

Active Directory (AD) و Identity Service Engine (ISE) مهف

تايتوت حمل

[عمدق مل](#)

[ةيساس أال تابلط مل](#)

[تابلط مل](#)

[عمدختس مل تانوك مل](#)

[AD تالوك وتورب](#)

[Kerberos لوك وتورب](#)

[MS-RPC لوك وتورب](#)

[Active Directory \(AD\) عمدخ عم ISE جم د](#)

[AD لى ل ISE مامض نا](#)

[AD لاجم لى ل مامض نا ل](#)

[AD لاجم كرت](#)

[رمتس مل رايت ل لش ف زواجت](#)

[LDAP لال خ نم ISE-AD لاصتا](#)

[AD: قفدت ل باقم مدختس مل ع قداصم](#)

[ISE شح بة يفصت لم اوع](#)

عمدق مل

Identity Service Engine (ISE) و Active Directory (AD) لاصتا ة يفك دن تس مل اذه حضوي، تاقفدت ل او، AD ة يفصت لم اوع و، عمدختس مل تالوك وتورب ل او.

ةيساس أال تابلط مل

تابلط مل

: بة يساس أة ف رعم Cisco دي عتست

- Active Directory و ISE 2.x جم د .
- ISE لى عة ج راخ ال ة يوه ل ع قداصم .

عمدختس مل تانوك مل

- ISE 2.x .
- Windows (Active Directory) م داخ .

ةصاخ ة لم عم ة ئب ب يف ة دوجوم ل ة زه أال نم دن تس مل اذه يف ة دراو ل تامول عم ل عاشن ا مت تنك اذ ا . (يفضارت ف ا) حوسمم ن يوك تب دن تس مل اذه يف عمدختس مل ة زه أال ع يمج ت ا ب رم ا يال لم تح مل ري ثا تل ل كم هف نم دك ا ت ف ، لي غ ش ت ل دي ق ك ت ك ب ش .

AD تالوكوتورب

Kerberos لوكوتورب

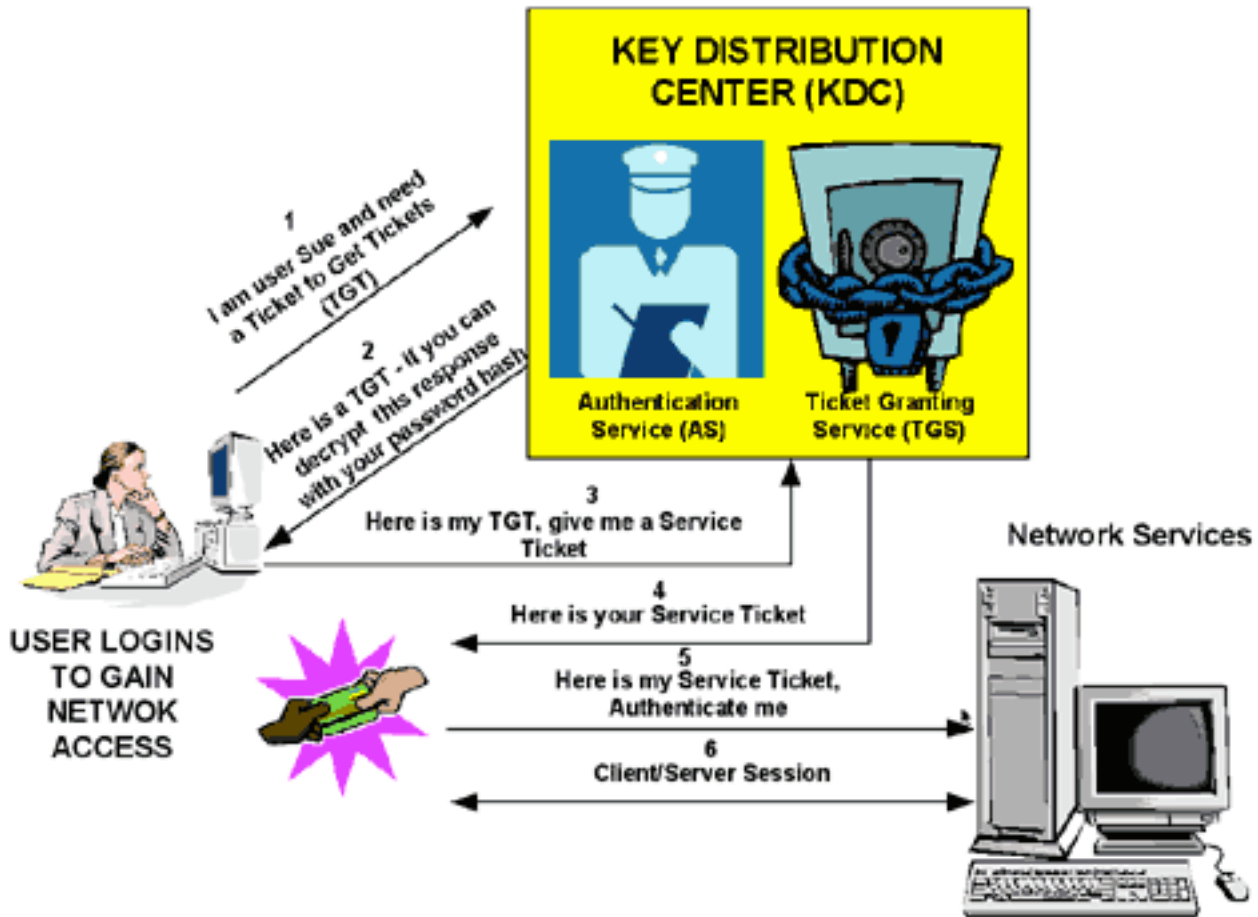
مداخل او ليمعمل مدختسمو (KDC) حيتافملا عيزوت زكرم نم ةثالثال Kerberos سوور فلأتت هيل لوصولا بجي يذلا.

ممدخ: تامدخلل نيئف يظو يدوتو (DC) لاجملاب مكحتلال ةدحو نم عزك KDC تيبتت متي (TGS) ركاذتلال حنم ةمدخو (AS) ةقداصملا.

ممدخ دروم يلا ةيادبلا يف لوصولاب ليمعمل موقوي امندنع لدابت تاي لمع ثالث نيئمضت متي:

1. ليديبك.
2. لدابت TGS.
3. ممدخال/ليمعمل لدابت (CS).

KERBEROS TICKET EXCHANGE



- KDC (AS + TGS) = لاجملاب مكحتلال ةدحو.
- ك.ب ةصاخلا رورملا ةملك مادختساب (SSO لخدم) AS يلا ةقداصم.
- (ةسلج طابترا فيرعت فلم) (TGT) حنم ةركذت يلع لوصولال.
- (SRV01) ةمدخ يلا لوخذلا ليحست بلط.
- KDC يلا كهيجوت ةداعاب SRV01 موقوي.
- (لعفلا ب هيلع قداصم انأ) - KDC يلا TGT راهظا.
- SRV01 ل KDC TGS ةكرش كل مدقت.

- SRV01 ىل هيجوتلا ةداعإب مق .
- SRV01 ىل ةمدخلا ةركذت راهظإ .
- اهب قوئولا وأ ةمدخلا ةركذت نم ققحتلاب SRV01 موقى .
- ب ةصاخلا تامولعملا عيمج ىل عيوتحت ةمدخلا ةقاطب .
- ىل وخذ ليجستب SRV01 موقى .

نأشب ضوافتلا نيمدختسملا ىل عيجي ، ةكبش ىل ةيادبلا ىف لوخدلا ليجست دنع KDC نم AS عزج ةطساوب هنم ققحتلل رورملا ةملاك و لوخدلا ليجست مساري فوتو لوصولا مهلاجم لخاد .

، هتقداصم درجمبو . Active Directory مدختسم باسح تامولعم ىل لوصولا ةيناكمإ KDC ىدل ىل حملا لاجملا ةحلاص (TGT) حنم ةركذت مدختسملا حنم متي .

مدختسملا لوخد ليجست لمع ةسلج لالخ هديجت متي و تااعاس 10 ىضارتفالا TGT رمع غلبى . هب ةصاخلا رورملا ةملاك لالخدا ةداعإ ىل ةحاحلا نوب .

بلطل همدختسإ متي و ةرياطتم ةركاذ ةحاسم ىف ىل حملا زاهجلا ىل عاتقؤم TGT نيزخت متي . ةكبشلا ربع تامدخال عم لمعلا تاسلج .

مدخال ةمدخ ىل لوصولا ىل ةحاحلا دنع KDC نم TGS عزج ىل TGT مدختسملا مدقى .

لمع ةسلج حاتفم و ةركذت عاشنإ و مدختسملا TGT ةقداصمب KDC ىل ع دوجوملا TGS موقى . اتقؤم (ةمدخلا ةقاطب) تامولعملا هذه نيزخت كلذ دعب متي . ديعلل مداخل او لىمعل نم لكل لىمعل زاهج ىل اىلحم .

متي ، لىمعل بلط ىل ع TGS قفاو اذإ . صاخلا هحاتفمب هأرقى و TGT لىمعل TGS ىقلتي . فدهلا مداخل او لىمعل نم لكل ةمدخ ةركذت عاشنإ .

AS در نم اقبس م هادرتسإ مت ىذل TGS ةسلج حاتفم عم هبىصن لىمعل أرقى .

لدابت ةلىممع ىف فدهلا مداخل ىل ع TGS درب صاخلا مداخل عزج مديقتب لىمعل موقى . ةيلالات مداخل/لىمعل .

لالم:

Test User Authentication

* Username

* Password

Authentication Type

Authorization Data Retrieve Groups
 Retrieve Attributes

Authentication Result	Groups	Attributes
<pre> Authentication time : 57 ms. Groups fetching time : 18 ms. Attributes fetching time : 4 ms. Processing Steps: 14:05:37:440: Resolving identity - user1 14:05:37:440: Search for matching accounts at join point - ralmaait.com 14:05:37:449: Single matching account found in forest - ralmaait.com 14:05:37:449: Identity resolution detected single matching account 14:05:37:476: Authentication Ticket (TGT) request succeeded - user1@ralmaait.com 14:05:37:478: Service Ticket request succeeded - user1@ralmaait.com 14:05:37:486: Service Ticket validation succeeded - user1@ralmaait.com 14:05:37:486: Account validation succeeded </pre>		

هتقد اصم مت مدختسمل ISE نم مزلح طاقالت:

111	2020-01-13 16:17:53.082713	10.48.60.50	10.48.60.51	TCP	66 53610 → 88 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=105462807 TSecr=280789807 ✓
112	2020-01-13 16:17:53.082735	10.48.60.50	10.48.60.51	KRB5	346 AS-REQ ✓
113	2020-01-13 16:17:53.083625	10.48.60.51	10.48.60.50	KRB5	1576 AS-REP ✓
114	2020-01-13 16:17:53.083649	10.48.60.50	10.48.60.51	TCP	66 53610 → 88 [ACK] Seq=281 Ack=1511 Win=32256 Len=0 TSval=105462808 TSecr=2807... ✓
115	2020-01-13 16:17:53.083678	10.48.60.50	10.48.60.51	TCP	66 53610 → 88 [FIN, ACK] Seq=281 Ack=1511 Win=32256 Len=0 TSval=105462808 TSecr... ✓
116	2020-01-13 16:17:53.083908	10.48.60.51	10.48.60.50	TCP	66 88 → 53610 [ACK] Seq=1511 Ack=282 Win=532726 Len=0 TSval=280789809 TSecr=105... ✓
117	2020-01-13 16:17:53.084022	10.48.60.51	10.48.60.50	TCP	60 88 → 53610 [RST, ACK] Seq=1511 Ack=282 Win=0 Len=0 ✓
118	2020-01-13 16:17:53.084449	10.48.60.50	10.48.60.51	KRB5	1480 TGS-REQ ✓
119	2020-01-13 16:17:53.085475	10.48.60.51	10.48.60.50	KRB5	1446 TGS-REP ✓
120	2020-01-13 16:17:53.110397	10.48.60.50	10.48.60.51	TCP	66 48959 → 3268 [ACK] Seq=1700 Ack=536 Win=31360 Len=0 TSval=105462835 TSecr=28... ✓

TGT رفوت AS م د خ ن ا ف ، ع ح ي ح ص رورم ال م ل ك ت ن ا ك ا ذ ا . م د خ ت س م ل م س ا ي ل ع AS-REQ ي و ت ح ت ل و ص ح ل ل TGT م د خ ل TGT ر ي ف و ت م ت ي ك ل ذ د ع ب و . م د خ ت س م ل رورم م ل ك م ا د خ ت س ا ب ا ر ف ش م ل م ع س ل ج ع ر ك ذ ت ي ل ع .

.. ل م ع س ل ج ع ر ك ذ ت م ا ل ت س ا د ن ع ع ح ج ا ن ع ق د ا ص م ل ن و ك ت .

ة : ئ ط ا خ ل ي م ع ل ا ن م م د ق م ل رورم ال م ل ك ت ي ح ل ا ث م ا ذ ه

117	2020-01-14 08:51:03.846603	10.48.60.50	10.48.60.51	KRB5	318 AS-REQ
118	2020-01-14 08:51:03.848340	10.48.60.51	10.48.60.50	KRB5	194 KRB Error: KRB5KDC_ERR_PREAUTH_FAILED

TGT: ي ق ل ت م ت ي ا ل و AS ب ل ط ل ش ف ي ، ع ح ي ح ص ر ي غ رورم ال م ل ك ت ن ا ك ا ذ ا

Processing Steps:					
13:19:55:837:	Resolving Identity - User1				
13:19:55:837:	Search For Matching Accounts At Join Point - Ralmaait.com				
13:19:55:843:	Single Matching Account Found In Forest - Ralmaait.com				
13:19:55:843:	Identity Resolution Detected Single Matching Account				
13:19:55:856:	Authentication Ticket (TGT) Request Failed - User1@ralmaait.com, ERROR_PASSWORD_MISMATCH				

ة : ح ي ح ص ر ي غ رورم ال م ل ك ت ن و ك ت ا م د ن ع ad_agent.log ف ل م ي ل ل و خ د ل ا ل ي ح س ت ب م ق

2020-01-14 13:36:05.442 إلى (تاياب 276) لسرم بلط ، 140574072981248.krb5:ءاطخألأحيحصت RALMAIT.COM،LwKrb5TraceCallback(),lwadvapi/threaded/lwkrb5.c:1325

2020-01-14 13:36:05.444 DEBUG، 140574072981248.krb5: نم أطيقلت مت - 1765328360/Preauthentication failed، LwKrb5TraceCallback(),lwadvapi/threaded/lwkrb5.c:1325

2020-01-14 13:36:05.444 ةلواحمال ةداعإتالخدإعاونأ ، 140574072981248.krb5:ءاطخألأحيحصت ةقبااسللا: 16، 14، 19، 2،LwKrb5TraceCallback(),lwadvapi/threaded/lwkrb5.c:1325

2020-01-14 13:36:05.444 ريذحت ، 140574072981248.[LwKrb5GetTgtImpl/lwadvapi/threaded/krbtgt.c:329] أطيخلالزمر KRB5: -1765328360 (ةلاسرا) ةقداصملا لشف (ةقبااسملا)، LwTranslateKrb5Error(),lwadvapi/threaded/lwkrb5.c:892

2020-01-14 13:36:05.444 ءاطخألأحيحصت ، 140574072981248.[LwKrb5InitializeUserLoginCredentials()] أطيخلالزمر (زمرلا): 40022 (LW_ERROR_PASSWORD_MISMATCH).LwKrb5InitializeUserLoginCredentials(),lwadvapi/threaded/lwkrb5.c:1453

MS-RPC لوكوتورب

ةلصفنم ةسلج بلطتتالو ةقداصملا SMB رفوتو SMB ربع ISE MS-RPC مدختسي "سمسالتانايبالررم" سمستةيلا مدختسيوهو. ةنيعم RPC ةمدخ عقوم يلع روثعلل مدخالاوليמעلا نيبلالصتال

- SMB لمع ةسلج لاصتاءاشنإ
- لقنك 445 ذفنم SMB/CIFS.TCP ربع RPC لئاسرلقن
- ةقداصم جلاعتو هليغشتب ةنيعم RPC ةمدخ موقت يذلا ذفنملا SMB لمع ةسلج ددحت مدختسملا
- تايلمعلا نيبلالصتاللةي فخملا ةكراشم لل IPC\$ بل لاصتالا
- ةبولطملا RPC ةفيظو/درومل بسانم يمسم تانايبالررم حتف

SMB ربع RPC لدابت

No.	Time	Source	Destination	Protocol	Length	Info	Text Item
59	2020-01-14 14:56:01.082699	10.48.60.50	10.48.60.51	SMB	128	Negotiate Protocol Request	✓
60	2020-01-14 14:56:01.083241	10.48.60.51	10.48.60.50	SMB2	318	Negotiate Protocol Response	✓
61	2020-01-14 14:56:01.083255	10.48.60.50	10.48.60.51	TCP	66	26963 → 445 [ACK] Seq=63 Ack=253 Win=30336 Len=0 TSval=186950807 TSecr=36227...	✓
72	2020-01-14 14:56:01.086109	10.48.60.50	10.48.60.51	SMB2	1589	Session Setup Request	✓
73	2020-01-14 14:56:01.086341	10.48.60.51	10.48.60.50	TCP	66	445 → 26963 [ACK] Seq=253 Ack=1586 Win=66560 Len=0 TSval=362277347 TSecr=186...	✓
74	2020-01-14 14:56:01.087051	10.48.60.51	10.48.60.50	SMB2	328	Session Setup Response	✓
75	2020-01-14 14:56:01.087268	10.48.60.50	10.48.60.51	SMB2	212	Tree Connect Request Tree: \\WIN-E051AB1Q9BK.ralmaait.com\IPC\$	✓
76	2020-01-14 14:56:01.087592	10.48.60.51	10.48.60.50	SMB2	150	Tree Connect Response	✓
77	2020-01-14 14:56:01.087721	10.48.60.50	10.48.60.51	SMB2	206	Create Request File: netlogon	✓
78	2020-01-14 14:56:01.088023	10.48.60.51	10.48.60.50	SMB2	222	Create Response File: netlogon	✓
79	2020-01-14 14:56:01.088207	10.48.60.50	10.48.60.51	DCERPC	314	Bind: call_id: 9, Fragment: Single, 1 context items: RPC_NETLOGON V1.0 (32bi...	✓
80	2020-01-14 14:56:01.088500	10.48.60.51	10.48.60.50	SMB2	150	Write Response	✓
81	2020-01-14 14:56:01.088665	10.48.60.50	10.48.60.51	SMB2	183	Read Request Len:8192 Off:0 File: netlogon	✓
82	2020-01-14 14:56:01.088899	10.48.60.51	10.48.60.50	DCERPC	230	Bind ack: call_id: 9, Fragment: Single, max_xmit: 4280 max_rcv: 4280, 1 res...	✓
83	2020-01-14 14:56:01.089118	10.48.60.50	10.48.60.51	RPC_NETLOGON	574	NetrLogonSamLogonEx request	✓
84	2020-01-14 14:56:01.089373	10.48.60.51	10.48.60.50	SMB2	150	Write Response	✓
85	2020-01-14 14:56:01.089517	10.48.60.50	10.48.60.51	SMB2	183	Read Request Len:8192 Off:0 File: netlogon	✓
86	2020-01-14 14:56:01.090160	10.48.60.51	10.48.60.50	RPC_NETLOGON	608	NetrLogonSamLogonEx response	✓
88	2020-01-14 14:56:01.129364	10.48.60.50	10.48.60.51	TCP	66	26963 → 445 [ACK] Seq=2862 Ack=1635 Win=34688 Len=0 TSval=186950854 TSecr=36...	✓
145	2020-01-14 14:56:09.910387	10.48.60.50	10.48.60.51	RPC_NETLOGON	574	NetrLogonSamLogonEx request	✓
146	2020-01-14 14:56:09.910714	10.48.60.51	10.48.60.50	SMB2	140	Write Response	✓

```
> Secure Channel Verifier
Microsoft Network Logon, NetrLogonSamLogonEx
Operation: NetrLogonSamLogonEx (39)
[Response in frame: 86]
LogonServer: \\WIN-E051AB1Q9BK.ralmaait.com
Referent ID: 0x00000001
Max Count: 31
Offset: 0
Actual Count: 31
Computer Name: \\WIN-E051AB1Q9BK.ralmaait.com
Computer Name: ISERIRI24
Referent ID: 0x00000001
Max Count: 10
Offset: 0
Actual Count: 10
Computer Name: ISERIRI24
Level: 2
LEVEL: LogonLevel
Level: 2
NETWORK_INFO:
Referent ID: 0x00000001
IDENTITY_INFO: user@ralmaait.com
Challenge: cdc343b187f9b4e1
```

ةريغصلا تاكرشلا ةجهل ىلع رطسلا ضوافت negotiate protocol request/response رمألا ضرعي ةقداصملا يرحي session setup request/response رمألا ضرعي. ةطسوتملاو

ةصاخ ةكراشمب لصتم تنأ .بولطملا دروملاب ةباجتسالاو ةرجشلا لاصتا بولط لاصتا IPC\$.

ةفيضملا ةزهجالا نيب لاصتالا لئاسو تايلمعل نيب لاصتالا يف ةكراشملا هذه رفوتو MSRPC فئاظول لقن ةلپسوك كلذكو

اذه يف Netlogon ةمدخ) ةلصتمةمدخل مسا وه فلملا مسا او Create Request File وه 77 ةمزحلا يف (لثملا).

مسا لاسراب هيف موقت يذلا ناكلما وه NetlogonSamLogonEX بولط نوكي، 86 و 83 مزحلا يف network_info لقحلا يف AD لىل ISE لىل ةقداصملا ةمدختسملا

جئاتنلا عم درلاب NetlogonSamLogonEX ةباجتسال ةمزح موقت

NetlogonSamLogonEX ةباجتسال تامالعل ميق ضعب
0xc00006a status_wrong_password
0x000000 وه status_success
0x0000103 وه status_pending

Active Directory (AD) ةمدخ عم ISE جم د

ةيلمع ءانثأ نالعالاب لاصتالا MSRPC و KRB و LDAP لوكوتورب ISE مدختسي ةقداصملاو ةرداغملا/مامضنالا

ب لاصتالا ةمدختسملا تايلاالاو شحبلا قيسنتو تالوكوتوربلا ةيلالاتلا ماسقألا رفوت اذه DC لباقم مدختسملا ةقداصملاو AD يف ددح DC

يف ISE لشفي، بابسألا نم ببس يأل (DC) لاجملا ب مكحتلا ةدحو لاصتا مدع ةلاح يفو ةقداصملا ةيلمع رثأتت الو ةحاتملا ةيلالاتلا (DC) لاجملا ب مكحتلا ةدحو لىل لوصول

تانئاك ةفاك نم خسن نيزختب موقت لاجملا ب مكحت ةدحو وه (GC) يمومعل جولاتكلا مداخ ةباغلا يف Active Directory

نم تانئاكل لك نم ةيئزج ةخسنو لاجم ليلد يف تانئاكل لك نم ةلماك ةخسن نيزخي وهو ىرخألا تاباغل تالاجم لك

يا يف تانئاكل لىل روثعل تاقببطللاو نيمدختسملا يمومعل جولاتكلا حيتي، لياتلابو GC يف ةنمضم تامس نع شحبلا عم ةيلالاتلا ةباغلا تالاجم نم لاجم

يف ةباغ نئاكل لك تامسلا نم (ةلماك ريغ) ةيساسأ ةومجم لىل يمومعل جولاتكلا يوتحي (PAT، ةيئزج تامس ةومجم) لاجم لك

ةمدخل مادختساب اهخسن متي. ةباغلا يف لاجملا ليلد ماسقألا لك نم تانئاب GC لىل قىلتي AD مادختساب لثامتملا خسنلل ةيسايقل

AD إلى ISE مامضنا

ISE و Active Directory لمكتلة أساسيات تابلطتم

1. ISE يف ريديم ماطن وأ ريديم ربوس نم زايتمما يقلتني تنأ نأ تققد.
2. عم دخو Cisco مداخل نيبتقولا نمامزمل (NTP) ةكبشلال تقولوكوتورب مداخل تاداعإ مدختسأ قئاقد 5 وه AD و ISE نيبت هب حومسمل تقولا قرفل يصقأل دحل Active Directory.
3. SRV تامالعتسا يلع درلا يلع ارداق ISE يلع هنيوكت مت يذلا DNS نوكتي نأ بجي. اهنودب وأ ةيفاضلال عقومل تامولعم عم KDCs و GCs و DCs ب ةصاخلا
4. يأل ةيسكعلاو ةيمامأل DNS تامالعتسا يلع درلا اهنكمي DNS مداوخ ةفاك نأ نم دكأت. Active Directory ل لمحتحم DNS لاجل
5. لوصول نكميوليغشلال ديقلقأل يلع دحاو يمومع جولتكم مداخل AD ل نوكتي نأ بجي. Cisco هيل مضمنت يذلا لاجملا يف، Cisco ةطساوب هيل

AD لاجم إلى مامضنال

لحارم ثالث يف مامضنال لاجم لوح تامولعم يلع لوصحلل لاجملا فاشتك ISE قبطي:

1. تالاجملاو اهتباغ نم تالاجملا—فاشتك—تالاجملا إلى تامالعتسال مامضنال مت. مضمنل لاجملا ايحراخ اهب قووثوملا
2. ةباغل عم ةقثلا سسؤي - هتباغ يف ةيرذل تالاجملا نع ملعتسي.
3. تاباغل نم تالاجملا فاشتك—اهب قووثوملا تاباغل يف ةيرذل تالاجملا تامالعتسا. اهب قووثوملا

UPN تاقحالو، (UPN تاقحال) DNS تالاجم عامسأ Cisco ISE فاشتك، كلذ إلى ةفاضلال و NTLM لاجم عامسأو، ةلديبال

GCs و DC تادحو لوح تامولعملا عيجم يلع لوصحلل DC فاشتك قيبطت ISE موقبي ةرفوتمل.

1. AD يلع زيمتملا لوؤسملاب ةصاخلا لاخدإل دامتعا تانايبب مامضنال ةيلمع أدبت. ةطحالم بجيف، فل تخم ي عرف لاجم وأ لاجم يف ادوجوم ناك اذا. هسفن لاجملا يف ةدوجوملا (username@domain) UPN نيودت يف مدختسملا مسلا دريوتحي مل اذا. KDCs و GCs و DCs تالجمع يمجل DNS مالمالعتسا لاسراب ISE موقبي DNS طبترملا أطخل عم لمكتلا لشفي، هتباغ يف اهنم دحاو يأل يلع DNS
3. CLDAP تابلطلال عم GCs و DCs عيجم فاشتكال CLDAP لاصتا رابتخا ISE مدختسي. ةباجتسا ممدختسا متي. SRV لجم يف اهتايولوا عم قفاوتت يتلوا DCs إلى ةلسرمل لاجملا مكدتلا ةدحو اذهب ISE ليصوت متي مثنمو إلى وال (DC) لاجملا مكدتلا ةدحو DC.

رايتلا هقربغتسي يذلا تقولا وه رشابملا رايتلا ةيولوا باسحل عم مدختسملا لماول دحاو يلع ةيولوا ب يظحت عرسأل ةباجتسالاف؛ CLDAP تاعامتجال ةباجتسالل رشابملا

مكدتلا تادحو عم لاصتا عاشنال ISE اهم مدختسي يتللا ةيألل يه CLDAP: ةطحال مل اذا لشفي. DC ل درلوا يتح ةباجتسال تقوسيقي. هيل طافحلوا DC لاجملا حسم. ةيناث 2.5 نم ربكأ ةباجتسال تقو ناك اذا ربح. رمتسملا رايتلا نم ةباجت حسم متي هنإف، عقوم دوجو مدع ةلاح يف) عقوملا يف DC لاجملا مكدتلا تادحو ةفاك DC عقوم يلع CLDAP ةباجتسا يوتحت. (لاجملا يف DC لاجملا مكدتلا تادحو ةفاك (هيلي ISE زاهج نييعت مت يذلا عقوملا) ليمعلا عقوم)

4. "مدخستسم لىل مامضنال" دامتعا تانايب عم ISE TGT لبقتسي م ث.
5. (SAM و SPN) MSRPC. مادختساب ISE زاغ باسح مسا عاشناب مق.
6. ادوجوم ISE زاغ نكي مل اذا. لعللاب ادوجوم ISE زاغ باسح ناك اذا SPN ةطساوب AD ثح ب. ديذج زاغ عاشناب ISE موقى.
7. لىل لوصولا ةينام نم ققحتلاو، ISE زاغ باسح رورم ةملك نييعتو، زاغلا باسح حتف. ISE زاغ باسح.
8. (هباش امو dnsHostname و SPN) ISE زاغ باسح تامس نييعتب مق.
9. عيمج فشتك او KRB5 مادختساب ISE زاغ دامتعا تانايب مادختساب TGT لىل لصلحا. اهب قووثوملا تالاجملا.
10. اهب ةنرتقملا SIDS و AD تاعومجم شيذحتب ISE ةدقع موقت، مامضنال لامتكا دنعو. AD بناج لىل ةيلعملل هذه لامك ةينام نم ققحت. ايئاقلت SID شيذحت ةيلعملل ادبتو.

AD لاجم كرت

رابتعالا نيعب نالعالا ذخأي نا بجى، ISE رداغى ام دنع

1. باسح ةلازا نم ققحتي اذهو. ةرداغملا تايلعملل ءارجال لمك AD لوؤسم مدخستسم مدختسا. Active Directory تانايب ةدعاق نم ISE زاغ.
2. ايودي هفذح بجى و AD نم ISE باسح ةلازا متي الف، دامتعا تانايب نودب AD كرت مت اذا.
3. خسنلا دعب نيوكتلا ةداعتسا و (CLI) رماوالا رطس ةهجاو نم ISE نيوكت طبض ةداع دنع. نم ISE ةدقع لاصتا عطقى و جورخ ةيلعملل ذي فنن تب موقى هناف، ةيقرتلا و ايطايتحال لاجم نم ISE ةدقع باسح ةلازا متت مل، كذ لعمو. (مامضنال مت اذا). Active Directory لاجم Active Directory.
4. هنأل Active Directory دامتعا تانايب عم لوؤسملا لخدم نم جورخ ةيلعملل ءارجاب ي صوي مسا ريغت دنع كذ ب ي صوي امك. Active Directory لاجم نم ةدقعل باسح اضيأ ليزي ISE فيضم.

رمتسملا رايتلا لشف زواجت

يال هيل لوصولا رذعتي واصلت م ريغ حبصي ISE ب DC لاجملا ب مكحتلا ةدحو لاصتا دنع ليغشت نكمي. ISE لىل ايئاقلت DC لاجملا ب مكحتلا ةدحو لشف زواجت ليغشت متي، ببس ةيلاتلا طورشلا ةطساوب رمتسملا رايتلا لشف زواجت:

1. و Cldap لاصتا ةلواجم ءانثأ رفوتم ريغ حبصأ ايلاح ددحملا DC نأ AD لصوصم فشتكي. LDAP و Kerberos و RPC و Kerberos. اذيدج ددحملا DC لىل لوصولا.
2. نكلو، CLDAP لاصتا رابتخال ةباجتسالو (DC) لاجملا ب مكحتلا ةدحو ليغشت مت. ةدحو تناك و، RPC ذفنم رطح مت: لاثم) ام ببسل هب لاصتال AD لصوصم لىل رذعتي ةدحو ليغشت فاقى متي ملو، "لطعملل لثامتملا خسنلا" ةلاح في DC لاجملا ب مكحتلا (ححص لكش ب DC لاجملا ب مكحتلا).
- DC عضو متي) ةروظحم ةمئاقب DC ديذحت ةئيهتب AD لصوصم موقى، تالاحل هذه لثم في مكحتلا ةدحو نيذخت متي مل. ددحملا DC ب لاصتال لواحى و (ةروظحملا ةمئاقلا في "ئيس") اتقوم ةروظحملا ةمئاقلا في ددحملا (DC) لاجملا ب.

مل اذا لشفلا و) ةلوقعم ةينمز ةرتف لالخ لشفلا زواجت لامك اب AD لصوصم موقى نا بجى زواجت ءانثأ DC تادحو نم دودحم ددع ةبرجت AD لصوصم لواحى، ببسل اذهلو. (انكمم كلذ نكي لشفلا).

ةكبشلا في دادرستلال لباق ريغ أطخ كانه ناك اذا AD لاجملا ب مكحتلا تادحو رطح ISE موقى

1. رادقم ب حيصلا ريغ رورملا ةملك دادع نم رورم ةملك ب AD درت ذئدنعف ، نيدرالو رورملا ةملك و ةيوهلا عم باسح ي ا قباطت ي مل اذ ا .

ثحبلا ةيفصت لم اوع (ISE) ةيوهلا فشك تامدخ كرحم

نع امئاد ISE ثحبت AD ب لاصتالا دير ي ذللا نايل ل فيرعتل ةيفصتلا لم اوع مدختست تالالاو ني مدختس م اوعوم حم ي ف نايل ل اذه

ثحبلا ةيفصت لم اوع يلع ةلثم ا

1. **SAM Search:** اذ ا ISE ناك اذ ا ISE ن ا ف ، ل اجم ةمالع ي ا نود طقف مدختس م ساك ةيوه ي قتل تي ISE ناك اذ ا SAM Search: ةزهجالا و ا ةزهجالا ي مدختس م عي م جل AD ي ف ثحبي و SAM ك اذه مدختس م ا مسا لم اعي SAM. م ساك ةيوهلا كلت اهل ي تل ا

ني مدختس م ا ني ب زي م تل ل رورملا ةملك مدختس ي ISE ن ا ف ، ادير ف SAM مسا نكي مل اذ ا EAP-TLS لثم رورم ةملك فرعم ريغ لو كوتورب مادختس سال انوكم ISE ناك و

عم ةقداصملا ي ف ISE لش ف ي ك لذل ، بس انملا مدختس م ا ع قوم دي دحتل ريخ ا ري اعم دجوت ال " ةضماغ ةيوه " اطخ ثودح

ةنراقم Cisco ISE مدختس ي ، Active Directory ي ةدوجوم مدختس م ا ةداهش تناك اذ ا ، كلذ عمو ةيوهلا لحل ةيئانث

```

219 2020-01-20 16:33:48.251918 10.48.60.206 10.48.60.101 LDAP 295 SASL GSS-API Integrity: searchRequest(2) "dc=aaaalab,dc=com" wholeSubtree ✓
220 2020-01-20 16:33:48.253244 10.48.60.101 10.48.60.206 LDAP 384 SASL GSS-API Integrity: searchResEntry(2) "CN=anas Jehad,CN=Users,DC=aaaalab,DC=aaaalab,DC=com" ✓
258 2020-01-20 16:33:48.306966 10.48.60.206 10.48.60.101 LDAP 105

```

```

> Frame 219: 295 bytes on wire (2360 bits), 295 bytes captured (2360 bits) on interface 0
> Ethernet II, Src: Vmware_b6:ed:17 (00:50:56:b6:ed:17), Dst: Vmware_d5:6a:7d (00:0c:29:d5:6a:7d)
> Internet Protocol Version 4, Src: 10.48.60.206, Dst: 10.48.60.101
> Transmission Control Protocol, Src Port: 19997, Dst Port: 3268, Seq: 1430, Ack: 213, Len: 229
> Lightweight Directory Access Protocol
  SASL Buffer Length: 225
  SASL Buffer
    GSS-API Generic Security Service Application Program Interface
      GSS-API payload (197 bytes)
        LDAPMessage searchRequest(2) "dc=aaaalab,dc=com" wholeSubtree
          messageID: 2
          protocolOp: searchRequest (3)
            searchRequest
              baseObject: dc=aaaalab,dc=com
              scope: wholeSubtree (2)
              derefAliases: neverDerefAliases (0)
              sizeLimit: 0
              timeLimit: 0
              typesOnly: False
              filter: (&(|(objectCategory=person)(objectCategory=computer))(sAMAccountName=anos))
                filter: and (0)
                  and: (&(|(objectCategory=person)(objectCategory=computer))(sAMAccountName=anos))
                    and: 2 items
                      Filter: (|(objectCategory=person)(objectCategory=computer))
                        and item: or (1)
                          or: (|(objectCategory=person)(objectCategory=computer))
                          Filter: (sAMAccountName=anos)
                            and item: equalityMatch (3)
                              equalityMatch
                                attributeDesc: sAMAccountName
                                assertionValue: anos
                    attributes: 4 items
                      AttributeDescription: sAMAccountName
                      AttributeDescription: userPrincipalName
                      AttributeDescription: objectCategory
                      AttributeDescription: userAccountControl

```

2. **UPN و Mail:** اذ ا ISE ناك اذ ا ISE ن ا ف ، ل اجم ةمالع ي ا نود طقف مدختس م ساك ةيوه ي قتل تي ISE ناك اذ ا UPN و Mail: ةزهجالا و ا ةزهجالا ي مدختس م عي م جل AD ي ف ثحبي و SAM ك اذه مدختس م ا مسا لم اعي SAM. م ساك ةيوهلا كلت اهل ي تل ا

AAA قفدت عم Cisco ISE رمتس ي ، دير ف قباطت كانه ناك اذ ا

Cisco ن ا ف ، دير ل او UPN س فن و رورم ةملك و UPN س فن اهل ةددعتم طبر طاقن كانه تناك اذ ا " سبتلم فرعم " اطخ ثودح عم ةقداصملا ي ف لش ف ي ISE

461	2020-01-20 16:33:58.134338	10.48.60.206	10.48.60.101	LDAP	336 SASL GSS-API Integrity: searchRequest(3) "dc=aaalab,dc=com" wholeSubtree ✓
464	2020-01-20 16:33:58.137942	10.48.60.101	10.48.60.206	LDAP	384 SASL GSS-API Integrity: searchResEntry(3) "CN=anas Jehad,CN=Users,DC=aaalab,DC=..." ✓
471	2020-01-20 16:33:58.170678	10.48.60.206	10.48.60.101	LDAP	179 SASL GSS-API Integrity: searchRequest(6) "CN=anas Jehad,CN=Users,DC=aaalab,DC=..." ✓
472	2020-01-20 16:33:58.172663	10.48.60.101	10.48.60.206	LDAP	1413 SASL GSS-API Integrity: searchResEntry(6) "CN=anas Jehad,CN=Users,DC=aaalab,DC=..." ✓
476	2020-01-20 16:33:58.174754	10.48.60.206	10.48.60.101	LDAP	189 SASL GSS-API Integrity: searchRequest(7) "CN=anas Jehad,CN=Users,DC=aaalab,DC=..." ✓
479	2020-01-20 16:33:58.175528	10.48.60.101	10.48.60.206	LDAP	255 SASL GSS-API Integrity: searchResEntry(7) "CN=anas Jehad,CN=Users,DC=aaalab,DC=..." ✓
480	2020-01-20 16:33:58.176236	10.48.60.206	10.48.60.101	LDAP	241 SASL GSS-API Integrity: searchRequest(8) "dc=aaalab,dc=com" wholeSubtree ✓
481	2020-01-20 16:33:58.177307	10.48.60.101	10.48.60.206	LDAP	635 SASL GSS-API Integrity: searchResEntry(8) "CN=Users,CN=Builtin,DC=aaalab,DC=..." ✓
484	2020-01-20 16:33:58.178414	10.48.60.206	10.48.60.101	LDAP	271 SASL GSS-API Integrity: searchRequest(9) "dc=aaalab,dc=com" wholeSubtree ✓

> Frame 461: 336 bytes on wire (2688 bits), 336 bytes captured (2688 bits)
 > Ethernet II, Src: Vmware_b6:ed:17 (00:50:56:b6:ed:17), Dst: Vmware_d5:6a:7d (00:0c:29:d5:6a:7d)
 > Internet Protocol Version 4, Src: 10.48.60.206, Dst: 10.48.60.101
 > Transmission Control Protocol, Src Port: 19997, Dst Port: 3268, Seq: 1659, Ack: 531, Len: 270

Lightweight Directory Access Protocol
 SASL Buffer Length: 266
 SASL Buffer
 > GSS-API Generic Security Service Application Program Interface
 > GSS-API payload (238 bytes)
 LDAPMessage searchRequest(3) "dc=aaalab,dc=com" wholeSubtree
 messageID: 3
 protocolOp: searchRequest (3)
 searchRequest
 baseObject: dc=aaalab,dc=com
 scope: wholeSubtree (2)
 derefAliases: neverDerefAliases (0)
 sizeLimit: 0
 timeLimit: 0
 typesOnly: False
 Filter: (&((objectCategory=person)(objectCategory=computer))((userPrincipalName=anos@aaalab.com)(mail=anos@aaalab.com)))
 filter: and (0)
 and: (&((objectCategory=person)(objectCategory=computer))((userPrincipalName=anos@aaalab.com)(mail=anos@aaalab.com)))
 and: 2 items
 Filter: ((objectCategory=person)(objectCategory=computer))
 and item: or (1)
 or: ((objectCategory=person)(objectCategory=computer))
 Filter: ((userPrincipalName=anos@aaalab.com)(mail=anos@aaalab.com))
 and item: or (1)
 or: ((userPrincipalName=anos@aaalab.com)(mail=anos@aaalab.com))

3. **NetBIOS:** لاجم NetBIOS (ex: Cisco\Sajedah)، شحبت، اه يلع روثع ال درجم بو. NetBIOS لاجم نع تاباغل ي ف شحبلاب ISE موقت ذئدنع (هلثمن يذلا لاثمل ي ف ةدجاس) رفوتمل SAM مسا نع

654	2020-01-20 17:06:29.243747	10.48.60.206	10.48.60.101	LDAP	295 SASL GSS-API Integrity: searchRequest(2) "dc=aaalab,dc=com" wholeSubtree ✓
655	2020-01-20 17:06:29.245154	10.48.60.101	10.48.60.206	LDAP	682 SASL GSS-API Integrity: searchResEntry(2) "CN=anas Jehad,CN=Users,DC=aaalab,DC=..." ✓
684	2020-01-20 17:06:29.290383	10.48.60.206	10.48.60.101	LDAP	179 SASL GSS-API Integrity: searchRequest(3) "CN=anas Jehad,CN=Users,DC=aaalab,DC=..." ✓
685	2020-01-20 17:06:29.292939	10.48.60.101	10.48.60.206	LDAP	1413 SASL GSS-API Integrity: searchResEntry(3) "CN=anas Jehad,CN=Users,DC=aaalab,DC=..." ✓
687	2020-01-20 17:06:29.294515	10.48.60.206	10.48.60.101	LDAP	189 SASL GSS-API Integrity: searchRequest(4) "CN=anas Jehad,CN=Users,DC=aaalab,DC=..." ✓
688	2020-01-20 17:06:29.295469	10.48.60.101	10.48.60.206	LDAP	255 SASL GSS-API Integrity: searchResEntry(4) "CN=anas Jehad,CN=Users,DC=aaalab,DC=..." ✓
689	2020-01-20 17:06:29.296186	10.48.60.206	10.48.60.101	LDAP	241 SASL GSS-API Integrity: searchRequest(5) "dc=aaalab,dc=com" wholeSubtree ✓
692	2020-01-20 17:06:29.297557	10.48.60.101	10.48.60.206	LDAP	635 SASL GSS-API Integrity: searchResEntry(5) "CN=Users,CN=Builtin,DC=aaalab,DC=..." ✓
693	2020-01-20 17:06:29.298761	10.48.60.206	10.48.60.101	LDAP	271 SASL GSS-API Integrity: searchRequest(6) "dc=aaalab,dc=com" wholeSubtree ✓
694	2020-01-20 17:06:29.299690	10.48.60.101	10.48.60.206	LDAP	650 SASL GSS-API Integrity: searchResEntry(6) "CN=Domain Users,CN=Users,DC=aaala..." ✓

SASL Buffer
 > GSS-API Generic Security Service Application Program Interface
 > GSS-API payload (197 bytes)
 LDAPMessage searchRequest(2) "dc=aaalab,dc=com" wholeSubtree
 messageID: 2
 protocolOp: searchRequest (3)
 searchRequest
 baseObject: dc=aaalab,dc=com
 scope: wholeSubtree (2)
 derefAliases: neverDerefAliases (0)
 sizeLimit: 0
 timeLimit: 0
 typesOnly: False
 Filter: (&((objectCategory=person)(objectCategory=computer))(sAMAccountName=anos))
 filter: and (0)
 and: (&((objectCategory=person)(objectCategory=computer))(sAMAccountName=anos))
 and: 2 items
 Filter: ((objectCategory=person)(objectCategory=computer))
 and item: or (1)
 or: ((objectCategory=person)(objectCategory=computer))
 Filter: (sAMAccountName=anos)
 and item: equalityMatch (3)
 equalityMatch

4. **ISE موقوي، ةئداب/ف يضم ةي وهب، زاهج ةقداصم يقلت ي ISE ناك اذ:** زاهجلا ةدعاق نع شحب. ةقباطتم servicePrincipalName ةمس نع ةباغل ي ف شحبلاب.

لا ثمل ل ي بس يلع، ةي وهل ي ف لمالك لاب ةلهؤم لاجم ةقحال دي دحت مت اذ
 لاجم ل اذه دجوي شيح ةباغل ي ف شحبي Cisco ISE نإف، host/machine.domain.com.

مسا نع تاباغل عي مج ي ف شحبلاب Cisco ISE موقوي، زاهج/ف يضم لكش ي ف ةي وهل تناك اذ
 ي. ساسألا ةمدخل

فرعم "أطخ مادختساب ةقداصم ل ي ف Cisco ISE لش ي ف، دحاو قباطت نم رثكأ كانه ناك اذ
 "سبتمل".

2744	2020-01-20 16:35:32.108609	10.48.60.206	10.48.60.101	LDAP	373 SASL GSS-API Integrity: searchRequest(3) "dc=aaalab,dc=com" wholeSubtree	✓
2745	2020-01-20 16:35:32.109744	10.48.60.101	10.48.60.206	LDAP	393 SASL GSS-API Integrity: searchResEntry(3) "CN=ISE24P,CN=Computers,DC=aaalab,DC=com"	✓
2747	2020-01-20 16:35:32.109951	10.48.60.206	10.48.60.101	LDAP	185 SASL GSS-API Integrity: unbindRequest(7)	✓
2757	2020-01-20 16:35:32.114862	10.48.60.206	10.48.60.101	LDAP	1495 bindRequest(1) "<ROOT>" sasl	✓
2758	2020-01-20 16:35:32.115898	10.48.60.101	10.48.60.206	LDAP	278 bindResponse(1) success	✓
2760	2020-01-20 16:35:32.116176	10.48.60.206	10.48.60.101	LDAP	348 SASL GSS-API Integrity: searchRequest(2) "dc=aaalab,dc=com" wholeSubtree	✓
2761	2020-01-20 16:35:32.116855	10.48.60.101	10.48.60.206	LDAP	740 SASL GSS-API Integrity: searchResEntry(2) "CN=ISE24P,CN=Computers,DC=aaalab,DC=com"	✓
2762	2020-01-20 16:35:32.145535	10.48.60.206	10.48.60.101	LDAP	179 SASL GSS-API Integrity: searchRequest(3) "CN=ISE24P,CN=Computers,DC=aaalab,DC=com"	✓

Ethernet II, Src: Vmware_b6:ed:17 (00:50:56:b6:ed:17), Dst: Vmware_d5:6a:7d (00:0c:29:d5:6a:7d)
 Internet Protocol Version 4, Src: 10.48.60.206, Dst: 10.48.60.101
 Transmission Control Protocol, Src Port: 28089, Dst Port: 3268, Seq: 1746, Ack: 267, Len: 307
 Lightweight Directory Access Protocol

```

SASL Buffer Length: 303
SASL Buffer
  > GSS-API Generic Security Service Application Program Interface
  > GSS-API payload (275 bytes)
  > LDAPMessage searchRequest(3) "dc=aaalab,dc=com" wholeSubtree
    messageID: 3
    protocolOp: searchRequest (3)
      searchRequest
        baseObject: dc=aaalab,dc=com
        scopes: wholeSubtree (2)
        derefAliases: neverDerefAliases (0)
        saslLimit: 0
        timeLimit: 0
        typesOnly: False
        filter: (&([(objectCategory=person)(objectCategory=computer)](sAMAccountName=ise24p$))
          filter: and (0)
            and: (&([(objectCategory=person)(objectCategory=computer)](sAMAccountName=ise24p$))
              and: 2 items
                filter: ((objectCategory=person)(objectCategory=computer))
                  and item: or (1)
                    or: ((objectCategory=person)(objectCategory=computer))
                  filter: (sAMAccountName=ise24p$)
                    and item: equalityMatch (3)
                      equalityMatch
                        attributeDesc: sAMAccountName
                        assertionValue: ise24p$
  
```

ISE Ad-Agent.log تافل م يف تاحش رمل س فن رهظت :ةظالم

اقبسم ني ددحمل ني مدخت سمل و 1 حي حصت 2.3 و قب اسلا و 4 حي حصت 2.2 ISE :ةظالم
 2.3 و ، يلع أو 5 حي حصت 2.2 رادصلإا ، Cisco ISE ، امهالك وأ CN أو SAM صئاصلإ عم
 ةيضا رتفا ةمسك طقف sAMAccountName ةمس مدخت سا ، يلع أو 2 حي حصت

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ 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 ل ا ة مچرت 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 مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا ة ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
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 دن ت س م ل ا