RHEL 7 Arabic Notes

تلخيص الطالب : أحمد عبدالمنعم

فيديوهات المهندس : مصطفى حموده

رابط ال Play List

https://www.youtube.com/playlist?list=PLy1Fx2HfcmWBpD_PI4AQpjeDK5-5q6TG7

ملاحظات

1- موضوع ال **IPA SERVER** ده فيه كلام نظرى كتير جدا جدا وانا كتبت كل كلمة قالها البشمهندس مصطفى حموده ، فانا اسف لو حضرتك لقيت كلام خارجى كتير ، لان انا حاولت اكتب كل حاجة علشان الموضوع يكون سهل ان شاء الله بالنسبة لاى واحد اول مرة يعرف يعنى اى **IPA SERVER** او ما يسمى بال **Central Authentication**

2- بالنسبة للفديو اللى مشروح فيه الكلام ده ، فهو عبارة عن الفديو رقم 60 اليوم رقم 29 وده عنوان الفديو

60-Day-29_Central Authentication_IPA

وبرضو التكملة بتاعته موجودة فى الفديو اللى بعده رقم 61 اليوم رقم 30 وده عنوان الفديو

61-Day-30_Central Authentication_MS AD

IPA Server

موضوع ال Centralized Authentication ، تعتبرمن اهم المواضيع بالنسبالك ك System Admin وتعالى بقى اقولك هو ليه مهم

بص من حوالى 10 سنين مثلا الدنيا كانت صغيرة الى حد ما يعنى عن الموجود دلوقتى بمعنى ان انت دلوقتى لو بصيت لاى شركة حتى لو كانت Startup هتلاقى فيها بتاع 10 مستخدمين على الاقل ، وبالتالى هتلاقى ال Requirements بتاع الشركة دى انه يكون عندها ما يسمى

بال Centralized Policy ، او بمعنى ادق يكون عندك Rules الناس كلها تمشى عليها ، وطبعا ال Policy دى لازم يتعملها Enforcement ، فمثلا بقى لو عندك 50 موظف فى الشركة دى وعايز تطبق عليهم ال Centralized Policy ، يعنى مثلا ال Password بتاعت الناس تكون كلها 10 Characters ، او مثلا الباسورد دى تتغير كل شهر ، طيب افرض بقى ان كل موظف عنده جهاز يبقى انت عندك 50 جهاز ، وتخيل بقى لو انت عايز تعمل enforcement ل policy زى دى ، اللى هى ان الباسورد بتاعهم تكون 10 حروف ويتغير كل شهر مثلا ، يبقى ينهار ابيض لو انت system admin هيطلع عينيك حرفيا ، وطبعا هيبقى شاق عليك انك ت administrate الكلام ده كله

الحاجة التانية بقى وهى افرض انك عايز تعمل Advanced Setup زى مثلا انك تكون عايز ال user الفلانى ينفذ tasks معينة ، تخيل بقى لو عايز تعمل setup زى ده ، طيب وانهى user هيعمل login من انهى جهاز بالظبط ، طبعا ده فى حد ذاته مشكلة

وهنا بقى ياجى دور انه يكون عندك Centralized Policy ، ودى هتسمحلك انك ت Push ال Policy دى من اى مكان ، يعنى ال Policy هتكون موجودة على مكان واحد ،واى واحد هيعمل Login على اى جهاز هيروح ياخد ال Policy من ال Central Server اللى موجود

طيب عادة احنا قبل مانتكلم على اى Policy واى حاجة اصلا كنا بنسمع ان الناس كانت بتتكلم على ان انت لو عندك مجموعة اجهزة ، فكان الطبيعى ان كل جهاز يكون عليه ال Policy الخاصة بيه والجهاز التانى عليه برضو ال Policy الخاصة بيه ، وبالمناسبة برضو كل جهاز بيكون عليه ال username وال password الخاصة بيهم ، طيب افرض بقى ان انت عندك فى الشركة دى user واحد بس ، وال user ده كان موجود على جهاز معين ، وحب انه يتنقل لجهاز جديد خالص ، اى اللى هيحصله ، اكيد طبعا حاجة عذاب بالنسبالك لانك عايز تاخد ال username وال password بتاعه وتنقله على كل جهاز موجود فى الشركة ، فتخيل بقى لو انت عندك 10 اجهزة يبقى هتنقل ال username وال password بتاعه 10 مرات ، والكلام ده لكل user لوحده

فكان الحل الطبيعى ان انت يكون عندك Directory Service

وال directory service دى جات من مصطلح بسيط جدا بالنسبالهم ، وهو انهم اعتبروا ان الخدمة او ال service اللى هيكون فيها كل المستخدمين دول بالظبط عاملة زى ال Notebook بتاع التيليفونات ، اللى هى بيكون فيها كل مستخدم ومعاه رقم التيليفون بتاعه ، هنا بقى نفس الفكرة بالظبط انه هيكون عندك مثلا Data Base او Central Data Base ، وطبعا

ال Central Data Base دى هيكون فيها المستخدم وبياناته ، وبالمناسبة البيانات دى هتكون بالنسبالك Extensible يعنى قابلة للتمدد والزيادة ، بمعنى انك خزنت النهارده مثلا ال username وال password ، ممكن انت تيجى بكره عادى وتخزن كمان الاوامر اللى ممكن ينفذها واى حاجة انت عايزها

وبكده انت ممكن تعتبر ال Directory Service بالنسبالنا هى عبارة عن Special Data Base ، هتسمحلك انك تخزن كل بيانات الموظفين وتقدر كمان انك تسترجعهم بعد كده

طيب حلو ، موضوع ال setup هيكون ازاى بقى ، قالك انت هيكون عندك Server واحد مثلا ، وال Server ده هيكون عليه ال Directory Service ، وهنا بقى كل مرة ياجى user معين يحاول انه يعمل Login على جهاز فى الشركة ، فالجهاز ده هيروح يسأل ال Server ده ،ويقوله هل ال user ده Authorized انه يعمل login على الجهاز الفلانى ده

وبكده انت هتعمل maintain ل data base واحدة بس ، وده طبعا انجاز كبير ، لان لو مفيش ال Central Data Base دى ، فانت هتضطر تعمل maintain لكل جهاز ، يعنى من الاخر كده هتعمل maintain لكل نسخة Policy على كل جهاز لوحده ، طيب ما احنا كده عندنا سؤال بخصوص ال High Availability ، وهو افرض بقى ال Server ده وقع ، هل كده اى حد ممكن انه يعمل Login ؟

اكيد طبعا لأ مفيش اى حد هيقدر يعمل Login ، لانه ببساطة هيكون عندك Server تانى معمول ليه install وكل حاجة تمام عليه ، وهيشتغل ك Secondary سيرفر

وده فى حالة ان ال Server الاولانى اللى هو ال Primary وقع ، وبكده السيرفر التانى ده هياخد كل حاجة من السيرفر ال Primary ، يعنى اى Policy هيتعملها تغيير فى السيرفر الاول ، اوتوماتيك هتنتقل للسيرفر التانى ، كل اللى انت هتعمله انك هتقول لل Clients انكم عندكم 2 Central Servers

وبكده السيرفر الاول ده عامل زى ال **AD** اللى هى ال **Active Directory** ودى عبارة عن Central Authentication Server وطبعا من خلالها تقدر انك تعمل Push ال Policy لل Client

طيب دلوقتى انا هعمل 2 جهازين ، واحد هيكون هو ال Central Server والتانى هيكون هو ال Client ، اى اللى هيحصل بقى ؟

اللى هيحصل ان ال Server ده انا هعمل install ل Services عليه ، وال Services دى هتسحملى انى اعمل Authentication ، اللى هى هتكون ال Central Data Base ، طب اى هى ال Services اللى هعملها install ؟؟

ال Services دى عبارة عن مجموعة Packages اسمها **Free IPA** ودى اختصار ل **Identity Policy Audit** ، ودى بقى عبارة عن Service او بشكل ادق عبارة عن Integrated Solution اللى عملته هى شركة RedHat علشان يكون عبارة عن Central Authentication Server ، طيب ال **IPA** بيضم شوية حاجات كده مع بعض ، اولا هو بي Integrate حاجة اسمها NTP Service لل Time اللى هى Network Time Protocol ، وده علشان تدى Accurate Time بين ال Machines وبعضها ، وكمان بيضم DNS Service

وكمان بيضم حاجة كده اسمها **LDAP Service** وده اختصار ل **Lightweight Directory Access Protocol** ، وبيضم برضو حاجة اسمها **Kerberos Service** ، بالاضافة لكده هو ليه كمان HTTPS GUI علشان تقدر تعمل Manage للكلام ده كله

تعالى بقى نتكلم عن كل Service من اللى فوق دول ، اولا ال NTP وظيفتها ان ال Time يكون Synchronized بين الاجهزة وبعضها ، يعنى مثلا ميكونش فيه جهاز ويكون عليه الوقت الساعة 3 وجهاز تانى الوقت يكون عليه الساعة 8 مثلا ، وبالتالى مينفعش جهاز يكون بيبعت معلومة لجهاز تانى يقولى معلش اعملى Authenticate ويكون ال Time بين الجهازين مختلف

طب ليه ؟؟ لانه بكل بساطة ممكن يكون قاعد واحد ابن حلال عمال بيعمل sniff للداتا دى ، شغال ياخد ال Request اللى جهاز ال Client بعته ويبدأ يعمله Decrypt وبعدين يبعته لل Central Server يعنى نفس فكرة
ال Man In The Middle Attack ، فا طبعا علشان نمنع حاجة زى دى ، يبقى لازم ال Client وهو بيبعت المعلومة لل Server ، لازم يحط معاها

ال Time اللى موجود عنده وبالتالى السيرفر لما يرد ، هيرد ويقول ان الرد بتاعه valid لمدة كام دقيقة او كام ثانية بالظبط ، بحيث ان لو حد عمل attack على ال Network وعمل Decrypt للكلام ده هيبقى بالنسباله بعد كام ثانية **invalid** او المعلومات اللى حصل عليها هتكون useless ، علشان كده انت محتاج ان ال Time يكون Synchronized بين ال Client وبين ال Server

بعد كده ال DNS ، وده ببساطة علشان مش كل مرة ال Client هيحتاج انه يعمل Authenticate يعمل عن طريق ال IP ، تخيل مثلا لو عندك مثلا شبكة والشبكة دى فيها 1000 جهاز هل تفتكر ان الالف جهاز كل واحد فيهم لما يحب ي connect هيعمل connect عن طريق ال IP ولا ان كل واحد يكون ليه اسم اسهل واحسن ؟؟ اكيد طبعا انك تعمل connect عن طريق الاسم هيكون اسهل بكتير ، يعنى انت مثلا ممكن تسمى كل جهاز باسم **PC1-domain** وهكذا بقى ، وكذلك السيرفرات برضو ممكن تديها اسماء ، يعنى من الاخر حاجة تكون سهلة ليك علشان تفتكرها بحيث ان لو فى client معين عمل connect عليك ويقولك عندى مشكلة فانت ساعتها ممكن تسأله ان جهازك اسمه اي او رقمه كام وبالتالى يكون سهل عليك انك تعمل Trouble Shooting للمشكلة دى ، طيب خلى بالك برضو انه مش حاجة Mandatory يعنى مش حاجة ضرورية

لان انت ممكن تعمل Complete Central Authentication من غير ما يكون عندك DNS ده مجرد حاجة Optional بالنسبالك ، بس هو فى الحقيقة هيسهل عليك الدنيا خالص

تالت حاجة نتكلم عنها وهى ال **LDAP** ، ودى بقى عبارة عن ال Directory Service ذات نفسها ، يعنى من الاخر هى ال Service المسؤلة عن انها تخزن معلومات ال users واى حاجة عنهم وكمان ال Policy بتاعتهم لو حبيت يعنى ، او لو انت بت Integrate مع DNS ،يعنى لو انت بت Integrate ال DNS او لو هتشغل ال Free IPA ، فانت ممكن تشغله انه ي host او انه ي contain ال Data Base بتاعت ال DNS Server ، وساعتها بقى كل المعلومات دى هتتخزن فى ال LDAP ، وطبعا ال LDAP هو اختصار
ل **Lightweight Directory Access Protocol** وده عبارة عن بروتوكول اتعمل من التمانينات ، واللى بدأ يعمله هو شركة IBM ،وبقى **defacto standard** العالم كله شغال بيه

يبقى الداتا بيز نفسها اللى عليها كل المعلومات هى عبارة عن **LDAP Backend** او **LDAP Data Base** ، وكمان ال LDAP وظيفتها برضو تتأكد ان الوقت بين ال Machines وبعضها Synchronized

طيب بالنسبة للـ HTTPS GUI ده عبارة عن utility علشان تسهلك الدنيا ك system admin ، لان تقريبا من الصعب انك ت manage كل حاجة عن طريق الـ Command Line

اخر حاجة بقى وهى الـ **Kerberos** ، وده عبارة عن **Authentication System** ، وده برضو Open Standard العالم كله شغال فيه ، وبالمناسبة كمان هتلاقى اسمه **MIT Kerberos** وطبعا ليه اكتر من Implementation ، يعنى مثلا الجماعة بتوع اللينكس عندهم الـ Implementation الخاصة بيهم بتاعت الـ Kerberos ، وميكروسوفت عندها الـ Implementations الخاصة بيها

واللى احنا هنعمله دلوقتى هو اننا هنعمل setup للـ Central Authentication Server ، وهنعمل Configure من عند الـ Client ونخليه انه يعمل Authenticate من عند السيرفر ده

يبقى كده احنا اول حاجة محتاجينها وهى اننا نعمل install للـ freeIPA

اه حاجة مهمة ليك جدا جدا جدا ، اوعى بعد ما تعمل setup لسيرفر معين ، اوعى تسيب الـ defaults بتاعت كل حاجة زى ما هى ، لا طبعا غير فيها ، مثلا اول ما تعمل setup لسيرفر

ابدأ غير فى ال Names بتاعت ال Network Interfaces ، يعنى اوعى تخلى ال Name بتاع ال Profiles Interface زى بعض ، لا خلى الاسم لوحده وخلى ال Interface ياخد اسم تانى

بمعنى انك ممكن تعمل delete لل connection ال default اللى عندك وترجع تعمل new connection من اول وجديد عن طريق الامر nmcli ، مثلا

nmcli connection delete eno16777

وبعدين ارجع اعمل بقى

nmcli connection add type ethernet ifname ens33 con-name company

وهكذا بقى ، طيب ليه اصلا انت لازم تعمل الحوار ده ، بكل بساطة علشان موضوع ال Trouble Shooting يكون سهل عليك ومتنساش ان انت ممكن برضو تستخدم ال **nmtui** ، اللى **Network Manager Text User Interface**

طيب احنا دلوقتى بدأنا فى عملية ال Installing لل ipa-server ، عن طريق الامر

yum install ipa-server

وطبعا مش عايز اقولك بقى ال ipa هيروح يعمل install لكمية كبيرة فشخ من ال Dependencies اللى هو محتاجها زى ال apache web server وزى ال kerberos وغيرهم وتقريبا كمان هينزل معاهم ال pki

والمرة التانية هنعمل install لل **ipa-client** عن طريق الامر

yum install ipa-client

علشان دى اللى هتسمحلك انك تعمل authenticate من السيرفر

طيب دلوقتى بقى قبل ما نعمل configure لل ipa-server او حتى ال ipa-client ، لازم يكون عندك DNS Infrastructure ، طبعا برضو متنساش انه مش حاجة ضرورية بالنسبالك

وده معناه انك بكل بساطة ممكن تستخدم زى ما انت عارف ال **hosts file** او ممكن برضو متستخدمهاش اساسا ، بس مع ال IPA Server انت لازم يكون عندك Resolution ، يعنى اى نوع من ال Resolution سواء عن طريق ال Hosts File او عن طريق ال DNS ، يعنى زى انك تعدل ملف ال

/etc/hosts

بس ده طبعا مش ال recommended settings

ولكن الحاجة ال recommended وهى انه يكون عندك DNS Infrastructure وده طبعا موضوع مفيهوش نقاش خالص ، و اى شبكة فى الدنيا فى حاجتين مهمين مينفعش ميكونوش موجودين اول حاجة وهى ال NTP Service ودى طبعا لل Time والحاجة التانية وهى ال DNS Server

طيب دلوقتى ال IPA علشان يشتغل ، لازم يكون عندك اى نوع من ال Resolution ، طيب اولا انت هتفتح ملف ال

/etc/hosts

وهتضيف ip كل جهاز عندك واسمه زى كده مثلا

```
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
172.16.214.128          centos-server       server
172.16.214.129          mini-server         client
```

ودلوقتى بقى تجرب تعمل ping على ال server وعلى كلمة client علشان تتأكد ان كله تمام

ping server

ping client

طيب دلوقتى بقى هناخد secure copy من ملف ال /etc/hosts ونحطه فى الجهاز التانى عن طريق الامر

scp /etc/hosts client:/etc/

وبعدين تروح للجهاز اللى نقلتله ملف ال hosts وتجرب ال ping على ال **client** وعلى ال **server** ، وعن طريق الحركة دى او الطريقة دى ، كده الجهازين ممكن يكلموا بعض عن طريق الاسم وليس عن طريق ال ip ، وده اللى كنا بنتكلم عليه فوق

وبكده انت مش محتاج ال DNS فى حاجة ، لانك كده انت هت hard code الكلام ده بايدك

تعالى بقى نعمل install لل ipa سيرفر ، عن طريق الامر

ipa-server-install

ولو طلعلك ال error ده وانت بتعمل install لل ipa

Example: master.example.com.

Server host name [centos-server]:

ipa.ipapython.install.cli.install_tool(CompatServerMasterInstall):
ERROR

Invalid hostname 'centos-server', must be fully-qualified.

ipa.ipapython.install.cli.install_tool(CompatServerMasterInstall): ERROR

The ipa-server-install command failed. See /var/log/ipaserver-install.log for more information

طيب يبقى انت لازم تعدل فى ملف ال hosts ، وتخلى اسم ال domain كامل زى مثلا

centos.server.com

وترجع تعمل install لل IPA من تانى

دلوقتى بالنسبة بقى لل ipa admin passwd فدى عبارة عن الباسورد بتاع ال admin اللى انت هت login منه من خلال ال GUI ، يبقى كده ال Directory Manager دى وظيفتها علشان تعمل manipulate لل LDAP DataBase من خلالها ، اه وحاجة كمان لازم متخليش السيرفر يبقى idle يعن متخليهوش يدخل فى وضع ال hibernate ، يعنى لازم تنفذ الامر

ls -lhR /

فى shell تانية علشان الجهاز يكون active

وطبعا ال IPA تعتبر من ال Best Infrastructe Solutions الموجودة حاليا فى العالم ، وطبعا من مميزاته انه ممكن ي integrate مع ال Active Directory بكل سهولة ، وبكده ممكن يكون عندك دومين واحد ، وكل الاجهزة اللى عليها ويندوز بت **Authenticate** من ال Active Directory ، وبرضو لو عندك اجهزة شغالة لينكس فهى بت Push ال Policy من ال IPA

وده معناه انك ممكن تحقق حاجة اسمها **Single Sign ON** للشركة اللى انت شغال فيها او للمؤسسة

وحاجة كمان لو انت وانت بتسطب ال IPA ، جالك رسالة وهى

Your system is running out of entropy

فده معناه انه بيحذرك وبيقولك ان الجهاز بتاعك شبه IDLE يعنى زى معمول ليه hibernate كده ، وهو كده مش قادر يعمل generate ل bits كفاية علشان يعمل generate لل keys بتاعتك ، فانت اللى عليك انك تخلى السيرفر او الجهاز يعمل اى مجهود زى انه مثلا يبفذ الامر الكبير ده

ls -lhR /

او بشكل ادق انها تعمل generate لل keys اللى ال installation محتاجها علشان يكمل

كده هو بعد ما خلص عملية ال installation للل ipa-server ، جابلك الملحوظة دى

Next steps:

1. You must make sure these network ports are open:

TCP Ports:

*** 80, 443: HTTP/HTTPS**

*** 389, 636: LDAP/LDAPS**

*** 88, 464: kerberos**

UDP Ports:

*** 88, 464: kerberos**

*** 123: ntp**

2. You can now obtain a kerberos ticket using the command: 'kinit admin'

This ticket will allow you to use the IPA tools (e.g., ipa user-add)

and the web user interface.

فاول حاجة انت لازم تعمل allow للل ports دى عن طريق ال firewall ، ولحسن حظك انك لو شغال على centos 7 core ، فانت اصلا مش محتاج تعمل allow ، علشان centos بتعمل accept لاى connection جايلها الا فى حالات

طيب علشان نبدأ نشتغل بقى ، تعالى بقى ننفذ الامر التالى وهو

kinit admin

ودى انا بنفذها علشان اخد حاجة اسمها **Ticket** من ال Kerberos Service

طب اى بقى ال Ticket دى ؟

بص دى ممكن تعتبرها زى ال Ticket كده علشان تقدر تتعامل مع ال

Kerberos Service ، وخليك فاكر ان ال Kerberos هو ال Authentication

Server اللى موجود عندك ، فعلشان اقدر انى اتعامل مع ال kerberos ك

admin ، فانا روحت طلبت ال Ticket عن طريق ال **kinit admin** مستخدما

انهى rule بقى ؟ طبعا هستخدم ال rule بتاعت الراجل اللى اسمه admin ،

طبعا هيطلب منك ال password بتاع ال admin بتاع ال domain اللى عندك

بعد كده هو راح جابك ال Ticket وخلاها تكون valid لمدة 24 ساعة

icket cache: KEYRING:persistent:0:0

Default principal: admin@SERVER.COM

Valid starting Expires Service principal

06/18/2018 22:46:28 06/19/2018 22:46:22

krbtgt/SERVER.COM@SERVER.COM

وبكده انت ممكن تنفذ او تدى اى administrative commands للل ipa server اللى عندك

تعالى بقى نعمل check للل Status بتاعت ال ipa server عن طريق الامر

ipactl status

كده بالمنظر ده كل ال service شغالة

Directory Service: RUNNING
krb5kdc Service: RUNNING
kadmin Service: RUNNING
httpd Service: RUNNING
ipa-custodia Service: RUNNING
ntpd Service: RUNNING
pki-tomcatd Service: RUNNING
ipa-otpd Service: RUNNING
ipa: INFO: The ipactl command was successful

كده بقى ال **ipa server** بتاعك **fully running**

الخطوة اللى بعد كده تعالى نضيف user ، عن طريق الامر

ipa user-add

بعدا ما يخلص بقى الاسم اللى هيقدر يعمل منه login هو ده

Principal name: ahmed@SERVER.COM

تعالى بقى نضيف باسوورد لليوز ده عن طريق الامر

ipa passwd ahmed

كده احنا خلصنا جزء ال ipa server install

نروح بقى على جهاز ال client ونخليه يعمل authenticate من عند ال server

يبقى اول خطوة هنعملها وهى اننا هنسطب ال ipa client على جهاز ال client عن طريق الامر

ipa-client-install

ومتنساش برضو الامر

ls -lhR /

علشان تطلع الجهاز من حالة ال ide او ال hibernate اللى هو فيها

ملحوظة لو انت مش ظابط الوقت هيظهرك التحذير ده

WARNING: ntpd time&date synchronization service will not be configured as
conflicting service (chronyd) is enabled
Use --force-ntpd option to disable it and force configuration of ntpd

سيبه شوية وهو هيكمل لوحده وهيسألك شوية اسئلة

ولو جاتلك الرسالة دى

DNS discovery failed to determine your DNS domain

معناها انك معندكش dns ،وده عادى لاننا اصلا هنا مش فى بيئة production حقيقية

خلى بالك بقى من الاسئلة اللى هيسألهالك وانت بتعمل setup لل ipa-client اول سؤال

Provide the domain name of your IPA server (ex: example.com)

هنا بيقولك ادينى اسم ال domain بتاع ال ipa server ، وهنا انت هتكتب server.com كلمتين بس

وبعدين هيسألك

Provide your IPA server name (ex: ipa.example.com):

هنا هو عايز الاسم بتاع ال IPA Server ، يبقى انت هتكتب الاسم كامل

centos.server.com

وبعدين yes ، وبعديها برضو yes ، وبعدها بقى اكتب admin واكتب الباسورد بتاعه

فى شوية ملحوظات كتيرة هنا بمناسبة عملية تسطيب ال IPA Server ، اولا ال ipa-server لازم تكون على **subnet mask 24** مش 32 ، والا مش هتتسطب ، ثانيا بقى لو انت جيت تنفذ الامر اللى هو

kinit admin

وظهرتلك رسالة الخطأ دى

kinit: Cannot contact any KDC for realm 'AHMED.COM' while getting initial credentials

فدى اسبابها كالاتى

Cause:

This issue occurs for multiple reasons, such as the following:

Network connectivity issues

DNS issues – Can be isolated by hard coding KDC server in /etc/hosts

Firewall rules – Use telnet <KDC_Server> 88 to identify the issue

Missing KDC server info in krb5.conf

Missing [domain_realm] in krb5.conf

Unresponsive / dead KDC server (either AD or MIT KDC)

فانت كل اللى عليك انك تفتح ملف ال

/etc/hosts

وتشوف الايبى بتاع الجهاز صح ولا لأ ، بمعنى انك وانت بتسطب ال ipa-server كان مثلا الايبى

192.168.1.9

جيت انت طفيت الجهاز وبعدين فتحته ، فراح الجهاز واخد ايبى جديد مثلا

192.168.1.7

هنا بقى لازم تعدل ملف ال /etc/hosts من تانى وبعدين تعمل reboot للجهاز ، هتلاقى ال service دى رجعت اشتغلت معاك تانى

ابقى بص على اللينك ده

https://community.hortonworks.com/content/supportkb/150207/errorcannot-contact-any-kdc-for-realm-abccom-while.html

الملحوظة التانية والاخطر وهى انك لو جيت تنفذ الامر ده

ipa user-add

وطلعتلك رسالة الخطأ دى

ipa: ERROR: did not receive Kerberos credentials

فانت هنا لسه مخدتش صلاحيات ال admin ، يعنى المفروض تنفذ قبلها **kinit admin** ولكن خلى بالك ، ان فى فرق لما تنفذ الامر اللى هو **kinit admin** وتكون كاتب sudo قبلها وفى فرق لما تنفذه وانت مش كاتب sudo قبله وده فى حالة ان انت مش بتستخدم ال root ك user فى الترمنال

وخلى بالك برضو ان لازم يكون اسم ال **hostname** بتاع ال Central Server هو هو نفس الاسم بتاع ال Client ، بمعنى ان انت لو عندك مثلا سيرفر باسم **company.ahmed.com**

فلازم برضو الجهاز بتاع ال Client يكون ال hostname بتاعه برضو مشترك فى ال domain اللى هو ahmed.com ، يعنى هيكون كده **client.ahmed.com**

تعالى بقى نجرب نعمل connect على ال central server ونستخدم ال user name اللى احنا عملناه عن طريق الامر ipa user-add

طيب الموضوع هيتم ازاى ، اول حاجة انت هتعمل اتصال ssh عن طريق ال ip بتاع جهاز ال client وهتستخدم اليوزر نيم اللى انت عملته عن طريق ip user-add

يعنى ال connection هيبقى كده

ssh ahmed@192.168.1.8

بعدها هيطلب منك الباسورد اللى انت عملته لل user ده ، عن طريق الامر ipa passwd ahmed ، يبقى هتكتب الباسورد

وبعدها بقى هيطلب منك انك تغير الباسورد بتاعتك اللى اتعملت عن طريق الامر ipa passwd ahmed ، يعنى هتشوف الرسالة دى

[user1@server ~]$ ssh ahmed@192.168.1.8
Password:
Password expired. Change your password now.
Current Password:

اول حاجة هتكتب الباسورد القديمة ، وبعديها بقى هتكتب الباسورد الجديدة ، وكده مبروك عليك انت قدرت تعمل authenticate من ال Central Server

Could not chdir to home directory /home/ahmed: No such file or directory
-sh-4.2$
-sh-4.2$

خلى بالك كده انت عملت connect على جهاز ال Client ، وانت كده بتستخدم ال user اللى اتعمله create على ال Central Server

طيب لو عايز تدمر ال session اللى انت خدتها عن طريق الامر kinit admin ممكن تستخدم الامر

kdestroy

وطبعا انت دلوقتى لو جيت تجرب فى المتصفح

192.168.1.8

ممكن فى الغالب انه ميفتحش معاك ، لان من اسوأ الحاجات انه بيحاول يجيب ديما من الاسم اللى انت عملته فى etc/hosts

فكده الحل انك تعدل فى ملف ال hosts بتاع النظام الرئيسى بتاعك ، وتخلى ال ip بتاع ال Central Server بيقابله الاسم ده مثلا

company.ahmed.com

كده انت محتاج انك تعمل home directory لل user اللى هيعمل connect من خلال جهاز ال client ، يبقى انت هتروح على جهاز ال client وتنفذ الامر ده علشان يعمل يعمل autocreate لل home directory بتاعت كل user

authconfig --enablemkhomedir --update

يبقى ملخص اللى احنا عملناه ان اليوزر بيكون موجود على السيرفر واحنا بنعمل **authenticate** من جهاز تانى خالص

اخر حاجة وهو ان انت طبعا ممكن تغير ال shell بتاعت كل يوزر ، وزى ما انت عارف ان فى shell اسمها **sh** وواحدة اسمها **bash** وهكذا بقى يعنى الشكل ده هو ال shell بتاعت ال sh

-sh-4.2$

وبتكون موجودة فى

/bin/sh

ولما تغيرها وتخليها bash ، هتتغير وتبقى كده

[ahmed@client ~]$

وخليك فاكر ان لو ال shell متغيرتش ، يبقى لازم تعمل reboot لل central server و لجهاز ال client كمان تقريبا

Every Thing Working With reboot 😂😂

اخر ملحوظة وهى ان ال IPA لما تحاول تشغله فى اى Production Environment حاول يكون عندك Proper Sizing لل IPA ، وده اهم حاجة ، يعنى لازم تكون عامل plan لل size بتاع ال ipa مش مجرد انه يكون عندك جهاز شغال وتروح تسطب ال ipa عليه او تعمل install لاى Identity Managment عليه ، لانه زى ما انت عارف ال Identity Managment ده مش بيكون مجرد service واحدة ، لا لا دى عبارة عن collection من ال services

لحد هنا كده احنا خلصنا الفديو رقم 60 ، لسه باقى بقى الفديو اللى بعده رقم 61 وده مفيهوش تلخيص او بمعنى اخر عبارة عن انك بتطبق الكلام اللى قولنا عليه فوق لكن مع الويندوز

وده لينك Guide مجانى تبع RedHat بيتكلم عن ال Identity Managment

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/linux_domain_identity_authentication_and_policy_guide/installing-ipa

وده برضو لينك لموقع **Certdpot** بيشرح بطريقة سهلة جدا ازاى تسطب ال IPA Server ياريت تبص عليه ، هيفيدك جدا

https://www.certdepot.net/rhel7-configure-freeipa-server/