Hálózati köztes rendszerek

HORVÁTH GÁBOR

ELTE Informatikai Igazgatóság
hg@ludens.elte.hu

Kulcsszavak: hálózatmenedzsment, hálózati incidenskezelés és eszköznyilvántartás, konfiguráció- és szűrőlista-karbantartás

Az utóbbi pár évben a hálózatos szakemberek munkája egyre inkább megváltozott. Az egyre több szolgáltatás miatt egyre több szervert és konfigurációs fájlt kell karbantartani. Hogyan tudjuk csökkenteni ezt az adminisztrációs terhet? A sok kicsi, nem dokumentált script használatának nincsen sok értelme. Mit értünk middleware rendszer alatt és hogyan tudjuk használni a hálózatmenedzsment egyes területein?

1. Bevezetés

Bizonyára sok számítógéphálózat üzemeltető és tervező kolléga érzi úgy, hogy valami változik, nem pusztán a kapcsolatok sávszélessége és a hálózati berendezések csomagtovábbító képessége növekszik, hanem az elvárt szolgáltatáspark és a munkafolyamatok szerkezete változik lassan és biztosan, nem a legkellemesebb irányba. Mik ennek a változásnak a mozgatórugói, pontosan hogyan zajlik le és miket tehetünk a munkánk szakmai színvonalának megóvása érdekében? Hol találkoznak a hálózattal a sokat emlegetett middleware rendszerek, mit nyújtanak nekünk és milyen veszélyeket jelent, ha nem valódi middleware rendszert állítunk üzembe?

2. A probléma

A 90-es évek hálózati rendszergazdái (azon informatikus szakemberek, akik nagyvállalatok gerinchálózati infrastuktúráját működtetik) elsősorban a fizikai kapcsolatok létesítésére és fenntartására összpontosítottak, a gyors és megbízható csomagtovábbítás általában elegendő volt a felhasználói / megbízói elégedettséghez.

A hálózatos szakember munkaidejének jelentős részében célberendezések (router, switch) installálásával, cseréjével, felügyeletével foglalkozott és azokat a problémákat oldotta meg előszeretettel, amik ezen a szinten igényes szakmai megoldásokkal kezelhetők voltak (például vonalszakadás, router fizikai meghibásodás). Ami a lokális hálózat egyik portján „beesett", azt minél gyorsabban megpróbáltuk a megfelelő kimeneti porton kiadni, függetlenül annak tartalmától, valamint azzal sem foglalkoztunk, hogy mit tud vele kezdeni a címzett.

A szolgáltatási helyzet azonban változott, ami a hálózatüzemeltetőktől is más megközelítést kívánt. A változás főbb komponensei:

1. A számítógépes hálózat még az oktatói és kutatói területen is kinőtte a „hobbilevelezés" besorolást és az intézmény napi életének elengedhetetlen része lett. A dolgozók (és az intézmény vezetése) egyre inkább „közműként" tekint a hálózatra, elvárja a nagy rendelkezésre állást a teljes szolgáltatási területen, elvárja a szűk keresztmetszetek megszüntetését. Emiatt minden kulcsfontosságú berendezést, szervert minimum duplikálni kell, az automatikusan működésbe lépő redundancia valamint a terhelésmegosztó megoldások a hálózattervezés alappillérei lettek.

2. A gyakorlatban a hálózat „haszonélvezői", a jóhiszemű felhasználók nem tudták magukat (és gépeiket) megvédeni az Internet irányából rájuk leselkedő veszélyektől. (Valljuk be, a személyi tűzfalak és VPN kliensek installálása nem is várható el például a középkori történelem professzorától.) A hálózatosok tehát elkezdtek tűzfalakat és szűrőlistákat konfigurálni, megvédeni a felhasználókat a rosszindulatú forgalomtól.

3. Egyre több olyan hálózati entitás jelent meg, ami adatot termelt vagy igényelt. A legtöbb hálózatban már működik valamilyen hálózatmonitorozó, szolgáltatás-figyelő program, amiknek aktuális konfiguráció szükséges, és a keletkező adatokat fel kell dolgozni.

4. Több olyan „kényelmi" szolgáltatás vált a felhasználás részévé, ami eredetileg nem volt a kiszolgálás része, de nagyon kellemesek, mint a DHCP vagy a wireless hozzáférés. Ezek azonban saját konfigurációs komponensekkel rendelkeznek.

Mindezeknek van egy markáns és megkerülhetetlen hatása: a hálózatos rendszergazdáknak egyre több adatot kell egyre több helyre (általában konfigurációs fájlba) beírniuk. Ezeket a konfigurációkat konzisztensen, ellentmondásmentesen kell vezetni, a növekvő követelményeknek megfelelően egyre kisebb reakcióidővel. Ha például a felhasználó igényel egy új hálózati végpontot, akkor ennek adatait (IP-, VLAN-, hardware Ethernet cím, végponti azonosító) a DHCP és DNS szerverekbe fel kell venni, a megfelelő switch portot VLAN-ba kell helyezni, a router szűrőlistákba, firewall-adatbázisokba be kell jegyezni stb. Mindezek nagyon gondos és mennyiségileg jelentős adminisztrációt igényelnek, ami nem tekinthető igényes szakmai munkának.

3. A megoldás lehetőségei

A hálózatos szakemberek joggal érzik úgy, hogy munkidejükben túl sok a mechanikus munka, automatizálható adminisztráció, keveset tudnak a tervezéssel, mérnöki problémákkal foglalkozni. Ugyanakkor pazarlás is a „drága" mérnököket text konfigurációs fájlok karbantartására használni. A probléma megoldására a következő megoldások kínálkoznak:

a) Vegyünk fel kevésbé képzett, szerződéses munkatársakat a konfigurációs fájlok karbantartására. Nem túl jó megoldás, mivel a hálózati komponensek jogosultsági rendszere általában nem támogatja az ilyen irányú feladatmegosztást, tehát a munkatárs gyakran teljes jogosultsággal tud „garázdálkodni". Ezenkívül a módosításokat továbbra is ember végzi, aki tévedhet, fáradt lehet, elgépelhet stb.

Rövidítések és fogalmak jegyzéke

DHCP – Dynamic Host Configuration Protocol:
Lehetővé teszi, hogy mindazokat az adatokat, amik a hálózatra kapcsolódáshoz és a forgalmazáshoz szükségesek (pl. IP-cím, DNS szerver címe stb.) ne az egyes számítógépeken, hanem központi szerveren tároljuk.

Firewall – tűzfal:
Egyszerűbb változatai a hálózati csomagok szűrésével, bonyolultabb megoldásai a hálózati kapcsolatok nyilvántartásával és a bennük folyó kommunikáció követésével próbálják meg a nemkívánatos forgalmat azonosítani és eltávolítani. Nagy sávszélességű változatai általában célberendezések. A személyi tűzfal (personal firewall) egy olyan program, ami a gazdagépet védi a megengedett kapcsolati mintázatok megtanulása után.

IDS – Intrusion Detection System:
Olyan célberendezés, ami a hálózati forgalom megadott minták szerinti figyelésével a rosszindulatú használatot próbálja meg valós időben jelezni. A logfile elemző rendszerek utólag azonosítják a gyanús hálózati tevékenységet.

Router – forgalomirányító:
A csomagok továbbküldési irányának kiválasztásához nem csak a saját konfigurációját, hanem más forgalomirányítók elküldött irányítási adatait is felhasználja.

SNMP – Simple Network Management Protocol:
A hálózati entitások tulajdonságainak szabványos lekérdezésére és módosítására kifejlesztett kapcsolati felület. Használata – több műszaki ok miatt – csak a lekérdezés területén terjedt el.

VLAN – Virtual Local Area Network:
Virtuális helyi hálózat – A helyi hálózat fizikai struktúrájának további tagolását lehetővé tevő eszköz, amivel a hálózaton terjedő csomagok halmazokba sorolhatók.

VPN – Virtual Private Network:
Virtuális magánhálózat – Lehetővé teszi, hogy egy hálózat egy tagját (vagy részhálózatát) egy – általában titkosított – kapcsolaton keresztül egy másik hálózat tagjaként (tagjaiként) használjuk.

b) Irjunk „okos" script-eket, amik konzisztens módon elvégzik a szükséges konfigurációs módosításokat. Ez egy sok helyen alkalmazott és (kisebb cégeknél) jelenleg is működő megoldás. A következő problémák vannak vele:

– A script-ek dokumentáltsági foka (a legtöbb helyen) alacsony. Aki már „örökölt" ilyen programot szabadságolt kollégájától, és hibát kellett keresnie benne, az nem lelkesedik annyira ezért a megoldásért.
– A remek hálózatos mérnökök (tisztelet a kivételeknek) nem túl igényes programozók, a hibakezelés, portolhatóság, erőforrás-takarékosság nem jellemzői ezeknek a mágikus script-eknek.
– Az üzemeltetési környezet, a gerinchálózat felépítése folyamatosan változik. Ezeket az adatokat a script-ek „beépítve" tartalmazzák, nincsen törzsadatbázis vagy topológia adatbázis. Például egy új router üzembe állítása esetén a script-eket egyenként kell megtanítani az új interfészekre, ismét csak fájlokat editálunk, nagy fegyelemmel és odafigyeléssel...

c., Vásároljunk olyan programot, ami ezt a terhet leveszi a vállunkról. De ez nem annyira egyszerű dolog, mint amennyire az eladói oldal beállítja. Mit is kell tudnia egy ilyen programnak? Az biztos, hogy valahol a sok hálózati entitás között áll, adatokat cserél velük, azokat tárolja, ellenőrzi, átalakítja, továbbítja. Az ilyen alkalmazásokat nevezzük köztes rendszernek, middleware-nek.

4. A hálózati middleware funkciói

1) Kapcsolatot tart fent a hálózati entitásokkal, adatcserét folytat velük. Ezen entitások jelentős része nem rendelkezik olyan kapcsolati interfésszel, amin ez az adatcsere univerzálisan megtörténhet, általában a middleware oldalnak ismernie kell a másik fél saját adattárolási vagy kapcsolati formátumát. (például a SNMP erre a célra nagyon nehézkesen és korlátozottan alkalmazható csak, különösen problémás a hálózati eszköz konfigurációjának módosítása ezen a módon.)

Milyen hálózati komponensekről van szó?

– Hálózati célberendezések, router-ek, switch-ek. A berendezés saját formátumában szűrőlistákat, interfész- és port konfigurációkat kell előállítani és a berendezésre tölteni azokat. Le kell kérdezni konfigurációs beállításokat és interface/port állapotokat, számlálókat.
– Hálózatbiztonsági célberendezések, tűzfalak, IDS-ek, VPN koncentrátorok. Szűrőlistákat, konfigurációs beállításokat kell előállítani a részükre, jelzéseket kell kezelni.
– Hálózati szolgáltató szerverek, DHCP szerver, DNS szerver, authentikációs szerverek stb. Konfigurációs adatokat, bejegyzéseket kell aktualizálni. Delegált zónák, külső szervezetek esetében zónalekérdezés is szükséges.

2) Felhasználói felületet biztosít a rendszer „humán” komponenseinek:
– Hálózatos mérnökök.
Bizony ők is a rendszer komponensei, reguláris felületet kell biztosítani nekik a „kézi” módosítások elvégzésére, az általános szabályok (pl. szűrési policy) felvitelére. Ezen a felületen kell kezelni a berendezések és fizikai konfigurációk változását (kábelkönyv).
– Operátorok, helpdesk.
Ők azok, akik a felhasználói igényeket, módosítási kérelmeket felviszik a rendszerbe, az érdeklődő felhasználót tájékoztatják. A hálózati middlewarenek tehát ügykezelő funkcionalitással is kell rendelkeznie.
– Felhasználók.
Sok esetben (pl. letiltott gépek listája) meg kell adni a közvetlen lekérdezés lehetőségét.
Zárt felhasználói kör esetében a közvetlen ügyfelvitel (DNS bejegyzés igénylése) lehetőségét is érdemes biztosítani. Ekkor a hálózat üzemeltetői csak engedélyezik a folyamat lefutását és a konfigurációs módosulások életbe lépését.
Az emberi kapcsolati interfésznek a web felület kézenfekvő, mivel a szükséges kliens már a legtöbb desktop gépen rendelkezésre áll. Természetesen nem „sportszerű” egy bizonyos web böngésző használatát előírni.

3) Karbantartja a saját adatbázisát. A hálózatról rendelkezése álló információk alapján eldönti, hogy a beérkezett kérések kiszolgálhatók-e, az adatokon tartalmi ellenőrzést is végez. A módosulások átvezetése után eldönti, mely komponenseknek szükséges a változásokat továbbítani. Lehetőséget biztosít a törzsadatok (kapcsolattartók, berendezés adatok) karbantartására, a hálózati topológia lekérdezésére. Lehetőleg kapcsolatot tud létesíteni a cég saját törzsadattáraival (pl. LDAP kapcsolat).

4) Kapcsolatot tart fent a „társrendszerekkel”, hálózatfigyelő, szolgáltatás-monitorozó alkalmazásokkal (pl. MRTG, Nagios), illetőleg a cég saját, speciális hálózati alkalmazásaival. Részükre konfigurációkat, topológiai információkat továbbít, fogad állapot- és terhelési adatokat.

5. Hogyan működik a hálózati middleware?

A hálózati middleware működését érdemes néhány gyakorlati példán keresztül megismerni.

1. példa: Végponti igénykezelés

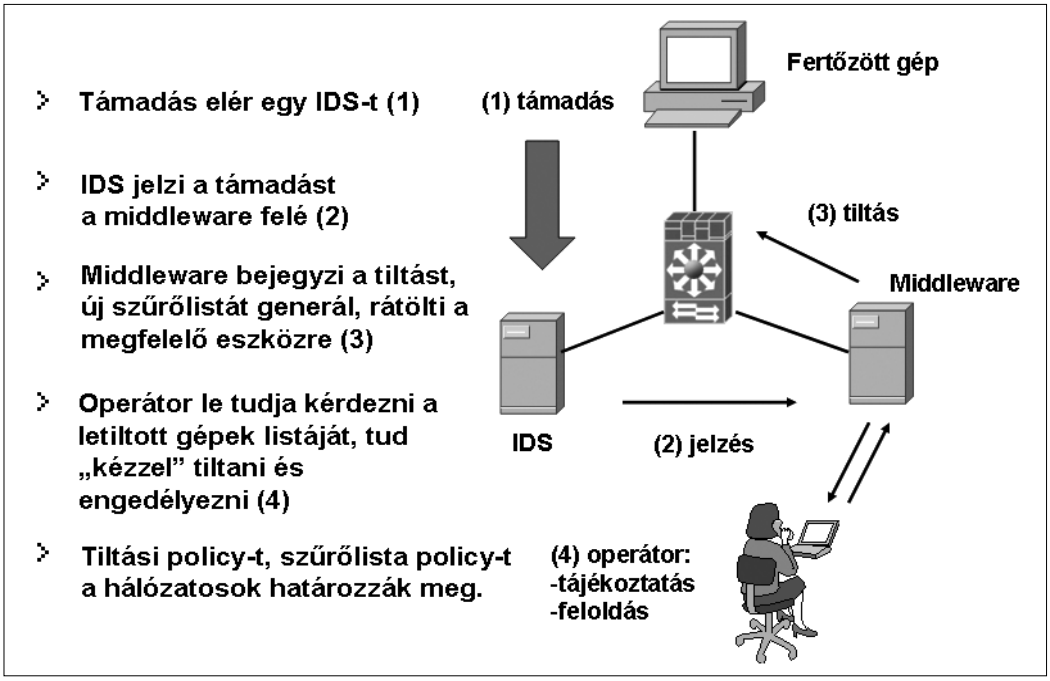
– A felhasználó a végpont bekötési (vagy módosítási) igényét annak jellemző adataival egy web felületen (web form) felviszi a middleware-be. (Vagy papír/fax/e-mail alapú igénylőlapot ad le, ekkor az adatok rögzítését az operátor végzi.)

– A middleware az adatok formai és tartalmi ellenőrzése (például szabad-e az IP cím, létezik-e az igényelt végpont) elkészíti az ügyet, értesíti a szükséges fizikai beavatkozást (pl. patchkábel csatlakoztatást) végző munkatársat.

– Ha a technikus (a fizikai módosítások elvégzése után) lezárja az ügyet, a middleware elvégzi a DNS módosítást, a kiszolgáló port VLAN-ba helyezését, az esetleges DHCP bejegyzést, a router/firewall szűrőlista módosítást (hogy az új gép az intézményen kívülre is tudjon forgalmazni). Az adatbázis a név, IP cím, végpont új állapotát és kapcsolati adatait tartalmazza.

– Természetesen ismerjük a várakozó és a teljesített ügyek számát.

DNS vagy VPN igénylés esetén fizikai beavatkozásra nincs is szükség, a 3. lépés pusztán a folyamat lefutásának engedélyezéséből áll.



1. ábra

Fertőzött felhasználói gép szűrése hálózati middleware-en keresztül

2. példa: Hálózati incidenskezelés

– A hálózat egy komponensét támadás éri egy fertőzött gépről. Erről tájékoztathatja a middleware-t maga a támadott komponens, de egy IDS vagy egy logfile elemző alkalmazás is.

– A middleware a saját topológiai képe alapján megállapítja a beavatkozási pontot (router szűrőlista, firewall szűrőlista), elkészíti az új szűrőlista szabályokat és rátölti a megfelelő eszközre.

– A letiltott gépek listája és az indokok lekérdezhetők (publikus web felületen is).

– A támadó gép „fertőtlenítése" után az operátorok a kezelői felületen feloldják a korlátozást, a middleware ismét engedélyezi a gép forgalmazását.

3. példa: Eszközgazdálkodás

– Eszközvásárlás esetén a szállítólevél alapján megtörténik az eszköz felvitele a middeware adatbázisába. Az eszköz raktárba kerül.

– Miután a technikus kiviszi az eszközt helyszínre és beszereli, könyveli a middeware kábelkönyvi moduljában, hogy mely rackszekrény melyik pozíciójába került, milyen konfigurációban (milyen kártyákkal, modulokkal) és milyen kábeles kapcsolatokkal rendelkezik.

– A lekérdező felületek pontosan informálnak arról, hogy milyen típusú eszközből mennyivel rendelkezünk és azok hol vannak. Hogyan épülnek fel a rackszekrények, milyen eszköznek milyen másikkal van fizikai kapcsolata.

Természetesen a berendezés adatok származhatnak egy raktári rendszerből is, az aktuális fizikai konfiguráció nyilvántartására azonban az alkalmatlan, mert például azt sem tudja eldönteni, hogy mely kártya mely slot-ba illeszthető be. Ezek a middleware eszköztulajdonság adatbázisával dönthetők csak el.

4. példa: Hálózatfelügyelet

– Gyakori probléma, hogy az installált hálózat- vagy szolgáltatás monitorozó alkalmazást nem látjuk el topológiai információkkal, ezért egy hiba esetén sok riasztást kapunk, amiből egy a valódi hiba, a többi annak következtében fellépő másodlagos jelenség, amire a mérnök nem kíváncsi. Ezek a másodlagos riasztások kiszűrhetők, ha a middleware a monitorozó alkalmazásnak „el tudja magyarázni" a hálózat felépítését.

– Ha felveszünk egy új hálózati tartományt, egy új router interfészt, akkor milyen komfortos, ha ezeket mindjárt a monitorozó, terhelésmérő alkalmazás (pl. MRTG) is megismeri.

– A middleware-ben a módosítások tematikusan és időrendben visszakereshetők. Nem kell tehát hosszan vallatni a kollégákat, ha pár napig nem vettünk részt az operatív hálózatkonfigurálási munkában.

Fenti példák jól illusztrálják a hálózati middleware rendszerek közös tulajdonságát, a nagyfokú flexibilitást, nyitottságot, a többi rendszerrel való kommunikációs hajlamot.

6. A piac jelenlegi állapota

Ha hálózati middleware-t szeretnénk vásárolni, nehéz helyzetben vagyunk! A jelenleg kapható programrendszerek főbb kategóriái:

– Vannak olyan programrendszerek, amik a teljes funkcionalitást biztosítják. Ezek azonban komplex informatikai irányítási rendszerek, amik megvásárlása, bevezetése, az informatikai szegmens működésének „átszabása" komoly terhet jelent. Kisebb cégek esetében nehéz ehhez forrást és motivációt találni. Ezek a rendszerek általában tartalmazzák a kapcsolati komponenseket (törzsadattár, kábelkönyv, ügykezelő, hálózatmonitor és felderítő komponensek stb.) A rendszer zárt, a kapcsolati felület más rendszerekkel license köteles (ha létezik egyáltalán). Itt tehát nem middleware alkalmazásról van szó, hanem olyan zárt világról, ami megpróbálja maga megoldani a felmerülő feladatokat.

– Vannak kisebb programok, amik a fenti funkcionalitás egy részét biztosítják és megfizethetőek a kisebb ügyfeleknek is. Bevezetést, pilótavizsgás specialistát nem igényelnek. Ezek azonban általában jól működő hálózatmonitorozó, hálózatfelderítő programokból alakultak ki, a tapasztalat szerint az adatbázis és az alkalmazás-logika zárt, az alkalmazás tervezésekor egyáltalán nem volt szempont a sokoldalú kapcsolódási lehetőség. Ne hagyjuk magunkat áltatni: kis kozmetikázással és színes marketingmunkával ezekből sem lesz middleware.

– Most jelennek meg a piacon az igazi hálózati middleware-ek első generációi. Ezen rendszerek adatbázisait, alkalmazás-logikáját, kapcsolati felületeit a fent vázolt céloknak megfelelően tervezték, és alapkövetelmény az egyedi igények (ügyfél modulok) támogatása is dokumentált interfészeken keresztül. Itt fontos szempont a gyártófüggetlen támogatás. Ha egy hálózatmonitorozó alkalmazást a beleépített néhány middleware funkcióval együtt „komplex hálózatmenedzsment rendszerként" adnak el nekünk, akkor valószínűleg keresztet vethetünk arra, hogy más gyártótól származó vagy saját fejlesztésű rendszereinket elegáns módon ezzel összekapcsoljuk. Amennyiben egy gyártó hálózatmonitorozó, beavatkozó rendszere nem választható el a middleware komponenstől (nem installálható és használható külön az egyik vagy a másik) akkor az valójában nem is middleware alapú megoldás, csupán felszínes mutáció az aktuális marketingszlogenek meglovagolására.

7. Összefoglalás

A jelenleg elérhető hálózati middleware rendszerek még csak szárnyaikat bontogatják. Installálásuk, feltöltésük az induló adatokkal még nehézkes, csak kevés adatbáziskezelőhöz, hálózati entitás-típushoz tartalmaznak kész kapcsolati modulokat. Megéri azonban kipróbálni őket és figyelemmel kísérni lendületes fejlődésüket, mert az univerzálisnak szánt, de zárt rendszereket sok területen hamarosan fel fogják váltani.