "Time_ConnectionIdle")

```
File Edit Format View Help
#Software: Microsoft HTTP API 2.0
#Version: 1.0
#Date: 2019-05-02 07:19:06
#Fields: date time c-ip c-port s-ip s-port cs-version cs-method cs-uri sc-status s-siteid s-reason s-queueName
2019-05-02 07:19:06 10.10.10.1 53875 192.168.1.1 5985 - - - - Timer_ConnectionIdle -
2019-05-02 07:19:06 10.10.10.1 51797 192.168.1.1 5985 - - - - Timer_ConnectionIdle -
2019-05-02 07:19:06 10.10.10.1 56144 192.168.1.1 5985 - - - - Timer_ConnectionIdle -
2019-05-02 07:19:06 10.10.10.1 3923 192.168.1.1 5985 - - - - Timer_ConnectionIdle -
2019-05-02 07:19:06 10.10.10.1 52949 192.168.1.1 5985 - - - - Timer_ConnectionIdle -
2019-05-02 07:19:06 10.10.10.1 53338 192.168.1.1 5985 - - - - Timer_ConnectionIdle -
2019-05-02 07:19:06 10.10.10.1 53877 192.168.1.1 5985 - - - - Timer_ConnectionIdle -
```

למרות שם התיקיה המטעה (HTTPERR = "http error"), אירוע ה-"Time_ConnectionIdle" אינו מהווה תקלה, אלא כאמור: עדות לקיומו של מנגנון Keep-Alive.

■ הסברים והמלצות נוספות של מייקרוסופט ניתן למצוא בקישור שלהלן:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection>

5. תקלות

5.1 Error Code 5004

לוג מקומי אחד שיכול להצביע לנו על תקלות במנגנון ה-WEF נמצא בנתיב הבא ב-Event Viewer:

Applications and Services Logs → Microsoft → Windows → Eventlog-ForwardingPlugin → Operational

שם ניתן לראות אזכור ל-"error code 5004" –

Level	Date and Time	Source	Event ID	Task Category
Error	04/02/2018 16:44:56	Eventlog-ForwardingPlugin	102	None
Error	04/02/2018 16:44:56	Eventlog-ForwardingPlugin	102	None

Event 102, Eventlog-ForwardingPlugin

General Details

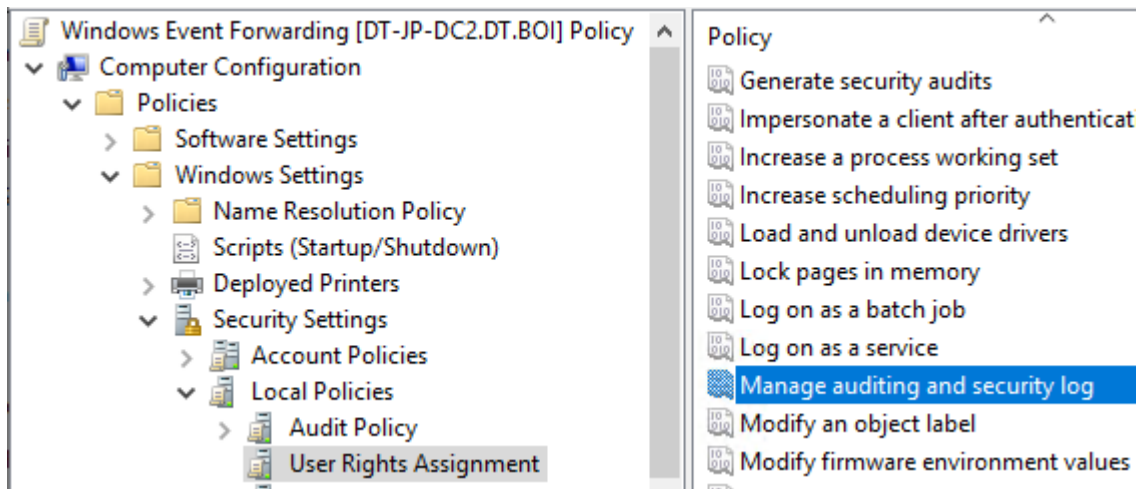
The subscription Sysmon - WScript Monitoring can not be created. The error code is 5004.

אתר התמיכה של מייקרוסופט טוען שהתקלה נובעת מכך שהחשבון של "Network Service" לא הוגדר להיות מורשה לקרוא את הלוגים, ומציע את הפתרון שמופיע כאן:

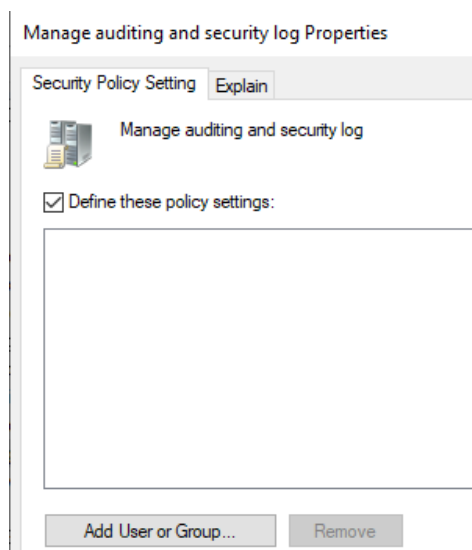
מקור הבעיה היא ש-WinRM (אשר רץ תחת NETWORK SERVICE) אינו יכול לקרוא את ה-Security log מכיוון שאין לו הרשאות תחת "Manage auditing and security log". על מנת לאפשר זאת עבורו, יש להגדיר את ההגדרות הבאות ב-GPO הרלוונטי של "Windows Event Forwarding" –

א. יש לגשת לנתיב הבא, ולפתוח את האפשרות "Manage auditing and security log":

Computer Configuration → Policies → Windows Settings → Security Settings →
Local Policies → User Rights Assignment → Manage auditing and security log



ב. יש לסמן את האפשרות "Define these policy settings", ולהקליק על הכפתור "Add user or group".



ג. יש להוסיף את הקבוצות והיזרים הבאים:

- Administrators
- Local Service
- NETWORK SERVICE

הגדרת ה-Audit הנ"ל ("Manage auditing and security log") ממופה ל-user-right constant שנקרא SeSecurityPrivilege. ניתן לבדוק אילו יוזרים או קבוצות משוייכים אליו באמצעות הרצת הפקודות הבאות:

```
secedit /export /mergedpolicy /areas user_rights /cfg C:\Temp\righs.inf
type C:\Temp\righs.inf | findstr /i SeSecurityPrivilege
```

אנחנו אמורים לראות שורה בנוסח הבא:

```
sesecurityprivilege = *S-1-5-32-544,*S-1-5-19,*S-1-5-20
```

באשר –

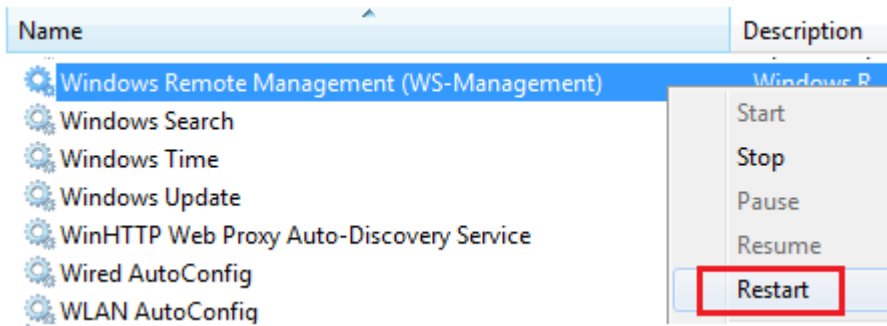
SID	Name
S-1-5-32-544	BUILTIN\Administrators
S-1-5-19	NT AUTHORITY\LOCAL SERVICE
S-1-5-20	NT AUTHORITY\NETWORK SERVICE

במידה ופתרון זה אינו עובד, יש לבצע את הפעולות הבאות:

1. יש לפתוח חלון CMD כאדמיניסטרטור ולהריץ את הפקודה הבאה:

```
Sc config WinRM type= own
```

2. יש לבצע אתחול לשירות של ה-WinRM –



פקודה זו מגדירה למעשה "פ" להריץ את השירות של WinRM תחת תהליך svchost משלו. במילים אחרות: הפרמטר "type" יכול להיות אחד משתי קטגוריות: "share" או "own". במצב של "share", עץ התהליכים ייראה באופן הבא:

svchost.exe (shared)

- |— WinRM
- |— EventLog
- |— Other services

לעומת זאת, במצב של "own", הוא ייראה כך:

svchost.exe (WinRM only)

- |— WinRM

ההגדרה של הרצת WinRM תחת תהליך אב ללא שיתוף עם תהליכים ושירותים אחרים לעתים מסיר תלויות או בעיות שיכולות לנבוע משיתוף משאבים שכזה.

5.2 בעיה ברישום תחנות בשרת האיסוף

אם תחנות לא מופיעות בשרת האיסוף (לא נרשמו לקבל Subscriptions) – הנה פתרון אפשרי לבעיה:

<https://social.technet.microsoft.com/Forums/windows/en-US/8d19afb7-bd41-4aeb-9dc3-ec1c852f5f6c/event-log-forwarding-push-not-working-collector-http-url-not-available?forum=winservergen>

5.3 הגדרות חסרות ב-GPO

- כאמור, על מנת להגדיר הגדרות נחוצות של WinRM בתחנה (הרמת Listener שיאזין בפורט 5985), יש להריץ בה את הפקודה הבאה:

winrm quickconfig -q

- על מנת לבדוק מה הסטטוס של ה-Listener, ניתן להקליד את הפקודה הבאה:

winrm e winrm/config/listener

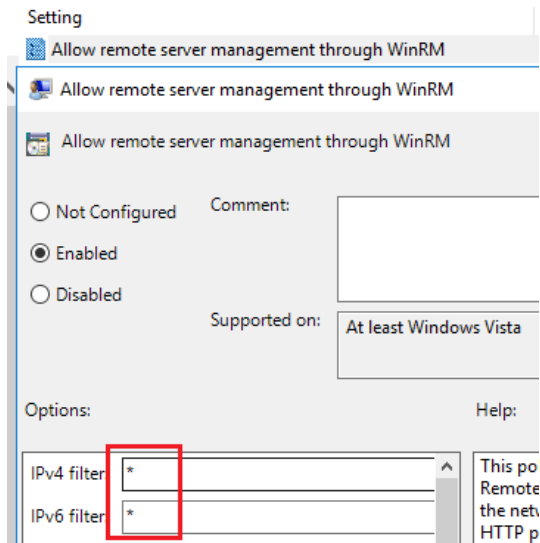
- במידה ואנו נתקלים בהודעה הבאה (מסומנת כאן באדום) –

```
Listener [Source="GPO"]  
Address = *  
Transport = HTTP  
Port = 5985  
Hostname  
Enabled = true  
URLPrefix = wsman  
CertificateThumbprint  
ListeningOn = null
```

פירושו של דבר ש-WinRM אמנם הוגדר, אולם לא קונפג להאזין על Network Interface כלשהו. מקור הבעיה הוא ב-GPO עצמו. יש לגשת ב-GPO הרלוונטי בארגון האחראי ל-WinRM, ולהגיע להגדרה שנמצאת בנתיב הבא –

WinRM service → Policies → Administrative Templates → Windows Components → Windows Remote Management (WinRM) → WinRM Service → **"Allow remote server management through WinRM"**

שם יש לסמן בכוכביות את שדות הטקסט הבאים –



5.4. לוגים לא מופיעים בשרת ה-WEC

5.4.1. אתחול ה-Windows Event Log

- ייתכן מצב שבו הגדרנו Subscription בשרת ה-WEC, תחנה נרשמה לקבל את ה-Subscription ומופיעה בשרת ה-WEC, אבל לא שולחת לוגים של אותו Subscription.

5.4.2. טיפול ב-Windows Event Collector בשרת ה-WEC

- אם בדקנו וראינו שאין חסימות ב-FW מהתחנות הרשומות ל-Subscriptions אל שרת ה-WEC (ניתן גם להריץ פקודת `netstat -ano` בשרת ה-WEC עצמו ולוודא שיש Connections מהתחנות לשרת), אבל לוגים מהתחנות עדיין לא מופיעים בלוג של Forwarded Events, ייתכן שה-Service שאחראי על ניהול ה-Subscriptions נפל.
- מדובר ב-Service בשם "Windows Event Collector", והוא אמור להיות בסטטוס של "Running" ו-"Automatic (Delayed Start)".

Name	Description	Status	Startup Type
 Windows Event Collector	This service manages persistent subscriptions...	Running	Automatic (Delayed Start)

במידה והוא נפל, יש להרים אותו.

תופעה אחרת יכולה להתרחש בשרתי Windows Server 2016 / 2019: אם ניכנס ללוגים בנתיב הבא –
Applications and Services Logs → Microsoft → Windows → Eventlog-ForwardingPlugin → Operational

ונראה שם Event ID 105 עם התיאור:

The description for Event ID 105 from source Microsoft-Windows-Forwarding cannot be found.

Either the component that raises this event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer.

Operational Number of events: 43

Level	Date and Time	Source	Event ID	Task Category
Error	07/05/20 2:10:01 PM	Eventlog-ForwardingPlugin	105	None

Event 105, Eventlog-ForwardingPlugin

General Details

The description for Event ID 105 from source Microsoft-Windows-Forwarding cannot be found. Either the component that raises this event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer.

If the event originated on another computer, the display information had to be saved with the event.

The following information was included with the event:

<http://boi-jp-saturn:5985/wsman/SubscriptionManager/WEC>

5

<f:WSManFault xmlns:f="http://schemas.microsoft.com/wbem/wsman/1/wsmanfault" Code="5" Machine="boi-jp-saturn.ad.boi.gov.il"><f:Message>Access is denied.</f:Message></f:WSManFault>

The handle is invalid

אזי הבעיה נובעת מעניין של הרשאות ל-Processes של WinRM ו-WecSvc; ניתן לקרוא בהרחבה על מהות הבעיה בקישור הבא:

<https://support.microsoft.com/en-us/help/4494462/events-not-forwarded-if-the-collector-runs-windows-server>

הפתרון הנו לפתוח חלון CMD כאדמיניסטרטור, ולהריץ את הפקודות הבאות:

- `netsh http delete urlacl url=http://+:5985/wsman/`

- netsh http add urlacl url=http://+:5985/wsman/ sddl=D:(A;;GX;;;S-1-5-80-569256582-2953403351-2909559716-1301513147-412116970)(A;;GX;;;S-1-5-80-4059739203-877974739-1245631912-527174227-2996563517)
- netsh http delete urlacl url=https://+:5986/wsman/
- netsh http add urlacl url=https://+:5986/wsman/ sddl=D:(A;;GX;;;S-1-5-80-569256582-2953403351-2909559716-1301513147-412116970)(A;;GX;;;S-1-5-80-4059739203-877974739-1245631912-527174227-2996563517)

Event ID 111 5.5

במידה ואנחנו רואים בלוג של ה-ForwardedEvents אירועים עם Event ID 111:

The description for Event ID 111 from source Microsoft-Windows-EventForwarder cannot be found. Either the component that raises this event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer.

Level	Date and Time	Source	Event ID	Task Category	Log	Computer
Information	07/05/20 2:11:28 PM	Microsoft-Win...	111	None		PRD-SP13...
Event 111, Microsoft-Windows-EventForwarder						
General Details The description for Event ID 111 from source Microsoft-Windows-EventForwarder cannot be found. Either the component that raises this event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer. If the event originated on another computer, the display information had to be saved with the event. The following information was included with the event:						

אזי הפתרון הוא: לא לעשות דבר.

להלן ההסבר לתופעה, כפי שהוא מופיע בקישור הבא:

<https://social.technet.microsoft.com/Forums/windowsserver/en-US/93cd6c41-c502-48bc-9db7-077405fff829/error-from-event-log-forwarding-setup-the-description-for-event-id-111-from-source?forum=winserverManagement>

"Solution: This is just the initial bookmark event that Event forwarding plugin uses to mark the beginning of a subscription; it can be ignored."

דיונים נוספים בנוגע לאיבוד לוגים וחוסר רספונסיביות של שרת ה-WEC:

<https://github.com/palantir/windows-event-forwarding/issues/35>

<https://learn.microsoft.com/en-us/windows/win32/winrm/installation-and-configuration-for-windows-remote-management#winrm-service-default-configuration-settings>

5.6. חוסר רספונסיביות של ה-Event Viewer בעת צפיה ב-Subscriptions בשרת ה-WEC

ישנה התייחסות לכך ב[דוקומנטציה של מייקרוסופט](#).

6. נקודות נוספות

כאשר הגדרות WEF מוגדרות באמצעות GPO, ניתן למצוא ברג'יסטרי של התחנה המקומית את הנתונים הבאים:

▪ כתובת שרת ה-WEC שאליו יש לשלוח לוגים:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EventLog\EventForwarding\
SubscriptionManager