

ةدحو فاشتك ةيلمع ءاطخأ فاشكتسأ فاشتك ةيلمع؛ ؛ Cisco ISE لاجملاب مكحتلا ةمدخ ىلإ مامضنالا ءانثأ لاجملاب مكحتلا ةدحو Active Directory

تايوتحمل

ةلأسم

لشفو (DCs) لاجملاب يف مكحتلا تادحو فاشتك Cisco (ISE) ةيوهلا تامدخ كرحم ىلع رذعتي
ISE Active Directory (AD) ةمدخ ىلإ مامضنالا

ةئيبل

- ثدحلأ تارادصلإاو 3.x رادصلإ - Cisco (ISE) نم ةيوهلا تامدخ كرحم
- ىلعأو 2016 - Microsoft Active Directory (AD)
- 53 UDP/TCP - DNS) لاجملاب مسامظن
- مت اذا 636 TCP لوكتورب؛ 389 TCP - LDAP) ليلدلل لوصولل فيفخلال لوكتوربال
(LDAPs) نمآال LDAP لوكتورب مادختسإ
- 389 UDP - لصتمال ريغ (CLDAP) ليلدلل لوصولل فيفخلال لوكتوربال

رارق

ديحتل ةددعتم ريياعم مدختسيو، AD ىلإ مامضنالا ةيلمع ءانثأ Cisco ISE DCs فشتك
هرايتخإ متيس يذال DC

DNS: فاشتك

- تاجولات كلالا ةرفوت مل DCs فاشتكال DNS (SRV) ةمدخ لجس تامالعتسا ISE مدختسي تادحو ةمئاق عاجراب DNS مداخل موقى (KDCs) حيتافملا عيزوت زكرم (GCs) ةمومعلا ةرفوت مل KDCs و GC و DC لاجملاب مكحتلا
- غالبالا او AD لىل مامضنالا ةيلمع ةعباتم هنكمي الف ، تامولعمل هذه ISE ملتسي مل اذا DNS. ب قلعتم أطخ نع
- : مداخلتساب AD SRV تالجس نم ققحت ، ISE (CLI) رماوا رطس ةهجاو نم

nslookup

- لاثم

```
nslookup 1dap.tcp.example.com querytype SRV
```

```
nslookup kerberos.tcp.example.com querytype SRV
```

```
nslookup 1dap.tcp.dc._msdcs.example.com querytype SRV
```

- فيضم مسا نأ نم ققحت مث . ءحلاص DC تافيفضم ءامسا تامالعتسال عجرت نأ بجي : ءحصل IP ناو نع لىل هلح مت دق هعاجرا مت يذل DC

```
nslookup dc01.example.com
```

- مداوخل ةمئاق نيوكتل ليغشتب موقى يذل ISE يف هنيوكت مت يذل DNS مداخل عجري ةرفوت مل
- رمالا اذه ليغشت لالخن نم كيذل DNS ISE مداخل نيوكت نم ققحت

```
show running-config
```

```

mysoreas36san/admin#show running-config
interface GigabitEthernet 0
 ip address [REDACTED] 255.255.255.0
 ipv6 enable
 ipv6 address autoconfig
 !
 ntp server [REDACTED]
 repository local
 url disk: /
 !
 hostname mysoreas36san
 icmp echo on
 ip domain-name mysoreas36san.iselab.local
 ip default-gateway [REDACTED]
 ip name-server [REDACTED]
 ipv6 enable
 logging loglevel 6

```

- وأ AD إلى مامضنالا ذيفنت ءانثأ ISE إلى ع ةمزل طاقنل مدختسأ ، CLDAP ل ةبس نلاب بسانملا AD صيخشنت ليعشت
- نم ققحتلاو DC و ISE نيبتانايبال رورم ةكرح طاقنل ، لاثملا ليعبس إلى ع

ISE → DC01 : UDP/389 CLDAP Request
DC01 → ISE : UDP/389 CLDAP Response

- ماق اذإ .اهي إلى لوصولو نكمي (DC) لوصولو ي ف مكحت ةدحولك نم ةباجتسالو يقلت بجي رادج دعاوق نم ققحت ف ، ةباجتسإ يأ يقلت ي ال هنكلو CLDAP بلط لاسراب ISE DC و ISE نيبت UDP 389 لاصتاو هيحوتلاو لوصولو ي ف مكحتلا ةمئاق/ةيامحل

عقوملا فيرعت

- هليضفتو Active Directory عقوم س فن ي ف DCs ديحتل CLDAP تامولعم ISE مدختسي نكمأ ام لك
- نأ نم اضيأ ققحت .حيحصلال AD عقوم إلى يمتنت ISE ةيعرفلا ةكبشلا نأ نم ققحت AD عقوم س فن إلى يمتنت ةعقوتملا DCs

لاصتالا ةبقارم

- DC. لاجملاب مكحتال دحو رفوت ةبقارمل يرود لكشب ISE CLDAP مدختسي
- نيب ةخأتمل CLDAP تاباجتسا وأ ةمزحل نادقف وأ عطقتمل UDP 389 لاصتا نم ققحت مزحل طاقتال مادختساب DCs و ISE
- مدع ةلاح يف .ريذحت عاشناب ةيئات 2.5 نم رثكأ قرغتست يتل CLDAP ةباجتسا موقت AD. مامضنا لشفي ،(DC) لوصولا يف مكحتال دحو ةباجتسا

ببسل

- DC. فاشتكا ISE ىلع رذعتي
- .ةبولطمل AD تالچس عاجراب DNS موقي ال
- .ةفشتكمال DC تادحو ىل لوصولا ISE ىلع رذعتي
- .CLDAP تابلطل (DC) لاجملاب مكحتال تادحو بيچتست ال
- .حيحص ريغ AD عقوم نييعتب ISE ةيعرفال ةكبشل موقت
- .LDAP لاصتا ددحمل DC لبق ي ال

ةلصلال يذىوتحمل

- [Active Directory لم اكاك لي لدو \(ISE\) Identity Service Engine](#)
- [Cisco نم تاليزنتال او ينفال معدل](#)

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