

# مماظن ىل عة قءاصم لاء نئاك نم ققحت لاء ربع Microsoft AD ة قءاصم لاء FireSIGHT SSL/TLS

## المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [الإجراء](#)

## المقدمة

يمكنك تكوين مركز إدارة FireSIGHT للسماح لمستخدمي Active Directory LDAP الخارجيين بمصادقة الوصول إلى واجهة مستخدم الويب و CLI. تناقش هذه المقالة كيفية تكوين كائن المصادقة لمصادقة Microsoft AD عبر SSL/TLS واختباره واستكشاف أخطائه وإصلاحها.

## المتطلبات الأساسية

توصي Cisco بأن تكون لديك معرفة بنظام إدارة المستخدم والمصادقة الخارجية على مركز إدارة FireSIGHT.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

## الإجراء

الخطوة 1. قم بتكوين كائن المصادقة دون تشفير SSL/TLS.

1. قم بتكوين كائن المصادقة كما تفعل عادة. خطوات التكوين الأساسية للمصادقة المشفرة وغير المشفرة هي نفسها.

2. تأكد من أن كائن المصادقة يعمل ويمكن لمستخدمي AD LDAP المصادقة غير المشفرة.

الخطوة 2. اختبر كائن المصادقة عبر SSL و TLS بدون شهادة CA.

اختبر كائن المصادقة عبر SSL و TLS بدون شهادة CA. إذا واجهت مشكلة، فيرجى إستشارة مسؤول النظام لحل هذه المشكلة على خادم AD LDS. إذا تم تحميل شهادة مسبقاً إلى كائن المصادقة، يرجى تحديد تم تحميل الشهادة (حدد لمسح الشهادة المحملة) لمسح الشهادة واختبار AO مرة أخرى.

إذا فشل كائن المصادقة، فيرجى إستشارة مسؤول النظام للتحقق من تكوين AD LDS SSL/TLS قبل الانتقال إلى الخطوة التالية. ومع ذلك، يرجى الاستمتاع بمواصلة الخطوات التالية لاختبار كائن المصادقة بشكل أكبر باستخدام شهادة المرجع المصدق.

### الخطوة 3. تنزيل شهادة Base64 CA.

1. تسجيل الدخول إلى AD LDS.
  2. افتح مستعرض ويب واتصل ب <http://localhost/certsrv>
  3. انقر على تنزيل شهادة CA أو سلسلة الشهادات أو CRL
  4. أختَر شهادة المرجع المصدق من قائمة شهادة المرجع المصدق "وBase64" من طريقة الترميز
  5. انقر على الارتباط تنزيل شهادة المرجع المصدق " لتنزيل ملف certnew.cer.
- الخطوة 4. تحقق من قيمة الموضوع في الوحدة.

1. انقر بزر الماوس الأيمن فوق certnew.cer وحدد فتح.
2. انقر فوق علامة التبويب تفاصيل وحدد <all> من خيارات show المنسدلة
3. تحقق من القيمة لكل حقل. تحقق بشكل خاص من مطابقة قيمة الموضوع لاسم مضيف الخادم الأساسي لكائن المصادقة.
5. قم باختبار شهادة على جهاز يعمل بنظام التشغيل Microsoft Windows. يمكنك إجراء هذا الاختبار على "مجموعة عمل" أو "مجال" متصل بجهاز Windows.

**تلميح:** يمكن استخدام هذه الخطوة لاختبار شهادة المرجع المصدق على نظام Windows قبل إنشاء كائن المصادقة على مركز إدارة FireSIGHT.

1. انسخ شهادة المرجع المصدق إلى C:\Certificate أو أي دليل مفضل.
2. قم بتشغيل سطر الأوامر في Windows. cmd.exe كمسؤول
3. إختبار شهادة المرجع المصدق باستخدام الأمر certutil

```
cd c:\Certificate
```

```
certutil -v -urlfetch -verify certnew.cer >cacert.test.txt
```

إذا كان جهاز Windows منضمًا بالفعل إلى المجال، يجب أن تكون شهادة المرجع المصدق في مخزن الشهادات ويجب ألا يكون هناك خطأ في cacert.test.txt. ومع ذلك، إذا كان جهاز Windows على مجموعة عمل، فقد ترى إحدى الرسالتين وفقاً لوجود شهادة CA في قائمة المرجع المصدق الموثوق به.

أ. تم الوثوق ب CA ولكن لم يتم العثور على CRL ل CA:

```
ERROR: Verifying leaf certificate revocation status returned The revocation function was unable to check revocation because the revocation server was offline. 0x80092013 (-2146885613)
```

```
CertUtil: The revocation function was unable to check revocation because the .revocation server was offline
```

ب. المرجع المصدق غير موثوق به:

```
Verifies against UNTRUSTED root  
Cert is a CA certificate
```

```
Cannot check leaf certificate revocation status  
.CertUtil: -verify command completed successfully
```

إذا ظهرت لك أي رسائل خطأ أخرى مثل أدناه، فيرجى إستشارة مسؤول النظام لحل المشكلة الموجودة على AD LDS و CA الوسيط. رسائل الخطأ هذه هي دلالة على شهادة غير صحيحة، موضوع في شهادة CA، سلسلة شهادات مفقودة، إلخ.

Failed "AIA" Time: 0

Failed "CDP" Time: 0

Error retrieving URL: The specified network resource or device is no longer available

الخطوة 6. بمجرد التأكد من صحة شهادة CA واجتياز الاختبار في الخطوة 5، قم بتحميل شهادة المنتج إلى كائن المصادقة ثم قم بتشغيل الاختبار.

الخطوة 7. قم بحفظ كائن المصادقة وإعادة تطبيق نهج النظام.

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 ا ة مچرت ل ض ف ا ن ا ة ظ حال م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب  
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه  
ي ل ا م ا 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