Моніторинг доступності ресурсів мережі

Авінов Д.С.
Науковий керівник – к.т.н., доц. Кльоц Ю.П.
Хмельницький національний університет

Постійний контроль за роботою локальної мережі, що становить основу будь–якої корпоративної мережі, необхідний для підтримки її в працездатному стані. Контроль – це перший етап, який повинен виконуватися при управлінні мережею. Зважаючи на важливість цієї функції її часто відокремлюють від інших функцій систем управління і реалізують спеціальними засобами. Такий поділ функцій контролю і власне управління корисно для невеликих і середніх мереж, для яких установка інтегрованої системи управління економічно недоцільна. Використання автономних засобів контролю допомагає адміністратору мережі виявити проблемні ділянки мережі, а їх відключення або реконфігурацію він може виконувати в цьому випадку вручну.

Процес контролю роботи мережі зазвичай ділять на два етапи – моніторинг і аналіз.

На етапі моніторингу виконується більш проста процедура – процедура збору первинних даних про роботу мережі: статистики про кількість циркулюючих в мережі кадрів і пакетів різних протоколів, стан портів концентраторів, комутаторів і маршрутизаторів і т. п.

Далі виконується етап аналізу, під яким розуміється більш складний і інтелектуальний процес осмислення зібраної на етапі моніторингу інформації, зіставлення її з даними, отриманими раніше, і вироблення припущень про можливі причини сповільненої або ненадійної роботи мережі.

Завдання моніторингу вирішуються програмними і апаратними вимірниками, тестерами, мережевими аналізаторами, вбудованими засобами моніторингу комунікаційних пристроїв, а також агентами систем управління. Завдання аналізу вимагає більш активної участі людини і використання таких складних засобів, як експертні системи, що акумулюють практичний досвід багатьох мережевих фахівців.

Всі засоби моніторингу та аналізу мереж, можна розділити на кілька великих класів:

Системи управління мережею (Network Management Systems) – централізовані програмні системи, які збирають дані про стан вузлів і комунікаційних пристроїв мережі, а також дані про трафік в мережі. Ці системи не тільки здійснюють моніторинг і аналіз, а й виконують в автоматичному чи напівавтоматичному режимі управління мережею – включення і відключення портів пристроїв, зміна параметрів мостів адресних таблиць мостів, комутаторів і маршрутизаторів і т.п. Прикладами

систем управління можуть служити популярні системи HPOpenView, SunNetManager, IBMNetView.

Засоби управління системою (System Management). Засоби управління системою часто виконують функції, аналогічні функціям систем управління, але відносно інших об'єктів. У першому випадку об'єктом управління є програмне і апаратне забезпечення комп'ютерів мережі, а у другому – комунікаційне устаткування. Разом з тим, деякі функції цих двох видів систем управління можуть дублюватися, наприклад, засоби управління системою можуть виконувати найпростіший аналіз мережевого трафіку. До найбільш відомих систем управління системами відносяться LANDesk, IBM Tivoli, Microsoft Systems Management Server, HP OpenView, Novell ZENworks і CA Unicenter.

Вбудовані системи діагностики і управління (Embedded Systems). Ці системи виконуються у вигляді програмно–апаратних модулів, які встановлюються в комунікаційне обладнання, а також у вигляді програмних модулів, вбудованих в операційні системи. Вони виконують функції діагностики і управління тільки одним пристроєм, і в цьому їх основна відмінність від централізованих систем управління. Прикладом засобів цього класу може служити модуль управління концентратором Distrebuted 5000, реалізує функції автосегментації портів при виявленні несправностей, приписування портів внутрішнім сегментам концентратора і деякі інші. Як правило, вбудовані модулі управління також виконують роль SNMP–агентів, які поставляють дані про стан пристрою системам управління.

Аналізатори протоколів (Protocolanalyzers). Представляють собою програмні або апаратно–програмні системи, які обмежуються на відміну від систем управління лише функціями моніторингу і аналізу трафіку в мережах. Хороший аналізатор протоколів може захоплювати і декодувати пакети великої кількості протоколів, що застосовуються в мережах – зазвичай кілька десятків. Аналізатори протоколів дозволяють встановити деякі логічні умови для захоплення окремих пакетів і виконують повне декодування захоплених пакетів, тобто показувати в зручній для користувача формі вкладеність пакетів протоколів різних рівнів один в одного з розшифруванням змісту окремих полів кожного пакета.

Відповідно до рекомендацій ISO можна виділити такі функції засобів управління мережею:

Управління конфігурацією мережі – полягає в конфігурації компонентів мережі, включаючи їх місце розташування, мережні адреси і ідентифікатори, управління параметрами мережевих операційних систем, підтримку схеми мережі: також ці функції використовуються для іменування об'єктів.

Обробка помилок – це виявлення і усунення наслідків збоїв у роботі мережі.

Аналіз продуктивності – допомагає на основі накопиченої статистичної інформації оцінювати час відповіді системи і величину трафіка, а також планувати розвиток мережі.

Управління безпекою – включає в себе контроль доступу та збереження цілісності даних. У функції входить процедура аутентифікації, перевірки привілеїв, підтримка ключів шифрування, управління правами. До цієї ж групи можна віднести важливі механізми управління паролями, зовнішнім доступом, з'єднання з іншими мережами.

Облік роботи мережі – включає реєстрацію і управління використовуваними ресурсами і пристроями. Ця функція оперує такими поняттями як час використання і плата за ресурси.

Типовими представниками засобів управління мережами є системи HPOpenView, SunNetManager і IBMNetView.

Останнім часом в області систем управління спостерігаються дві досить чітко виражені тенденції:

– інтеграція в одному продукті функцій управління мережами і системами;

– розподіленість системи управління, при якій в системі існує кілька консолей, які збирають інформацію про стан пристроїв і систем та видають керуючі дії.

Нині найуспішнішим сімейством стандартів є SNMP. Він лідирує за кількістю керованих систем (агентів). Керуючі системи (менеджери) зазвичай підтримують безліч стандартів, тому тут складно говорити про лідерство SNMP.

Майже всі успіхи SNMP пов'язані з особливостями процесу стандартизації в IETF:

– безкоштовні і вільно розповсюджувані;

– легко доступні в електронній формі;

– швидкий розвиток стандартів, продумані етапи стандартизації;

– на всіх етапах ведеться технічна експертиза;

– робочі групи очолюють технічні, а не політичні лідери;

– прототипи систем на основі стандартів демонструють їх придатність.

Протокол SNMP підтримують сотні виробників. Головні переваги – це простота, доступність, незалежність від виробників. Він розроблений для управління маршрутизаторами в мережі Internet і є частиною стека TCP/IP.

На сьогодні існує кілька стандартів на бази даних управляючої інформації для протоколу SNMP. Основними є стандарти MIB–I і MIB–II, а також версія бази даних для вилученого управління RMON MIB. Крім цього існують стандарти для спеціальних пристроїв MIB конкретного типу (наприклад, MIB для концентраторів або MIB для модемів), а також частки MIB конкретних фірм– виробників устаткування.

З перерахованих вище протоколів та стандартів саме протокол SNMP дозволяє розробити систему моніторингу доступності ресурсів мережі, що забезпечує мінімальне навантаження на мережу та вчасне інформування адміністраторів про втрату зв'язку з критичними вузлами.

Перелік посилань

1. Фейт С. TCP / IP. Архитектура. Протоколы. Реализация / Сидни Фейт. – Издательство Лори, 2016. – 424 с.

2. Эделман Д. Автоматизация программируемых сетей/ Джейсон Эделман, Мэтт Осуолт, Скотт С. Лоу. − Издательство : ДМК, 2019. – 616 с.

Контроль цілісності інформації за допомогою хешування

Акатов О.В.
Науковий керівник: ктн. доц. Огнєвий О.В.
Хмельницький національний університет

Більш надійними, ніж методи «парності», «контрольних сум», «циклічного контрольного коду» і «турбо-коду», можуть бути методи, побудовані на використанні односпрямованих криптографічних функцій хешування. Аналіз цілісності окремого об'єкта (тексту, файлу) може бути заснований на обчисленні хешу цього об'єкта за узгодженим алгоритмом і на наступному порівнянні його з початковим хешем об'єкта. Подібний аналіз використовують при синхронізації даних, при архівації, при резервуванні при здійсненні цифрового підпису, а також при інших процедурах.

Однак цей метод вразливий, тому що при навмисному порушенні цілісності інформації, особливо якщо порушення проводиться особою з санкціонованим доступом, може бути замінений і її контрольний хеш.

Окремим сформованим напрямком контролю цілісності даних є реєстрація часу надходження даних, що використовує засоби для виявлення порушення їх цілісності заднім числом – TSP (Time-Stamp Protocol). Цьому напрямку приділено увагу в багатьох роботах: від ранніх до однієї з останніх. Принцип реєстрації даних в цих роботах заснований на формуванні ланцюжка об'єднаних хешів (hash-chain based protocols for time-stamping and secure logging) за схемою, наведеною на рисунку 3, і на закріпленні реєстрації шляхом публікацій, що дозволяє виявляти порушення цілісності даних, вироблених заднім числом [1].

Метод полягає в тому, що реєструючу інформацію піддають хешуванню (отримують її хеш H), потім обчислюють об'єднуючий хеш H, враховуючий h і значення попереднього об'єднаного хеша. Кожен *N*-ий об'єднаний хеш публікують.