№10-AMALIY ISHI

Mavzu: Tarmoq monitoring dasturlari bilan ishlash.

Ishning maqsadi: Talabalarga tarmoq monitoring dasturlari bilan Amaliy ishlashni o‘rgatish.

Ish uchun kerakli jihozlar: kompyuterlar, tarmoq uchun kerakli qurilmalar va dasturiy vositalar.

Qisqacha nazariy ma’lumot. Tarmoq ishidagi muammolar foydalanuvchilarga xizmat ko‘rsatish sifatini sezilarli darajada yomonlashtirishi, ularning tarmoq xizmatlaridan qanoatlanganligi darajasini pasaytirishi va ushbu xizmatlarni taqdim qilayotganlarga nisbatan noroziligini keltirib chiqarishi mumkin. Shuning uchun muammolarni maksimal darajadagi tezkorlik bilan payqab topish, aniqlab olish (diagnostika qilish) va bartaraf qilish g‘oyat muhimdir. Tarmoq monitoringining har xil tizimlari va aniqlash (diagnostika) vositalari muammolarning payqab topilishini va tahlil qilinishini jadallashtiradi, hamda bu bilan muammo paydo bo‘lishi va uning bartaraf qilinishi orasidagi vaqtning qisqarilishiga yordam beradi. Bundan tashqari, monitoring vositalari, tarmoq ishi to‘g‘risidagi ma’lumotlarni yig‘ib va tahlil qilib, kutilayotgan muammolarni aniqlab topish va ularning paydo bo‘lishiga yo‘l qo‘ymaslik imkoniyatini yaratadi.

Tarmoq xizmatlarining sifatini ta’minlash uchun AT (axborot texnologiyalari) mutaxassislari infratuzilmaga oid alohida tarmoq qurilmalarining holatini monitoring qilish o‘rniga borgan sari ko‘proq qo‘llanmalar va xizmatlar ishini nazorat qilishga e’tibor berishmoqda. Xizmatlar ishining sifatini baholash uchun, ularning trafigini tarmoqning har xil nuqtalarida (masalan, yuklanganlikni muvozanatga keltiruvchidan, ma’lumotlar bazasi serveridan hamda boshqalaridan oldin va keyin) jalb qilish va uni tahlil qilish kerak. Trafikning tahlil qilinishi shuningdek tarmoq ishini optimallashtirish va xakerlik faollikni oshkor qilish uchun hamda boshqa maqsadlarda amalga oshiriladi.

Korxonalar o‘z tarmoqlari ishlashining to‘liq nazorat qilinishida manfaatdor. Shu bilan birga, uzatilayotgan trafikning hajmlari, eng katta trafikni keltirib chiqaradigan bog‘lamalar, tarmoq va qo‘llanmalar ishidagi to‘xtalib qolishlar, tarmoqni o‘tkazish yo‘lidan har xil qo‘llanmalar va mijozlar tomonidan foydalanganligi to‘g‘risidagi hamda boshqa ma’lumotlar yig‘iladi va tahlil qilinadi. Ushbu ma’lumotlar tarmoqni hammadan ko‘p yuklayotgan bog‘lamalarni aniqlash, va qo‘llanmalar ishidagi muammolarni bartaraf qilishga yordam beradi. Shuningdek monitoring vositalari yordamida qo‘llanmalardagi tranzaksiyalar va foydalanuvchilar tomonidan yo‘l qo‘yilishi mumkin bo‘lgan lavozim yo‘riqnomalariga rioya qilmaslik holatlarini aniqlash maqsadida (misol uchun, foydalanuvchilar mahfiy (oshkor qilib bo‘lmaydigan) ma’lumotlarni tarmoqdan tashqariga uzatishlari va korporativ siyosat tomonidan taqiqlangan veb-saytlarga tashrif qilishlari mumkin) ularning harakatlari nazorat qilinadi. Bundan tashqari, axborot texnologiyalari (AT) mutaxassislari VoIP seanslarining sifatini monitoring qilishda va videoni uzatishda, hamda tarmoqning ishlash ko‘rsatkichlari yo‘l qo‘yilishi mumkin bo‘lgan chegaraviy qiymatlarga ko‘ra yomonroq bo‘lganda, tegishli xabarlarni qabul qilishda manfaatdor.

Tarmoqni tahlil qilish, monitoring qilish va aniqlash (diagnostika qilish) vositalari dasturiy yoki apparatga oid bo‘lishi mumkin. So‘nggi holatda trafikni egallash bo‘yicha almashtiriladigan maxsus platalarni va egallangan trafikni tahlil qilish bo‘yicha oldindan o‘rnatilgan dasturiy ta’minotni (DT) o‘z ichiga olgan server yoki kompyuter maslaklariga (platformalariga) tayangan sinov vositalari (probniklar), shuningdek Plug-and-Play turidagi yaxlit holga keltirilgan (integratsiya qilingan) tarmoqni monitoring qilish moslamalari nazarda tutilgan. Egallab olinadigan trafikning katta hajmlarini yozib olish uchun server maslaklariga tayangan sinov vositalari RAID turidagi yetarli darajadagi katta sig‘imga ega bo‘lgan tez harakatlanadigan diskli tizimlar bilan jihozlanadi. Trafikni tahlil qilish bo‘yicha dasturiy vositalar bepul (masalan, Wireshark yoki nTop) yoki tijorat (pul to‘lanadigan) bo‘lishi mumkin. So‘nggi holatdagilar qolganlaridan kengroq ko‘lamli funktsional imkoniyatlarining xususiyatlari bilan ajralib turadi, shuningdek, tijorat vositalarining xaridorlari ularning ishlab chiqaruvchilari va yetkazib beruvchilari tomonidan qo‘llab-quvvatlanishiga ishonishlari mumkin. Katta ko‘lamdagi tarmoqlarni nazorat qilish uchun tarmoq bo‘yicha taqsimlangan sinov vositalarini qamrab olgan markazlashgan holda boshqariladigan monitoring qilish tizimlaridan foydalaniladi. Har qanday ko‘lamdagi korporativ IP-tarmoqlarini tahlil qilish, monitoring qilish va aniqlash (diagnostika qilish) uchun tijorat qo‘llanmalarining eng yaxshilaridan biri bo‘lib WildPackets kompaniyasining OmniPeek dasturiy ta’minoti (DT) hisoblanadi.

Topshiriqlar:

1. “10-Strayk: Tarmoq monitoring” dasturi vazifalari Amaliy ko‘rsating.
2. cFosSpeed dasturining vazifalari Amaliy ko‘rsating.
3. Throttle dasturining vazifalari Amaliy ko‘rsating.
4. Wireshark dasturining vazifalari Amaliy ko‘rsating.
5. CommView dasturining vazifalari Amaliy ko‘rsating.