

Active Directory WMI J رفوم عم ISE 2.2 PIC نيوكت Directory

تايوت حمل

[عمدق مل](#)

[قيساس الابلط مل](#)

[تابلط مل](#)

[عمدخت س مل تانوك مل](#)

[قيساس ا تامول عم](#)

[كك بش لل يطيخت مل مسر مل](#)

[لمعل ريس](#)

[نيوكت مل](#)

[ISE PIC رشن نيوكت](#)

[اهب قووثوم مل تاداهش ل تيبثت \(قيرايتخ\) 1 ةوطخ مل](#)

[ماظن مل تاداهش تيبثت \(قيرايتخ\) 2 ةوطخ مل](#)

[رشن مل ل قيوناث ةدقع ةفاضاب مق 3 ةوطخ مل](#)

[Active Directory عمدخ يرفوم نيوكت](#)

[ل اجم مل ل ISE PIC ل ماضنا 1 ةوطخ مل](#)

[AD ل ل تانوذال طبض 2 ةوطخ مل](#)

[PassiveID ءالك و ةفاضاب 3 ةوطخ مل](#)

[ةحصل مل نم ققحت مل](#)

[رشن مل](#)

[رشن مل ةحفص](#)

[تامول عم مل ةحول ةحفص](#)

[انوبتت كم](#)

[ماظن مل صخلم](#)

[تاسل ل او نورفوم مل](#)

[قيس يئرل ةحفص مل](#)

[قرشاب لمع تاسل ل](#)

[اهحال ص او ءاطخ ال فاشكت سا](#)

[رشن مل](#)

[غولبل ل ءلباق ريغ قيوناث ل ةدقعل: ءكرتشن مل ءلكشن مل](#)

[Active Directory و WMI](#)

[لعل يذيفنتل فل مل ل ل يغشت رذعتي "ISE PIC Throws": ءعئاش ل ءلكشن مل](#)

عمدق مل

قيوهل تامدخ كرحمل (ISE PIC) لمخال قيوهل ل صوم رشن نيوكت قيفي دنن س مل اذه حضوي
Active Directory Windows Management Instrumentation (AD WMI). ISE PIC رادصل وه
ةلمخال فرعم تازيم لعل زكري نزول قيفي ISE رادصل وه ISE PIC.

اذه و. طقف قيوهل س ل قيوهل مدختست يتل Cisco نام مزح عيمل دحاو فرعم ل ح وه ISE PIC
نيفلتخم نيرفوم معددي وه. ISE PIC لعل تاسايس ل و ل ل وختل نيوكت نكمي ال هن ينعني

تاردق هيدل REST. تاقىب طت ةجر رب ةه جاو رب ع مه جمد نكم يو (API و Syslog و WMI و ءال كولا) ةطقن لانت ال له ؟لوخدلا ليجستب مدختس مل اقا له) ةياهنلا طاقن نع مالع تسال (؟ ةلصتم ةياهنلا)

ةيساس ال اابل طتم ال

اابل طتم ال

ةيلاتل عيضاوم لابل ةيساس ا ةفر عم كيدل نوكت نأب Cisco ي صوت

- Cisco نم ةيوهلا ةمدخ كرحم
- Microsoft Active Directory
- Microsoft WMI

ةمدختس مل اناوكم ال

ةيلاتل ةيدام ال اناوكم ل اوجمار بل اارادصا ال دننتس مل اذ ه ف ةدراول ا تامول عم ال دننتس

- Cisco Identity Service Engine Passive Identity Connector، رادصا ال 2.2.0.470
- Microsoft Windows 7 Service Pack 1
- Microsoft Windows Server 2012 R2 لىغش تال ماظن

ةصاخ ةيلم عم ةئيب ي ف ةدوحو مل ازه جال نم دننتس مل اذ ه ف ةدراول ا تامول عم ال اناوكم دننتس مل اذ ه ف ةمدختس مل ازه جال ا عي مج اءب تناك اذ ا. (يضا رتفا) حوس مم نيوك تب دننتس مل اذ ه ف ةمدختس مل ازه جال ا عي مج اءب رما ال لمحتس مل اريثا تال ك م ه ف نم دكا ت ف ، ةرشابم ك تكبش

ةيساس ا تامول عم

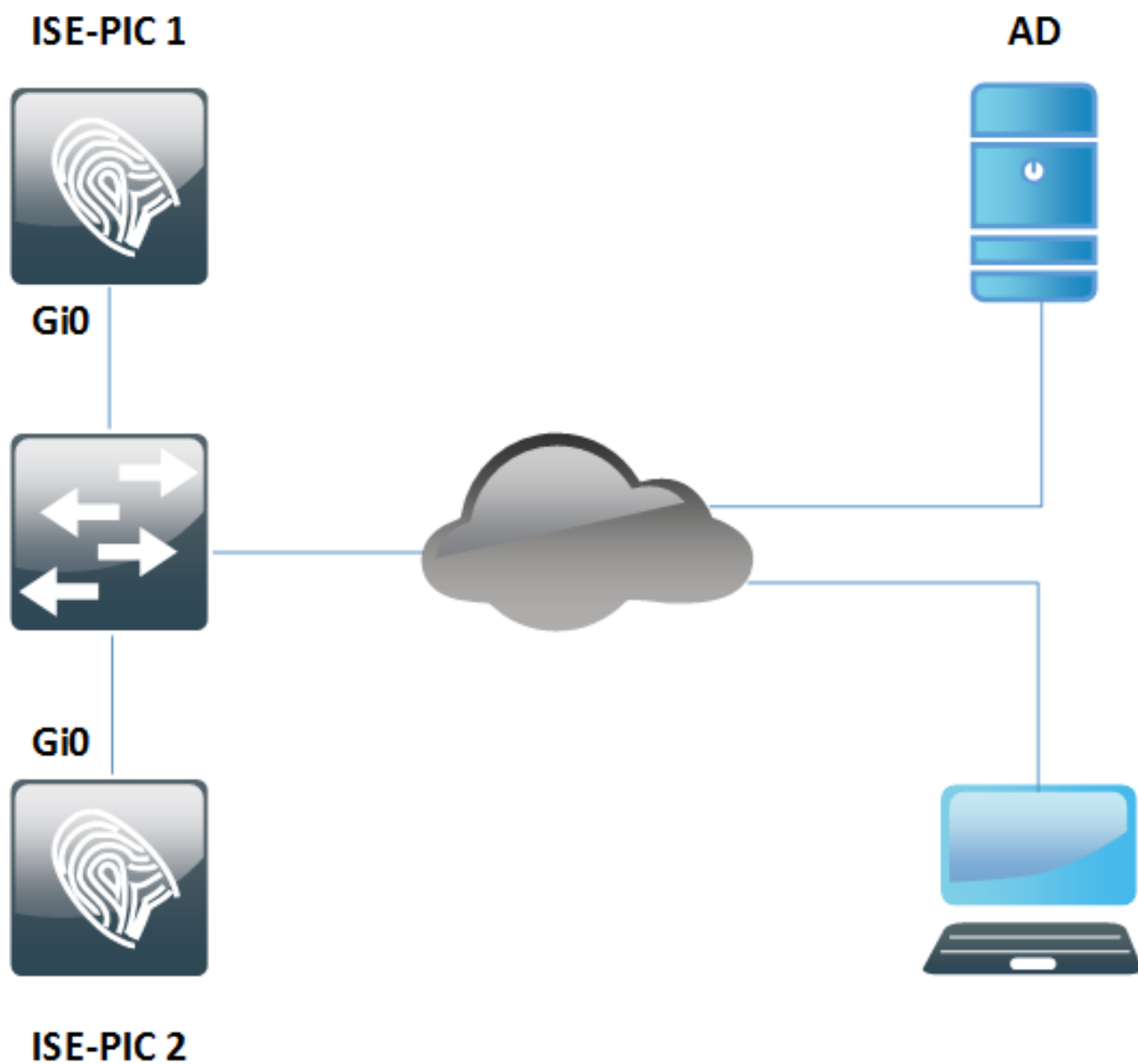
نيوك ةيفي ك لاثم ال اذ ه حضوي 2. وه ISE PIC ةقاطب رشن ي ف دقعل ا ددعل ىصق ال ا دحل ني يضا رتفا ني زا ه مادختسا م تي يلات لابل و ، ل ا ع رفوت ىلع لوصح ل ال ISE PIC ةقاطب رشن ةدقعل ا هذ ه ي ف . يوناثو يساسا : راودا دقعل ل نو ك ي نا نكم ي ، ISE PIC ةقاطب رشن ي ف (VM) لال خ نم طاق اي ودي راودال ا ريغ ت نكم يو ةدحاو ل ا ةرمل ا ي ف ةيساسا نوكت نا نكم ي ةديحو ل ا دي ق تازي مل ا عي مج لانت ال ، يساسا ل لش فال ا ل ا ح ي ف (GUI) ةيموسر ل ا مدختس مل ا ةه جاو ىوس مدختس مل ا ةه جاو نكم ي ال . مدختس مل ا ةه جاو اناثتساب ةيوناثال ىلع لىغش تال يساسا ال ا ةي ودي ل ا ةي قرتل ا

نم ةعومجم نم WMI نوكت ي . Active Directory ل WMI رفوم نيوك ةيفي ك لاثم ال اذ ه حضوي اهل لال خ نم رفوت لىغش ت ماظن ةه جاو رفوت Windows لىغش ت جم اناوكم ل ا ةدوخل ا ةرادا ري ياع مل Microsoft قىب طت يه WMI . تاراعش ال او تامول عم ال ا او دال ا ب ةدوزم ل ا ناوكم ال ل مع قيرف نم (CIM) ةكرتس مل ا تامول عم ال ا جذومنو (WBEM) بيولا ىلع ةمئاق ل ا تاسس و مل ا (DMTF) ةعزوم ل ا ةرادال ا

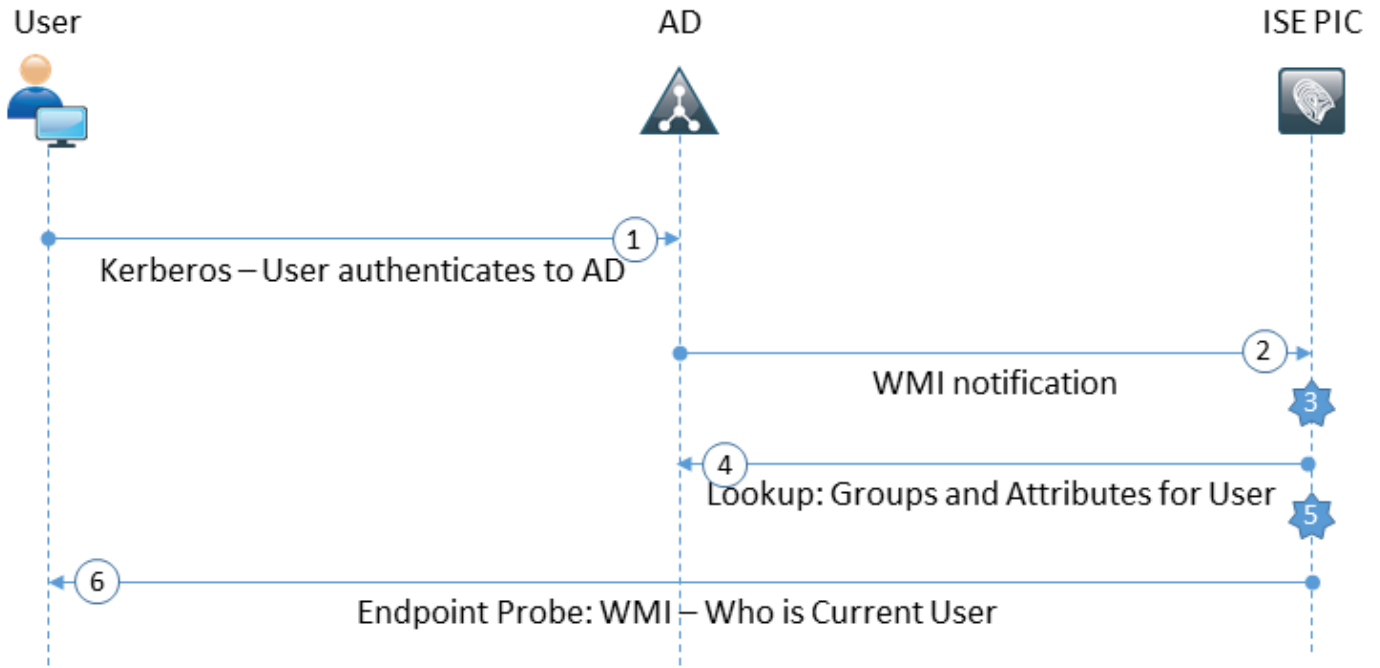
ي م سر ل ا Microsoft ع قوم ي ف WMI ل و ح تامول عم ال ا نم ديزم ىلع رو ثع ال ا نكم ي : [ةظح الم ل و ح WMI](#)

ةكبش لل يطي طختلا مسرلا

ةروصلا يف حضوملا ةكبشلا دادع| دنن سمللا يف ةدراولا تامولعمللا مدختست



لمعللا ريس



1. AD يلع هيلع ةقداصملا متتو رتويبمكلا ىلإ لوخدلا ليحستب مق.
2. ةقداصملا هذه لوح ISE PIC مالعاب WMI موقت.
3. هب صاخلا لمعلا ةسلج ليلد ىلإ IP_ADDRESS: طب رلا مدختسم مس ISE فيضي.
4. AD نم مدختسملا تامسو تاعومجم ISE عجرتسي.
5. هب صاخلا لمعلا ةسلج ليلد في تامولعمل هذه ظفح ISE موقى.
6. Endpoint Probe: ليغشتب (نيوكتلل ةلباق ريغ) تاعاس 4 لك ISE PIC ةقابط موقت. ليغشتب ISE PIC موقى، WMI لشف ةلاح في. ةياهنلا ةطقن ىلإ WMI لواحى، الوأ ةرملا في WMI نيكمتمو مدختسملل ةياهنلا ةطقن مالعتساب موقى. ISEExec. ماظن عونو ةياهنلا ةطقن ب صاخلا MAC ناو نع ديعتسي ISE PIC نأ امك. ةمداقلا ليغشتلا ةدقعل موقت. ةياهنلا ةطقن تارابتخا ليطعت/نيكمت طقف نكمملا نم، ISE PIC في ةلاح في ةيوناتلا ةدقعل مدختست امنب، ةياهنلا طاقن ةفاك مالعتساب ةساسلا طقف يلاعلا رفوتلا.

نيوكتلا

ISE PIC رشن نيوكت

اهب قوٲوملا تاداهشلا تيبتت (ةيرايخا) 1 ةوطخلا.

ISE نزم ىلع (CA) "قدصملا عجرملا" ب ةصاخلا ةلمكلا تاداهشلا ةلسلس تيبتت بجي تاداهشلا ىلإ لقتناو ISE PIC ةيموسرلا مدختسملا ةهجاو ىلإ لوخدلا ليحستب مق. قوٲوملا نم قدصملا عجرملا ةداهش دحو داريست ىلع رقنا. اهب قوٲوملا تاداهشلا > تاداهشلا قراد > رتويبمكلا.

تاداهش عي مجل ةوطخلل هذه ررك .تاريي غتلا ظفحل لاسرا قوف رونا ،ةروصلل ي ف حضورم وه امك اضيا ةيونائل ةدقعلال ل ع تاوطخلل ررك .ةلسل لل

▼ Certificates Management ▶ Certificates Authority

System Certificates Trusted Certificates OCSP Client Profile Certificate Signing Requests Cert. Periodic Check Settings

Import a new Certificate into the Certificate Store

* Certificate File WinServCer.cer

Friendly Name

Trusted For: ⓘ

Trust for authentication within ISE

Trust for client authentication and Syslog

Trust for authentication of Cisco Services

Validate Certificate Extensions

Description

ماظنل تاداهش تي ب ت .(ةي راي تخا) 2 ةوطخلل

صاخال حا فملا لى ل ةفاضل اب CA ةطساوب ل ع فلاب اهواشن م تي ل تاداهش ل .1 رايخ

ةداهش ل فلم ددح .داري تس ل رونا و ماظنل تاداهش > تاداهش ل ةراد ل > تاداهش ل لى ل قتنا صاخال حا فملا ريفش ت م اذا رورملا ةم لك ل قح ل خدا ، صاخال حا فملا فلم و

ةروصلل اب مادختسالل نم ققحتل تاراخي ف حضورم وه امك

Import Server Certificate

* Select Node

* Certificate File ise22pic1vku...alise22p.pem

* Private Key File ise22pic1vku...alise22p.pvk

Password

Friendly Name (i)

Allow Wildcard Certificates (i)

Validate Certificate Extensions (i)

Usage

- Admin: Use certificate to authenticate the ISE Admin Portal
- EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling
- RADIUS DTLS: Use certificate for the RADSec server
- pxGrid: Use certificate for the pxGrid Controller
- SAML: Use certificate for SAML Signing
- Portal: Use for portal

إلى أنه سبب اهليوحت نكمي و ISE زمري إلى دنست ISE PIC قاطب نأل ارطن: **عظالم** عرفتو م ادختسال ااراخي عي مج نإف، ع بس انم ال صيخار التا عم تازي م ال لم اك ISE ماظن ISE PIC ع طساوب Portal و SAML و RADIUS DTLS و EAP قداصم لثم راودأل مدختست ال

اضياً عيوناث ع دقع يلع عارج ال اذه ررك. عداهش ال تي بثت ل لاسر يلع رقنا

داري تسإ دع ب ISE PIC ع دقع يلع ع دوجوم ال تامدخال عي مج لي غشت ع داعإ متت: **عظالم** مداخل عداهش

ISE يلع طبرل او CA م ادختساوب ه عي قوتو، (CSR) عداهش ال عي قوتو بلط عاشنإ. 2. رايخل

تابل ط عاشنإ رقنا و تاداهش ال عي قوتو تابل ط ع حفص > تاداهش ال قرادإ > تاداهش ال يلى لقتنا (CSR) تاداهش ال عي قوتو

رمأل مزل اذا يرخأل لوقح ال لخدأو م ادختسال او ع دقع ال دح

ISE Certificate Authority Certificates:

- ISE Root CA - This is not a signing request, but an ability to generate a brand new Root CA certificate for the ISE CA functionality.
- ISE Intermediate CA - This is an Intermediate CA Signing Request.
- Renew ISE OCSP Responder Certificates - This is not a signing request, but an ability to renew the OCSP responder certificate that is signed by the ISE Root CA/ISE Intermediate CA.

Usage

Certificate(s) will be used for

Allow Wildcard Certificates ⓘ

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
<input checked="" type="checkbox"/> ise22-pic-2	ise22-pic-2#Admin

Subject

Common Name (CN)	<input type="text" value="\$FQDN\$"/> ⓘ
Organizational Unit (OU)	<input type="text"/>
Organization (O)	<input type="text"/>
City (L)	<input type="text"/>
State (ST)	<input type="text"/>
Country (C)	<input type="text"/>

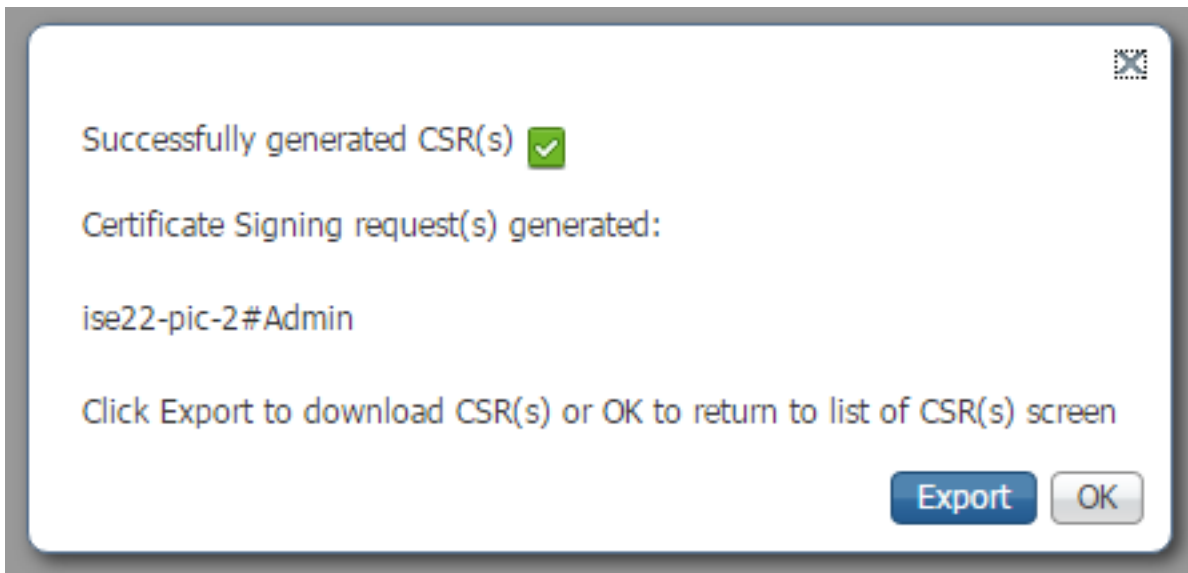
Subject Alternative Name (SAN) - + ⓘ

* Key Length

* Digest to Sign With

Certificate Policies

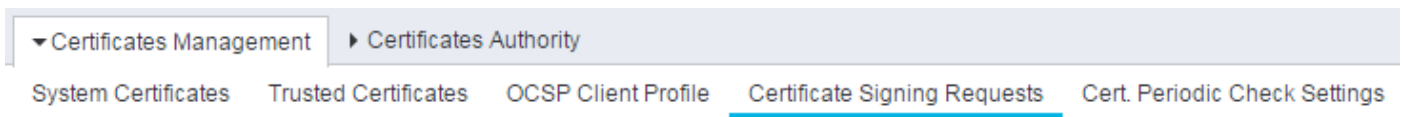
هؤاشنإ مت ېذلا CSR ري دصت رايخ عم ةديج ةذفان رهظت. ءاشنإ يلع رقنأ



م تي ام دن ع CA. م ادخ ت ساب ه ع ق و ت و ه و ا ش ن ا م ت ي ذ ل ا PEM ف ل م ظ ف ح ا ، ر ي د ص ت ي ل ع ر ق ن ا CSR د ح ، ت ا د ا ه ش ل ا ع ق و ت ت ا ب ل ط > ت ا د ا ه ش ل ا ة ر ا د ا > ص ي خ ا ر ت ل ا ي ل ا ل ق ت ن ا ، ع ق و ت ة د ا ه ش ل ا ط ب ر ر ق ن ا و ك ب ص ا خ ل ا :

View Export Delete Bind Certificate						
<input type="checkbox"/>	Friendly Name	Certificate Subject	Key Length	Portal group tag	Timestamp	Host
<input checked="" type="checkbox"/>	ise22-pic-2#Admin	CN=ise22-pic-2.vkumov.local	2048		Thu, 23 Feb 2017	ise22-pic-2

ت ا ر ي غ ت ل ا ق ي ب ط ت ل ل ا س ر ا ي ل ع ر ق ن ا و ق د ص م ل ا ع ج ر م ل ا م ة ع ق و م ل ا ة د ا ه ش ل ا د ح :



Bind CA Signed Certificate

* Certificate File certnew.cer

Friendly Name ⓘ

Validate Certificate Extensions ⓘ

Usage

Admin: Use certificate to authenticate the ISE Admin Portal

ل ا س ر ا ق و ف ر ق ن ل ا د ع ب ISE PIC ة د ق ع ي ل ع ة د و ج و م ل ا ت ا م د خ ل ا ع ي م ج ل ي غ ش ت ة د ا ع ا م ت ة د ا ه ش ل ا ت ي ب ط ت ل .

ر ش ن ل ا ي ل ا ة ي و ن ا ت ة د ق ع ة ف ا ض ا ب م ق 3. ة و ط خ ل ا

رمألا ب ل ط تي ال . ق ئ ا ف ر ف و ت ي ل ع ل و ص ح ل ل ر ش ن ة ي ل م ع ي ف ن ي ت د ق ع د و ج و ب ISE PIC ح م س ي ة د ق ع ة ف ا ض ا ل . (د ا ت ع م ل ISE ر ش ن ب ة ن ر ا ق م) ت ا د ا ه ش ل ل ا ب ه ا ج ا ت ا ل ا ة ي ئ ا ن ث ة ق ث ك ي د ل ن و ك ي ن ا و ه ا م ك ، ة ي س ا س ا ل ISE PIC ة د ق ع ي ل ع ر ش ن ة ح ف ص > ة ر ا د ا ي ل ل ل ق ت ن ا ، ر ش ن ل ا ي ل ل ة ي و ن ا ث ة ر و ص ل ا ي ف ح و م :

Deployment

Licensing

Logging

Maintenance

Admin Access

This Node

Role	Standalone
IP Address	10.48.26.51
FQDN	ise22-pic-1.vkumov.local

Add Secondary Node

FQDN * ise22-pic-2.vkumov.local

User Name * admin

Password *

Cancel

Save

ك ل ت ل ل و و س م ل ا د ا م ت ع ا ت ا ن ا ي ب و ، ة ي و ن ا ث ل ا ة د ق ع ل ل (FQDN) ل م ا ك ل ل ا ب ل ه و م ل ل ا ج م ل ا م س ا ل خ د ا ة د ا ه ش ن م ق ق ح ت ل ا ي ل ع ة ي س ا س ا ل ISE ة د ق ع ة ر د ق م د ع ة ل ا ح ي ف . ط ف ح ق و ف ر ق ن ا و ة د ق ع ل ا ه ب ق و ث و م ل ا ن ز خ م ل ا ي ف ة د ا ه ش ل ل ا ك ل ت ت ي ب ث ت ل ب ق ا د ي ك ا ت ب ل ط ت ، ة ي ن ا ث ل ا ة د ق ع ل ل و و س م .

Certificate Warning



The node you are trying to register uses a self-signed certificate which is not trusted.
Are you sure you want to trust this certificate and proceed with registration?

If you are unsure, please click 'Cancel Registration' and manually setup trust under 'Certificate Management' before registering the node.

Serial Number : 58 AE E4 EF 00 00 00 00 62 E0 F9 86 17 5A 34 91
Issued to : CN=ise22-pic-2.vkumov.local
Issued by : CN=ise22-pic-2.vkumov.local
Issued On : Thu Feb 23 14:34:39 CET 2017
Expires On : Sat Feb 23 14:34:39 CET 2019
Signature Algorithm : SHA256withRSA
SHA-256 Fingerprint : 2D 4C 9A 7D FF 72 C7 93 73 C4 FB F0 58 E0 59 2F 24 40 F0 F8 77 50 D4 52 E6 3D
EF 56 CA 5F 4E 15
SHA-1 Fingerprint : 11 AB F0 8F 0C 89 50 FE 06 AC 2F AD 81 03 1D 52 D2 17 AB 61
MD5 Fingerprint : DD 27 87 FA 5D 18 E9 5C 71 BD 6A 5A 47 10 95 66

Additional Warnings

Import Certificate and Proceed

Cancel Registration

نأ بجي .رشنلإىلإ ءءقءلإىلإ مامضنلالعباءوءءءاهشلالءارءءسإقوف رقنا ءلإءل هءه فى
ىلء ءامءءلالءمء لىءغشء ءءاعإ مءء .ءاءنءب اهءفاضإ ءمء ءق ءءقءلالنأب مالعإىلء لءصءء
ءىوناءلل ءءقءلال.




Node was registered successfully. Data will be sync'ed to the node, and then the application server will be restarted on the node. This process may take several minutes to complete.

OK



مءقءلالءءق نم ءءقءلالءلءرءىءءبءىوءءقءقءء 20 لىلإ 10 نوءضغ فى ءقءلالءنمزم بءى
لءصءء لىلإ:

This Node

Refresh

Role	Primary
IP Address	10.48.26.51
FQDN	ise22-pic-1.vkumov.local
Node Status	<input checked="" type="checkbox"/> Connected 

Secondary Node

Role	Secondary
IP Address	10.48.26.53
FQDN	ise22-pic-2.vkumov.local
Node Status	<input checked="" type="checkbox"/> Connected  

Deregister

Sync Now

Active Directory مرفوم نيوكت

تاسلج نع تامولعمل عمجل (WMI) ISE PIC Windows Management Instrumentation م دختسي
ينعي امم، Pub/Sub لاصتا لثم لمعيو AD نم لمعل

- نعي عم شادحأ في ISE PIC كرتشي
- دي دجت) 4770 و (Kerberos ل تاقاطبل ح نم) 4768 :شادحأل هذه شودح دنع ISE PIC WMI ه بنت
(ةلازالا) لمعللة سلج ليلدي في تالخاللة ح الصاءهت نا(Kerberos ل تاقاطبالا

ل. لامل ال ال ISE PIC ال مضا. 1. ةوطخا

ةفاضل قوف رقن او Active Directory > مرفوم ال لقتنا، لامل ال ال ISE PIC مضا لجا نم

Active Directory Agents API Providers SPAN Syslog Providers Mapping Filters Endpoint Probes

Connection

* Join Point Name ⓘ

* Active Directory Domain ⓘ

Submit Cancel

ظفحل لاسرا قوف رقن او Active Directory لاجم و لاصتال اطقن مسا يل قح ةئبع تب مق
 طقف ISE PIC ف همادختسا متي مسا وه طبرلا اطقن مسا. تاريخي غتال
 مت يذل DNS م داخ عم لجل ال باق نوكي نأ بجي و ISE PIC مض هي ف بجي يذل لاجملا مسا وه
 ISE PIC يلع هنيوكت

لاجملا يل دقعل مض ي ف بغرت تنك اذا كلأسي نأ بجي ISE PIC Join Point عاشن دعب
 لاجملا يل مامضن ال دامتعا تانايب رفوت يكل راطا رهظي نأ بجي. معلن ةق طقط

Join Domain ⓘ

Please specify the credentials required to Join node(s) to the Active Directory Domain.

* Domain Administrator ⓘ

* Password

Specify Organizational Unit ⓘ

Store Credentials ⓘ

OK Cancel

قفاوم يلع رقن او رورملا ةملك لوقحو لاجملا ري دم ألما

مادختسا ي رورضال نم سيل هنأ ال Domain Administrator يمسي لقحل نأ نم مغرلا يلع
 مدختسملا اذه عتمتي نأ بجي. لاجملا يل ISE PIC يل مامضن ال لوؤسملا مدختسم
 تاباسحل رورملا تاملك ريغي وا، اهتلازاو لاجملا ي ف ةزهجأ تاباسح عاشن ال ةيفاك تازايتماب
 ةبولطملا Active Directory باسح تانودا يلع روثعل نكمي. اقبس م اهواشن مت يتل ةزهجال
[دنتسمل](#) اذه ي ف ةفلتخم تاي لمع ذيفنتل

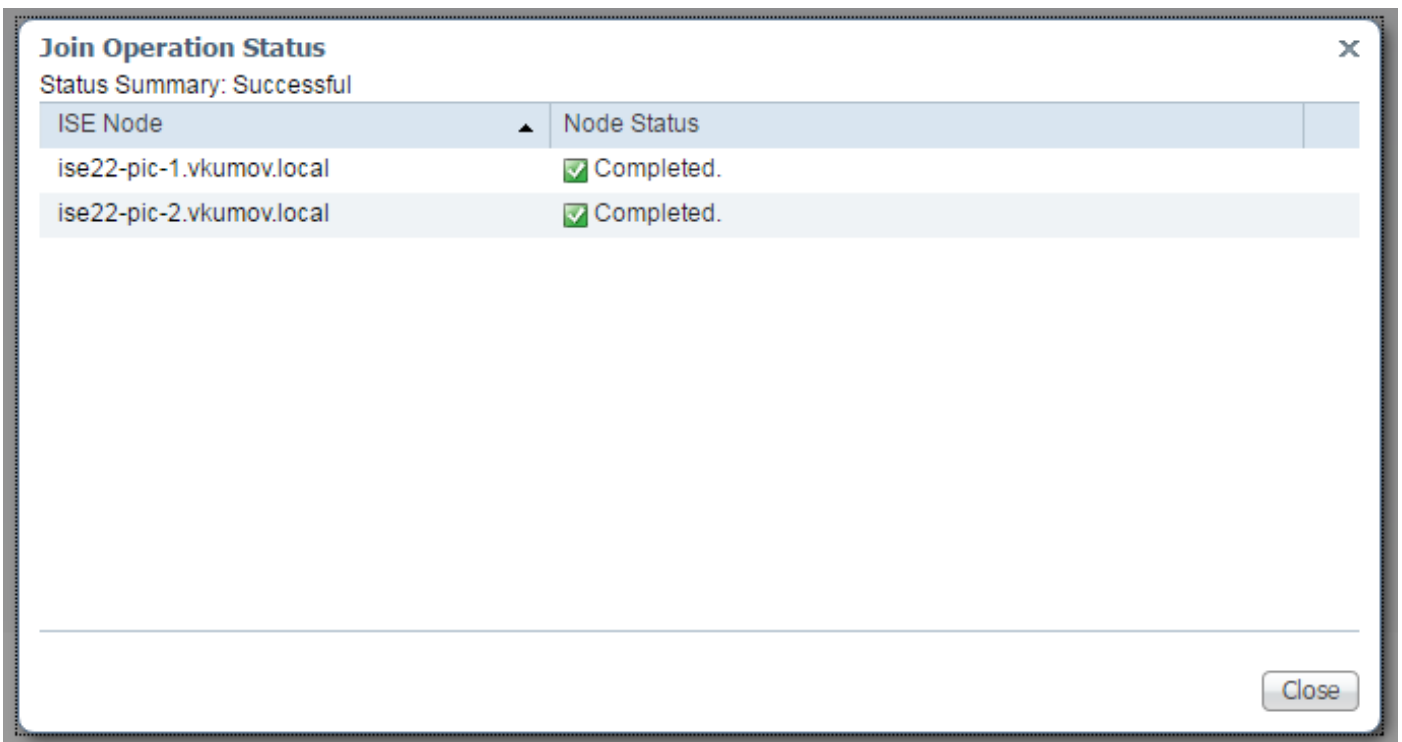
ي ف بغرت تنك اذا مامضن ال اناث لاجملا لوؤسم دامتعا تانايب مادختسا بجي، كلذ عمو
 WMI نيوكت راخي بلطتي. WMI مادختسا

- لجلسال تاريخي غت
- DCOM مادختسال تانودا
- دعب نع WMI مادختسال تانودا

- لاجمب مكحتلا ةدحوب صاخلا نامأل ا شادحأ لجس ةءارق لوصولا
- ءاشنا متيس) ISE PIC لىل/نم تانايبلا رورم ةكرح Windows ةيامح راج حمسي نأ بجي (WMI نيوكت ءانثأ ةقباطملا Windows ةيامح راج تاسايس

اهنأل ارظن ISE PIC ةقابط لىل ةنيزختلا دامتعا تانايب نيكم ت امئاد متي: **ةظحالم** (ISE) ةيوهلا تامدخ مسق موقى. WMI نيوكت و ةياهنلا طاقن تافاشك تسال ةبولطم ايلخاد ةرفشم تاجت نملا هذه نيختب

ةديج ةذفان يف ةيلعمل ءةجيتن ISE PIC ضرعت، ةروصلال يف حضوم وه امك



AD لىل تانوذال طبض. 2. ةوطخلا

ل: [Identity Engine Passive Identity Connector \(ISE-PIC\)](#) لىل دو: دنن سملل اقفو AD يف مدخت سملل تانوذأ نم ققحتلا

لاجملا لوؤسم ةعومجم يف AD مدخت سملل دنن تانوذال نيغت

كلمت ال، Windows 2012 R2 و Windows 2012 و Windows 2008 R2 لىل غشتلا ماظنل ةبسنلاب ماظن يف ةنيعم لىل جست حتافم يف لماكلا مكحتلا يضارتفا لكشب لاجملا ةرادا ةعومجم مدخت سملل لماكلا مكحتلا تانوذأ Active Directory لوؤسم حنمي نأ بجي. Windows لىل غشت لىل اتلا لىل جستلا حتافم لىل ع Active Directory

- HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}
- HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}

PassiveID. ءالك و ةفاض. 3. ةوطخلا

امك DC تافل مة فاضل قوف رقناو PassiveID بيوبتلا مةالع لىل لقتنا AD لاجم ةحفص ي فةروصلال ي ف حضم وه:

Active Directory Agents API Providers SPAN Syslog Providers Mapping Filters Endpoint Probes

Connection Whitelisted Domains **PassiveID** Groups Advanced Settings

PassiveID Domain Controllers

Refresh Edit Trash **Add DCs** Use Existing Agent Config WMI Add Agent

<input type="checkbox"/>	Domain	DC Host	Site
No data found.			

تادحو دح. ةرفوتملا لاجملا ب مكحتلا تادحو عيمجب ةمئاق ليحتب ISE موقتو ديدج راطا رهظي ظفحل قفاوم قوف رقناو اهيف WMI نيوكت ي ف بغيرت ي تلا (DC) لوصولال ي ف مكحتلا ةروصلال ي ف حضم وه امك، تاريغتلا:

Add Domain Controllers

1 Selected

<input type="checkbox"/>	Domain	DC Host	Site	IP Address
<input checked="" type="checkbox"/>	vkumov.local	MainDC.vkumov.local	Default-First-Site-Name	10.48.26.52
<input type="checkbox"/>	vkumov.local	maindc.vkumov.local		139.156.158.9

Cancel OK

PassiveID لاجملا ب مكحتلا تادحو ةمئاق لىل ةدجملا DC لاجملا ب مكحتلا تادحو ةفاضل متت WMI نيوكت رزلا قوف رقناو (DC) لوصولال ي ف مكحتلا تادحو دح:

Active Directory Agents API Providers SPAN Syslog Providers Mapping Filters Endpoint Probes License Warning

Connection Whitelisted Domains **PassiveID** Groups Advanced Settings

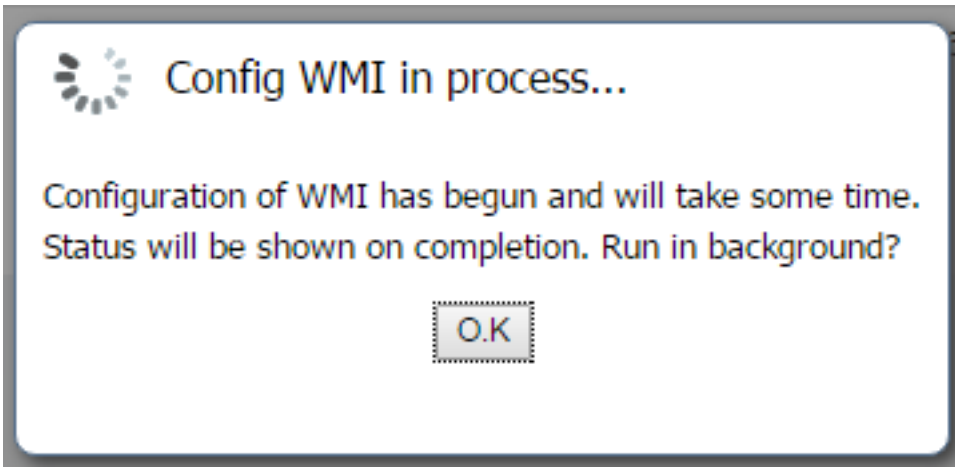
PassiveID Domain Controllers

1 Selected Rows/Page 1 / 1 Go 1 Total Rows

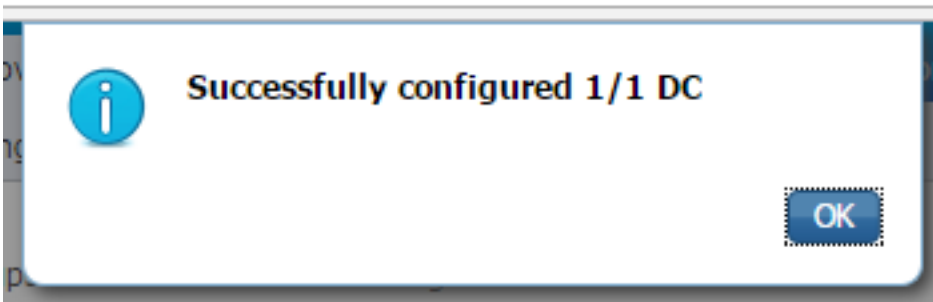
Refresh Edit Trash Add DCs Use Existing Agent **Config WMI** Add Agent

<input checked="" type="checkbox"/>	Domain	DC Host	Site	IP Address	Monitor Using
<input checked="" type="checkbox"/>	vkumov.local	MainDC.vkumov.local	Default-First-Site-Name	10.48.26.52	WMI

مدقتلا دي ق نيوكتلا ةيلمع نأ لىل ريشت ةلاس PIC ISE ضرعت:



مكحتلا تادحو ىلع حاجنب WMI نيوكت مت هنا اهدافم ةلاس رك رهظت ، ني تقي قد رورم دع ب
ةددم ل DC لاجم ل اب :



ةحصل ل نم ققحت ل

رشن ل

قرط ةدعب رشن ل ةل ا ح نم ققحت ل نكم ي :

رشن ل ةحفص

رشن ل ةل ا ح ل نم ققحت ل نكم ي رشن ل ةحفص > ةراد ل ل ل قتنا

This Node

Refresh

Role	Primary
IP Address	10.48.26.51
FQDN	ise22-pic-1.vkumov.local
Node Status	✔ Connected ⊕

Secondary Node

Deregister

Role	Secondary
IP Address	10.48.26.53
FQDN	ise22-pic-2.vkumov.local
Node Status	✔ Connected ⊕

Deployment Status

Registered : Thu Feb 23 2017 15:57:27 GMT+0100 (Central European Standard Time)

Sync Status : 0 messages to be synced.

نم ازمال ادب نكمي .رمأل مزل اذا ةيونال ةدقعال ليجست اغل نكمي ةحفصال هذه نم ةنم ازمال ةلاح نم ققحتال نكمي و ةيودال

تامول عمل ةحول ةحفص

اذه dashlet مادختساب .نكركرتشم يمسي dashlet كانه ةيسيئرل ISE PIC ةحفص يف ةروصلال يف حضوم وه امك ، ISE PIC دقل ةيلاال ةلاال نم ققحتال نكمي

SUBSCRIBERS



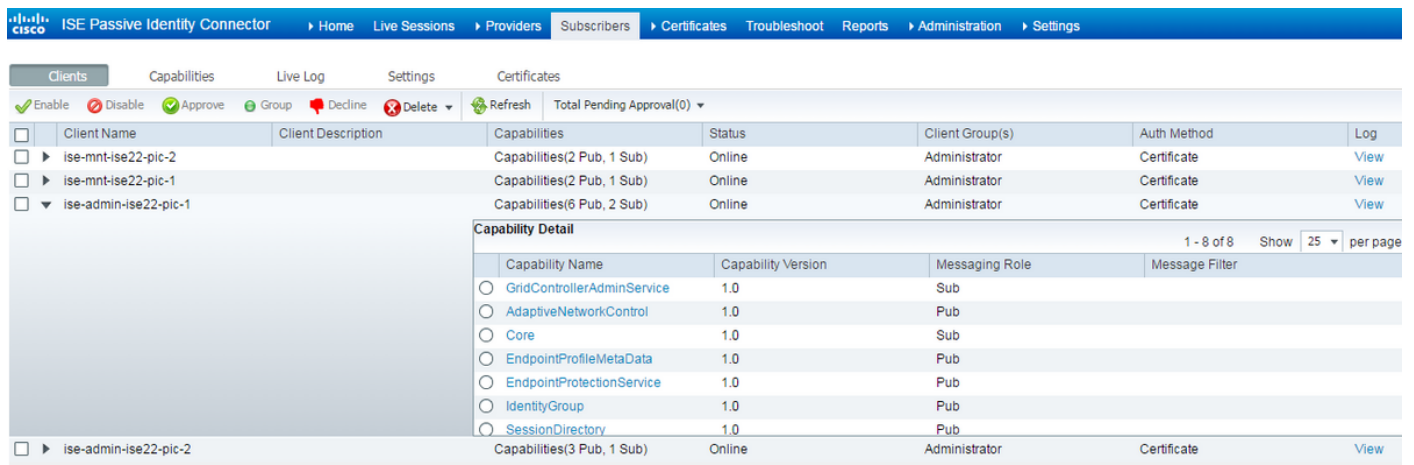
Name	Status	Description
<input type="text" value="Name"/>	<input type="text" value="Status"/>	<input type="text" value="Description"/>
ise-admin-ise22-pic-1	Online	
ise-admin-ise22-pic-2	Online	
ise-mnt-ise22-pic-1	Online	
ise-mnt-ise22-pic-2	Online	

Last refreshed: 2017-02-24 09:31:58

عضو يف اه عي مج نوكت نا بجي . admin وmnt - ةدق ع لك ل ني كرت شم ءاش ن اب ISE PIC موق ي اه لي غش ت و طي ش ن ت ل ل ة ل با ق دق ع ل نا ي ن ع ي ام م ل ص ت م

ان و ب ت ت م

ل ISE ل ة ي س ي ئ ر ل ا ة ح ف ص ل ل ا ن م ن ي ك ر ت ش م ل ل dashlet ن م ع س و م ر ا د ص ا ي ه ن ي ك ر ت ش م ل ا ة ح ف ص ل ISE PIC. دق ع ة ل ا ح ن م ق ق ح ت ل ل ن ك م ي ك ل ذ ع م و ، ة ل ص ل ل ا ت ا ذ PxGrid ع ي م ج ة ح ف ص ل ل ا ه ذ ه ر ه ط ت . ISE PIC ا ن ه ا ض ي ا ا ن ه :



Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method	Log
<input type="checkbox"/> ▶ ise-mnt-ise22-pic-2		Capabilities(2 Pub, 1 Sub)	Online	Administrator	Certificate	View
<input type="checkbox"/> ▶ ise-mnt-ise22-pic-1		Capabilities(2 Pub, 1 Sub)	Online	Administrator	Certificate	View
<input type="checkbox"/> ▼ ise-admin-ise22-pic-1		Capabilities(6 Pub, 2 Sub)	Online	Administrator	Certificate	View

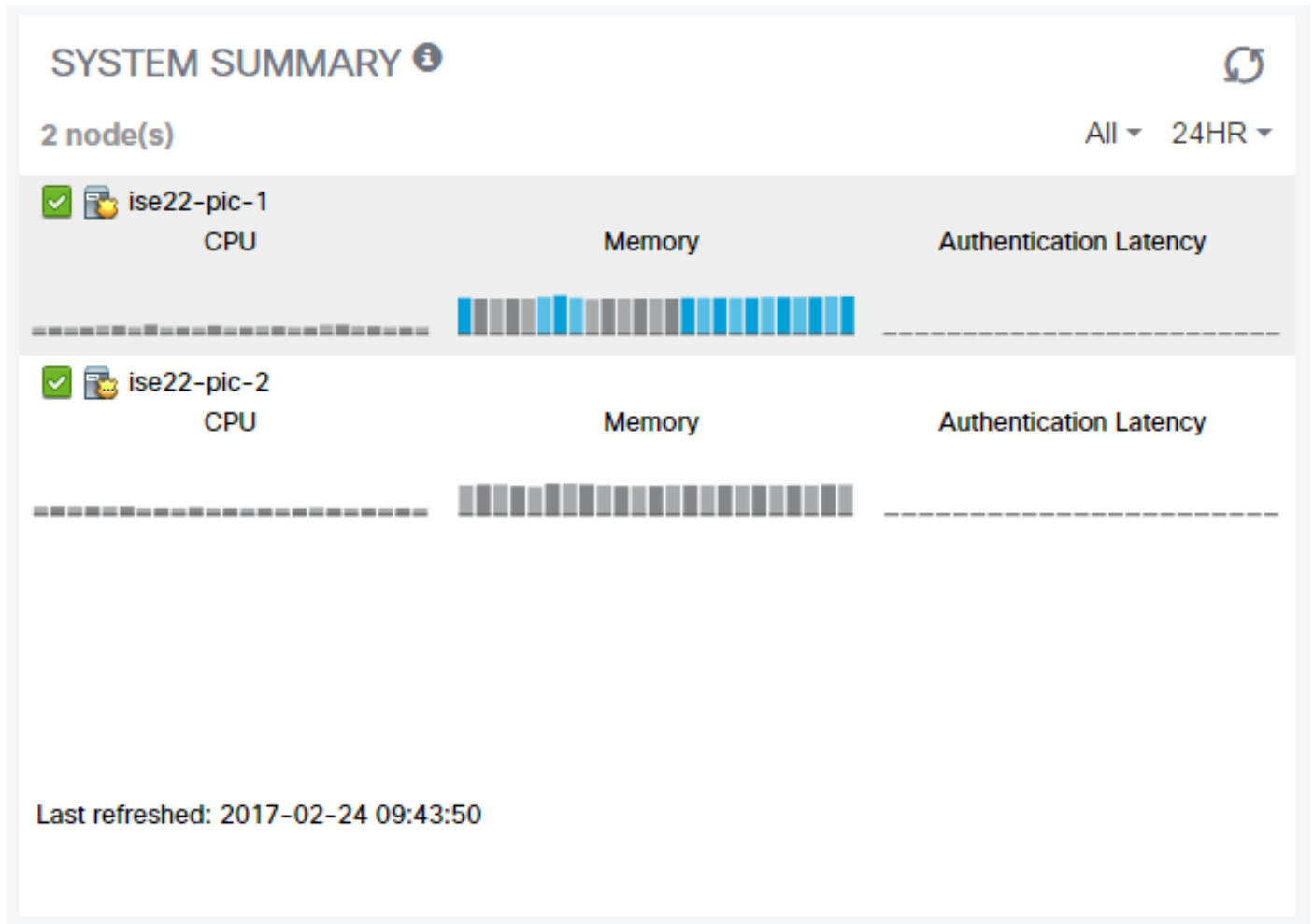
Capability Name	Capability Version	Messaging Role	Message Filter
<input type="radio"/> GridControllerAdminService	1.0	Sub	
<input type="radio"/> AdaptiveNetworkControl	1.0	Pub	
<input type="radio"/> Core	1.0	Sub	
<input type="radio"/> EndpointProfileMetaData	1.0	Pub	
<input type="radio"/> EndpointProtectionService	1.0	Pub	
<input type="radio"/> IdentityGroup	1.0	Pub	
<input type="radio"/> SessionDirectory	1.0	Pub	

<input type="checkbox"/> ▶ ise-admin-ise22-pic-2	Capabilities(3 Pub, 1 Sub)	Online	Administrator	Certificate	View
--------------------------------------------------	----------------------------	--------	---------------	-------------	----------------------

م ا ظ ن ل ا ص خ ل م

ي ف ا ذ ه dashlet ل ع ر و ث ع ل ا ن ك م ي . ك ل ذ ك د ق ع ل ل ة ي ا م ح ل ا ص خ ل م ة ب ق ا ر م ب ISE PIC ح م س ي

ي: فاضا | > تامولعمل ةحول > لزنملا



يأب موقوي ال ISE PIC نأ شيح 0ms ةقداصم لل لوصولا نمز نوكي ام امئاد
ل.يوقت/ةقداصم

تاسلجال او نورفوملا

ةيسيئرلا ةحفصل

اهيلع روثعلال متي لالعمل تاسلجال رادقم ومهتلامكو نيرفوملا تالاح نم ققحتلال نكمي
تامولعمل ةحول ةحفص > ةيسيئرلا ةحفصلال لال قننتالءانثأ

PASSIVE IDENTITY METRICS

Sessions ⓘ



1

Providers ⓘ

1

PROVIDERS ⓘ



Status	Name	Domain	Type	IP/Host	Agent
<input type="checkbox"/>	<input type="text" value="Name"/>	<input type="text" value="Domain"/>	<input type="text" value="Type"/>	<input type="text" value="IP/Host"/>	<input type="text" value="Agent"/>
<input checked="" type="checkbox"/>	MainDC.vkumov.lo...	vkumov.local	DC	MainDC.vkumov.lo...	WMI

ةرشابم لمع تاسلج

روثعال مت يتي الل نيمدختسمل لمع تاسلج عي مج لوح ةيلي صفت تامولعم يلع روثعال نكمي
 Live: لمع تاسلج ةحفص ي ف اه يلع

Initiated	Updated	Account S...	Action	Endpoint ID	Identity	IP Address	Server	Session Source	Provider	User Dom...	User NetBI...	AD User Resolved Id...
Feb 24, 2017 09:16:45:721 AM	Feb 24, 2017 09:16:45:721 AM	0 s	Show Actions	10.48.26.51	Administrator	10.48.26.51	ise22-pic-2	PassiveID	WMIEndPoint	vkumov/local	VKUMOV	Administrator@vkumov...

لثم تامولعم يلع يوتحي ووه:

- هذه لمعلا ةسلج فيرعتل مهم ادختسا مت نيذلا نورفوملا وه ام - رفوملا
- كلذل اقفو اهثي دحتو ةسلجال ادب دنع ةينمزل عباوطلا - اهثي دحتو ةسلجال ادب
- ةياهنلا ةطقن ناووع - IP ناووع
- ةلاح نم ققحتلا، لثملا ليلبس يلع اهذيفنت ISE ل نكمي يتي تاءارجال - عارجال

(ةس لجال حسم ل بلط لاس را م ث pxGrid عم ISE PIC جم د مت اذ ا و ا، ةياهن ل ا ةطقن

اه حال ص ا و ا ط خ ا ل فاش ك ت سا

رشن ل ا

هذه ل ج س ل ا ت ا ف ل م ي ف ث ح ب ا ، ا ه حال ص ا و ا ل ث ا م ت م ل ا خ س ن ل ل ا و ر ش ن ل ل ا ا ط خ ا فاش ك ت سا ل

- خ س ن ل ل ا ف ل م
- deployment.log
- ise-psc.log

ح ي ح ص ت ل ج س ن ي و ك ت > ل و خ د ل ا ل ي ج س ت > ة ر ا د ل ا ل ي ل ل ق ت ن ا ، ا ط خ ا ل ا ح ي ح ص ت ن ي ك م ت ل ا ط خ ا ل ا

Node List > ise22-pic-1.vkumov.local
Debug Level Configuration

Component Name	Log Level	Description
portal-web-action	INFO	Base Portal debug messages
posture	INFO	Posture debug messages
previewportal	INFO	Preview Portal debug messages
profiler	INFO	profiler debug messages
provisioning	INFO	Client Provisioning client debug messages
prrt-JNI	INFO	prrt policy decision request processing layer related messages
pxgrid	INFO	pxGrid messages
Replication-Deployment	DEBUG	Logger related to Deployment Registration, Deregistration, Sync and ...
Replication-JGroup	WARN	Logger related to JGroup Node State
ReplicationTracker	INFO	PSC replication related debug messages
report	INFO	Debug reports on M&T nodes
RuleEngine-Attributes	INFO	Additional rule evaluation attributes in audit logging at DEBUG
RuleEngine-Policy-IDGroups	INFO	Additional policy vs id group audit logging at DEBUG

ل ث ا م ت م خ س ن ة ي ل م ع ي ل ع ل ا ث م ي ل ي ا م ي ف . replication.log ف ل م ي ل ا ط خ ا ل ا هذه ة ب ا ت ك م ت ا ة ي د ا ع

```
2017-02-24 10:11:06,893 INFO [pool-215-thread-1][  
cisco.cpm.deployment.replication.PublisherImpl -::::- Calling the publisher job from  
clusterstate processor  
2017-02-24 10:11:06,893 DEBUG [pool-214-thread-1][  
cisco.cpm.deployment.replication.PublisherImpl -::::- Started executing publisher job  
2017-02-24 10:11:06,894 DEBUG [pool-214-thread-1][  
cisco.cpm.deployment.replication.PublisherImpl -::::- Number of messages with no sequence number  
is 0  
2017-02-24 10:11:06,894 DEBUG [pool-214-thread-1][  
cisco.cpm.deployment.replication.PublisherImpl -::::- Finished executing publisher job  
2017-02-24 10:11:06,895 DEBUG [pool-214-thread-1][  
api.services.persistence.dao.ChangeDataDaoImpl -::::- Data returned in getMinMaxBySequence  
method=[id=[63ce2fe0-f8cd-11e6-b0ad-005056991a2e],startTime=[0],endTime=[0],applied=[false],data  
length=[794],sequenceNumber=[502]2017-02-22 08:06:10.782]  
2017-02-24 10:11:06,895 DEBUG [pool-214-thread-1][  
api.services.persistence.dao.ChangeDataDaoImpl -::::- Data returned in getMinMaxBySequence
```

```

method=[id=[3ded93c0-fa70-11e6-b684-005056990fbb],startTime=[0],endTime=[0],applied=[false],data
length=[794],sequenceNumber=[1600]2017-02-24 10:04:26.364]
2017-02-24 10:11:06,895 DEBUG [pool-214-thread-1][]
cisco.cpm.deployment.replication.ClientNodeProxy -:::- Calling setClusterState(name: ise22-pic-
1, minSequence: 502, sequence: 1600, active: {ise22-pic-1-5015})
2017-02-24 10:11:06,896 INFO [pool-214-thread-1][]
cisco.cpm.deployment.replication.PublisherImpl -:::- Finished sending the clusterState !!!
2017-02-24 10:11:06,899 DEBUG [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:- MonitorJob starting
2017-02-24 10:11:06,901 DEBUG [pool-216-thread-1][]
cisco.cpm.deployment.replication.ClientNodeProxy -:::NodeStateMonitor:- Calling getNodeStates()
2017-02-24 10:11:06,904 INFO [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:- Nodes in
distrubution: {ise22-pic-2=nodeName: ise22-pic-2, status: SYNC COMPLETED, transientStatus: ,
lastStatusTime: 1487927436906, seqNumber: 1600, createTime: 2017-02-24 10:04:26.364} --- Nodes
in cluster: [name: ise22-pic-2, Address: ise22-pic-2-38077, sequence: 1600, createtime: 2017-02-
24 10:04:26.364]
2017-02-24 10:11:06,904 DEBUG [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:- Adding [ nodeName:
ise22-pic-2, status: SYNC COMPLETED, transientStatus: , lastStatusTime: 1487927436906,
seqNumber: 1600, createTime: 2017-02-24 10:04:26.364 ] to liveDeploymentMembers
2017-02-24 10:11:06,905 DEBUG [pool-216-thread-1][]
api.services.persistence.dao.ChangeDataDaoImpl -:::NodeStateMonitor:- Data returned in
getMinMaxBySequence method=[id=[63ce2fe0-f8cd-11e6-b0ad-
005056991a2e],startTime=[0],endTime=[0],applied=[false],data
length=[794],sequenceNumber=[502]2017-02-22 08:06:10.782]
2017-02-24 10:11:06,905 DEBUG [pool-216-thread-1][]
api.services.persistence.dao.ChangeDataDaoImpl -:::NodeStateMonitor:- Data returned in
getMinMaxBySequence method=[id=[3ded93c0-fa70-11e6-b684-
005056990fbb],startTime=[0],endTime=[0],applied=[false],data
length=[794],sequenceNumber=[1600]2017-02-24 10:04:26.364]
2017-02-24 10:11:06,905 INFO [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:- Primary node
current status minmum sequence[ 1600 ], cluster state: [ name: ise22-pic-1, minSequence: 502,
sequence: 1600, active: {ise22-pic-1-5015} ]
2017-02-24 10:11:06,905 DEBUG [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:- Processing node
state [ name: ise22-pic-2, Address: ise22-pic-2-38077, sequence: 1600, createtime:2017-02-24
10:04:26.364 ]
2017-02-24 10:11:06,905 DEBUG [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:- ise22-pic-2 - [
nodeName: ise22-pic-2, status: SYNC COMPLETED, transientStatus: , lastStatusTime: 1487927436906,
seqNumber: 1600, createTime: 2017-02-24 10:04:26.364 ]
2017-02-24 10:11:06,905 DEBUG [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:- Adding nodeName:
ise22-pic-2, status: SYNC COMPLETED, transientStatus: , lastStatusTime: 1487927436906,
seqNumber: 1600, createTime: 2017-02-24 10:04:26.364 to liveJGroupMembers
2017-02-24 10:11:06,905 INFO [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:- No Of
deployedNodes: [ 1 ], No Of liveJGroupNodes: [ 1 ], deadOrSyncInPrgMembersExist: [ false ],
latestMinSequence: [ 502 ]
2017-02-24 10:11:06,905 DEBUG [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:-
deadOrSyncInPrgMembersExist =[false], minSequence=[1598],clusterState=[502]

```

نم ةل اسر ise-psc.log:

```

2017-02-24 10:19:36,902 INFO [pool-216-thread-1][]
api.services.persistence.dao.DistributionDAO -:::NodeStateMonitor:- Host Name: ise22-pic-2, DB
'SEC_REPLICATIONSTATUS' = SYNC COMPLETED, Node Persona: SECONDARY, ReplicationStatus obj status:
SYNC_COMPLETED

```

غولبلل ةلباق ريغ ةيوناثلا ةدقعل: ةكرتشملا ةلكشملا

> ةرادلا ةحفص يف اهضرع متيسف ، حالصل ةلباق ريغ ةيوناثلا ةدقعل تحبصاً اذا
رشنلا:

Deployment Licensing ▶ Logging ▶ Maintenance ▶ Admin Access

This Node

Refresh

Role	Primary
IP Address	10.48.26.51
FQDN	ise22-pic-1.vkumov.local
Node Status	✔ Connected ⊕

Secondary Node

Role	Secondary
IP Address	10.48.26.53
FQDN	ise22-pic-2.vkumov.local
Node Status	✘ Disconnected ⊕

Deployment Status

Registered : Thu Feb 23 2017 15:57:27 GMT+0100 (Central European Standard Time)

Sync Status : Node not reachable
since : Fri Feb 24 2017 10:27:36 GMT+0100 (Central European Standard Time)

ةلاسرلا هذه ىل ع ISE-psc.log يوتحي:

```
2017-02-24 10:43:21,587 INFO [admin-http-pool155][  
admin.restui.features.deployment.DeploymentIDCUIApi -:::- Replication status for node ise22-  
pic-2 = NODE NOT REACHABLE
```

ىل ةدقعل بيجتست ال لاثملا لىبس ىلع ، هيل لوصولنا نكمي ال ام ةلاسرلا هذه حضوت
ping:

```
2017-02-24 11:03:53,359 INFO [counterscheduler-call-1][  
cisco.cpm.infrastructure.utils.GenericUtil -:::- Received pingNode response : Node is reachable
```

نم ققحت ، ةيوناثلا ةدقعل ل FQDN ل ةيونانكم نم ققحتلا: اهاختا بيجي يتلا تاءارجلا
دقعل نيب نيب ساسالا ةكبشلا لاصتا

نيب ةيامح رادج دوجو ةلاح يف و ةيوناثلا ةدقعل يف تاقيبطتلا ليغشت مدع ةلاح يف
ةيلاتلا لئاسرلا ISE-psc.log ضرعي دق ، دقعل

```

2017-02-24 11:08:14,656 INFO [Thread-10][] com.cisco.epm.util.NodeCheck -::::- Now checking
against secondary pap ise22-pic-2
2017-02-24 11:08:14,656 INFO [Thread-10][] com.cisco.epm.util.NodeCheckHelper -::::- inside
getHostConfigRemoteServer
2017-02-24 11:08:14,766 WARN [Thread-10][]
deployment.client.cert.validator.HttpsCertPathValidatorImpl -::::- Error while connecting to
host: ise22-pic-2.vkumov.local. java.net.ConnectException: Connection refused
2017-02-24 11:08:14,871 WARN [Thread-10][] com.cisco.epm.util.NodeCheckHelper -::::- Unable to
retrieve the host config from standby pap java.net.ConnectException: Connection refused
2017-02-24 11:08:14,871 WARN [Thread-10][] com.cisco.epm.util.NodeCheckHelper -::::- returning
null from getHostConfigRemoteServer
2017-02-24 11:08:14,871 INFO [Thread-10][] com.cisco.epm.util.NodeCheck -::::-
remotePrimaryConfig.getNodeRoleStatus() NULL
2017-02-24 11:08:14,871 INFO [Thread-10][] com.cisco.epm.util.NodeCheck -::::-
remoteClusterInfo.getDeploymentName NULL

```

لاصتا نم ققحت، ةيونالثا ةدقعل الى ع قيبطتلا ةلاح نم ققحت: اذاخا بتا ي تال تاءارال
دقعل ن بتا لاصتالا عي مجب حمسي ناك اذا ةكبشلا

Active Directory و WMI

تافلملا هذه في ثحبا، اءالاص او WMI Active Directory ءاطخا فاشكتسا

- passive-wmi.log
- passive-endpoint.log
- ise-psc.log
- ad_agent.log

ءاطخالا لفس نيوكت > لوخدلا لفسست > ةرادالا في فديفملا ءاطخالا حيحصت نيكمت نكميو

Deployment Licensing Logging Maintenance Admin Access

Local Log Settings Debug Log Configuration Download Logs

Node List > ise22-pic-2.vkumov.local Debug Level Configuration

Edit Reset to Default

Component Name	Log Level	Description
<input type="radio"/> org-apache-cxf	WARN	CXF messages
<input type="radio"/> org-apache-digester	WARN	XML processing apache internal messages
<input type="radio"/> PanFailover	INFO	Pap Failover related messages
<input type="radio"/> PassiveID	DEBUG	PassiveID events and messages
<input type="radio"/> policy-engine	INFO	Policy Engine 2.0 related messages
<input type="radio"/> portal	INFO	Portal (Guest, Hotspot, BYOD, CP) debug messages

و:

<input type="radio"/> Active Directory	DEBUG	Active Directory client internal messages
----------------------------------------	-------	-------------------------------------------

ءاطخالا حيحصت نيكمت عم passive-wmi.log نم ةسلج ملعي فديج نم لاثم انه

```
2017-02-24 11:36:22,584 DEBUG [Thread-11][ ] com.cisco.idc.dc-probe- New login event retrieved from Domain Controller. Identity Mapping.ticket = instance of __InstanceCreationEvent { SECURITY_DESCRIPTOR = {1, 0, 20, 128, 96, 0, 0, 0, 112, 0, 0, 0, 0, 0, 20, 0, 0, 0, 2, 0, 76, 0, 3, 0, 0, 0, 0, 20, 0, 69, 0, 15, 0, 1, 1, 0, 0, 0, 0, 0, 5, 18, 0, 0, 0, 0, 24, 0, 69, 0, 0, 0, 1, 2, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0, 0, 0, 24, 0, 65, 0, 0, 0, 1, 2, 0, 0, 0, 0, 5, 32, 0, 0, 0, 61, 2, 0, 0, 1, 2, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0, 1, 1, 0, 0, 0, 0, 5, 18, 0, 0, 0}; TargetInstance = instance of Win32_NTLogEvent { Category = 14339; CategoryString = "Kerberos Authentication Service"; ComputerName = "MainDC.vkumov.local"; EventCode = 4768; EventIdentifier = 4768; EventType = 4; InsertionStrings = {"Administrator", "vkumov.local", "S-1-5-21-2952046201-2792970045-1866348404-500", "krbtgt", "S-1-5-21-2952046201-2792970045-1866348404-502", "0x40810010", "0x0", "0x12", "2", ":", "0", "", "", ""}; Logfile = "Security"; Message = "A Kerberos authentication ticket (TGT) was requested. \n \nAccount Information: \n\tAccount Name:\tAdministrator \n\tSupplied Realm Name:\tvkumov.local \n\tUser ID:\t\t\tS-1-5-21-2952046201-2792970045-1866348404-500 \n \nService Information: \n\tService Name:\t\tkrbtgt \n\tService ID:\t\t\tS-1-5-21-2952046201-2792970045-1866348404-502 \n \nNetwork Information: \n\tClient Address:\t\t:1 \n\tClient Port:\t\t0 \n \nAdditional Information: \n\tTicket Options:\t\t0x40810010 \n\tResult Code:\t\t0x0 \n\tTicket Encryption Type:\t0x12 \n\tPre-Authentication Type:\t2 \n \nCertificate Information: \n\tCertificate Issuer Name:\t\t \n\tCertificate Serial Number:\t \n\tCertificate Thumbprint:\t\t \n \nCertificate information is only provided if a certificate was used for pre-authentication. \n \nPre-authentication types, ticket options, encryption types and result codes are defined in RFC 4120."; RecordNumber = 918032; SourceName = "Microsoft-Windows-Security-Auditing"; TimeGenerated = "20170224103621.575178-000"; TimeWritten = "20170224103621.575178-000"; Type = "Audit Success"; }; TIME_CREATED = "131324061825752057"; }, Identity Mapping.dc-domainname = vkumov.local , Identity Mapping.dc-connection-type = Current events , Identity Mapping.dc-name = MainDC.vkumov.local , Identity Mapping.dc-host =
```



```
MainDC.vkumov.local/10.48.26.52 ,
2017-02-24 11:36:22,587 DEBUG [Thread-11][] com.cisco.idc.dc-probe- Replaced local IP. Identity
Mapping.ticket =
instance of __InstanceCreationEvent
{
SECURITY_DESCRIPTOR = {1, 0, 20, 128, 96, 0, 0, 0, 112, 0, 0, 0, 0, 0, 0, 20, 0, 0, 0, 2, 0,
76, 0, 3, 0, 0, 0, 0, 0, 20, 0, 69, 0, 15, 0, 1, 1, 0, 0, 0, 0, 0, 5, 18, 0, 0, 0, 0, 24, 0,
69, 0, 0, 0, 1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0, 0, 0, 24, 0, 65, 0, 0, 0, 1, 2,
0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 61, 2, 0, 0, 1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0, 1,
1, 0, 0, 0, 0, 0, 5, 18, 0, 0, 0};
TargetInstance =
instance of Win32_NTLogEvent
{
Category = 14339;
CategoryString = "Kerberos Authentication Service";
ComputerName = "MainDC.vkumov.local";
EventCode = 4768;
EventIdentifier = 4768;
EventType = 4;
InsertionStrings = {"Administrator", "vkumov.local", "S-1-5-21-2952046201-2792970045-1866348404-
500", "krbtgt", "S-1-5-21-2952046201-2792970045-1866348404-502", "0x40810010", "0x0", "0x12",
"2", ":", "0", "", "", ""};
Logfile = "Security";
Message = "A Kerberos authentication ticket (TGT) was requested.
\n
\nAccount Information:
\n\tAccount Name:\t\tAdministrator
\n\tSupplied Realm Name:\tkumov.local
\n\tUser ID:\t\t\tS-1-5-21-2952046201-2792970045-1866348404-500
\n
\nService Information:
\n\tService Name:\tkrbtgt
\n\tService ID:\t\tS-1-5-21-2952046201-2792970045-1866348404-502
\n
\nNetwork Information:
\n\tClient Address:\t\t::1
\n\tClient Port:\t\t0
\n
\nAdditional Information:
\n\tTicket Options:\t\t0x40810010
\n\tResult Code:\t\t0x0
\n\tTicket Encryption Type:\t0x12
\n\tPre-Authentication Type:\t2
\n
\nCertificate Information:
\n\tCertificate Issuer Name:\t\t
\n\tCertificate Serial Number:\t
\n\tCertificate Thumbprint:\t\t
\n
\nCertificate information is only provided if a certificate was used for pre-authentication.
\n
\nPre-authentication types, ticket options, encryption types and result codes are defined in RFC
4120.";
RecordNumber = 918032;
SourceName = "Microsoft-Windows-Security-Auditing";
TimeGenerated = "20170224103621.575178-000";
TimeWritten = "20170224103621.575178-000";
Type = "Audit Success";
};
TIME_CREATED = "131324061825752057";
};
, Identity Mapping.dc-domainname = vkumov.local , Identity Mapping.dc-connection-type = Current
events , Identity Mapping.probe = WMI , Identity Mapping.event-local-ip-address = ::1 , Identity
Mapping.dc-name = MainDC.vkumov.local , Identity Mapping.dc-host =
```

```
MainDC.vkumov.local/10.48.26.52 , Identity Mapping.server = ise22-pic-2 , Identity
Mapping.event-ip-address = 10.48.26.52 ,
2017-02-24 11:36:22,589 DEBUG [Thread-11][] com.cisco.idc.dc-probe- Received login event.
Identity Mapping.ticket =
instance of __InstanceCreationEvent
{
SECURITY_DESCRIPTOR = {1, 0, 20, 128, 96, 0, 0, 0, 112, 0, 0, 0, 0, 0, 20, 0, 0, 0, 2, 0,
76, 0, 3, 0, 0, 0, 0, 0, 20, 0, 69, 0, 15, 0, 1, 1, 0, 0, 0, 0, 5, 18, 0, 0, 0, 0, 24, 0,
69, 0, 0, 0, 1, 2, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0, 0, 0, 24, 0, 65, 0, 0, 0, 1, 2,
0, 0, 0, 0, 5, 32, 0, 0, 0, 61, 2, 0, 0, 1, 2, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0, 1,
1, 0, 0, 0, 0, 5, 18, 0, 0, 0};
TargetInstance =
instance of Win32_NTLogEvent
{
Category = 14339;
CategoryString = "Kerberos Authentication Service";
ComputerName = "MainDC.vkumov.local";
EventCode = 4768;
EventIdentifier = 4768;
EventType = 4;
InsertionStrings = {"Administrator", "vkumov.local", "S-1-5-21-2952046201-2792970045-1866348404-
500", "krbtgt", "S-1-5-21-2952046201-2792970045-1866348404-502", "0x40810010", "0x0", "0x12",
"2", ":", "0", "", "", ""};
Logfile = "Security";
Message = "A Kerberos authentication ticket (TGT) was requested.
\n
\nAccount Information:
\n\tAccount Name:\t\tAdministrator
\n\tSupplied Realm Name:\tkumov.local
\n\tUser ID:\t\t\tS-1-5-21-2952046201-2792970045-1866348404-500
\n
\nService Information:
\n\tService Name:\tkrbtgt
\n\tService ID:\t\tS-1-5-21-2952046201-2792970045-1866348404-502
\n
\nNetwork Information:
\n\tClient Address:\t\t::1
\n\tClient Port:\t\t0
\n
\nAdditional Information:
\n\tTicket Options:\t\t0x40810010
\n\tResult Code:\t\t0x0
\n\tTicket Encryption Type:\t0x12
\n\tPre-Authentication Type:\t2
\n
\nCertificate Information:
\n\tCertificate Issuer Name:\t\t
\n\tCertificate Serial Number:\t
\n\tCertificate Thumbprint:\t\t
\n
\nCertificate information is only provided if a certificate was used for pre-authentication.
\n
\nPre-authentication types, ticket options, encryption types and result codes are defined in RFC
4120.";
RecordNumber = 918032;
SourceName = "Microsoft-Windows-Security-Auditing";
TimeGenerated = "20170224103621.575178-000";
TimeWritten = "20170224103621.575178-000";
Type = "Audit Success";
};
TIME_CREATED = "131324061825752057";
};
, Identity Mapping.dc-domainname = vkumov.local , Identity Mapping.dc-connection-type = Current
events , Identity Mapping.probe = WMI , Identity Mapping.event-local-ip-address = ::1 , Identity
```

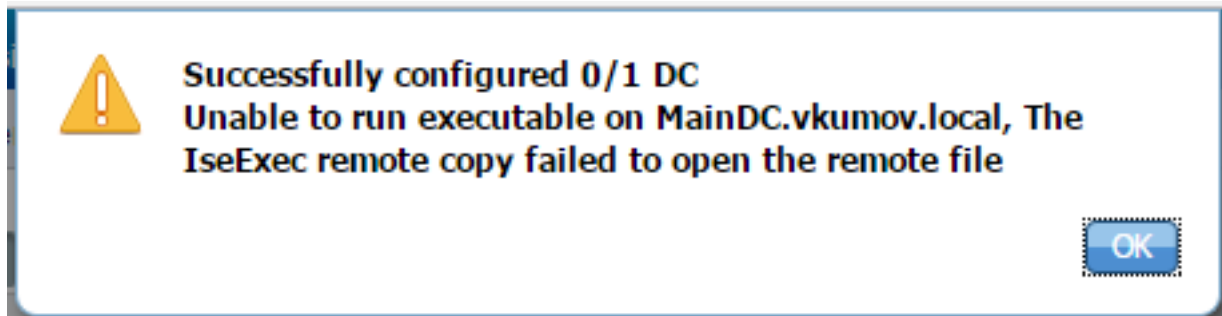
Mapping.dc-name = MainDC.vkumov.local , Identity Mapping.event-user-name = Administrator ,
Identity Mapping.dc-host = MainDC.vkumov.local/10.48.26.52 , Identity Mapping.server = ise22-
pic-2 , Identity Mapping.event-ip-address = 10.48.26.52 ,

عطقن تناك ةلأل هذه في) **passive-endpoint.log** نم ةياهنل ةطقن نم ققحتل لىل ةلأل
(ISE) نم اهلل لوصولل نكمي ال ةياهنل:

```
2017-02-23 13:48:29,298 INFO [EndPointProbe-Workers-Check-2][] com.cisco.idc.endpoint-probe-  
[Psexec-10.48.26.51] is User=vkumov.local/Administrator Still There ? ...  
2017-02-23 13:48:32,335 INFO [EndPointProbe-Workers-Check-2][] com.cisco.idc.endpoint-probe-  
[Psexec-10.48.26.51] Identity check result is - > Endpoint UNREACHABLE
```

"<DC name>... لىل ةذيفننل لملل لىل ةغشت رذعتي" اطح يمرت ISE PIC: ةعئاش ةلكشم

إلأل ISE PIC ةقابط لىل مامضنل ل مدختسمل مدختسمل مدختسمل لىل نكي مل إذا
WMI: نىوكت ءانثا اطح ي قتل ISE PIC ةقابط نإف، ةيفال تانوذال



ىوتسم نىيغت بىج) **ad_agent.log** فلم في ةبس انملا ءاطخال اىحصت لىل ةرولل نكمي
(ءاطخال اىحصت لىل Active Directory لىل):

```
26/02/2017 19:15:45,VERBOSE,139954093012736,SMBGSSContextNegotiate: state =  
1,lwio/server/smbcommon/smbkrb5.c:460  
26/02/2017 19:15:45,VERBOSE,139956055955200,Session 0x7f49bc001430 is eligible for  
reaping,lwio/server/rdr/session2.c:290  
26/02/2017 19:15:45,VERBOSE,139954101405440,Error at ../../lsass/server/auth-providers/ad-open-  
provider/provider-main.c:7503 [code: C0000022],lsass/server/auth-providers/ad-open-  
provider/provider-main.c:7503  
26/02/2017 19:15:45,VERBOSE,139954101405440,Extended Error code: 60190 (symbol:  
LW_ERROR_ISEEXEC_CP_OPEN_REMOTE_FILE),lsass/server/auth-providers/ad-open-provider/provider-  
main.c:7627  
26/02/2017 19:15:45,VERBOSE,139954101405440,Error at ../../lsass/server/auth-providers/ad-open-  
provider/provider-main.c:7628 [code: C0000022],lsass/server/auth-providers/ad-open-  
provider/provider-main.c:7628  
26/02/2017 19:15:45,VERBOSE,139954101405440,Error code: 5 (symbol:  
ERROR_ACCESS_DENIED),lsass/server/auth-providers/ad-open-provider/provider-main.c:7782  
26/02/2017 19:15:45,VERBOSE,139954101405440,Error code: 5 (symbol:  
ERROR_ACCESS_DENIED),lsass/server/auth-providers/ad-open-provider/provider-main.c:7855  
26/02/2017 19:15:45,VERBOSE,139954101405440,Error code: 5 (symbol:  
ERROR_ACCESS_DENIED),lsass/server/api/api2.c:2713  
26/02/2017 19:15:45,VERBOSE,139956064347904,(session:ee880a4e15e682f4-08401b84f371a140)  
Dropping: LWMSG_STATUS_PEER_CLOSE,lwmsg/src/peer-task.c:625  
26/02/2017 19:15:50,VERBOSE,139956055955200,RdrSocketRelease(0x7f496800b6e0, 38): socket is  
eligible for reaping,lwio/server/rdr/socket.c:2239
```

تاناي ب مادختس اب لأل ISE PIC ةق لىل مامضنل ءاع: اءاختل بىج يتل ءاءارل
لىل مامضنل ءللم عمل مدختسمل مدختسمل مدختسمل ءافاضل وأ لأل لىل لىل ءامتم
AD. في لأل لىل لىل ءومم

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسمل اذ ه Cisco ت مچرت
ملاعلاء ان ا عي مچ ي ف ن ي م دخت سمل ل معد ي و تح م مي دقت ل ة ي رش ب ل و
امك ة ق ي قد ن و ك ت ن ل ة ي ل ة مچرت ل ض ف ا ن ا ة ظ حال م ي ج ر ي . ة ص ا خ ل 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 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 (رف و ت م ط بار ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن تسمل ا