

اهحالصإو Kerberos ةقداصم ءاطخأ فاشكتسأ في SWA

تايوتحمل

[ةمدقملا](#)

[حلطصلما](#)

[ةيساسألا تابلطتلملا](#)

[تابلطتلملا](#)

[ةمدختسملل تانوكمللا](#)

[Kerberos ةكبش قفدت](#)

[SWA في Kerberos ةقداصم قفدت](#)

[SPN نم ضرغللا وه ام](#)

[Active Directory مداخ نيوكت](#)

[اهحالصإو ءاطخألا فاشكتسأ](#)

[SPN رماوأ مداختساب اهلحالصإو Kerberos ءاطخأ فاشكتسأ](#)

[SPN تاجرخمورماوأ ىلع ةلثمأ](#)

[SPN ىلع روثعللا متي مل: 1 ويرانيسللا](#)

[SPN ىلع روثعللا مت: نيناثللا ويرانيسللا](#)

[SWA ىلع اهلحالصإو Kerberos ءاطخأ فاشكتسأ](#)

[Kerberos تانايب ةدعاق في مداخللا ىلع روثعللا متي مل](#)

[ةيفاضا عجارموتامولعم](#)

ةمدقملا

ءاطخأ فاشكتساب ةصاخلا تاوطخللاو Kerberos ةقداصم تايساسأ دنتسمللا اذه فصوي (SWA) نمآلا بيو زاهج في اهلحالصإو Kerberos ةقداصم.

حلطصلما

اوس	(ببوللا ةيامح زاهج) Secure Web Appliance
CLI	رماوالا رطس ةهجاو
نالعا	طشنللا ليلدللا
يس يد	لاجلما لاب مكحتلا ةدحو

SPN	يَسَاسُ أَلَا مَدْخَلُ مَسَا
يَسَاسُ يَدِي كِ	Kerberos حَاتِفَم عِيَزُوت زَكْرَم
يَتِي جِي تِي	(عَرَكُذَلَا حَنَم عَقَاطِب) عَقَدَاصَمَلَا عَقَاطِب
TGS	رَكَاذَلَا حَنَم مَدْخَلُ
ههه	عَقَلَا عَقَاطِب
VRRP	يَرَهَاظَلَا هِيَجُوتَلَا زَاهَج رَارَكُت لُوكُوتُورِب
طوبش	عِئَاشَلَا نَاوَنَعَلَا رَارَكُت لُوكُوتُورِب
SPN	يَسَاسُ أَلَا مَدْخَلُ مَسَا
LDAP	لِيلِدَلَل لُوصُولَل فَيَفِخَلَا لُوكُوتُورِبَلَا

عَقَلَا تَابَلَطَتَمَلَا

تابَلَطَتَمَلَا

عَقَلَاتَلَا عِيَضَاوَمَلَا ب عَفَرَعَم كِيَدَل نُوكُت نَاب Cisco يَصُوت:

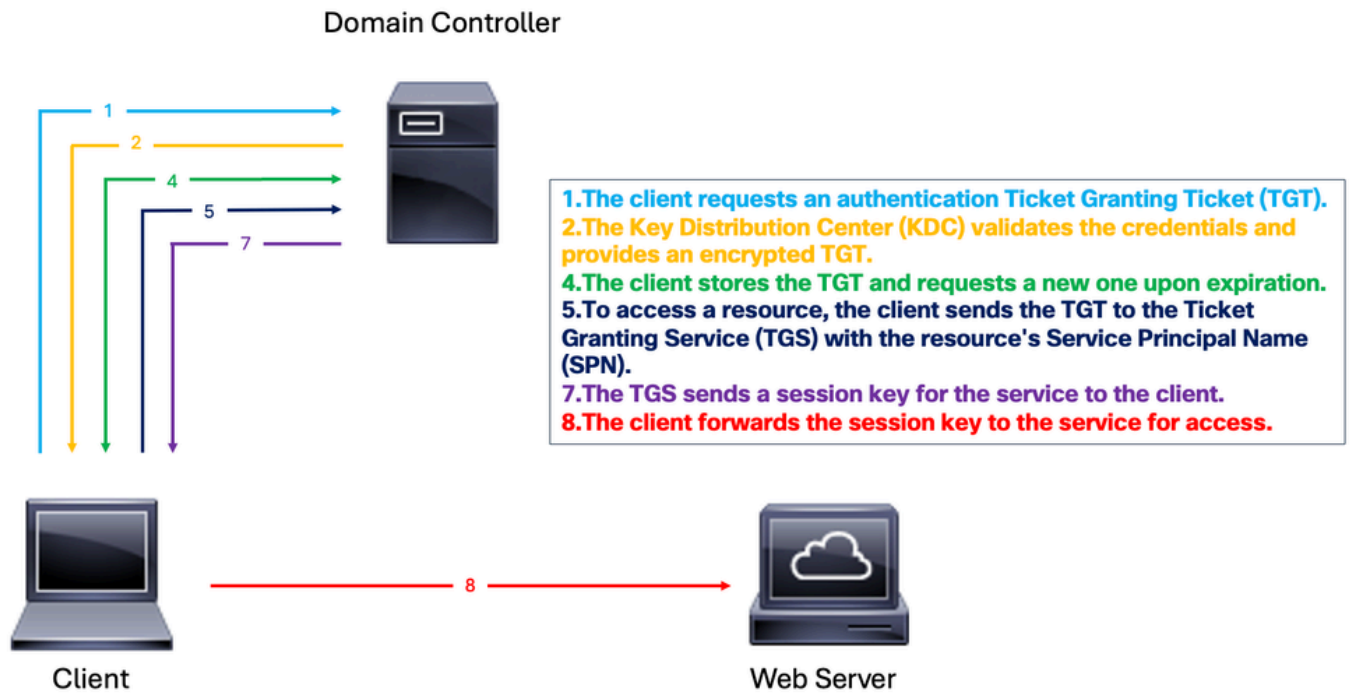
- Kerberos عَقَدَاصَمَو Active Directory.
- SWA. يَلَع لُولُحَلَاو عَقَدَاصَمَلَا.

عَمَدُخَتَسَمَلَا تَانُوكَمَلَا

عَنِيَعَم عَقَدَام تَانُوكَمُوجَمَارِب تَارَادَصَا يَلَع دَنَتَسَمَلَا اذَه رَصَتَقِي اَل.

عَصَاخ عَقِلَمَعَم عَقِيْب يَف عُدُوجُومَلَا عَزَهْأَلَا نَم دَنَتَسَمَلَا اذَه يَف عُدَاوَلَا تَامُولَعَمَلَا عَاشَنَامَت تَنَاك اذَا. (يَضَارَتَفَا) حُوسَمَم نِيُوكُتَب دَنَتَسَمَلَا اذَه يَف عَمَدُخَتَسُمَلَا عَزَهْأَلَا عِيَمَج تَأَدَب رَمَأ يَأَل لَمَتَحَمَلَا رِيَثَاتَلَل كَمَهَف نَم دُكَاتَف، لِيغَشَتَلَا دِيَق كَتَكَبَش.

Kerberos عَكَبَش قَفَدَت



Kerberos قفدت جڤوم ن: ةروصلا

Kerberized: ةئيب في ةقداصم لل ةيساسأل تاوطخل الي اميف

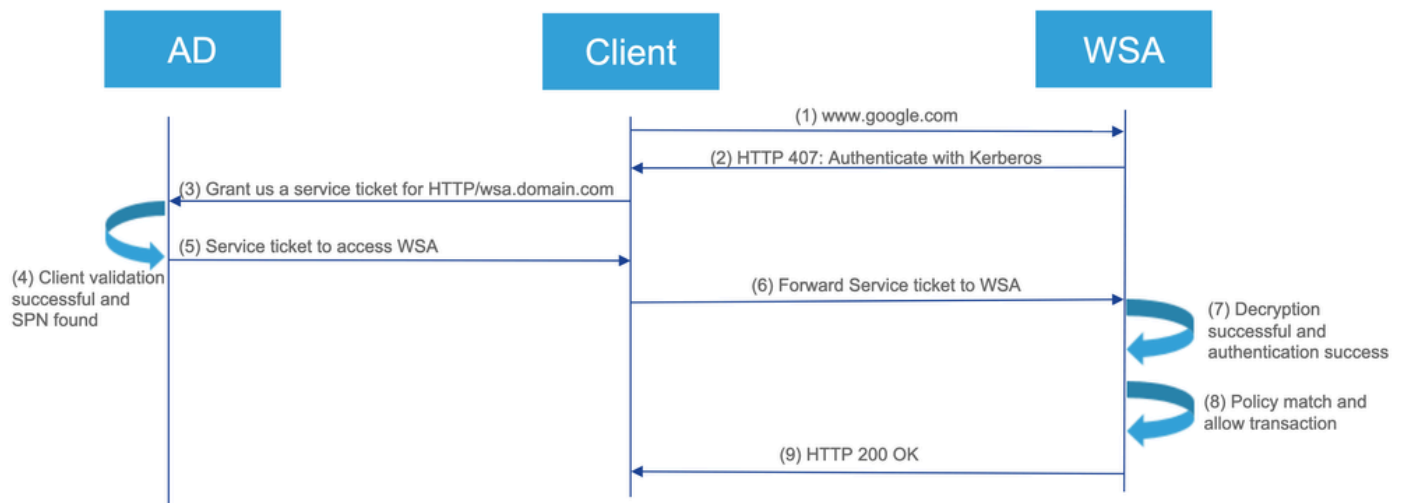
1. (KDC) حيتافم ال عيزوت زكرم نم (TGT) ةركذت حنم ةقاطب ليمع ال بلطي.
2. ةسلج حاتفم و TGT حاتفم لسري و ليمع ال زاهج مدختسم دامتعا تانايب نم KDC ققحتي. ارفشم لمع.
3. (TGS) ةركذت ال حنم ةمدخل يسر ال حاتفم ال مادختساب TGT ريفشت متي.
4. هتجالص ءاهتنا دنع ديدج مسا ايئاقلت بلطي و TGT نيزختب ليمع ال موقي.

دروم و ةمدخل ال لوصول

1. بولطم ال دروم لل (SPN) ةيساسأل ةمدخل مسا ال ةفاضل اب TGS ال TGT ليمع ال لسري.
2. ليمع زاهج ال لوصول و قوقح نم ققحتي و TGT نم ةكبش ال في مكحت ال زكرم ققحتي. مدختسم ال.
3. ليمع ال ال ةمدخل اب صاخ لمع ةسلج حاتفم TGS لسري.
4. لوصول ةمدخل حيتو، لوصول تاثل ةمدخل ل ةسلج ال حاتفم ليمع ال رفوي.

SWA في Kerberos ةقداصم قفدت

Kerberos authentication flow



1. SWA لالځ نم www.google.com ىلى لوصولو لىمعل بلطي.
2. ةقداصملا ةبلاط، HTTP 407 ةلاحب (SWA) لوحمل تانايب ةدعاق ةرادا درت.
3. TGT مادختساب HTTP/SWA.domain.com ةمدخل AD مداخل نم ةمدخ ةركذت لىمعل بلطي لالځم مامضنا ءانثأ هىلع لصحي يذلى.
4. SPN ىلى روثعل متو كلذ حجن اذو، ةمدخ ةركذت ردصو لىمعل ءحص نم AD مداخل ققحتي ةيلا لىلى ةوطخل ىلى لىلقتني هنإف، SWA ل (يسىئرلا ةمدخل مسا).
5. SWA ىلى ةركذتلا هذه لىمعل لسري.
6. ةقداصملا نم ققحتلاو ةركذتلا ريفشت ك فب SWA موقت.
7. تاسايسلا نم SWA ققحتي، ةقداصملا تحجن اذى.
8. ةلماعملاب حامسلا مت اذى لىمعل ىلى "HTTP 200/OK" ةباجتسا SWA لسرت.

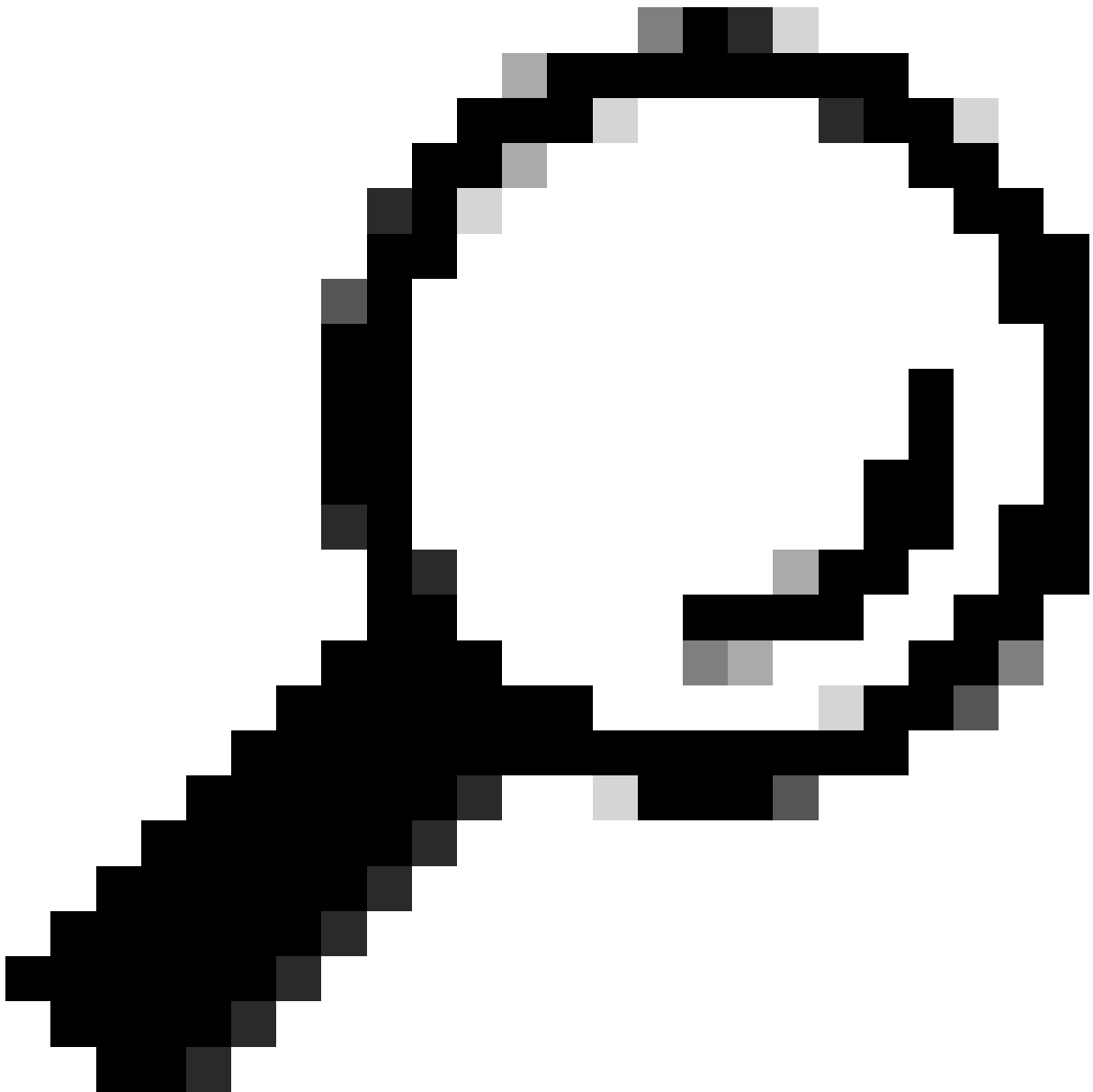
SPN نم ضرغل وه ام

طبري وه Kerberos ةقداصم ي ف ةمدخ لىثم ديرف لكشب (SPN) ىساسألا ةمدخل مسا ددحي مسا ىلى ةجالحا نود ةمدخل ةقداصملا بلطب ءالمعلل حمسي امم، ةمدخ باسحب ةمدخل لىثم لو، حوتفملا LDAP وأ AD لثم، (KDC) حىاتافملا عيزوت زكرم قىبطت ي ف باسح لك. باسحلا اناىحأ ئطاخ لكشب ممدختست هنإف، مراص لكشب ةمدخل ددحت SPN ءكبش نأ نيح ي ف SPN. لىمعل اضيأ ةمدخل اهيف لمعت يتلا تاهوي رانىسل ي ف (UPN) لىمعل مسا ىلى ةراشلال.

وهو. ءكبش لخد ةمدخ لىثم ديرف لكشب (SPN) ىساسألا ةمدخل مسا ددحي Kerberos، ي ف نكمي امم، هباسحب ةمدخل لىثم SPN طبري. ةنيعم ةمدخل ةقداصملا بلطب ءالمعلل حمسي ةمدخل كلت ىلى لوصولو تابلط لىفوتو حيحص لكشب ةقداصملا نم Kerberos.

Active Directory مداخل نيوكت

1. همادختسال دوجوم ممدختسم باسح رايتخا وأ ديدج ممدختسم باسح ءاشنإ.
2. راتخملا ممدختسملا باسح لباقم همادختسا دارملا SPN لىجست.
3. ةركم SPN تاكشب يأ لىجست مدع نم دكأت.



ةكرح ري دم وأ ليمحتلا نزاوم فلخ SWA عم Kerberos فلتخي فيك :خيملت
باسحب HA Virtual Hostname ل SPN نارتقا نم الدب ؟رورملا ةكرح لغاش/رورملا
لاثملا ليمبس ىلع HTTP رورم ةكرح هيجوت ةداعإ زاهج ل SPN نارقإب مق ،مدختسم
نالعإلا ىلع مدختسم باسح عم (رورملا ةكرح ري دم وأ ليمحتلا نزاوم

Kerberos: ذيفنتل تاسرامملا لصفأ ىلع روثعل نكمي

- [نمآلا بيولا زاهج تاسرامم لصفأ](#)
- [SWA تالاصتال ةياعملا رادج ذفانم نيوكت](#)

اهحالصإو عاطخألا فاشكتسا

SPN رماوأ مادختساب اهحالصإو Kerberos عاطخأ فاشكتسا

ةئيب ي ف (SPN) ةيساسأل تامدخل ءامسأ ةرادل ةديفم ال setSPN رم اوأ ةمئاق ي لي امي ف ةئيب ي ف ةيرادا تازايتما تاذ رماوأ رطس ةهجاو نم ةداع رماوالا هذه لي غشت متي Kerberos Windows.

نبي عم باسحل SPNs درس:	setSPN -L <User/ComputerAccountName> ددحمل باسحلل ةلجسم ال SPNs ةفاك درسي
باسح ىلإ SPN ةفاضل:	setSPN -A <SPN> <User/ComputerAccountName> ددحمل باسحل ال ىلإ ددحمل ال SPN ةفاضل
باسح نم SPN فذح:	setSPN -D <SPN> <User/ComputerAccountName> ددحمل باسحل ال نم ددحمل ال SPN ةلازا
SPN لي جست نم ققحت ال لعفلاب:	setSPN -Q <SPN> لحمل ال ي ف لعفلاب الجسم ددحمل ال SPN ناك اذا ام ققحت ال
لحمل ال ي ف SPNs ةفاك درس	setSPN -L <User/Computer account> لحمل ال ي ف SPN تاك بش عي مج درسي
باسحل SPN ني عت رتوي بمك ال:	setSPN -S <SPN> <User/CoumputerAccountName> راركت مدع نمضي امم ،رتوي بمك باسح ىلإ SPN ةفاضل تالاخلال
باسحل SPNs ني عت ةداعل ددحمل:	setSPN -R <User/CoumputerAccountName> لكاشم لح ي ف دعاسي امم ،ددحمل باسحلل SPNs ني عت ةداعل ةرركم ال SPN

SPN تاخلرمو رماو ىل ع ةلثمأ

مادختسال حضوت ةمدقم ال ةلثمأ

- vrpServiceUser :رتوي بمك ال/مدختسم ال باسح
- SPN: http/WsaHostname.com وأ http/proxyha.localdomain

مدختسم باسحب لعفلاب انرتقم SPN ناك اذا ام ققحت ال

setSPN -q <SPN>

setSPN -q http/proxyha.localdomain

SPN ىلع روثلال متي مل: 1 ويرانيال

```
Administrator: Command Prompt
C:\Users\Administrator.DC2MAIN>setspn -q http/proxyha.localdomain
Checking domain DC=ad2012main,DC=samba4integration
No such SPN found.
```

SPN ىلع روثلال مت: يثالثا ويرانيال

```
Administrator: Command Prompt
C:\Users\Administrator.DC2MAIN>setspn -q http/proxyha.localdomain
Checking domain DC=ad2012main,DC=samba4integration
CN=vrperviceuser,CN=Users,DC=ad2012main,DC=samba4integration
http/proxyha.localdomain
Existing SPN found!
```

- حل اص رت وي ب م ك / م د خ ت س م با س ح ب SPN ن ا ر ق ا |

< رت وي ب م ك ل / م د خ ت س م ل با س ح > < SPN > setSPN -s : ع غ ي ص ل ا

س ا ب س ل ل ا م ل ا ل ا ل ا : setSPN -s http/proxyha.localdomain vrpServiceUser

```
Administrator: Command Prompt
C:\Users\Administrator.DC2MAIN>setspn -s http/proxyha.localdomain vrperviceuser
Checking domain DC=ad2012main,DC=samba4integration
Registering ServicePrincipalNames for CN=vrperviceuser,CN=Users,DC=ad2012main,DC=samba4integration
http/proxyha.localdomain
Updated object
```

- رت وي ب م ك با س ح و ا م د خ ت س م ب ل ع ف ل ا ب ن ر ت ق م SPN ة ل ا ز ا / ف ذ ح :

< User/Computer account > < SPN > setSPN -d : ع غ ي ص ل ا

س ا ب س ل ل ا م ل ا ل ا ل ا : setSPN -d http/proxyha.localdomain pod1234-wsa0

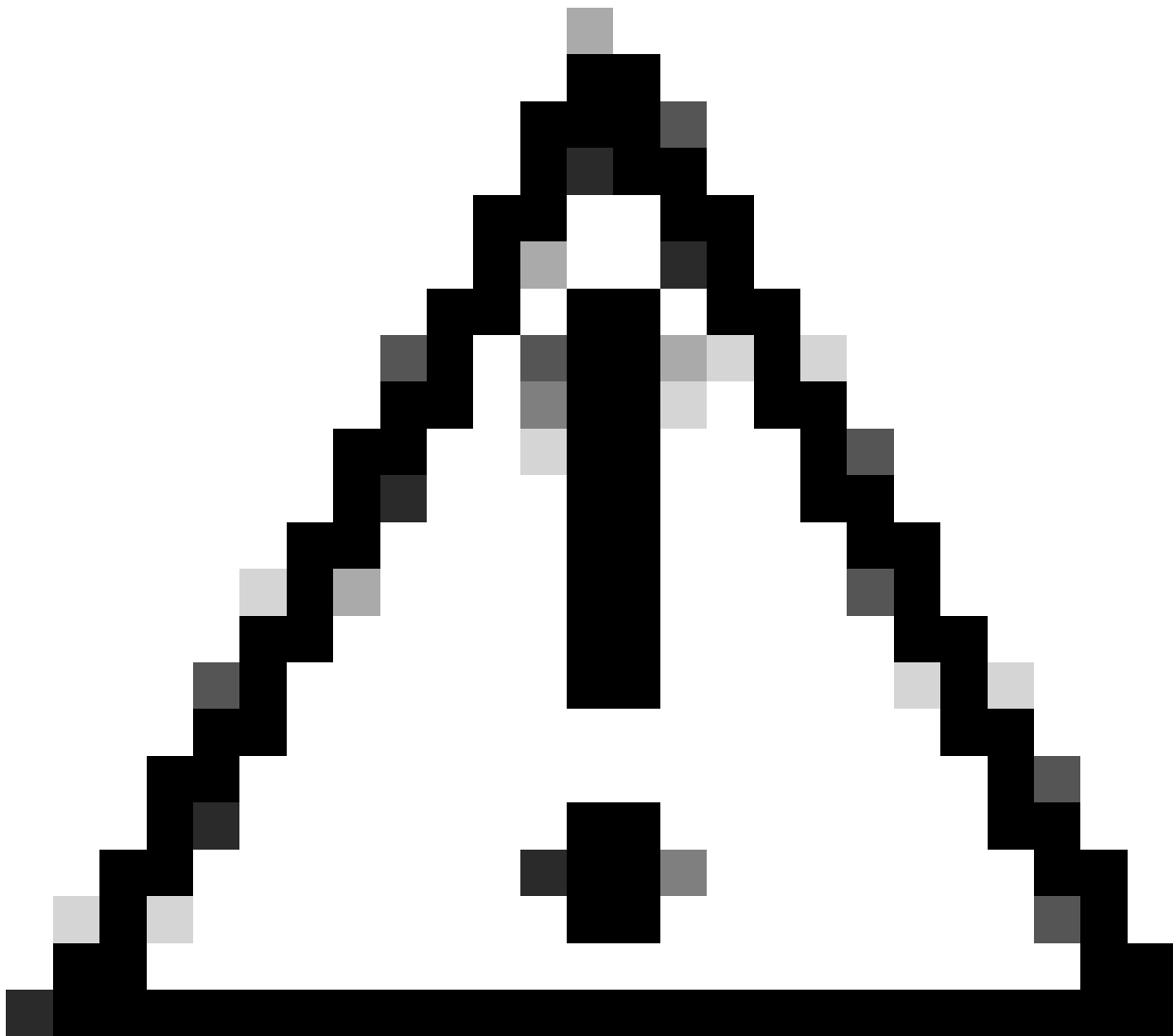
```
Administrator: Command Prompt
C:\Users\Administrator.DC2MAIN>setspn -d http/proxyha.localdomain pod1234-wsa02
Unregistering ServicePrincipalNames for CN=POD1234-WSA02,CN=Computers,DC=ad2012main,DC=samba4integration
http/proxyha.localdomain
Updated object
```

تالاح ث د ح ت ن ا ن ك م ي ث ي ح ، HA ي ر ه ا ظ ل ا ف ي ض م ل ا م س ا ل ة ر ر ك م SPN ت ا ك ب ش د و ج و م د ع ن م د ك ا ت ا ق ح ا ل ل ش ف ل ا .

- -x ن ي ب س ت ي س : م ا د خ ت س ا ل ر م ا

Kerberos ة ق د ا ص م ل ش ف ت و ، ل ي م ع ل ل Kerberos ة م د خ ة ر ك ذ ت ر ي ف و ت م ت ي ا ل ، ك ل ذ ل ع ج ي ت ن و .

```
C:\Users\Administrator.DC2MAIN>setspn -x  
Checking domain DC=ad2012main,DC=samba4integration  
Processing entry 0  
found 0 group of duplicate SPNs.
```



setSPN -d. رمأل مادختساب تاراركتال ةلازا ءاجرلا ،تاراركت ىلع روثعلال مت اذإ :ريذخت

- باسحب ةنرتقمال SPNs ةفاك درس :

الغىصلال : setSPN -l <User/Computer account>

الاثملال لىبس ىلع : setSPN -l vrpServiceUser


```

Administrator: Command Prompt
C:\Users\Administrator.DC2MAIN>setspn -l pod1234-usa07
Registered ServicePrincipalNames for CN=POD1234-USA07,CN=Computers,DC=ad2012main,DC=samba4integration:
HTTP/POD1234-USA07.LOCALDOMAIN.AD2012MAIN.SAMBA4INTEGRATION
HTTP/POD1234-USA07.AD2012MAIN.SAMBA4INTEGRATION
HTTP/pod1234-usa07.localdomain
HOST/pod1234-usa07.localdomain
HTTP/POD1234-USA07
HOST/POD1234-USA07

C:\Users\Administrator.DC2MAIN>setspn -l vrrpserviceuser
Registered ServicePrincipalNames for CN=vrrpserviceuser,CN=Users,DC=ad2012main,DC=samba4integration:
http/proxyha.localdomain

```

SWA لي ع احوال ص او Kerberos ع اطاخ فاشكت سا

احوال ص او Kerberos ع قداصم ع اطاخ فاشكت سا دن Cisco م عد تامول عم لي ع لوصحل مزلي

- لي لحوال ني وكتل لي صافت.
- (ع بتتال و اطاخ ال احي حصت عضو في نوكت ن ا لض في) ع قداصم ال تالجس.
- (ةب سانم ال افي صتال لم اوع عم) اهذي فننت مت ي تال مزحل طاق تال

لي م عمل زاهج (أ)

ةلماشل افي ع اطاق ال جهنل (ب)

- ةي لآ اذه ضرعي نأ بجي .m٪ ص صخم ال قيس ننتال ددحم ني كمت عم تالجس ال ال لوصول ا.
- ةني عم ةلماعمل اهم ادختسا مت ي تال ع قداصم ال
- ال ا ص صخم ال لوقحل هذه فضا، ةي لي صفتال ع قداصم ال لي صافت لي ع لوصحل ل نم دي زم لي ع لوصحل ل ني لماعل ريغ/ني لماعل ال ءال كول لي ع ةدوجوم ال لوصول تالجس [Access. تالجس في ةم ل عمل فيضي يذلا](#) ي بعش تال طاب ترال ال عجرا و ا تامول عمل
- > كارتشال لي جست > ماظنل ةرادا لي ل قنتا، SWA ةي موسرل م دختس م ال ةهجاو في ة قداصم ال لكاشم ل ءلس لس ال هذه ةفاض > ة ص صخم لوقح > لوصول تالجس

server IP address = %k, Client IP address= %a, Auth-Mech = %m, Auth_Type= %m, Auth_group= %g, Authentication

a;

- م دختس م ال ع قداصم لي صافتل SWA لوصول لجس.
- قيس ننت في اهت قداصم تمت ي تال ني م دختس م ال عامس اب Cisco نم SWA تالجس `username@authentication_realm` لاجم ال

Sample Authentication SWA Access log

```
17 [REDACTED] IP_MISS/200 39 CONNECT tunnel://www.cisco.com/
[Cisco\ADUsername@ADRealm] DIRECT/www.cisco.com. - OTHER-NONE-DefaultGroup-
DefaultGroup-NONE-NONE-DefaultGroup-NONE

<"IW_comp",3.0.0,"-",0.0.0.1,"-",,-,-,-,"0.0.0.0","-",,-,-,"IW_comp","Unknown","Computers and
Internet","-",,"Unknown","Unknown","-",,-,-,184.50.0,-,"Unknown","-",0,"-",0.0,"71",4,-,-,-,-> - - Request
Details: = 153450, User Agent = "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36 Edg/122.0.0.0" AD Group Memberships = (
Kerberos) - ] [ Tx Wait Times (in ms): 1st byte to server = 0, Request Header = 0, Request to Server =
0, 1st byte to client = 281, Response Header = 0, Client Body = 0 ] [ Rx Wait Times (in ms): 1st request
byte = 0, Request Header = 0, Client Body = 0, 1st response byte = 16, Response header = 0, Server
response = 2, Disk Cache = 0; Auth response = 0, Auth total = 0; DNS response = 0, DNS total = 0,
WBR5 response = 0, WBR5 total = 2, AVC response = 0, AVC total = 0, DCA response = 0, DCA total
= 0, McAfee response = 0, McAfee total = 0, Sophos response = 0, Sophos total = 15, Webroot
response = 0, Webroot total = 1, Anti-Spyware response = 0, Anti-Spyware total = 1, server IP address
= 1; [REDACTED] Auth-Mech
= Kerberos, Auth_Type= Kerberos, Auth_group= -, Authenticated_Username= 'Cisco\ADUsername'
Date= "19/Mar/2025:13:50:22 +1100", transaction_ID= 153450, Local Time = "19/Mar/2025:13:50:22
+1100", Latency = 298, amp-verdict = 0, amp-malware-name = -, amp-score = 0, amp-upload = 0,
amp-filename = , amp-sha = , p2p-amp-svc-time = 279, p2p-amp-wait-time = 0;
```

- (GUI) ةي م و س ر ل ا م د خ ت س م ل ا ه ج ا و ن م ر ا ب ت خ ا ل ا ة ق د ا ص م ل ا ج م ت ا د ا د ع ل ا ل ي غ ش ت ب م ق ر ا ب ت خ ا م س ق ي ف ك ب ص ا خ ا ل ل ا ج م ل م س ا ي ل ع ر ق ن ا م ث ، ة ق د ا ص م ل ا > ة ك ب ش ل ا ي ل ل ق ت ن ا ر ا ب ت خ ا ل ا ة ب ي ل ع ر ق ن ا . ة ي ل ا خ ا ل ت ا د ا د ع ل ا

Kerberos تاناي ب ة د ع ا ق ي ف م د ا خ ا ل ي ل ع ر و ث ع ل م ت ي م ل

ة د ع ا ق ي ف م د ا خ ا ل ي ل ع ر و ث ع ل م ت ي م ل " ع م ب ي و ل ا ت ا ب ل ط ل ش ف ي ه ة ع ئ ا ش ل ا ا ط خ ل ا ت ا ل ا ح ي د ج ا ب Kerberos تاناي ب :

```
curl -vx proxyha.local:3128 --proxy-negotiate -u: http://www.cisco.com/
* About to connect() to proxy proxyha.localdomain port 3128 (#0)
* Connected to proxyha.local (10.8.96.30) port 3128 (#0)
< HTTP/1.1 407 Proxy Authentication Required
< Via: 1.1 pod1234-wsa02.local:80 (Cisco-SWA/10.1.2-003)
< Content-Type: text/html
gss_init_sec_context() failed: : Server not found in Kerberos database
< Proxy-Authenticate: Negotiate
< Connection: close
* HTTP/1.1 proxy connection set close!
```

ل ي ك و ل ا ن ا و ن ع ة م ي ق ل ل ب ا ق م ل ا ي س ا س ا ل ا ة م د خ ل ا م س ا ن ا ي ل ا ا ط خ ل ا ر ي ش ي ، ة ل ا خ ل ا ه ذ ه ي ف ن م د ك ا ت ل ا ي ر و ر ض ل ا ن م ، ة ل ك ش م ل ا ل ح ل . Active Directory م د ا خ ي ل ع ل ج س م ر ي غ proxy proxy.local ب س ا ن م ة م د خ ب ا س ح ي ل ا ه ت ف ا ض ا و AD DC ي ل ع http/proxyha.local ل ي ج س ت

ةي فاضا عجارم و تامول عم

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 چ 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 ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط 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 چ 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 چ 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 چ 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