

زاهجلل يئانثلا لماعلا ةقداصم نيوكت بلطتملا ىلا لوصولل

تايوتحملا

[ةمدقملا](#)

[ةيساس الابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةكبش ليل يطيخ تلامس رلا](#)

[ةيساس ا تامولعم](#)

[تان نيوكتلا](#)

[C1000 ي ف نيوكتلا](#)

[Windows رتوي بيمك ي ف نيوكتلا](#)

[AD لاجملا رتوي بيمك ةفاضلا 1 ةوطخل](#)

[مدختسملا ةقداصم نيوكت 2 ةوطخل](#)

[Windows مداخ ي ف نيوكتلا](#)

[لاجملا رتوي بيمك ةزهجأ ديكأت 1 ةوطخل](#)

[لاجم مدختسم ةفاضلا 2 ةوطخل](#)

[ISE ي ف نيوكتلا](#)

[زاهج ةفاضلا 1 ةوطخل](#)

[Active Directory ةفاضلا 2 ةوطخل](#)

[زاهجلا ةقداصم دادعلا ديكأت 3 ةوطخل](#)

[ةي وهلا رخصم تاليس لسنت ةفاضلا 4 ةوطخل](#)

[لي وختلا في رعت فلمو DACL ةفاضلا 5 ةوطخل](#)

[جهن ةعومجم ةفاضلا 6 ةوطخل](#)

[ةقداصملا جهن ةفاضلا 7 ةوطخل](#)

[لي وختلا جهن ةفاضلا 8 ةوطخل](#)

[ةحصلا نم ققحتلا](#)

[مدختسملا ةقداصم و زاهجلا ةقداصم 1 طمنلا](#)

[Windows PC نم جورخل لي جسنت 1 ةوطخل](#)

[ةقداصملا لمع ةس لج ديكأت 2 ةوطخل](#)

[Windows PC لوخد لي جسنت 3 ةوطخل](#)

[ةقداصملا لمع ةس لج ديكأت 4 ةوطخل](#)

[Radius Live ل جس ديكأت 5 ةوطخل](#)

[طقف مدختسملا ةقداصم 2 طمنلا](#)

[Windows PC نم NIC ني كمت ولي طعت 1 ةوطخل](#)

[ةقداصملا لمع ةس لج ديكأت 2 ةوطخل](#)

[Radius Live ل جس ديكأت 3 ةوطخل](#)

[اهخالص او عا طخال فاش كتسا](#)

[قلص تاذا تامولعم](#)

ةمدقملا

مادختساب لم اوعلا ةيئانث ةقداصم نيوكتل ةبولطملا تاوطخلا دنتسملا اذه فصوي
dot1x و زاهلا ةقداصم

ةيساسال تابلطملا

تابلطملا

ةيلال عيضاوملاب ةفرعم كيديل نوكت نأب Cisco ي صوت:

- Cisco نم ةيوهلا تامدخ كرحم نيوكت
- Cisco Catalyst نيوكت
- IEEE802.1x رايعملا

ةمدختسملا تانوكملا

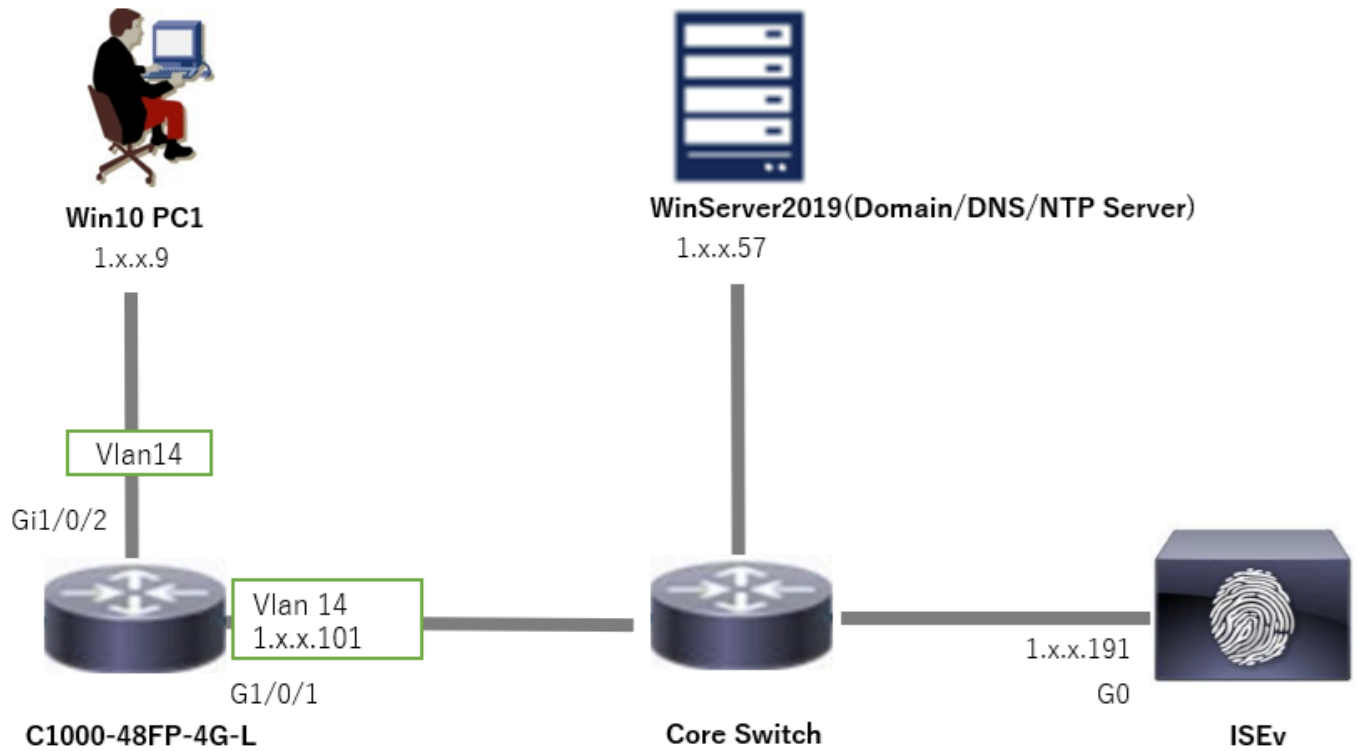
- Identity Services Engine Virtual 3.3 جحصتلا 1
- C1000-48FP-4G-L 15.2(7)E9
- Windows Server 2019 ليغشتلا ماظن

ةصاخ ةيلمعم ةئييب يف ةدوجوملا ةزهجالا نم دنتسملا اذه يف ةدراولا تامولعمل اءاشنإ مت
تناك اذإ. (يضاارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسملا ةزهجالا عيجم تادب
رمأ يأل لم تحملا ريثأتلل كمهف نم دكأتف، ليغشتلا دي قكتكبش

ةكبش ل ليطي طختلا مسرلا

دنتسملا اذه لاثمل همادختسا متي يذلا ططخملا ةروصل اذه ضرعت

متي يذلا او، ad.rem-xxx.com وه Windows Server 2019 ل ع هنيوكت مت يذلا لاجملا مسا
دنتسملا اذه يف لاثمك همادختسا



ةكبش ل ل يطي طختال مسرلا

ةيساسأ تامولعم

وأ ةكبش ل ل لوصولل عسي يذلا زاهجلا ةيوه نم ققحتت نيأت ةيلمع يه زاهجلا ةقداصم تانايب ل ل عءانب صخشلا ةيوه نم ققحتت يتلا، مدختسملا ةقداصم سكع ل ل ع. ماظن زاهجلا ةحص نم ققحتل ل ل ع زاهجلا ةقداصم زكرت، رورملا ةملاك و مدختسملا مسا ل ل ثم دامتعالا يتلا نامأل احي تافم وأ ةيمقرلا تاداهشلا مادختساب ك لذب ماي قلا م تي ام ابلاغو. هسفن زاهجل ةديرف نوكت

ةينامك ا نامض ةسسؤم ل ل نكمي، اعم مدختسملا ةقداصم و ةيالآ ةقداصملا مادختساب و ريفوت يلاتلاب و، طقف ني دمتم عملال ني مدختسملا و ةزهجال ل ل ل خ نم اهتكبش ل ل ل وصولا ةيامحل صاخ لكشب ةديفم هذه ل ماولا ةيئانث ةقداصملا ةقيرط دع و. انام ارثأ ةئي ب ةمراصلال ةيميظنتلا ريفياعم ل ل ل ل ا ل ا ل ا و ةساسحلل تامولعملال

تانيوكتال

ال C1000 في نيوكتال

ال C1000 CLI في نيوكتال ل ل ل ن دأل ا دحل و ه اذ

```
aaa new-model
```

```
radius server ISE33
address ipv4 1.x.x.191
key cisco123
```

aaa group server radius AAASERVER
server name ISE33

aaa authentication dot1x default group AAASERVER
aaa authorization network default group AAASERVER
aaa accounting dot1x default start-stop group AAASERVER
dot1x system-auth-control

interface Vlan14
ip address 1.x.x.101 255.0.0.0

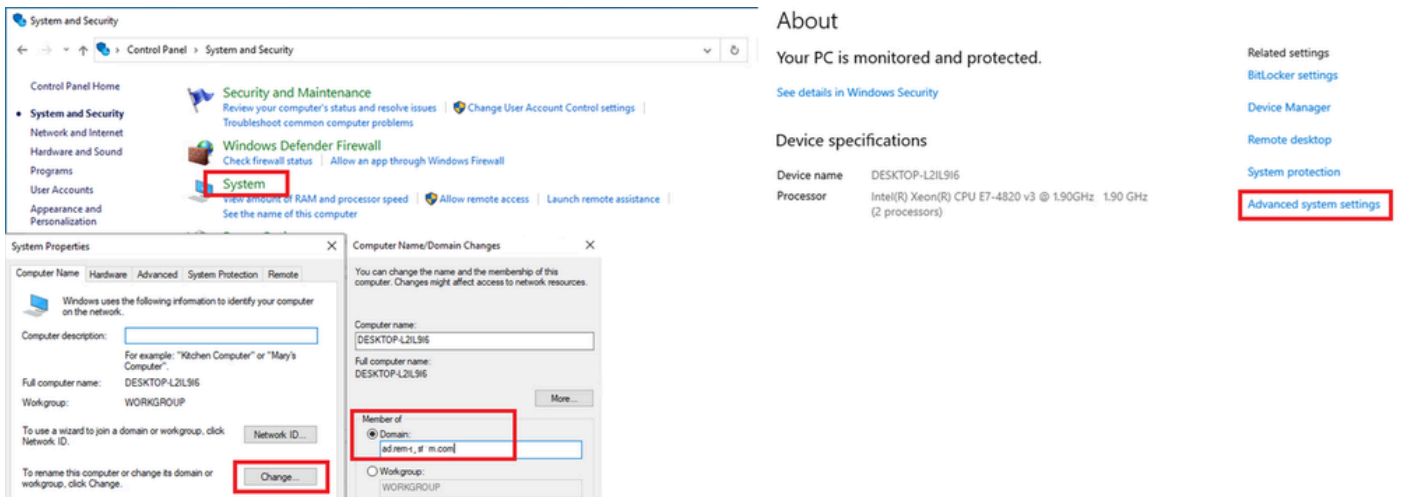
interface GigabitEthernet1/0/1
switchport access vlan 14
switchport mode access

interface GigabitEthernet1/0/2
switchport access vlan 14
switchport mode access
authentication host-mode multi-auth
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge

Windows رتوي بمك في نيوكتال

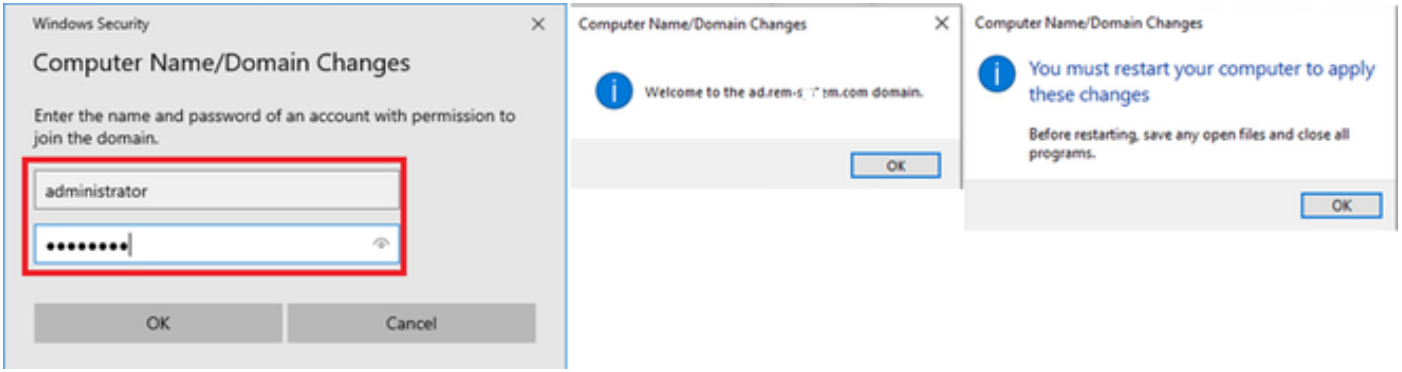
AD لاجم الى رتوي بمك ةفاض 1. ةوطخل

ماظنل تاداعل قوف رقنا م، ماظنل قوف رقنا و، نامال او ماظنل > مكحتل ةحول الى لقتنا لاجم ل مسا لخد او لاجم ل دح م، ريغت قوف رقنا، "ماظنل صئاصخ" راطل في. ةمدقتم ل



AD لاجم الى رتوي بمك ةفاض

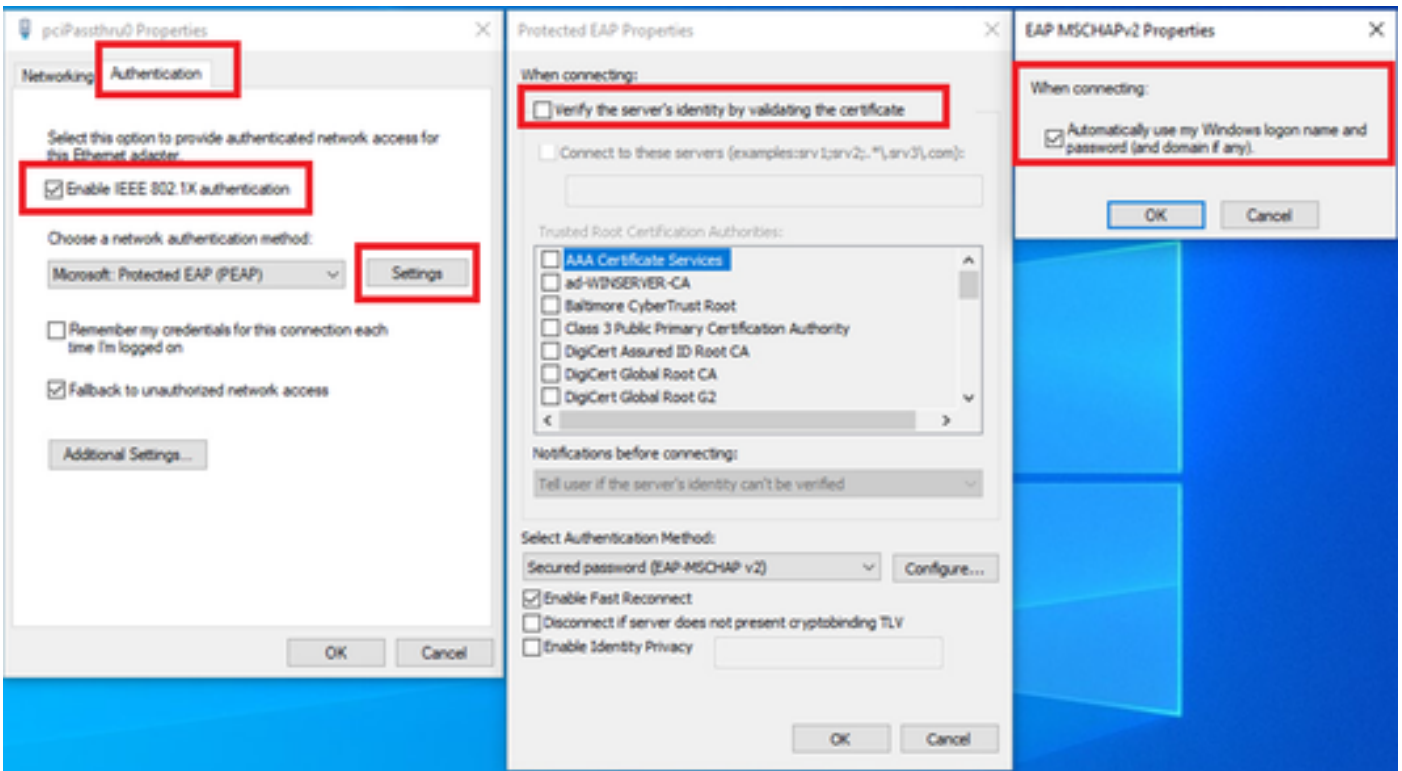
لاجم ل مداخل رورم ةملك و لاخلال مدختسم مسا، "Windows نام" ةذفان في



رورم ةم لك و مدخت سمل مس لاخدا

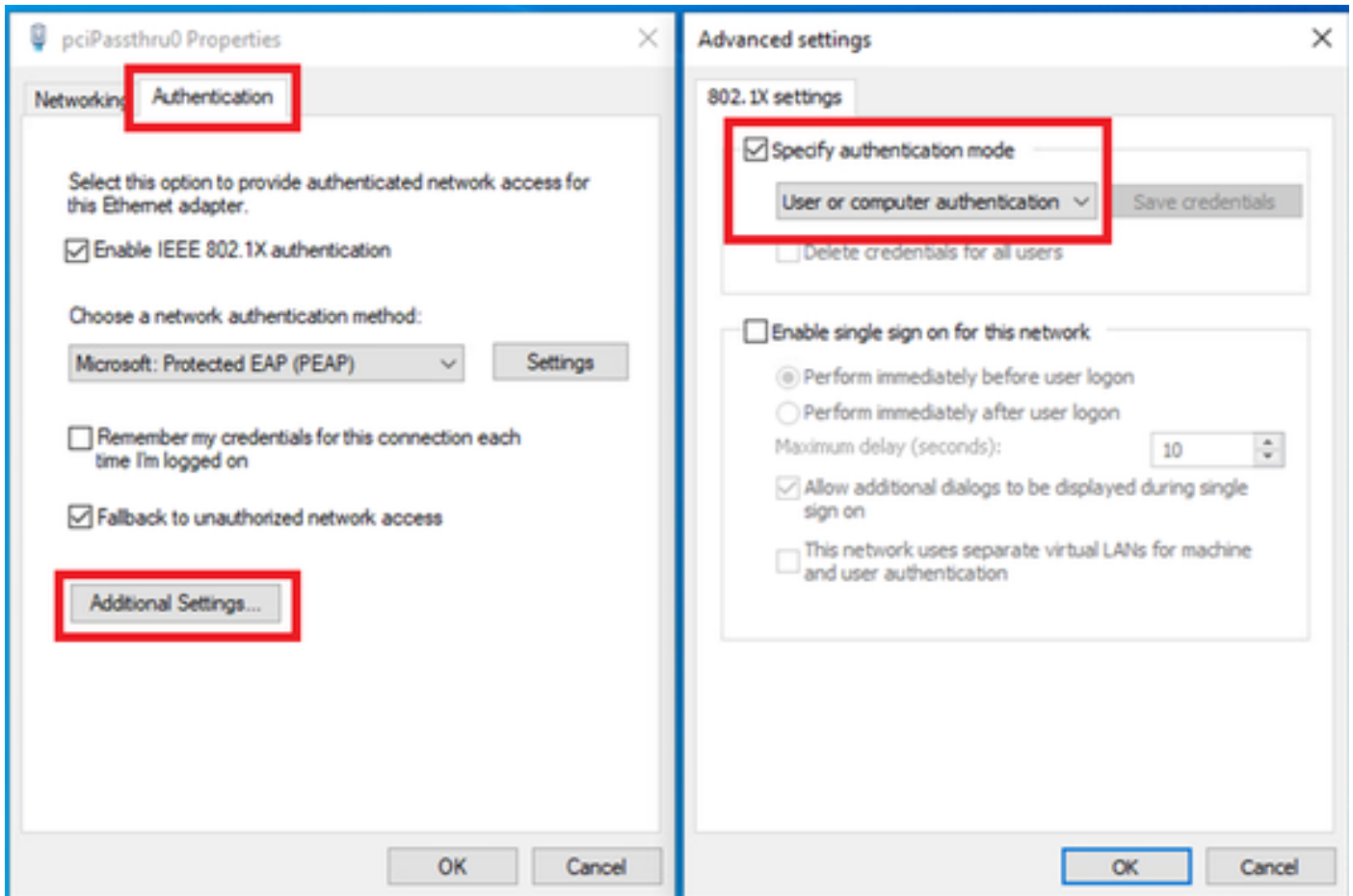
مدخت سمل ةقدا صم ني وكت 2. ةوطخل

ةذفان يف تادادع اىل ع رقنا IEEE 802.1X ةقدا صم ني كمت نم ققحت ،ةقدا صم اىل لقتنا ةداهشلا ةحص نم ققحتلاب مداخل ةي وه نم ققحتلا ديحت باغل اب مق ،ةي محمل EAP صئاصخ رورم ةم لك و مس ما دخت سمل نم ققحت ،EAP MSCHAPv2 صئاصخ راط ا يف .ني وكت اىل ع رقنا م مت يذل مدخت سمل مس ما دخت سمل (دج و ن ا ل اجم ل او) اىل اقل ل Windows اىل لوخذل ليجست مدخت سمل ةقدا صم ل Windows زاهج لوخذ ليجست انا ثا هلاخدا .



مدخت سمل ةقدا صم ني كمت

رتوي بمكلا و مدخت سمل ةقدا صم دح .ةي فاض اىل ا تادادع اىل نم ققحت ،ةقدا صم اىل لقتنا ةلدس نمل ةم اقل ا نم .

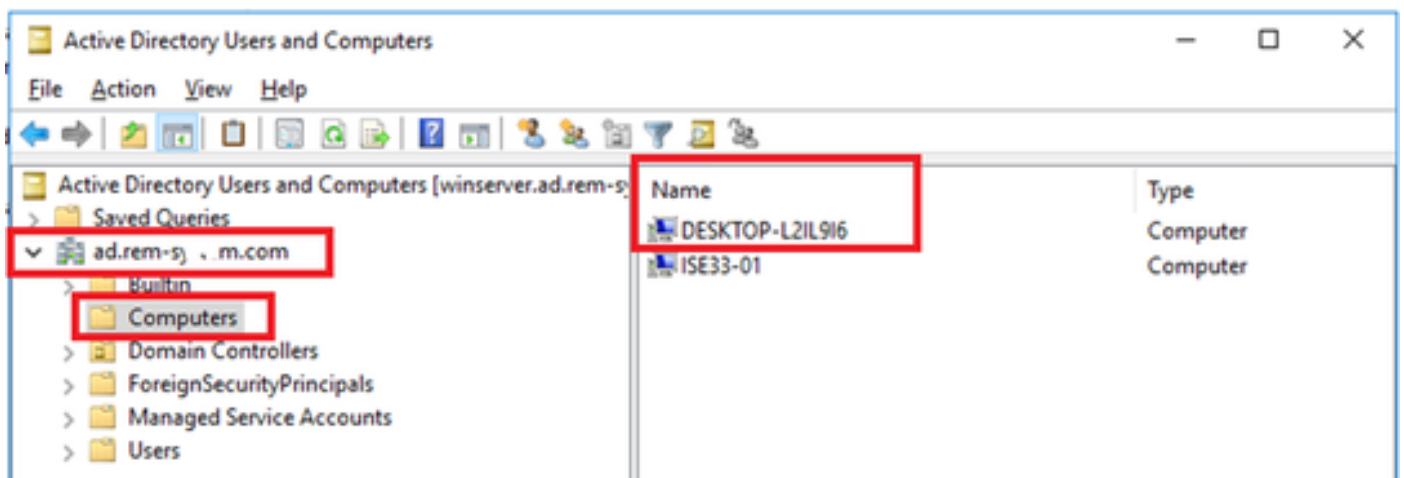


ةقادصلما عضو ديدحت

Windows مداخل في نيوكتال

لاجلال رتوي بمك ةزهجأ ديكأت 1. ةوطخلا

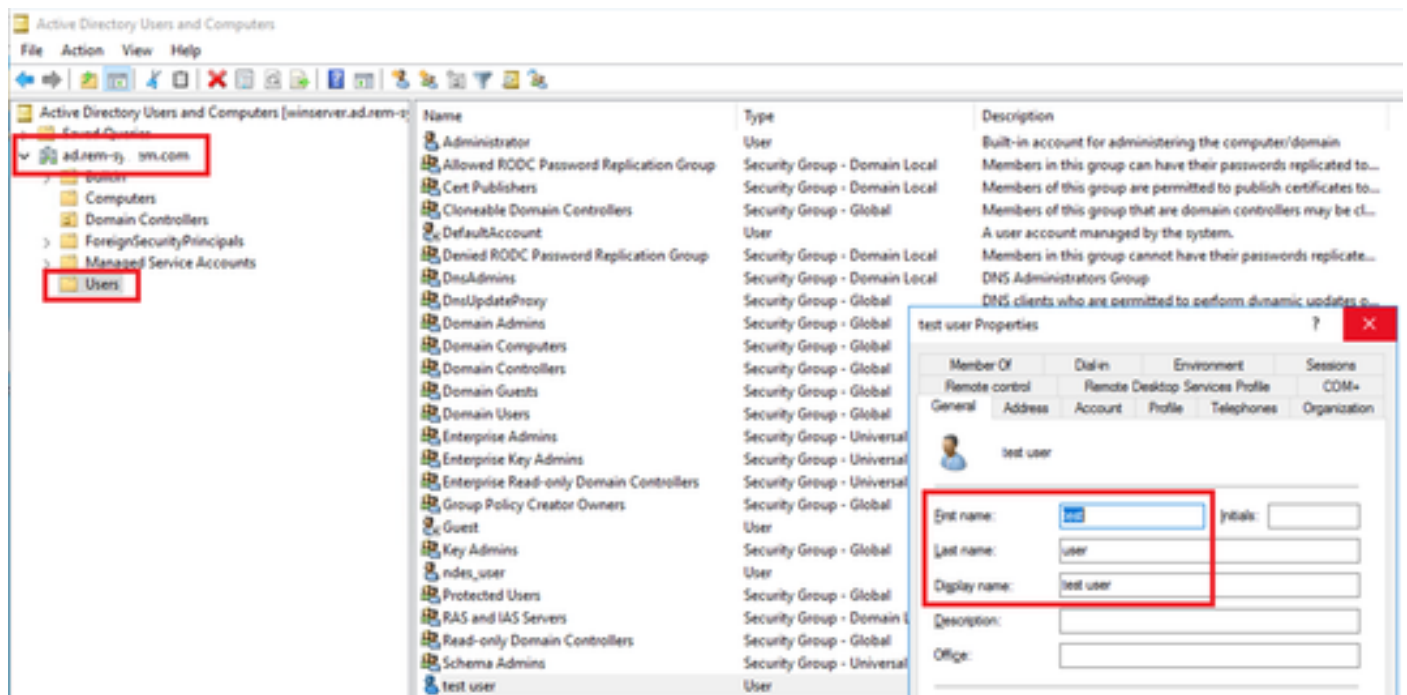
دكأت رتوي بمكال ةزهجأ قوف رقنا ،رتوي بمكال ةزهجأو Active Directory مي مدختسم لى لقتنا لاجلالم في Win10 PC1 جاردا نم



لاجلال رتوي بمك ديكأت

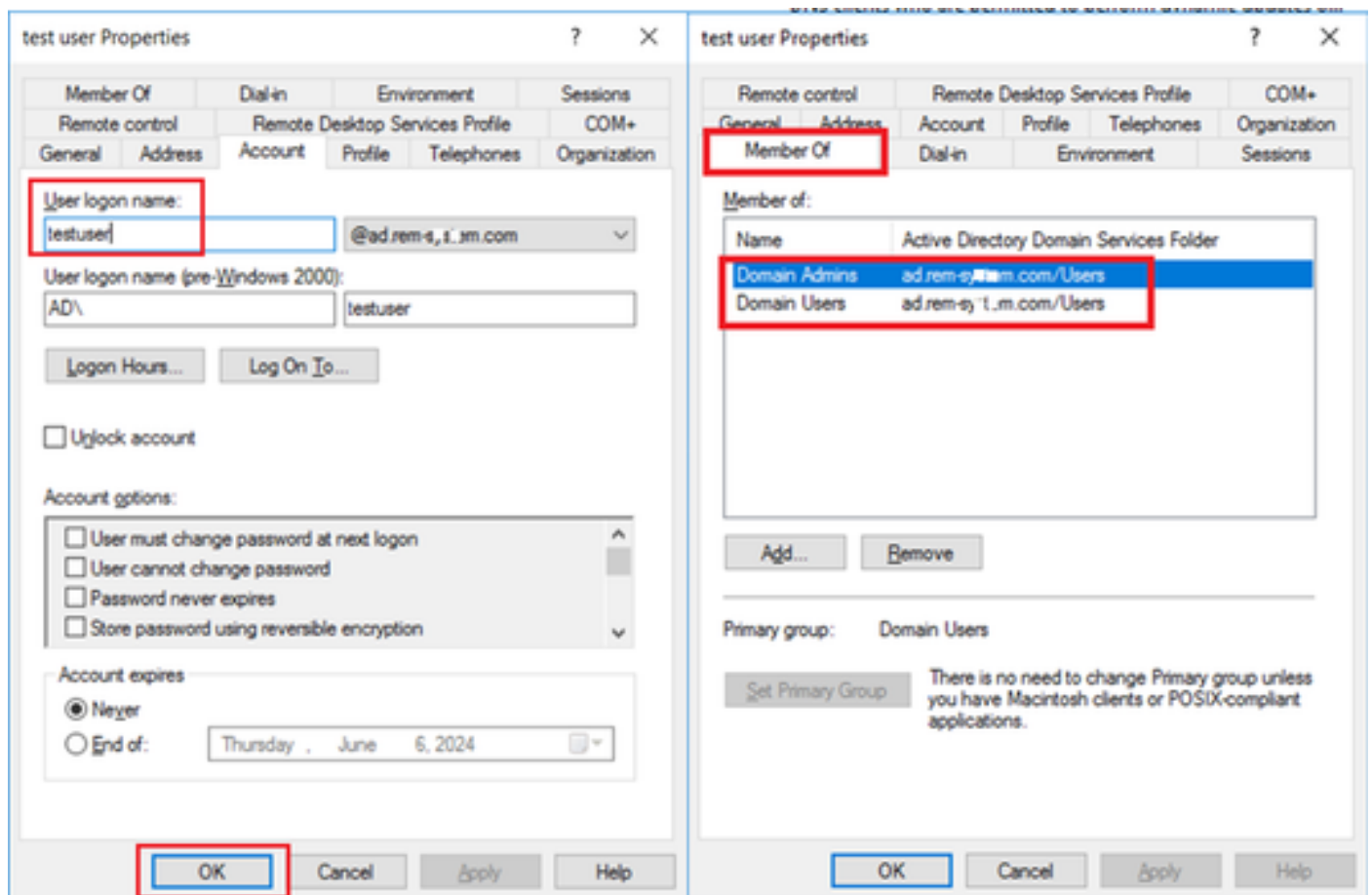
لاجل م مدختسم ةفاضل 2. ةوطخلا

ة فاضا . ن م د خ ت س م ق و ف ر ق ن ا ، ر ت و ي ب م ك ل ا ة ز ه ج ا و Active Directory م م د خ ت س م ي ل ا ل ق ت ن ا ل ا ج م ل م د خ ت س م ك ر ا ب ت خ ا م د خ ت س م .



ل ا ج م ل م د خ ت س م ة فاضا

ل ا ج م ل م م د خ ت س م و ل ا ج م ل ا ي ل و و س م و ض ع ي ل ا ل ا ج م ل م د خ ت س م ة فاضا .



ل ا ج م ل و م د خ ت س م و ل ا ج م ل و ل و و س م

ISE في نيوكتل

زاهج ةفاضل 1. ةوطخل

C1000. زاهج ةفاضل رز ةفاضل قوف رقنا، ةكبشلا ةزهجأ > ةرادل ىل لقتنا

The screenshot shows the Cisco Identity Services Engine (ISE) Administration interface. The main menu on the left includes Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (highlighted), Work Centers, and Interactive Help. The top navigation bar shows 'Administration / Network Resources' and tabs for Network Devices, Network Device Groups, Network Device Profiles, External RADIUS Servers, RADIUS Server Sequences, and NAC Managers. The 'Network Devices' tab is active, displaying a list of devices. The configuration page for a device named 'C1000' is shown. Key fields are highlighted with red boxes: 'Name' (C1000), 'IP Address' (1.1.1.101 / 32), 'Device Profile' (Cisco), and 'Shared Secret' (cisco123). The 'RADIUS Authentication Settings' section is expanded, showing 'RADIUS UDP Settings' with 'Protocol' set to 'RADIUS' and 'Shared Secret' set to 'cisco123'.

زاهج ةفاضل

Active Directory ةفاضل 2. ةوطخل

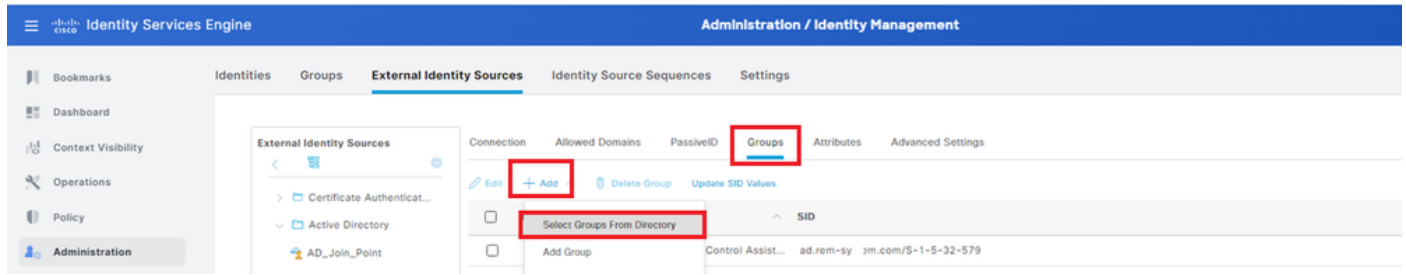
بيوبتل ةمالع قوف رقناو، Active Directory > ةجراخل ةيوهل رداصم > ةرادل ىل لقتنا ISE. Active Directory ةفاضل مقو، لاصتا

- طبرلا ةطقن مسا: AD_JOIN_POINT
- Active Directory ةمدخ لاجم: ad.rem-xxx.com

The screenshot shows the Cisco Identity Services Engine (ISE) Administration interface for Identity Management. The main menu on the left includes Bookmarks, Dashboard, Context Visibility, Operations, Policy, and Administration (highlighted). The top navigation bar shows 'Administration / Identity Management' and tabs for Identities, Groups, External Identity Sources (highlighted), Identity Source Sequences, and Settings. The 'External Identity Sources' tab is active, displaying a list of sources. The configuration page for an 'Active Directory' source is shown. Key fields are highlighted with red boxes: 'Join Point Name' (AD_Join_Point) and 'Active Directory Domain' (ad.rem-st...m.com).

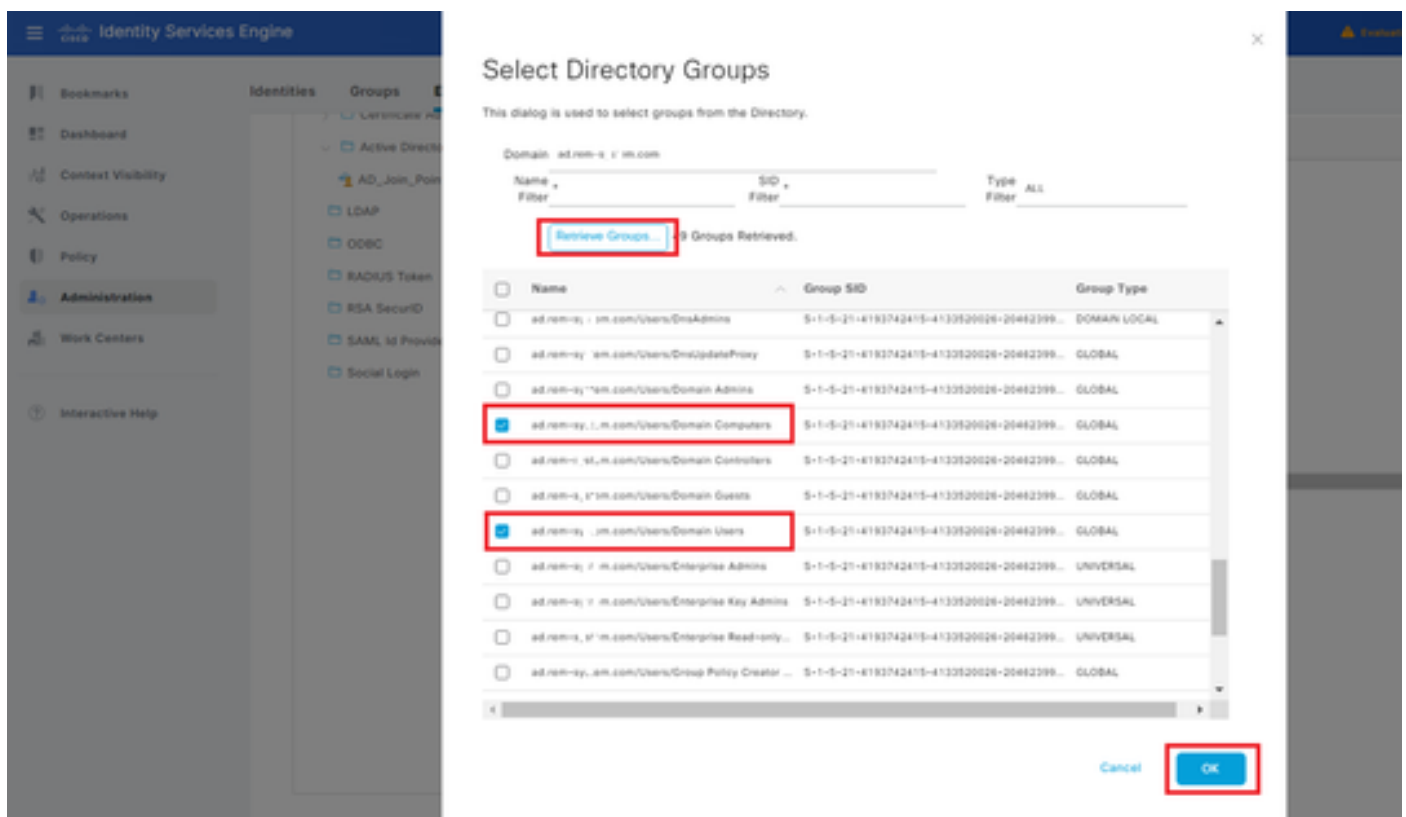
Active Directory ةفاضل

ةلدسنم الةمئاق الة نم ليلدل نم تاعومجم ديدحت دح ،تاعومجم بيوبت الة مالع الة لقتنا



ليلدل نم تاعومجم ديدحت

لعل رتوي بمك الة زهجة نم ققحت .ةلدسنم الةمئاق الة نم تاعومجم الة دادرست الة قوف رقنا قوف رقنا و ad.rem-xxx.com/Users/Domain يم دختستسو و ad.rem-xxx.com/Users/Domain ناو نال قافوم.



نيم دختستسو الة لاجم الة رتوي بمك زهجة افاضا

زاهج الة قداصم دادع الة ديك الة 3. ةوطخال

زاهج الة قداصم دادع الة نم دك الة و ،ةمدقتم تادادع الة بيوبت الة مالع الة لقتنا

- زاهج الة قداصم نيكم تل :زاهج الة قداصم نيكم ت
- ليوخت الة لبق ةل الة او مدختستسو الة قداصم جم دل : "زاهج الة الة لوصول ديق" نيكم ت

8760 إلى 1 نم وه مداقتلا تقول حيحصلال قاطنلا :ةظحالم

The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar shows 'Identity Services Engine' and 'Administration / Identity Management'. The main content area is titled 'External Identity Sources' and includes tabs for 'Connection', 'Allowed Domains', 'PassiveID', 'Groups', 'Attributes', and 'Advanced Settings'. The 'Advanced Settings' tab is selected and highlighted with a red box. Under 'Advanced Authentication Settings', the following options are checked and highlighted with a red box:

- Enable Password Change
- Enable Machine Authentication
- Enable Machine Access Restrictions

The 'Aging Time' is set to 5 hours. Below these settings, a note states: 'Machine Access Restrictions Cache will be replicated between PSN instances in each node group. To configure MAR Cache distribution groups: [Administration > System > Deployment](#)'. Other unchecked options include 'Enable dial-in check', 'Enable callback check for dial-in clients', and 'Use Kerberos for Plain Text Authentications'.

زاهج لة قءاصم ءاءع

ةي وه ل رءصم ءالسلست ءفاضا 4. ءوطخ ل

ةي وه رءصم لسلست ءفاضاب مقو، ءي وه ل رءصم ءالسلست > ءراءا ل ل لقتنا

- مسالا: Identity_AD
- قءاصم لنع ءءاب لة قءاصم ل: AD_JOIN_POINT

The screenshot shows the Cisco Identity Services Engine Administration / Identity Management interface. The 'Identity Source Sequences' tab is selected. The 'Identity Source Sequence' form is displayed, showing the 'Name' field set to 'Identity_AD' and the 'Description' field as an empty text area. Below the form, the 'Authentication Search List' section is visible, showing a list of available identity sources and a selected list. The 'Selected' list contains 'AD_Join_Point', which is highlighted with a red box. The 'Available' list includes 'Internal Endpoints', 'Internal Users', 'Guest Users', and 'All_AD_Join_Points'. Navigation buttons are present between the lists.

ةي وه ل رءصم ءالسلست ءفاضا

ل ءوخت ل ءي رعت فل م ءACL ءفاضا 5. ءوطخ ل

ةلباق ل (ACL) لوصول ءي مكءء ل مءاوق > ضي وفت ل > ءءائ ل > ءسايس ل ل ل لقتنا
(DACL) لوصول ءي مكءء ل ءفاضاب مقو، ل لزلزل

- مسالا: MAR_PASS
- ءب ل IP ل ءامس ل (DACL): ءيساس لة ل لوصول ءي مكءء ل ءفاضاب ل وءءم
ل ءفامس ل IP ل ءامس ل و 1.x.x.101 ءي ضم

إفاضة DACL

في فرع فلم فضاء أو، لي وخت ل اتا في صوت > لي وخت ل > جئاتن ل > ة سا ي س ل ل > ل ل ل ق ت ن ا لي وخت.

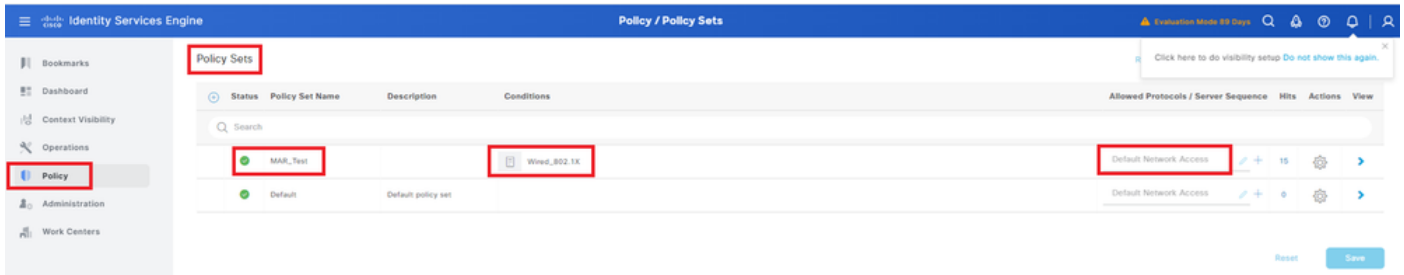
- م س ا ل : MAR_PASS
- م س ا DACL : MAR_PASS

لي وخت ل في فرع فلم فضاء

ج ه ن ة ة و م ج م ة فاضا 6 ة و ط خ ل ا

ج ه ن ة ة و م ج م ة فاضا ل + ق و ف ر ق ن ا ، ج ه ن ت ا ة و م ج م > ج ه ن ل ل ل ق ت ن ا

- ج ه ن ل ا ة و م ج م م س ا : MAR_TEST
- ط و ر ش ل ل : WIRED_802.1X
- ة ك ب ش ل ل ل ل ل ي ض ا ر ت ف ا ل ل و ص و ل ا : م د ا خ ل ل ل س ل س ت / ا ه ب ح و م س م ل ا ت ا ل و ك و ت و ر ب ل ل



چەن ەفازە مەجموعە

ەفازە مەجموعە لایق 7. ەفازە مەجموعە

ەفازە مەجموعە لایق 7. ەفازە مەجموعە لایق 7. ەفازە مەجموعە لایق 7.

- ەفازە مەجموعە: MAR_DOT1x
- ەفازە مەجموعە: WIRED_802.1X
- ەفازە مەجموعە: Identity_AD

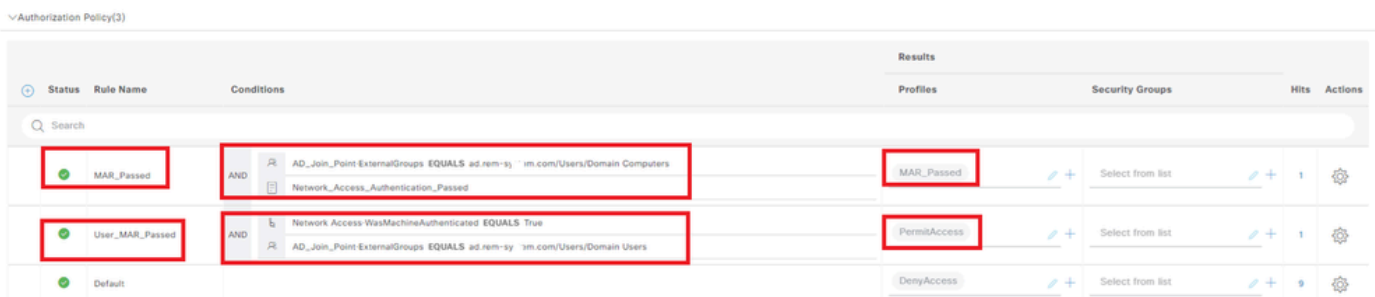


ەفازە مەجموعە لایق

ەفازە مەجموعە لایق 8. ەفازە مەجموعە لایق 8.

ەفازە مەجموعە لایق 8. ەفازە مەجموعە لایق 8. ەفازە مەجموعە لایق 8.

- ەفازە مەجموعە: MAR_PASS
- ەفازە مەجموعە: AD_JOIN_POINT·ExternalGroups ad.rem-xxx.com/Users/Domain Computers و Network_ACCESS_AUTHENTICATION_PASS
- ەفازە مەجموعە: MAR_PASS
- ەفازە مەجموعە: user_mar_pass
- ەفازە مەجموعە: Network Access·WasMachineAuthenticated True
- ەفازە مەجموعە: ad.rem-xxx.com/Users/Domain ەفازە مەجموعە
- ەفازە مەجموعە: PermitAccess




ەفازە مەجموعە لایق

ةحصلا نم ققحتلا

مدختسملا ةقداصم وزاهجلا ةقداصم 1. طمنلا

Windows PC نم جورخلا ليجست 1. ةوطخلا

زاهجلا ةقداصم ليجشتل Win10 PC1 نم جورخلا ليجست رز قوف رونا

 Change account settings


 Lock

 Sign out

 Switch user

  FileZilla FTP Client


  Firefox

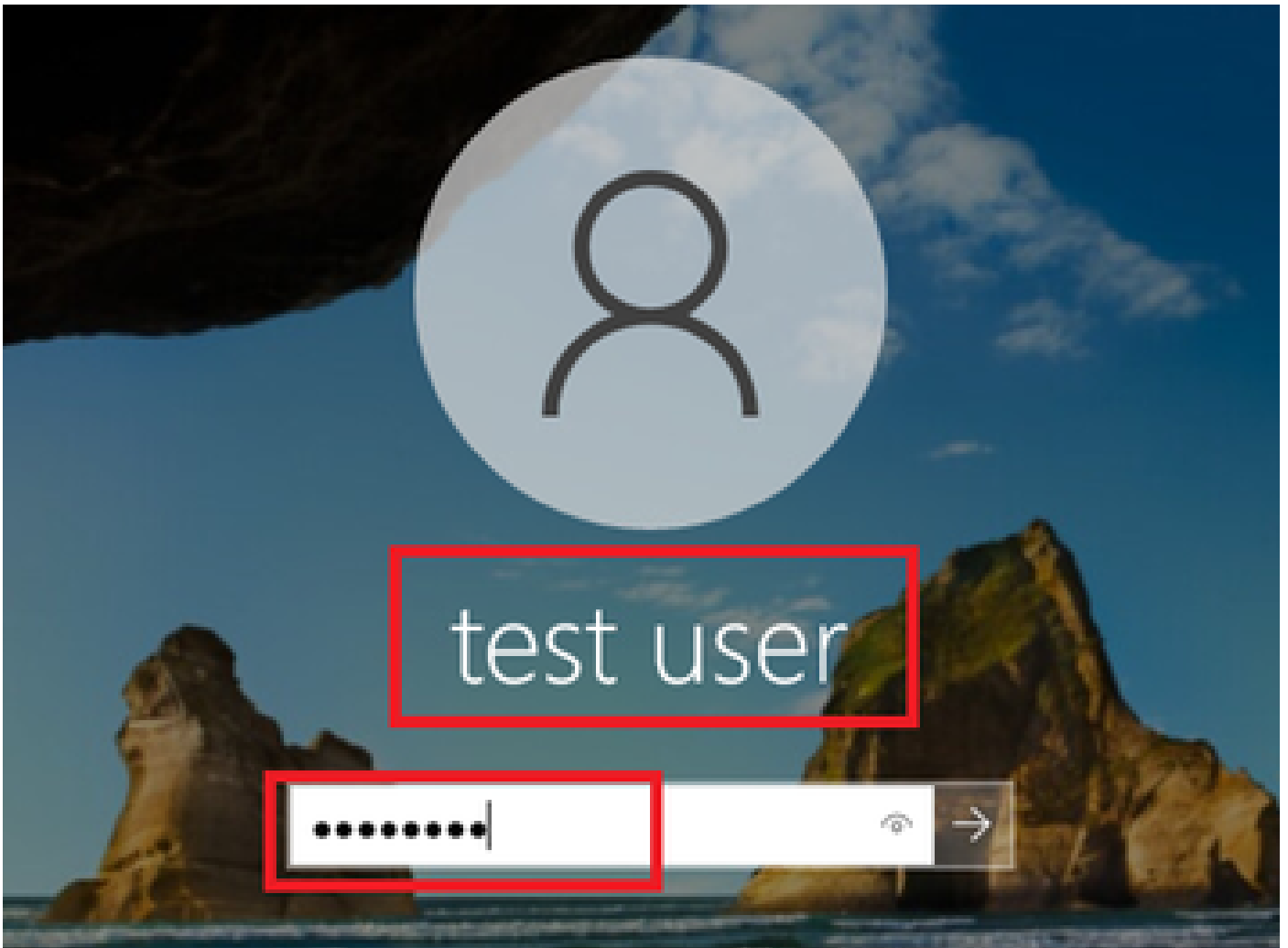
 G

  Get Help

  Google Chrome

 M

  Mail



Windows PC لودد ليجست

ةقداصملا لمع ةسلج ديكأت 4. ةوطخلال

C1000. في مدختسملا ةقداصم ةسلج ديكأتل رمأل show authentication sessions interface GigabitEthernet1/0/2 details ليجشتب مق

<#root>

Switch#

```
show authentication sessions interface GigabitEthernet1/0/2 details
```

```
Interface: GigabitEthernet1/0/2
```

```
MAC Address: b496.9115.84cb
```

```
IPv6 Address: Unknown
```

```
IPv4 Address: 1.x.x.9
```

```
User-Name:
```

```
AD\testuser
```

```
Status: Authorized
```

```
Domain: DATA
```

```
Oper host mode: multi-auth
```

```
Oper control dir: both
```

```
Session timeout: N/A
```

Restart timeout: N/A
Periodic Acct timeout: N/A
Session Uptime: 85s
Common Session ID: 01C2006500000049AA780D80
Acct Session ID: 0x0000003D
Handle: 0x66000016
Current Policy: POLICY_Gi1/0/2

Local Policies:
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:

Method status list:
Method State

dot1x Authc Success

Radius Live لجس دي كأت 5 ةوطخل

ةقداصلم ليغشتلا لجس نم دكأتو، (ISE) ةيموسرلا مدختسمل ةهجو يف قرشابملا تالجسلا > RADIUS > تايلمعلا ىل لقتنا مدختسمل ةقداصلم و زاهجلا

The screenshot shows the 'Live Logs' section of the Identity Services Engine. The 'Operations' menu item is highlighted. The main area displays a table of live sessions. The table has columns for Time, Status, Details, Repeats, Identity, Endpoint ID, Endpoint P, Authentication Policy, Authorization Policy, Authorization P..., IP Address, and Network De... The following table represents the data shown in the screenshot:

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint P	Authentication Policy	Authorization Policy	Authorization P...	IP Address	Network De...
May 07, 2024 04:36:14...	●		0	AD/issuser	84-96-91-15-84...	Intel-Dev...	MAR_Test => MAR_dot1x	MAR_Test => User_MAR_Passed	PermiAccess	1.1 - 3.9	
May 07, 2024 04:36:13...	●			AD/issuser	84-96-91-15-84...	Intel-Dev...	MAR_Test => MAR_dot1x	MAR_Test => User_MAR_Passed	PermiAccess	1.1 - 3.9	C1000
May 07, 2024 04:35:12...	●			WACSACL@IP-MAR_Passed-6637ba20							C1000
May 07, 2024 04:35:12...	●			hsn/DESKTOP-L2696-ad-nm-9-17m...	84-96-91-15-84...	Intel-Dev...	MAR_Test => MAR_dot1x	MAR_Test => MAR_Passed	MAR_Passed	169.254.90.1...	C1000

لجس Radius Live

زاهجلا ةقداصلم ليغشتلا لجس دي كأت.

Overview

Event	5200 Authentication succeeded
Username	host/DESKTOP-L2IL9I6.ad.rem-sy .em.com
Endpoint Id	B4:96:91:15:84:CB
Endpoint Profile	Intel-Device
Authentication Policy	MAR_Test >> MAR_dot1x
Authorization Policy	MAR_Test >> MAR_Passed
Authorization Result	MAR_Passed

Authentication Details

Source Timestamp	2024-05-07 16:35:12.222
Received Timestamp	2024-05-07 16:35:12.222
Policy Server	ise33-01
Event	5200 Authentication succeeded
Username	host/DESKTOP-L2IL9I6.ad.rem-sy .em.com
Endpoint Id	B4:96:91:15:84:CB
Calling Station Id	B4-96-91-15-84-CB
Endpoint Profile	Intel-Device
IPv4 Address	169.254.90.172
Authentication Identity Store	AD_Join_Point
Identity Group	Profiled
Audit Session Id	01C2006500000049AA780D80
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPv2)

Steps

Step ID	Description	Latency (ms)
11001	Received RADIUS Access-Request - AD_Join_Point	
11017	RADIUS created a new session - ad.rem-sy .em.com	0
15049	Evaluating Policy Group - AD_Join_Point	1
15008	Evaluating Service Selection Policy	0
15048	Queried PIP - Normalised Radius.RadiusFlowType	3
11507	Extracted EAP-Response/Identity	2
12500	Prepared EAP-Request proposing EAP-TLS with challenge	0
12625	Valid EAP-Key-Name attribute received	0
11006	Returned RADIUS Access-Challenge	1
11001	Received RADIUS Access-Request	6
11018	RADIUS is re-using an existing session	0
12301	Extracted EAP-Response/NAK requesting to use PEAP instead	0
12300	Prepared EAP-Request proposing PEAP with challenge	0
12625	Valid EAP-Key-Name attribute received	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	5
11018	RADIUS is re-using an existing session	0
12302	Extracted EAP-Response containing PEAP challenge-response and accepting PEAP as negotiated	1
61025	Open secure connection with TLS peer	1
12318	Successfully negotiated PEAP version 0	0
12800	Extracted first TLS record; TLS handshake started	0
12805	Extracted TLS ClientHello message	0
12806	Prepared TLS ServerHello message	0
12807	Prepared TLS Certificate message	0
12808	Prepared TLS ServerKeyExchange message	25
12810	Prepared TLS ServerDone message	0
12305	Prepared EAP-Request with another PEAP challenge	0
11006	Returned RADIUS Access-Challenge	1
11001	Received RADIUS Access-Request	14
11018	RADIUS is re-using an existing session	0

زاهج لة قداصم لي صافت

مدختسمل قداصم ل ص فم ل رشابم ل ل ج س ل ل دي ك أت ب مق

Overview

Event	5200 Authentication succeeded
Username	AD\testuser
Endpoint Id	B4:96:91:15:84:CB
Endpoint Profile	Intel-Device
Authentication Policy	MAR_Test >> MAR_dot1x
Authorization Policy	MAR_Test >> User_MAR_Passed
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2024-05-07 16:36:13.748
Received Timestamp	2024-05-07 16:36:13.748
Policy Server	ise33-01
Event	5200 Authentication succeeded
Username	AD\testuser
Endpoint Id	B4:96:91:15:84:CB
Calling Station Id	B4-96-91-15-84-CB
Endpoint Profile	Intel-Device
IPv4 Address	1.x.x.9
Authentication Identity Store	AD_Join_Point
Identity Group	Profiled
Audit Session Id	01C200650000049AA780D80
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPv2)

Steps

Step ID	Description	Latency (ms)
11001	Received RADIUS Access-Request - AD_Join_Point	
11017	RADIUS created a new session - ad.rem-sy .am.com	0
15049	Evaluating Policy Group - AD_Join_Point	0
15008	Evaluating Service Selection Policy	1
11507	Extracted EAP-Response/Identity	7
12500	Prepared EAP-Request proposing EAP-TLS with challenge	0
12625	Valid EAP-Key-Name attribute received	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	8
11018	RADIUS is re-using an existing session	0
12301	Extracted EAP-Response/NAK requesting to use PEAP instead	0
12300	Prepared EAP-Request proposing PEAP with challenge	1
12625	Valid EAP-Key-Name attribute received	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	11
11018	RADIUS is re-using an existing session	0
12302	Extracted EAP-Response containing PEAP challenge-response and accepting PEAP as negotiated	0
61025	Open secure connection with TLS peer	0
12318	Successfully negotiated PEAP version 0	1
12800	Extracted first TLS record; TLS handshake started	0
12805	Extracted TLS ClientHello message	0
12806	Prepared TLS ServerHello message	0
12807	Prepared TLS Certificate message	0
12808	Prepared TLS ServerKeyExchange message	28
12810	Prepared TLS ServerDone message	0
12305	Prepared EAP-Request with another PEAP challenge	1
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	30
11018	RADIUS is re-using an existing session	0
12304	Extracted EAP-Response containing PEAP challenge-	0

مدخستسمال ةقداصم لي صافت

طبق مدخستسمال ةقداصم 2. طم نال

Windows PC نم NIC ني كمت و لي طعت 1. ةوطخال

Win10 PC1 ب ةصخال (NIC) ةكبشال ةه او ةق اطب ني كمت و لي طعت ب مق ،مدخستسمال ةقداصم لي غشتل

ةقداصم ل مع ةس ل ج دي كأت 2. ةوطخال

C1000. في مدخستسمال ةقداصم ةس ل ج دي كأت ل رمأل show authentication sessions interface GigabitEthernet1/0/2 details لي غشتل ب مق

<#root>

Switch#

show authentication sessions interface GigabitEthernet1/0/2 details

Interface: GigabitEthernet1/0/2
 MAC Address: b496.9115.84cb
 IPv6 Address: Unknown
 IPv4 Address: 1.x.x.9
 User-Name: AD\testuser

Status: Authorized
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Session timeout: N/A
Restart timeout: N/A
Periodic Acct timeout: N/A
Session Uptime: 419s
Common Session ID: 01C2006500000049AA780D80
Acct Session ID: 0x0000003D
Handle: 0x66000016
Current Policy: POLICY_Gi1/0/2

Local Policies:
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:

Method status list:
Method State

dot1x Authc Success

Radius Live لجس دي كأت 3. ةوطخلال

طشنل لالجس لال دي كأت ب مقو، (ISE) ةيموسرللا مدختس مللا ةهجاو يف قرشابملا تالجالس لال > RADIUS > تاي لمعلا لال لقتنا
مدختس مللا ةقداصل مل.

مدخست سمل ةقداصم طقف مزلي، ISE في MAR ل تقؤملا نيزختلا ةركاذ نيزخت متي هنأل ارطن: ةظحالم

The screenshot shows the Identity Services Engine (ISE) interface. The 'Operations' menu item is highlighted in red. The main content area displays 'Live Logs' for 'Live Sessions'. There are five summary cards: Misconfigured Supplicants (0), Misconfigured Network Devices (0), RADIUS Drops (0), Client Stopped Responding (0), and Repeat Counter (0). Below these is a table of RADIUS logs. The table has columns for Time, Status, Details, Repeats, Identity, Endpoint ID, Endpoint Name, Authentication Policy, Authorization Policy, Authorization Profile, IP Address, and Network Device. One log entry is highlighted with a red border.

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authentication Policy	Authorization Policy	Authorization P...	IP Address	Network De...
May 07, 2024 04:42:05...			0	AD\testuser	84-96-91-15-84...	Intel-Devi...	MAR_Test => MAR_dotx	MAR_Test => User_MAR_Passed	PermiAccess	1.1	1.9
May 07, 2024 04:42:04...				AD\testuser	84-96-91-15-84...	Intel-Devi...	MAR_Test => MAR_dotx	MAR_Test => User_MAR_Passed	PermiAccess	1.1	3.9
May 07, 2024 04:36:13...				AD\testuser	84-96-91-15-84...	Intel-Devi...	MAR_Test => MAR_dotx	MAR_Test => User_MAR_Passed	PermiAccess	1.1	3.9
May 07, 2024 04:35:12...				RACSACL# IP-MAR_Passed-6639ba20							C1000
May 07, 2024 04:35:12...				host/DESKTOP-L2L966.ad.rem-s...sm...	84-96-91-15-84...	Intel-Devi...	MAR_Test => MAR_dotx	MAR_Test => MAR_Passed	MAR_Passed	169.254.90.1...	C1000

مدخستسملة قداصلمل لصفمالم رشابمالم لجسالم ديكأتب مق

Cisco ISE

Overview

Event: 5200 Authentication succeeded

Username: AD\testuser

Endpoint Id: B4:96:91:15:84:CB

Endpoint Profile: Intel-Device

Authentication Policy: MAR_Test >> MAR_dot1x

Authorization Policy: MAR_Test >> User_MAR_Passed

Authorization Result: PermitAccess

Authentication Details

Source Timestamp: 2024-05-07 16:42:04.467

Received Timestamp: 2024-05-07 16:42:04.467

Policy Server: ise33-01

Event: 5200 Authentication succeeded

Username: AD\testuser

Endpoint Id: B4:96:91:15:84:CB

Calling Station Id: B4-96-91-15-84-CB

Endpoint Profile: Intel-Device

IPv4 Address: 1.1.1.9

Authentication Identity Store: AD_Join_Point

Identity Group: Profiled

Audit Session Id: 01C2006500000049AA780D80

Authentication Method: dot1x

Authentication Protocol: PEAP (EAP-MSCHAPv2)

Service Type: Framed

Network Device: C1000

CiscoAVPair: service-type=Framed, audit-session-id=01C2006500000049AA780D80, method=dot1x, AuthenticationIdentityStore=AD_Join_Point, FQSubjectName=2ce19620-0842-11ef-a5ec-362cec4b4f3d@testuser@ad.rem-sy.te.1.com, UniqueSubjectID=9273f674e52338d8f4807c495e1ff4c2ef9217f9

AD-Groups-Names: ad.rem-sy.te.1.com/Builtin/Users

AD-Groups-Names: ad.rem-sy.te.1.com/Builtin/Administrators

AD-Groups-Names: ad.rem-sy.te.1.com/Users/Denied RODC Password Replication Group

AD-Groups-Names: ad.rem-sy.te.1.com/Users/Domain Admins

AD-Groups-Names: ad.rem-sy.te.1.com/Users/Domain Users

Result

Steps	Step ID	Description	Latency (ms)
	11001	Received RADIUS Access-Request - AD_Join_Point	
	11017	RADIUS created a new session - ad.rem-sy.te.1.com	0
	15049	Evaluating Policy Group - AD_Join_Point	1
	15008	Evaluating Service Selection Policy	0
	11507	Extracted EAP-Response/Identity	16
	12500	Prepared EAP-Request proposing EAP-TLS with challenge	2
	12625	Valid EAP-Key-Name attribute received	0
	11006	Returned RADIUS Access-Challenge	0
	11001	Received RADIUS Access-Request	5
	11018	RADIUS is re-using an existing session	0
	12301	Extracted EAP-Response/NAK requesting to use PEAP instead	0
	12300	Prepared EAP-Request proposing PEAP with challenge	0
	12625	Valid EAP-Key-Name attribute received	0
	11006	Returned RADIUS Access-Challenge	0
	11001	Received RADIUS Access-Request	25
	11018	RADIUS is re-using an existing session	0
	12302	Extracted EAP-Response containing PEAP challenge-response and accepting PEAP as negotiated	1
	61025	Open secure connection with TLS peer	0
	12318	Successfully negotiated PEAP version 0	0
	12800	Extracted first TLS record; TLS handshake started	0
	12805	Extracted TLS ClientHello message	0
	12806	Prepared TLS ServerHello message	0
	12807	Prepared TLS Certificate message	0
	12808	Prepared TLS ServerKeyExchange message	26
	12810	Prepared TLS ServerDone message	0
	12305	Prepared EAP-Request with another PEAP challenge	0
	11006	Returned RADIUS Access-Challenge	0
	11001	Received RADIUS Access-Request	14
	11018	RADIUS is re-using an existing session	0
	12304	Extracted EAP-Response containing PEAP challenge-response	1
	12305	Prepared EAP-Request with another PEAP challenge	0
	24422	ISE has confirmed previous successful machine authentication for user in Active Directory	0
	15036	Evaluating Authorization Policy	0
	24209	Looking up Endpoint in Internal Endpoints IDStore - AD\testuser	1
	24211	Found Endpoint in Internal Endpoints IDStore	3
	24432	Looking up user in Active Directory - AD\testuser	
	24355	LDAP fetch succeeded	
	24416	User's Groups retrieval from Active Directory succeeded	
	15048	Queried PIP - AD_Join_Point.ExternalGroups	11
	15016	Selected Authorization Profile - PermitAccess	5
	22081	Max sessions policy passed	0
	22080	New accounting session created in Session cache	0
	12306	PEAP authentication succeeded	0
	61026	Shutdown secure connection with TLS peer	0
	11503	Prepared EAP-Success	1
	11002	Returned RADIUS Access-Accept	2

مدخستسملة قداصلمل ليصافات

هالصالوا عاخال فاشكتسا

ISE. في قداصلمل ليصافات لكولسالم ديكأت يلع (prdt-server.log) هذه عاخال حيحصت تالجس كدعاست

- runtime-config

- ليغش التلا تقول ليحست
- Runtime-AAA

دنتس مل اذه يف مدختس مل قداصم و زاوجل قداصم 1. ظنل لل اءاطخ ال احيصت لجس يلع لاثم اذه

<#root>

// machine authentication

MAR,2024-05-08 16:54:50,582,DEBUG,0x7fb2fd3db700,cntx=0000034313,sesn=ise33-01/504417979/41,CPMSessionID=01C200650000049AA780D8

user=host/DESKTOP-L2IL9I6.ad.rem-xxx.com

,CallingStationID=B4-96-91-15-84-CB,FramedIPAddress=1.x.x.9,MARCache::checkInsertConditions:

subject=machine

, calling-station-id=B4-96-91-15-84-CB, HostName=DESKTOP-L2IL9I6\$@ad.rem-xxx.com,MARCache.cpp:105

// insert MAR cache

MAR,2024-05-08 16:54:50,582,DEBUG,0x7fb2fd3db700,cntx=0000034313,sesn=ise33-01/504417979/41,CPMSessionID

user=host/DESKTOP-L2IL9I6.ad.rem-xxx.com

,CallingStationID=B4-96-91-15-84-CB,FramedIPAddress=1.x.x.9,

Inserting new entry to cache

CallingStationId=B4-96-91-15-84-CB, HostName=DESKTOP-L2IL9I6\$@ad.rem-xxx.com, IDStore=AD_Join_Point and

MAR,2024-05-08 16:54:50,582,DEBUG,0x7fb2fd3db700,cntx=0000034313,sesn=ise33-01/504417979/41,CPMSessionID

user=host/DESKTOP-L2IL9I6.ad.rem-xxx.com

,CallingStationID=B4-96-91-15-84-CB,FramedIPAddress=1.x.x.9,MARCache::onInsertRequest: event not locally

// user authentication

MAR,2024-05-08 16:55:11,120,DEBUG,0x7fb2fdde0700,cntx=0000034409,sesn=ise33-01/504417979/45,CPMSessionID

user=AD\testuser

,CallingStationID=B4-96-91-15-84-CB,FramedIPAddress=1.x.x.9,MARCache::onQueryRequest:

machine authentication confirmed locally

,MARCache.cpp:222

MAR,2024-05-08 16:55:11,130,DEBUG,0x7fb2fe5e4700,cntx=0000034409,sesn=ise33-01/504417979/45,CPMSessionID

user=AD\testuser

,CallingStationID=B4-96-91-15-84-CB,FramedIPAddress=1.x.x.9,MARCache::onMachineQueryResponse:

machine DESKTOP-L2IL9I6\$@ad.rem-xxx.com valid in AD

,MARCache.cpp:316

ةلص تاذا تامولعم

[زاهجلا لىلا لوصولا دييقتب ةصاخلا لسالس لاوت اناجلا](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نء مء دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةللخت. فرتمة مچرت مء مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او
ىل إأمءءاد ءوچرلاب ةصوء و تاملرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزءل ءنل دن تسمل