



ainfct

المؤسسة العربية للاستشارات والتدريب وتطوير الأداء
AINFCT | info@ainfct.com | www.ainfct.com

Network Troubleshooting and Diagnostics

فكرة الدورة

تزداد أهمية استكشاف أعطال الشبكات مع اعتماد المؤسسات على الاتصال المستمر، والخدمات السحابية، والتطبيقات الموزعة، والبيئات الهجينة. وأي خلل في الأداء أو التوجيه أو العناوين أو الخدمات الأساسية قد يؤثر مباشرة في الإنتاجية وتجربة المستخدم واستقرار العمليات. لذلك يحتاج المختصون إلى منهجية تشخيص واضحة تجمع بين فهم طبقات الشبكة، وتحليل الأعراض، واستخدام أدوات القياس، وتوثيق النتائج، وتنفيذ المعالجات دون إحداث مخاطر تشغيلية إضافية.

يركز هذا البرنامج التدريبي من AINFCT على بناء قدرات عملية في تحليل مشكلات الشبكات وتشخيصها، بدءاً من جمع المعلومات وتحديد النطاق، مروراً بفحص الاتصال والتوجيه وخدمات DNS وDHCP وNAT، وصولاً إلى تحليل الحزم ومراقبة الأداء والتعامل مع الأعطال المتكررة. ويمنح البرنامج المشاركين إطاراً منظماً يساعدهم على تحويل البلاغات الفنية إلى قرارات تشخيصية دقيقة ومعالجات موثقة.

- يوفر البرنامج قيمة تطبيقية واضحة من خلال تمارين وسيناريوهات تحاكي بيئات تشغيل حقيقية.

أهداف الدورة

فيما يلي الأهداف الرئيسية لهذا البرنامج التدريبي:

- تطبيق منهجيات منظمة لتشخيص أعطال الشبكات.
- تحليل مشكلات الاتصال والتوجيه وخدمات الشبكة.
- استخدام أدوات فحص الشبكات وتحليل الحزم.
- تحديد أسباب ضعف الأداء والانقطاعات المتكررة.
- توثيق إجراءات التشخيص والمعالجة الفنية.
- تحسين جودة التصعيد والتواصل أثناء الأعطال.

منهجية الدورة

- شرح تفاعلي مدعوم بأمثلة تشغيلية واقعية.
- تمارين عملية على أدوات وأوامر التشخيص.
- تحليل سيناريوهات أعطال متعددة الطبقات.
- مناقشات موجهة حول التوثيق والتصعيد.
- مراجعات قصيرة لربط المفاهيم بالتطبيق.

أثر الدورة على المنظمة

- يمكن تعزيز استقرار الشبكات المؤسسية من خلال:
- تقليل زمن اكتشاف الأعطال ومعالجتها.
- تحسين موثوقية الخدمات والاتصال الداخلي.
- رفع جودة التوثيق الفني والتصعيد.
- دعم قرارات تشغيلية قائمة على بيانات.

أثر الدورة على المتدربين

يساعد البرنامج المشاركين على:

- تشخيص الأعطال بمنهجية فنية واضحة.
- قراءة مؤشرات الشبكة بثقة مهنية.
- استخدام أدوات التحليل والتتبع بكفاءة.
- إعداد تقارير فنية مختصرة ودقيقة.

الشهادات

شهادة معتمدة من AINFCT

الفئة المستهدفة

يناسب هذا البرنامج العاملين في تشغيل الشبكات والدعم الفني والبنية التحتية الذين يحتاجون إلى تحسين قدراتهم في التشخيص والمعالجة. كما يفيد المشاركين المسؤولين عن متابعة البلاغات الفنية وتحليل أسباب الانقطاع وضعف الأداء.

- مهندسو الشبكات ومشرفو البنية التحتية.
- فنيو الدعم الفني ومراكز الخدمة.
- مسؤولو تشغيل ومراقبة الشبكات.
- مختصو أمن الشبكات والجدران النارية.
- العاملون في بيئات الشبكات السحابية والهجينة.

اليوم الأول: أساسيات منهجية استكشاف الأعطال

- مفهوم العطل الشبكي والفرق بين العرض والسبب.
- خطوات جمع المعلومات وتحديد نطاق المشكلة.
- بناء الفرضيات الفنية واختبارها تدريجياً.
- توثيق التغييرات والنتائج أثناء التشخيص.
- معايير التصعيد وإغلاق البلاغات الفنية.

اليوم الثاني: مراجعة نماذج الشبكات والتدفق الطبقي

- استخدام نموذج OSI في عزل المشكلات.
- تحليل علاقة الطبقات بالأعراض التشغيلية.
- تتبع مسار البيانات من المستخدم إلى الخدمة.
- التمييز بين مشكلات الجهاز والشبكة والتطبيق.
- تحديد نقطة الفشل المحتملة بدقة.

اليوم الثالث: تشخيص مشكلات الطبقة الفيزيائية والربط

- فحص الكابلات والمنافذ وحالة الواجهات.
- قراءة مؤشرات السرعة والازدواج والأخطاء.
- تحليل مشكلات التوصيل والتقطيع المتكرر.
- استخدام أوامر حالة الواجهة والإحصاءات.
- ربط الأعطال الفيزيائية بتأثيرها التشغيلي.

اليوم الرابع: تشخيص عناوين IP والبوابات

- فحص إعدادات IP والقناع والبوابة الافتراضية.
- اكتشاف التعارضات والأخطاء في العناوين.
- اختبار الاتصال المحلي والبعيد تدريجياً.

- تحليل جداول ARP وسلوك الجيران.

- معالجة أخطاء التكوين الأساسية.

اليوم الخامس: تشخيص DHCP وDNS والخدمات الأساسية

- تحليل دورة الحصول على عنوان DHCP.

- فحص نطاقات العناوين والاستثناءات والحجوزات.

- تشخيص فشل الاستعلامات وحل الأسماء.

- مقارنة نتائج DNS الداخلية والخارجية.

- تحديد أثر الخدمات الأساسية على التطبيقات.

اليوم السادس: تشخيص التبديل وVLAN

- مراجعة حالة VLAN والعضوية على المنافذ.

- تشخيص أخطاء Trunk وNative VLAN.

- تحليل مشكلات Spanning Tree الأساسية.

- اكتشاف حلقات الشبكة والبث الزائد.

- ربط أخطاء التبديل بانقطاع المستخدمين.

اليوم السابع: تشخيص التوجيه والمسارات

- قراءة جدول التوجيه ومصدر كل مسار.

- استخدام Ping وTraceroute بفعالية.

- تحليل مشكلات المسارات الافتراضية والثابتة.

- تشخيص فقدان المسارات وعدم التماثل.

- تقييم تأثير التوجيه على جودة الخدمة.

اليوم الثامن: تشخيص NAT وACL والجدران النارية

- فحص ترجمات NAT وتأثيرها على الاتصال.

- تحليل قواعد ACL وسياسات السماح والمنع.

- تتبع الاتصال عبر الجدران النارية.

- تمييز مشكلات الشبكة عن المنع الأمني.
- توثيق نتائج الاختبارات قبل تغيير السياسات.

اليوم التاسع: أدوات التشخيص وأوامر الفحص

- استخدام أوامر ipconfig و ifconfig و ip.
- تحليل نتائج ping و traceroute و pathping.
- فحص المنافذ باستخدام telnet و nc.
- استخدام nslookup و dig في DNS.
- تنظيم نتائج الأوامر داخل سجل تشخيص.

اليوم العاشر: تحليل الحزم ومراقبة المرور

- مبادئ التقاط الحزم وتحليلها.
- اختيار نقطة الالتقاط المناسبة داخل الشبكة.
- قراءة TCP Handshake ومؤشرات الفشل.
- تحديد إعادة الإرسال والازدحام والرفض.
- استخدام المرشحات لتسريع التحليل.

اليوم الحادي عشر: تشخيص الأداء والازدحام

- مؤشرات الكمون والفقد والتذبذب.
- تحليل استهلاك النطاق والتدفقات الثقيلة.
- فحص أخطاء الواجهات وقوائم الانتظار.
- تشخيص بطء التطبيقات عبر الشبكة.
- تحديد العلاقة بين الأداء والتجربة النهائية.

اليوم الثاني عشر: مراقبة الشبكة والسجلات

- استخدام SNMP ومؤشرات الحالة التشغيلية.
- قراءة السجلات وربط الأحداث زمنياً.
- التعامل مع التنبيهات وتحديد الأولويات.

- بناء خطوط أساس للأداء الطبيعي.
- ربط المراقبة بالاستجابة الاستباقية.

اليوم الثالث عشر: تشخيص الشبكات اللاسلكية

- فحص التغطية والتداخل وقوة الإشارة.
- تحليل مشكلات المصادقة والارتباط.
- مراجعة القنوات والسعات ومناطق الخدمة.
- تمييز مشكلات اللاسلكي عن الشبكة الخلفية.
- توثيق نتائج الفحص اللاسلكي.

اليوم الرابع عشر: تشخيص البيئات الهجينة والسحابية

- فحص الاتصال بين المواقع والخدمات السحابية.
- تحليل VPN والأنفاق والتوجيه الهجين.
- تشخيص مشكلات DNS بين البيئات.
- مراجعة سياسات الأمن ومجموعات الشبكة.
- تحديد حدود المسؤولية في البيئات المشتركة.

اليوم الخامس عشر: تطبيقات عملية ومراجعة تكاملية

- تحليل سيناريوهات أعطال متعددة الطبقات.
- بناء خطة تشخيص من البلاغ إلى المعالجة.
- إعداد تقرير فني مختصر عن العطل.
- مناقشة أخطاء التشخيص الشائعة.
- مراجعة أفضل ممارسات التحسين المستمر.

يمتد البرنامج لمدة 15 يوماً تدريبياً، بواقع 4 ساعات تدريبية يومياً. يبدأ كل يوم بمراجعة موجزة لما سبق، ثم عرض المحور الفني، يتبعه تطبيق عملي أو سيناريو تشخيص، وينتهي اليوم بخلاصة تشغيلية تربط الأدوات والنتائج بقرارات المعالجة والتوثيق.

course _ assessment

يعتمد التقييم على المشاركة الفعالة، وتمارين التشخيص، وتحليل السيناريوهات، وجودة التوثيق الفني أثناء الأنشطة. يحصل المشاركون في نهاية البرنامج على شهادة حضور/إتمام من AINFCT وفق متطلبات الحضور والمشاركة المعتمدة.

course _ key _ competencies

- تشخيص أعطال الشبكات.
- تحليل الاتصال والتوجيه.
- استخدام أدوات الفحص.
- تحليل الحزم والأداء.
- توثيق البلاغات الفنية.
- إدارة التصعيد التشغيلي.

مكتب القاهرة الرئيسي

القاهرة، جمهورية مصر العربية
7 شارع وهران، الطيران، مدينة نصر
201152466358+
info@ainfct.com
ainfct.com

رقم التسجيل الضريبي: 472920235

مكتب مدريد الفرعي

مدريد، إسبانيا
شارع الصحة 3، وسط المدينة، 28013 مدريد

training@ainfct.com

ainfct.com