

لجس تانودا نم ققحتلل WEVTUTIL مادختسا شادحالا

تايوتحمل

[قمدقمل](#)

[شادحالا لجس تائراق - تايساسالا](#)

[تانودالا نم ققحتلا - wevtutil](#)

[يضايرتفال اعضولا، لالطبضل، قداغ - 1 حالصالا](#)

[wevtutil مادختساب SDDL شيحت - 2 حالصالا](#)

[GPO - 3 حالصالا](#)

قمدقمل

ىل لوخدلا ليجست شح تانودا نم ققحتلل WebSwitch مادختسا دنتسملا اذه فصلي
لصوملا.

رشابملا مكحتلا ةدحو نم لوخدلا ليجست شادحاً ةعارق هنكمي لصوملا ناك اذا ام رابتخا كنكمي
[WBemtest](#) مادختساب.

اذل، WMI/DCOM تانودا يف أطخ ببسب ةداع شحي كلذ نإف، لاصتالا يف WBemtest لشف اذا
[رخآ ناكم](#) نم ةدعاسملا بلطا.

شادحاً ةيأ راهظا متي ال نكلو لاصتالا متي، تالاحال ضعب يف، كلذ عمو

اذهل ناببس كانه:

- مكحتلا ةدحو ىلع لوخدلا ليجست شادحاً بقعت متي ال كلذل، حيحص ريغ قيقدتلا جهن
[قيقدتلا، سايس](#) يف ةدعاسملا بلط. لاجملاب
- ىدل دجوي ال نكلو DC لاجملاب مكحتلا ةدحو يف شادحالا ليجست نالا متي
...عبات. نامالا شادحاً لجس نم ةعارقلا اب نذال OpenDNS_Connector

شادحالا لجس تائراق - تايساسالا

ةعومجم ىل OpenDNS_Connector مدختسم ةفاضل لثم اطياسب كلذ نوكتي تالاحال مظعم يف
شادحالا لجس ةعارقلا اهجاتحي يتلا تانودالا هي طعي اذه. شادحالا لجس عارق

تانودالا نم ققحتلا - wevtutil

ةيضايرتفال تانودالا شادحالا لجس تائراق ةعومجمل نوكتي ال، ةردانلا تالاحال ضعب يف
نامالا شادحاً لجسل ةحونمملا تانودالا نم ةلوهسب ققحتلل WebTable مادختسا اننكمي

طيسب ليغشت:

1. يلي امك [SDDL](#) [غايص](#) مادختساب تانوذال جارخال حضوي:

```
channelAccess: 0:BAG:SYD:(A;;0x3;;;S-1-5-3)(A;;0x3;;;S-1-5-33)(A;;0x1;;;S-1-5-573)
```

2. ER. هراصتخا نكمي وأ S-1-5-32-573 وه شادخال لجس ئراق ل SID نإ.

3. لثم، تانوذال ل ةيرشعلا ةيسادسلا ةميقل نوكت:

- 0x1 = ةءارق
- 0x2 = ةباتكل
- 0x3 = ةباتك/ةءارق

يضرارتفال اعضولا لىا طبضل اءاعا - 1 اءالصالا

ىلع يوتحت لجس ةميقل فذح قيرط نع ةيضرارتفال اءاعا لىا تانوذال نييعت اءاعا نكمي ارق تىل اىخال اءماربال لىع رثوي دق هنكلو، عيرس اءالصالا اءه. ةصصخمل SDDL ةلسلس (نكمأ نإ) شادخال لجس نم.

HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Security نم 'CustomSD' ةميقل فذحا

wevtutil مادختساب SDDL شيدحت - 2 اءالصالا

WebSwitch. مادختساب ةرشابم تانوذال نييعت اننكمي، ةردان فورظ ي ف

1. رمالا اءه مادختساب، اقبس م حضوم وه امك ةيلالال تانوذال لىع لصحا:

```
wevtutil gl security
```

2. لاثم. ةانقلا لىا لوصول ةلسلس نود:

```
/ca:0:BAG:SYD:(A;;0x3;;;S-1-5-3)(A;;0x3;;;S-1-5-33)
```

3. OpenDNS_Connector: مدختسلم SID فاشتكا لىع لمعا:

```
wmic useraccount where name='OpenDNS_Connector' get sid
```

4. ةلسلسب هءافرا قيرط نع OpenDNS_Connector لىا ةءارقلل لوصول قح حنم كنكمي. OpenDNS_Connector نامأ فرع مب <sid> لدبتسا. يلي امك ةدوومل ةانقلا لوصول

```
wevtutil sl security /ca:0:BAG:SYD:(A;;0x3;;;S-1-5-3)(A;;0x3;;;S-1-5-33)(A;;0x1;;;<SID>)
```

ثادحأل لچس عارق ةعومچم ب صاخلا (SID) نامأل فرعم يلي امي ف ،عجرمك

573-32-5-1-س:ديس

BUILTIN/ثادحأل لچس تائراق :مسالا

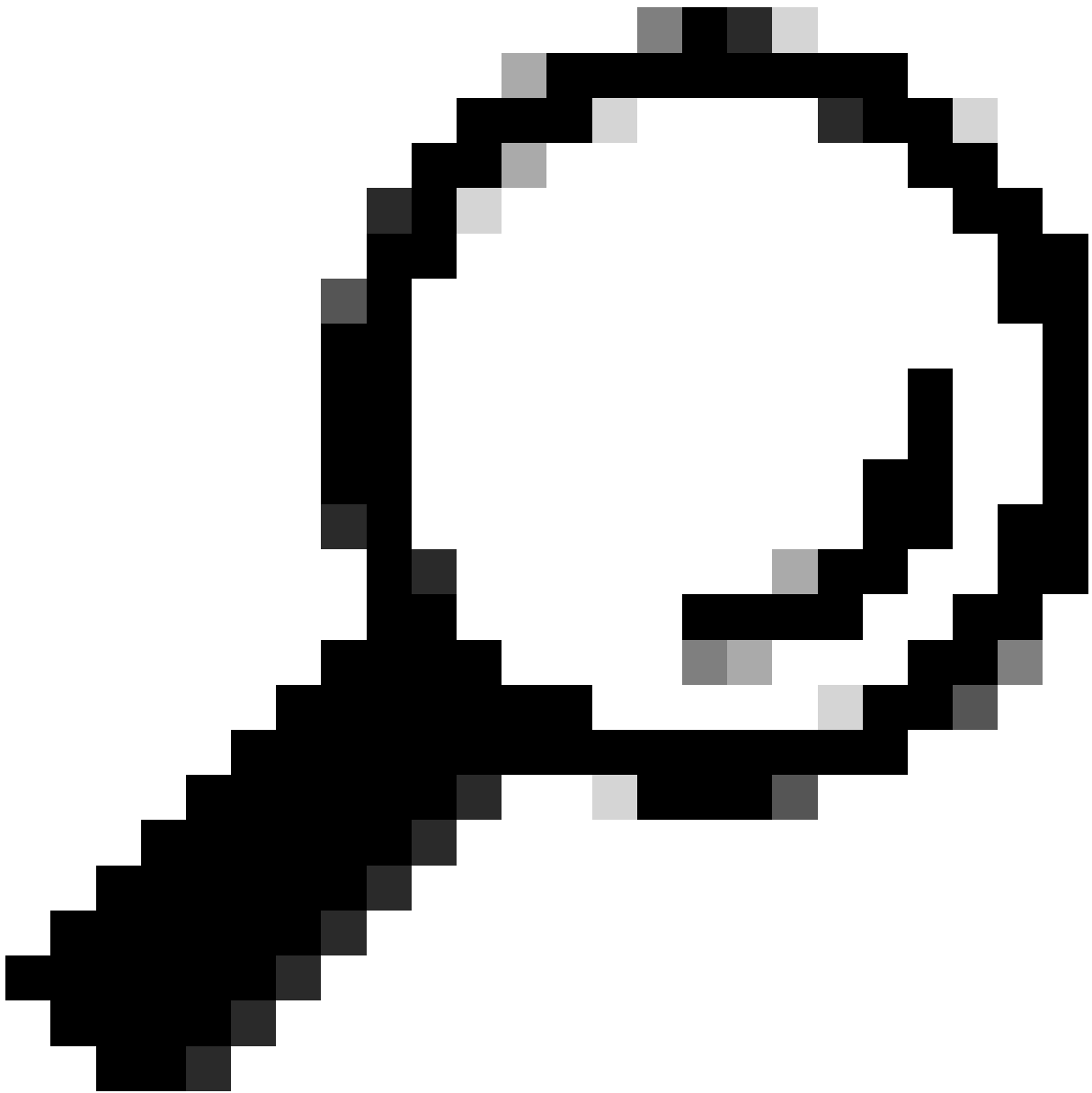
زاهال نم ثادحأل تالچس ةعارق ةعومچملا هذه عاضأل نكمي .يلحم ءانب قيرف :فصولا
يلحمل

GPO - 3 حالصإلا

مادختساب نامأل ثادحأل لچس (!ةباتكلاو) ةعارقل نذال OpenDNS Connector باسح حنم نكمي
،بولطم وه امم رثكأ تانوذأ ةينقتلا ةيحلل نم دادعإلا اذه يطيغي .اذه ةعومچملا جهن دادعإ
رييغتلا عارجال ةلهس ةقيرط هنكلو

قوقح نييعة\ةيلحمل جهن\نامأل تادادع\Windows تادادع\جهن\ارتيو\بمكل نيوكت
نامأل لچس وقيقدتلا ةرادإ\مدختسملا

ل.لحملاب مكحتلا ةدحو ىلع 'gpupdate /force' ليغشت عاجرلا ،رييغتلا عارجا دعب



دجوت ال دق، Windows 2003 / 2003 لي غشت ال ماظنل في في طول ال يوتسم ال ال ع: ع ط ح الم
حامس لل يساس ال بولس ال وه اذه GPO ن ف، م ث نمو، "ث ادح ال تال ح س تائراق" ع و م ح م
ة يساس ال م ظن ال ه ذه ال OpenDNS ل ص و م ل و ص و ب.

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م ج ر ت
م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م ج ر ت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م م ج ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م ج ر ت ل ا ع م ل ا ح ل ا و ه
ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م ج ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems
(ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا