Napjaink hálózati kihívásainak hatékony kezelése ThousandEyes, DNA Center, Catalyst 9000 app-hosting és Aironet szenzor eszközökkel

A pandémia olyan lépésekre kényszerítette a nagyvállalatokat, amelyek korábban elképzelhetetlenek voltak; tömegek vonultak home office-ba, a chiphiány és szállítási nehézségek miatt még gyorsabb ütemben költöznek a felhőbe az alkalmazások. Ennek nyilvánvaló előnyei mellett nem szabad elfeledkeznünk a hátrányokról sem; a vállalaton belüli hálózati vizibilitás elveszett, a hibakeresés sokkal nehezebbé vált. Korábban soha nem látott mértékben függ a vállalat működése az internet szolgáltatóktól, az üzemeltetés számára lépten-nyomon "vakfoltok" találhatóak a hálózati kapcsolatokban. Felhasználói panaszok esetén nem állnak rendelkezésre a korábban megszokott hibakeresési eszközök, hiszen már csak a komponensek egy része található "házon belül", az üzemeltetési felelősség azonban nem csökkent. A felhő az új adatközpont, az internet az új hálózat, az otthon az új iroda.

CISCO ThousandEyes

Erre próbál megoldást nyújtani a ThousandEyes. A Dashboard-on teszteket hozunk létre, amelyekben definiáljuk a számunkra kritikus alkalmazásokat, erőforrásokat, paramétereket – pl. rendelkezésre állás, válaszidő, DNS, BGP monitoring, csomagvesztés, stb. A "magasabb" rétegbeli mérések általában tartalmazzák az alacsonyabbakat is, pl. egy HTTP teszt magában foglalja a BGP route és útvonal vizualizációt is. Ezeket a teszteket végül az általunk kiválasztott cloud, endpoint vagy enterprise agent-ek futtatják, a mérések eredménye a ThousandEyes Dashboard-on követhető, de API-n keresztül természetesen bármilyen rendszerbe átemelhetőek.

A megoldás proaktív, gyártófüggetlen és egyszerűen telepíthető.

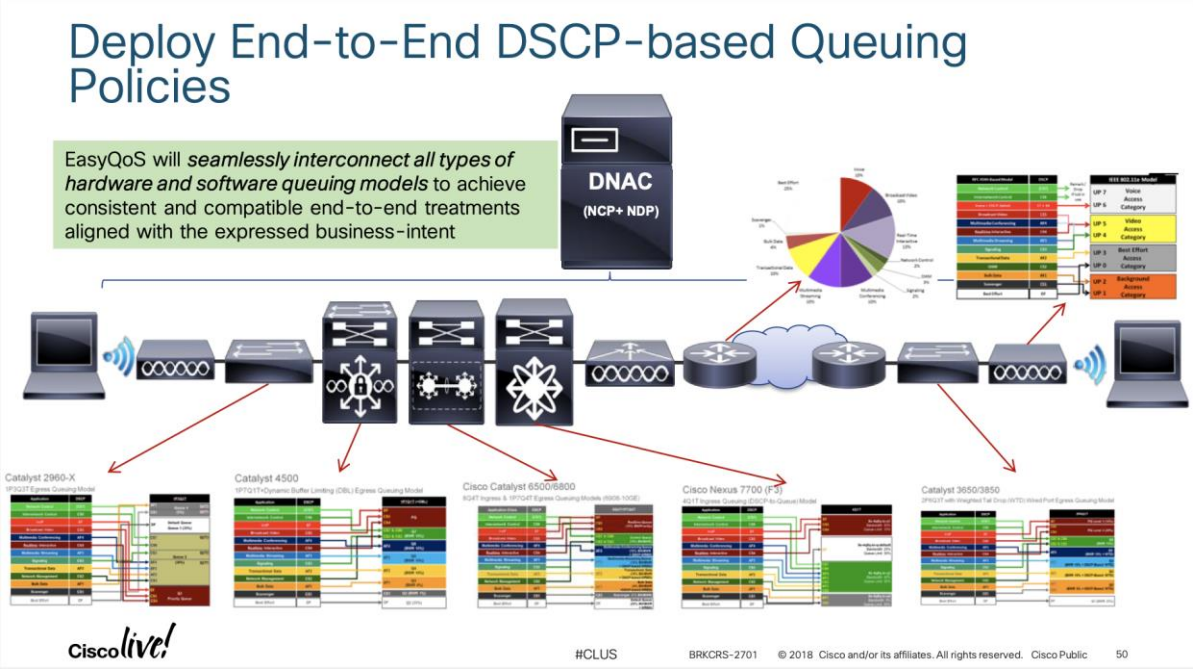
Az agent-ekből három változatot különböztetünk meg. Az első az ún. "cloud agent", amelyek több, mint 200 adatközpontban, Tier 1, 2, 3 szolgáltatóknál, felhőszolgáltatóknál találhatóak és a ThousandEyes üzemelteti őket. A második típus az "endpoint agent", amelyet a felhasználók számítógépére telepítünk. A harmadik opció pedig az enterprise agent használata, amelyet saját adatközpontba, VPC-be vagy akár hálózati eszközökre telepíthetünk. Ezek segítségével a vállalaton belüli, publikus interneten nem elérhető erőforrások is monitorozhatók.

Röviden összefoglalva tehát a ThousandEyes segítségével láthatóvá válnak azok nagyvállalati demarkációs ponton túlnyúló kapcsolatok is amelyek korábban rejtve voltak a hálózati mérnökök szeme előtt. Pontos, hiteles, gyors információkkal rendelkezünk több független szemszögből a szolgáltatások rendelkezésre állásáról és performanciájáról, a BGP útvonalakról, az online konferenciák video és hang minőségéről. Hiba esetén bizonyíték van a kezünkben egy alkalmazás rétegbeli hibára vagy szolgáltató oldali hálózati lassulásra, amelyet snapshot formájában meg is oszthatunk az érintettekkel, gyorsítva ezzel a hiba elhárítását.

Cisco DNA Center

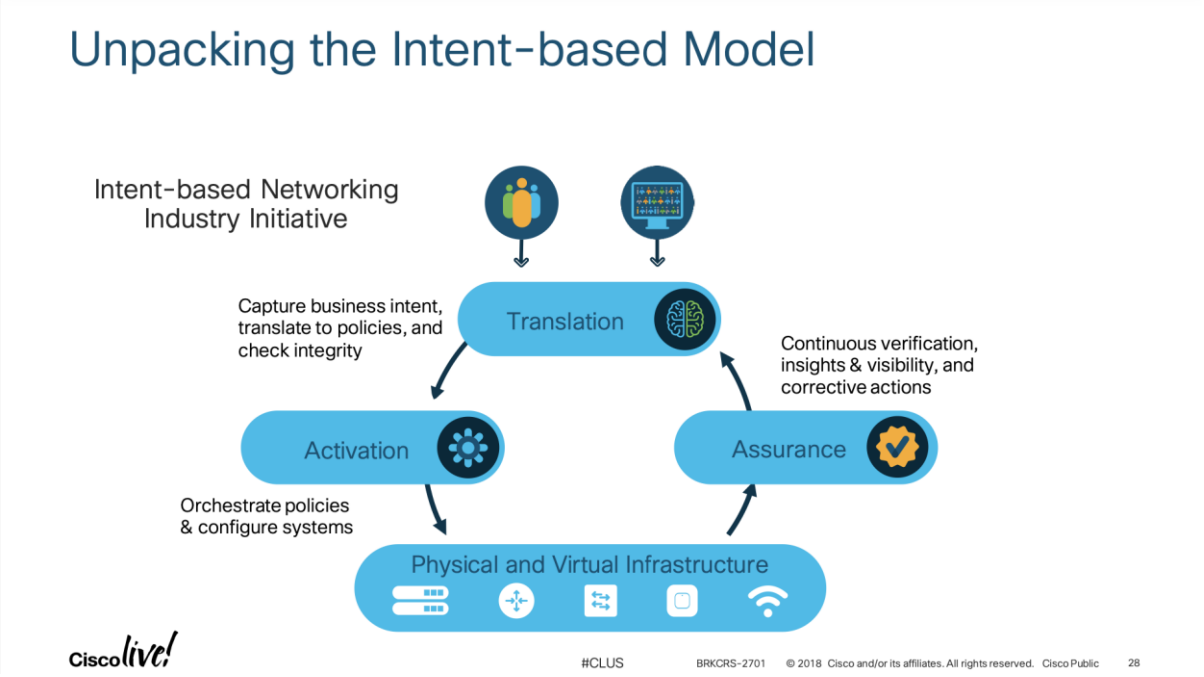
A nagyvállalati hálózati eszközök management platformja a Cisco DNA Center. Ahhoz, hogy szerepét megértsük definiálnunk kell az Intent-Based Networking – nagyon csúnyán magyarra fordítva “cél alapú hálózati működés” fogalmát, amelyet a Cisco-nál a DNA (Digital Network Architecture) segítségével valósítottak meg. Dióhéjban az IBN lényege, hogy a kívánt hálózati működést magas szinten definiáljuk, amelyet a kontroller “fordít le” a hálózati eszközök konfigurációjára.

Gondoljunk pl. egy QoS (Quality of Service) beállításra; gyakorlatilag ahány hardver platform annyi konfigurációs lehetőség és ASIC szintű kötöttség, szoftveres korlátozás. IBN architektúránál QoS esetén nekünk azt kell definiálnunk, hogy az adott alkalmazás üzletileg kritikus vagy nem kritikus és a DNA Center Application Policy-k segítségével – a Cisco Validated Design Guide-k alapján – felkonfigurálja az eszközöket, legyen az switch, router vagy akár WLC.



1. ábra QoS konfigurálása IBN hálózatban

A folyamat azonban itt nem ér véget; a teljes hálózat felfogható egy nagy szenzorszigetként, amelynek adatait a DNA Center gyűjti, korrelálja és elemzi, hogy valóban a kívánt beállításoknak megfelelően működik-e a hálózat. Amennyiben az ügyfél által meghatározott igények a jelenlegi konfigurációval nem teljesülnek a DNA Center adott esetben automatikusan javítja azokat.



2. ábra A hálózat mint szenzorsziget

A DNA Center tehát az IBN/DNA és SD-Access architektúrában a kontroller, orchestrator szerepet tölti be, itt kötelező, ki nem hagyható komponens. Lehetőség van azonban SDA nélkül is használni, tipikus példa a Cisco Prime Infrastructure kiváltása, amelyből a legfrissebb, 3.10-es verziót 2021. november végén adta ki a Cisco, komolyabb funkcionális frissítés ezen a terméken már nem várható.

Már jó ideje rendelkezésre áll a Prime Infrastructure-DNA Center funkció paritást és támogatott eszközöket vizsgáló gyártói tool (PDART) és Prime-DNA Center migrációs tool is, amelynek segítségével a Prime-ban lévő adatok könnyen a DNA Centerbe költöztethetők.

A legtöbb nagyvállalati hálózatban már régóta megtalálható a Catalyst 9000 termékcsalád egy vagy több komponense, a hozzájuk alapesetben 3 évig megvásárolt DNA licensz-szel használható a DNA Center, hiszen a kontrollert önmagában nem szükséges licenszelni (ahogy WiFi-nél a Catalyst 9800 WLC-t sem kell).

A DNA Center is rendelkezik a Prime-ból ismert és szeretett funkciókkal, mint pl. a szoftver frissítés, konfiguráció mentés, topológia rajzolás, és a kor elvárásainak megfelelően természetesen API-n keresztül is elérhető.

A DNA Center bevezetését erősen gátolja, hogy jelenleg csak fizikai appliance formában, azon belül is három méretben rendelhető, ezért a szállítási idők és a bekerülési költségek miatt körülményesebben és magasabb CAPEX-szel integrálható. Kevésbé kritikus monitoring

megoldásként és kisebb méretű hálózatok esetén elég egy szerver, de természetesen lehetőség van telephelyen belüli redundáns cluster és georedundáns cluster kialakítására is.

2023-ban azonban érkezik a virtuális verzió, amely a legkisebb modell skálázhatóságával egyezik meg és futtatható lesz on-prem környezetben vagy akár a felhőben is.

Catalyst 9000 app-hosting

A Catalyst 9000 termékcsalád sok éve velünk van már, a nagyvállalati hálózatok “alap” platformja.

Ahhoz, hogy a felhasználók alkalmazásokat futtathassanak a Cisco egy SDK keretrendszert fejlesztett, ez az ún. CAF, vagyis Cisco Application Hosting Framework. A CAF, vagy más néven IOx (IOS + Linux) eredetileg a fog/edge computing, IoT felhasználási igényeinek kiszolgálására készült. Ez a keretrendszer egységes interface-t biztosít applikáció hosting-hoz. A lényeg, hogy IOx Client segítségével tudunk alkalmazásokat futtatni IOS-XE-n, így a Catalyst 9000 termékcsalád tagjain is. Egy nagyon fontos feltétel, hogy ehhez legalább DNA Advantage licensz-re van szükségünk.

Az egyedileg fejlesztett alkalmazások futtatása komoly biztonsági kockázatot és instabil működést okozhat az eszközön, ezért természetesen a CPU és memória használatot a rendszer korlátozza, illetve 3rd party app-ok esetében a switch belső tárhelye továbbra sem hozzáférhető, követelmény a SSD használata amelyen az alkalmazást tároljuk. Tapasztalatok szerint az ügyfelek többsége az SSD drive-t nem rendeli meg a switch mellé, pedig app-hosting szerepen túl további funkciókat is elláthat, ilyen pl. loggolás. Az SSD pin kóddal védhető és AES-256 hardveres titkosítással ellátott, így a rajta tárolt adatok védve vannak illetéktelen kézbe kerüléskor.

Az IOS XE 17.3.3 verziótól lehetőség van a switch beépített flash-ének használata a Cisco által jóváhagyott alkalmazások számára, amilyen a ThousandEyes agent is, amely így SSD nélkül futtatható.

Az IOS XE már régóta, a 16.12.1 verziótól támogatja a natív Docker konténerizációt. A Docker alkalmazás a fejlesztői környezetből “docker save”-vel egy fájlba menthető, majd feltölthető az eszközre és ott futtatható.

Jogosan merül fel a kérdés, hogy egy switch stack vagy stackwise virtualk esetében hogyan biztosított az alkalmazás futtatás redundanciája. Támogatott az auto-restart, azaz switchover vagy eszköz újraindulás után az alkalmazás újraindul a standby tagon.

ThousandEyes + Catalyst 9300/9400 = Nyerő kombináció!

A Cisco promóciójának keretében minden Catalyst 9300 vagy 9400 switch vásárlásával – amennyiben az DNA Advantage vagy Premier – újabb nevén Expansion Pack – licensszel kerül megrendelésre – ThousandEyes unitokat járnak. Ingyen, ajándékba. ThousandEyes agentek telepítése után ezek a unitok felhasználhatóak tesztek futtatására. Így gyakorlatilag “ingyen” lehet hozzájutni a ThousandEyes szolgáltatásaihoz, amellyel akár egy PoC/PoV teszt, akár egy éles bevezetés elkezdhető.

Fontos tudni, hogy ezek a unitok enterprise agent kategóriához kötöttek, így a DNA előfizetéssel kapott ThousandEyes unitok cloud és endpoint agent-re nem használhatóak fel.

A unitok nincsenek viszont az adott eszköz sorozatszámához rendelve, azaz tetszőleges agenten felhasználhatóak, enterprise agenten belül tehát nincs korlátozás, pl. egy Catalyst 9400 switch rendelése után jóváírt unit mennyiség felhasználható pl. Hyper-V környezetben is.

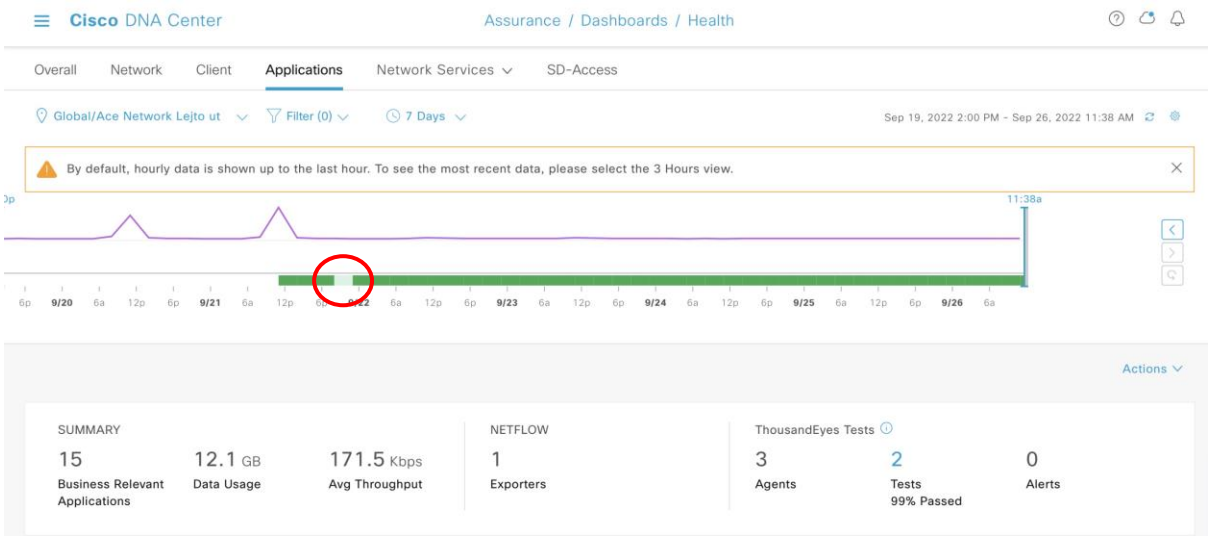
De miért előnyös, hogy a switchen futtatunk ThousandEyes agentet? A kérdésre több válasz is adható. Egyrészt költséghatékony, mert egy meglévő hardver erőforrást használunk ki még jobban. Másrészt lokális, de klienstől, operációs rendszertől, alkalmazástól független hálózati teszt eredményeket használhatunk fel hibabejelentések megoldása során; az érintett szegmens felhasználóit kiszolgáló switchen futtatott teszt mérései nagyon értékes információkat tartalmaznak a probléma helyének pontosabb behatárolásához.

Hiba megelőzés ThousandEyes segítségével

Az alábbi példában egy webhely tanúsítványával kapcsolatos hibát előzünk meg proaktív módon.

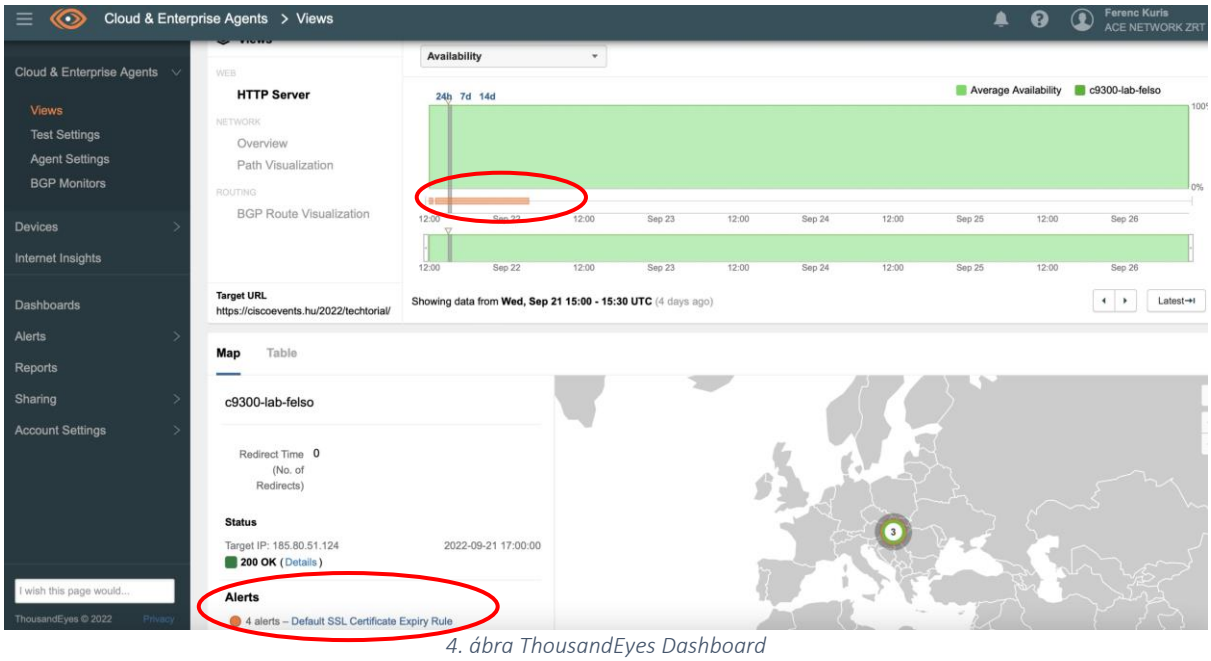
A ThousandEyes Dashboard-on egy HTTP tesztet definiáltunk, amely 5 percenként ellenőrzi az adott webhely elérhetőségét és performanciáját. A tesztet a nagyvállalati hálózatba telepített Catalyst 9300 switchekre aktiváltuk.

Ahogy az alábbi ábrán látjuk a Cisco DNA Centerben egy időintervallumban a ThousandEyes agentek hibát jeleztek.



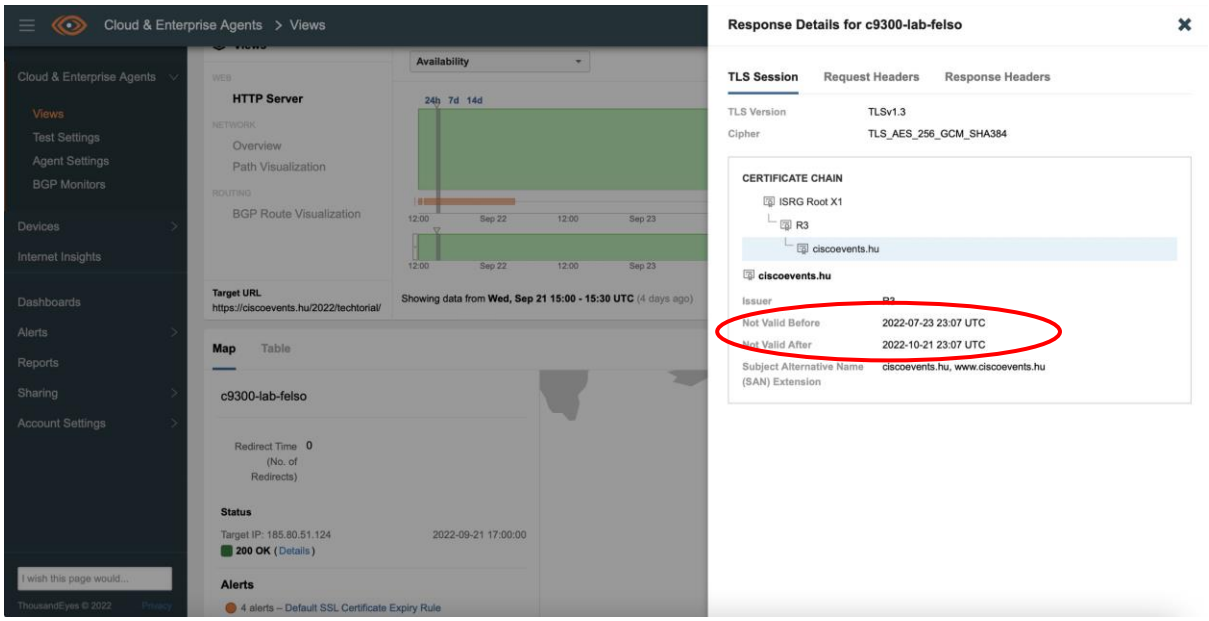
3. ábra Cisco DNA Center Assurance főoldal

A ThousandEyes Dashboard-ot megnézve látjuk, hogy 4 aktív riasztásunk van, amelyek az SSL tanúsítványra vonatkoznak.



4. ábra ThousandEyes Dashboard

Az agent mérési adatainak megnyitása után látszik, hogy a tanúsítvány 30 napon belül, október 21-én lejár.



5. ábra Szerver tanúsítvány érvényességi idő - az agent mérési adatai alapján

Egy lehetséges hibát tehát még azelőtt azonosítottunk, hogy azt a felhasználók észrevették volna.

Miután a hibáról értesítettük a szerver üzemeltetőket a tanúsítvány meghosszabbításra került.

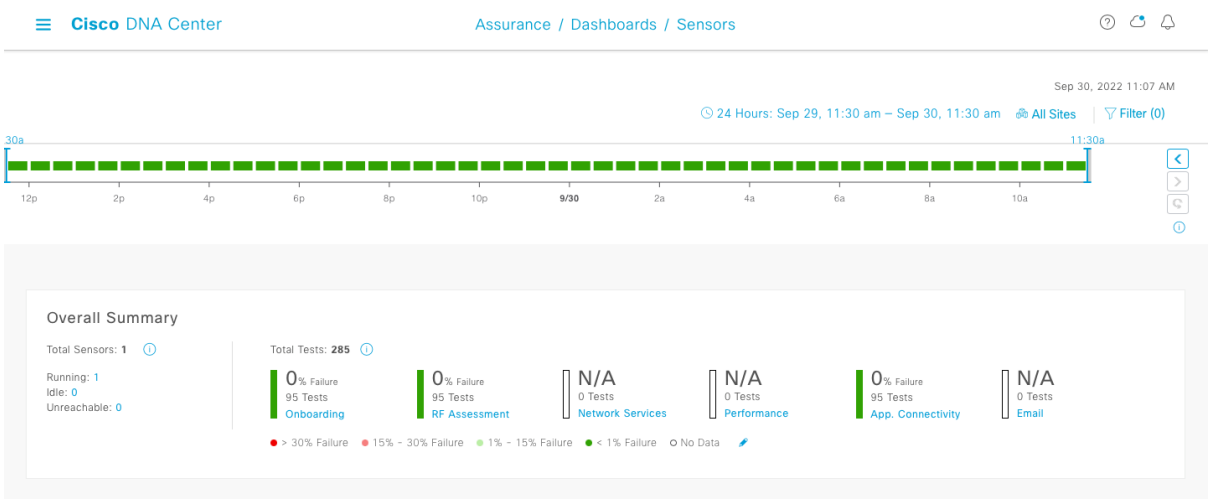
Vezeték nélküli hálózatokkal kapcsolatos hibakeresés intelligens szenzor segítségével

Mikor egy vezeték nélküli hálózattal kapcsolatos hibabejelentés érkezik egy távoli irodából kevés eszköz áll a rendelkezésünkre: hagyatkoznunk kell a felhasználó által elmondott információkra. Lehetőségünk van az Access Point-on packet capture-t készíteni, ez azonban már a hiba keletkezése után történt, a korábbi állapotról nincs információnk. Bizonyos esetekben elkerülhetetlen, hogy a telephelyen egy notebook segítségével mérjük és teszteljük a hálózatot.

A Cisco Aironet 1800S szenzor segítségével a helyszíni kiszállás elkerülhető. A szenzor valódi kliensként viselkedik, azaz pl. authentikál, IP címet kér és forgalmat generál. Mivel a méréseket az általunk beállított gyakorisággal futtatja ezért már a hibabejelentés előttről is vannak konkrét teszt eredmények, de jó eséllyel az is kimutatható, hogy egyedi problémáról vagy minden felhasználót érintő hibáról van szó.

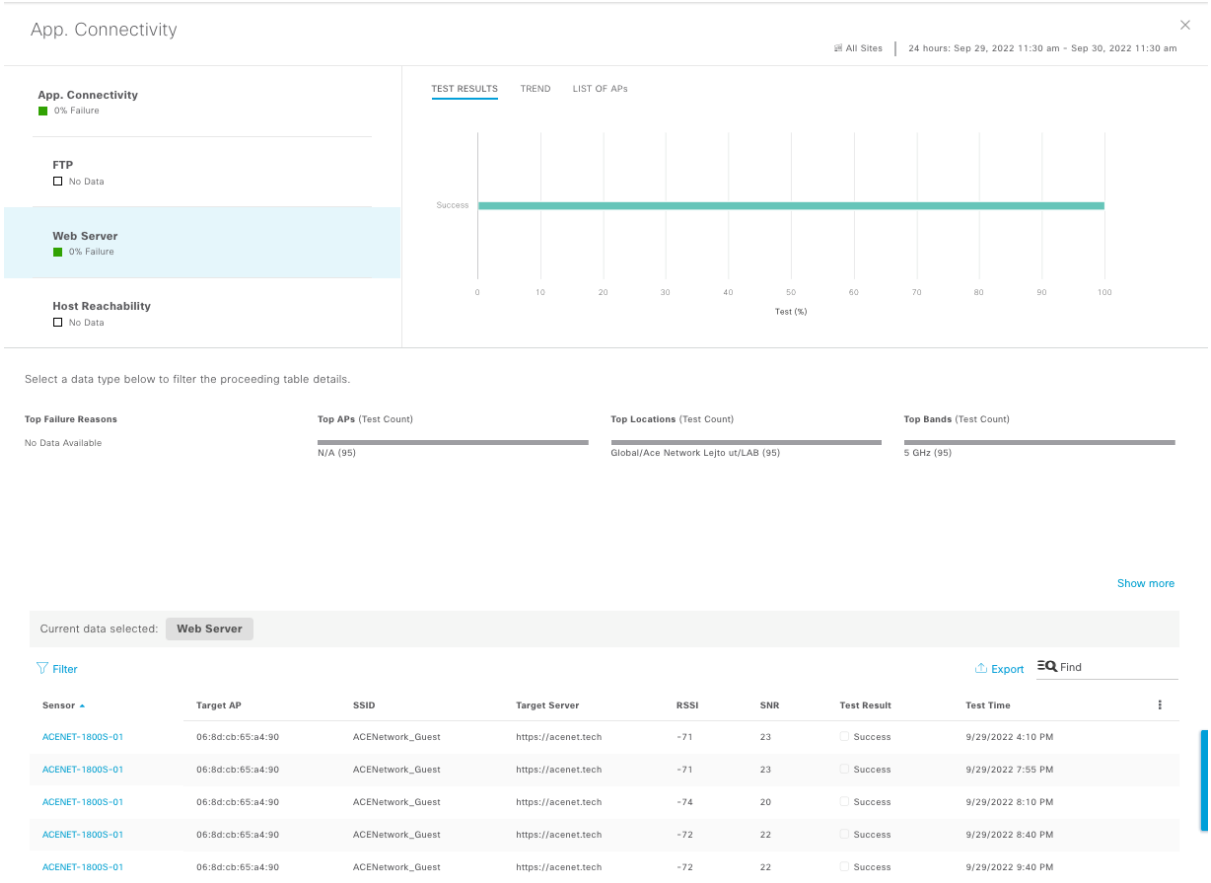
A szenzor a mérési eredményeket a Cisco DNA Centerbe küldi, ahol azok az Assurance menüpontban elemezhetők.

Az alábbi ábrán egy jól működő WiFi hálózat mérési eredményei láthatóak. A szenzor minden teszt feltételt sikeresen teljesített.



6. ábra WiFi hálózat performanciájának mérési eredményei Aironet szenzor használatával

A mérés részletes eredményei között az RSSI, SNR és válaszidő is látható, így általános képet kaphatunk a hálózat performanciájáról.



7. ábra Vezeték nélküli teszt részletes mérési eredményei