План лекції.

Тема 7. Моніторинг поштових сервісів, DNS та маршрутизації.

- Вступ. Роль поштових, DNS та мережевих сервісів у IT-інфраструктурі
- Архітектура поштових сервісів як об'єкта моніторингу
- Об'єкти моніторингу поштових сервісів
- Методи моніторингу поштових сервісів
- DNS як об'єкт моніторингу
- Методи та підходи до моніторингу DNS
- Безпека поштових сервісів: SPF, DKIM, DMARC
- Маршрутизація як об'єкт моніторингу
- Методи моніторингу маршрутів і мережевих шляхів
- Ключові метрики моніторингу пошти, DNS та маршрутизації
- Інструменти моніторингу
- Побудова системи моніторингу базових мережевих сервісів
- Типові проблеми та помилки
- Практичні сценарії та кейси
- Місце теми в загальній системі моніторингу та спостережуваності

Вступ. Роль поштових, DNS та мережевих сервісів у IT-інфраструктурі

У цій лекції ми будемо говорити не про те, як розгортаються або адмініструються поштові сервери, DNS-зони чи протоколи маршрутизації. Ми також не будемо детально зупинятися на конкретних програмних продуктах, їх конфігурації або внутрішніх механізмах роботи. Основний фокус цієї теми — підходи до моніторингу базових інфраструктурних сервісів, їхня роль у загальній картині доступності IT-систем та ті проблеми, які виникають, коли ці сервіси виходять з ладу або працюють некоректно.

Поштові сервіси, DNS та механізми маршрутизації належать до так званих базових інфраструктурних сервісів. Вони рідко сприймаються користувачами як окремі системи, проте саме вони формують фундамент, на якому працює практично будь-який сучасний IT-сервіс. У багатьох випадках їхня робота залишається «невидимою» до того моменту, поки не виникає проблема, наслідки якої можуть виглядати як відмова зовсім інших компонентів інфраструктури.

Сучасні веб-сервіси є хорошим прикладом такої залежності. Для користувача веб-додаток — це URL у браузері, але з точки зору інфраструктури цей запит проходить ланцюг залежностей: спочатку відбувається DNS-резолюція імені, потім трафік передається мережею відповідно до поточної маршрутизації, і лише після цього встановлюється з'єднання з веб-сервером. У результаті проблема на рівні DNS або маршрутизації може повністю заблокувати доступ до сервісу навіть за умови, що сам веб-додаток та сервери працюють коректно.

Аналогічна ситуація характерна і для корпоративних комунікацій. Електронна пошта є одним з ключових інструментів бізнес-взаємодії, але її працездатність залежить не лише від поштового сервера як такого. Доставка листів неможлива без коректної роботи DNS, мережевої доступності, механізмів шифрування та маршрутизації. У результаті проблема на будь-якому з цих рівнів може призвести до затримки або повної втрати поштових повідомлень, що напряму впливає на бізнес-процеси.

Однією з ключових особливостей відмов базових інфраструктурних сервісів є те, що вони не завжди супроводжуються падінням серверів або сервісів у класичному розумінні. Сервери можуть відповідати на запити, служби можуть бути запущені, а моніторинг інфраструктури — показувати «зелений» стан. Водночас користувачі не можуть скористатися сервісом, листи не доставляються, а доменні імена не резольвляться. Такі інциденти часто стають прикладом так званих «невидимих» проблем, які складно виявити без правильно побудованого сервісного та мережевого моніторингу.

Окремо варто зазначити і репутаційні ризики, пов'язані насамперед із поштовими сервісами. Некоректна робота DNS-записів, помилки у поштовій інфраструктурі або проблеми з мережею можуть призвести до погіршення доставлюваності листів, потрапляння у спам або блокування з боку зовнішніх поштових провайдерів. Такі наслідки часто проявляються не миттєво і можуть зберігатися навіть після усунення технічної проблеми.

У контексті цієї лекції важливо чітко розрізняти різні рівні моніторингу. Прикладний моніторинг зосереджується на роботі конкретних застосунків і їхніх бізнес-функцій. Сервісний моніторинг оцінює доступність і якість роботи сервісів з точки зору користувача або споживача послуги. Мережевий моніторинг, у свою чергу, охоплює рівні від L3 до L7 моделі OSI і дозволяє виявляти проблеми передачі даних, маршрутизації та доступності сервісів на транспортному і прикладному рівнях.

Саме на перетині цих підходів і знаходиться моніторинг поштових сервісів, DNS та маршрутизації. Він дозволяє побачити ті проблеми, які залишаються поза межами класичного моніторингу серверів, але безпосередньо впливають на доступність, стабільність і надійність IT-систем у цілому.

Архітектура поштових сервісів як об'єкта моніторингу

Розглядаючи поштові сервіси як об'єкт моніторингу, важливо одразу відокремити архітектурні принципи від конкретних реалізацій. Незалежно від того, чи використовується власний поштовий сервер, гібридна інфраструктура або повністю хмарне рішення на кшталт Google Workspace чи Microsoft 365, пошта залишається багатокомпонентною сервісною системою з чітко визначеним потоком обробки повідомлень.

У класичних on-premise або гібридних інфраструктурах центральним компонентом поштової системи є MTA (Mail Transfer Agent) — програмний елемент, відповідальний за прийом, передачу та маршрутизацію електронних листів між серверами. Типовими прикладами таких рішень є Postfix, Exim та Sendmail, які переважно працюють у середовищах Unix/Linux. Саме ці компоненти реалізують протокол SMTP, керують чергами повідомлень, повторними спробами доставки та взаємодіють із зовнішніми поштовими серверами. З точки зору моніторингу MTA є ключовою точкою спостереження за станом поштового трафіку.

Доставка повідомлень безпосередньо у поштові скриньки здійснюється за допомогою MDA (Mail Delivery Agent). Хоча цей компонент часто залишається «за лаштунками» для користувачів, саме на цьому етапі можуть виникати затримки або помилки, пов'язані з навантаженням, фільтрацією чи проблемами доступу до сховищ. Для моніторингу важливо відрізняти ситуації, коли лист уже прийнято сервером, від ситуацій, коли він фактично став доступним користувачу.

Кінцевою точкою взаємодії є MUA (Mail User Agent) — поштові клієнти, веб-інтерфейси або мобільні застосунки. У більшості випадків вони не є прямими об'єктами інфраструктурного моніторингу, проте саме на цьому рівні користувачі першими помічають проблеми, спричинені збоєм будь-якого з попередніх компонентів.

Сучасні поштові системи практично завжди доповнюються антиспам- та антивірусними механізмами, які можуть бути реалізовані як вбудовані модулі або окремі сервіси. Їхня робота істотно впливає на швидкість доставки та коректність обробки листів. З точки зору моніторингу ці компоненти є критичними, оскільки їхня деградація або некоректна конфігурація може призвести як до повної зупинки поштового потоку, так і до прихованих проблем, наприклад масового потрапляння листів у спам.

У багатьох інфраструктурах, навіть при використанні хмарних поштових сервісів, застосовуються relay-сервери або smart-host. Вони використовуються для централізованої відправки системної пошти, інтеграції з SaaS-поштою або контролю вихідного трафіку. У таких випадках власний MTA може бути єдиним поштовим компонентом, який перебуває під контролем організації, але при цьому залишається критично важливим об'єктом моніторингу.

З архітектурної точки зору поштове повідомлення проходить послідовний ланцюг обробки: спочатку відбувається DNS-резолюція домену отримувача, далі встановлюється SMTP-з'єднання, повідомлення потрапляє у черги, проходить етапи фільтрації та перевірок, після чого доставляється у поштову скриньку і стає доступним через IMAP або POP3. На кожному з цих етапів можливі збої або затримки, які не завжди супроводжуються явною відмовою сервісів.

Окремо слід наголосити на зовнішніх та внутрішніх залежностях, без яких поштові сервіси не можуть функціонувати коректно. Насамперед це DNS-записи, зокрема MX та пов'язані з ними записи, від яких напряму залежить можливість доставки пошти. Захищене з'єднання через TLS є не лише вимогою безпеки, але й умовою прийому пошти багатьма зовнішніми сервісами. Крім того, критичну роль відіграє IP-репутація поштових серверів, яка визначає рівень довіри з боку інших поштових систем.

Важливою особливістю сучасної поштової інфраструктури є залежність від зовнішніх списків блокування (RBL - Realtime Blackhole List або Realtime Blacklist) та інших репутаційних механізмів, які не належать до жодної конкретної організації, але безпосередньо впливають на доставку електронної пошти. RBL являють собою спеціалізовані сервіси, що ведуть списки IP-адрес і доменів, помічених у розсиланні спаму або іншій небажаній поштовій активності, і використовуються поштовими серверами по всьому світу під час прийому SMTP-з'єднань.

На практиці це означає, що рішення про прийом або відхилення листа часто приймається на стороні сервера-одержувача, на основі перевірок у зовнішніх репутаційних базах. При цьому власний поштовий сервер може працювати технічно коректно: SMTP-сервіс доступний, черги не переповнені, помилок у логах немає, — але значна частина повідомлень не доставляється, оскільки IP-адреса або домен відправника внесені до одного чи кількох списків блокування.

Особливу складність для моніторингу створює той факт, що вплив RBL не проявляється у вигляді класичних відмов сервісів. Проблема часто стає помітною лише через непрямі ознаки: зростання кількості bounce-повідомлень, скарги користувачів на недоставку листів, погіршення доставлюваності до окремих поштових провайдерів або зниження загальної репутації домену. У таких ситуаціях традиційний інфраструктурний моніторинг може не зафіксувати жодних відхилень.

З точки зору побудови системи моніторингу це означає необхідність виходу за межі спостереження виключно за власними сервісами та врахування зовнішнього репутаційного контексту. Ефективний моніторинг поштових сервісів має доповнюватися перевірками статусу IP-адрес у популярних RBL, аналізом причин недоставки повідомлень та кореляцією цих даних із загальним станом поштової інфраструктури.

Таким чином, незалежно від того, чи використовується власний поштовий сервер або хмарний поштовий сервіс, архітектура пошти залишається розподіленою системою з великою кількістю залежностей. Для ефективного моніторингу важливо не стільки знати конкретну реалізацію, скільки розуміти, на яких етапах потоку повідомлень можуть виникати проблеми і які сигнали дозволяють їх вчасно виявити.

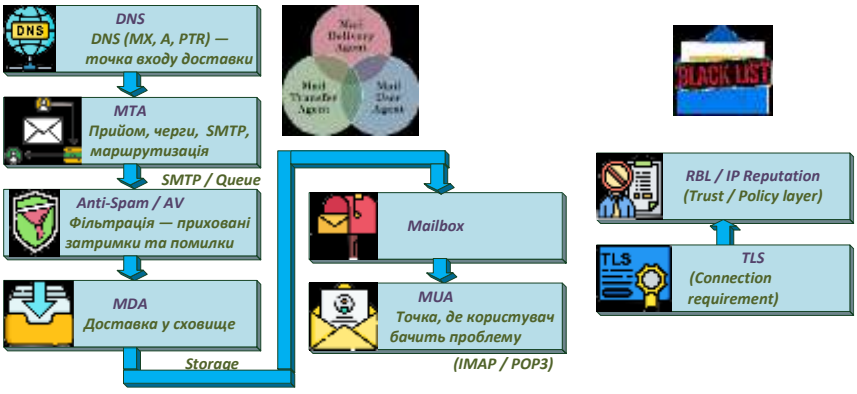

Рис. 7.01 Пошта — розподілений сервіс, а не окремий компонент.

Об'єкти моніторингу поштових сервісів

Розглядаючи поштові сервіси як об'єкт моніторингу, важливо відійти від спрощеного уявлення про «поштовий сервер як один сервіс». Насправді пошта — це ланцюжок взаємодіючих компонентів, кожен з яких виконує власну роль у процесі доставки повідомлень. Відмова або деградація будь-якого з цих компонентів може призвести до порушення роботи поштового сервісу загалом, навіть якщо решта елементів функціонують коректно.

- ***SMTP-сервіси***

SMTP-сервіси є центральним елементом поштової інфраструктури, оскільки саме вони відповідають за передачу повідомлень між системами. З точки зору моніторингу доцільно розділяти їх на кілька логічних ролей.

Вхідний SMTP (inbound) обробляє пошту, що надходить із зовнішнього світу. Його доступність і коректна робота визначають, чи здатна організація приймати листи від клієнтів, партнерів та зовнішніх сервісів. Проблеми на цьому рівні часто залишаються непоміченими зсередини, оскільки внутрішні користувачі можуть не відправляти пошту напряму на цей сервіс.

Вихідний SMTP (outbound) використовується для надсилання повідомлень за межі організації. Його робота безпосередньо впливає на бізнес-комунікації, розсилки та автоматичні повідомлення. Для моніторингу важливо контролювати не лише доступність сервісу, але й поведінку при встановленні SMTP-з'єднань, реакцію на помилки та стабільність доставки.

Relay-сервери та smart-host-и часто використовуються як проміжна ланка між внутрішніми системами та зовнішніми поштовими провайдерами. Вони можуть виконувати функції фільтрації, маршрутизації або централізованого виходу в інтернет. З точки зору моніторингу такі сервери є критичними, оскільки їхня деградація може одночасно вплинути на всі поштові потоки.

- ***IMAP / POP3***

IMAP та POP3-сервіси відповідають за доступ користувачів до поштових скриньок і часто сприймаються як «користувацький рівень» поштової системи. Проте з точки зору моніторингу вони мають не менше значення, ніж SMTP.

Доступність цих сервісів визначає, чи можуть користувачі отримати свою пошту через клієнти або веб-інтерфейси. Важливим аспектом є автентифікація, адже проблеми з нею часто маскуються під помилки поштових клієнтів або облікових записів. Навіть короткочасні збої автентифікації можуть призвести до масових звернень у службу підтримки.

Окрему увагу слід приділяти затримкам доступу до скриньок. Повільна робота IMAP-сесій, затримки при відкритті папок або синхронізації можуть свідчити про перевантаження серверів, проблеми зі сховищами або деградацію продуктивності, яка не завжди помітна на рівні простих перевірок доступності.

- ***Поштові черги***

Поштові черги є одним з найбільш інформативних об'єктів моніторингу, оскільки вони відображають реальний стан процесу доставки повідомлень. На відміну від перевірок портів або сервісів, аналіз черг дозволяє побачити, як система справляється з навантаженням у динаміці.

Збільшення розміру черг часто є першою ознакою проблем — як внутрішніх, так і зовнішніх. Час доставки повідомлень дає змогу оцінити, наскільки ефективно працює поштовий ланцюжок, і виявити приховані затримки.

Окрему категорію становлять «застряглі» повідомлення, які тривалий час перебувають у чергах без успішної доставки. Причини можуть бути різними: проблеми з DNS, блокування з боку одержувачів, обмеження з боку зовнішніх сервісів або репутаційні фактори. Саме моніторинг черг дозволяє виявити такі ситуації до того, як вони переростуть у масштабний інцидент.

- ***Антиспам та антифрод-системи***

Антиспам та антифрод-системи є невід'ємною частиною сучасної поштової інфраструктури, але з точки зору моніторингу вони часто залишаються «сірою зоною». Їхня робота безпосередньо впливає на якість поштового сервісу, навіть якщо всі інші компоненти функціонують коректно.

Збої або помилки в роботі таких систем можуть призводити до блокування легітимної пошти або, навпаки, до різкого зростання кількості спаму. Для моніторингу важливо відстежувати не лише їхню доступність, але й поведінкові показники, наприклад зміну кількості відхилених або відфільтрованих повідомлень, що може сигналізувати про некоректні правила або зовнішні атаки.

Рис. 7.02. Об'єкти моніторингу поштових сервісів

- ***Зовнішні сервіси доставки пошти***

У сучасних інфраструктурах значна частина поштового трафіку так чи інакше пов'язана із зовнішніми сервісами доставки, такими як Google, Microsoft 365, Mailgun та подібні платформи. Навіть якщо організація не управляє цими сервісами, їхній стан і політики безпосередньо впливають на результат доставки.

Проблеми взаємодії з такими сервісами часто проявляються вибірково: пошта може доставлятися до одних провайдерів і блокуватися іншими. З точки зору моніторингу це означає необхідність контролювати не лише власні сервіси, але й якість взаємодії з ключовими зовнішніми отримувачами або relay-провайдерами.

Методи моніторингу поштових сервісів

Після визначення об'єктів моніторингу логічно перейти до питання, яким чином ці об'єкти можна і потрібно контролювати. Моніторинг поштових сервісів відрізняється від класичного моніторингу серверів або мережевих пристроїв тим, що тут важливо враховувати не лише доступність сервісів, але й коректність їхньої поведінки на рівні протоколів та бізнес-логіки доставки повідомлень.

Жоден окремий метод моніторингу не дає повної картини стану поштового сервісу. Перевірка доступності порту не гарантує доставки листів, так само як успішне з'єднання з сервером не означає відсутності репутаційних або політичних обмежень з боку одержувачів. Тому на практиці використовують комбінацію кількох підходів — від низькорівневих протокольних перевірок до end-to-end тестування реальної доставки.

Першим і базовим рівнем такого контролю є SMTP-моніторинг, який дозволяє оцінити доступність і поведінку поштових серверів на рівні протоколу передачі повідомлень.

- ***SMTP-моніторинг***

SMTP-моніторинг є фундаментом контролю поштових сервісів, оскільки саме через SMTP відбувається передача повідомлень між серверами. Основна його мета — переконатися, що поштовий сервер доступний, коректно відповідає на запити та дотримується очікуваної протокольної логіки.

Найпростішим рівнем SMTP-моніторингу є перевірка TCP-з'єднання до відповідних портів. Залежно від конфігурації поштової інфраструктури використовуються стандартний порт 25, порт 587 для submission або порт 465 для SMTP з обов'язковим шифруванням. Успішне встановлення TCP-з'єднання підтверджує, що сервіс доступний на мережевому рівні, однак цього недостатньо для оцінки реальної працездатності SMTP.

Наступним рівнем є SMTP handshake, під час якого клієнт і сервер обмінюються службовими повідомленнями. Під час такого обміну моніторингова система може перевірити, чи сервер коректно вітається, чи приймає команду HELO або EHLO та чи повертає очікувані відповіді. Саме на цьому етапі часто виявляються проблеми з конфігурацією сервера, перевантаження або обмеження доступу за IP-адресою.

Важливим аспектом SMTP-моніторингу є аналіз кодів відповіді сервера. Коди класу 2xx свідчать про успішне виконання запиту, 4xx — про тимчасові помилки, які можуть бути пов'язані з перевантаженням або зовнішніми обмеженнями, а 5xx — про постійні помилки, що зазвичай

вказують на конфігураційні або політичні заборони. Для моніторингу особливо важливо відстежувати появу або зростання кількості відповідей 4xx та 5xx, оскільки саме вони часто сигналізують про проблеми з доставкою ще до того, як користувачі почнуть скаржитися.

Окрему увагу слід приділяти перевіркам STARTTLS, які дозволяють оцінити можливість встановлення захищеного з'єднання поверх SMTP. У сучасних поштових системах коректна робота TLS є обов'язковою вимогою для багатьох зовнішніх поштових сервісів. Моніторинг на цьому рівні може виявити проблеми з сертифікатами, застарілими алгоритмами шифрування або некоректною конфігурацією, які не впливають на встановлення TCP-з'єднання, але можуть призводити до відмови в прийомі або доставці пошти.

Таким чином, SMTP-моніторинг дозволяє контролювати поштовий сервіс на базовому протокольному рівні, виявляючи як явні відмови, так і приховані проблеми конфігурації або сумісності. Водночас він не дає відповіді на питання, чи дійсно листи доходять до кінцевих одержувачів, що зумовлює необхідність застосування додаткових методів моніторингу, які ми розглянемо далі.

- ***IMAP / POP3-моніторинг***

Якщо SMTP відповідає за передачу повідомлень між поштовими серверами, то протоколи IMAP і POP3 забезпечують доступ користувачів до вже доставленої пошти. З точки зору моніторингу це інший клас задач: тут важливо не лише те, що сервер "живий", а й те, що користувач може автентифікуватися та отримати доступ до своєї поштової скриньки без затримок.

Базовим елементом IMAP / POP3-моніторингу є перевірка доступності сервісу та успішності логіну. Моніторингова система встановлює з'єднання з відповідним портом (110 або 995 для POP3, 143 або 993 для IMAP), ініціює протокольний діалог і виконує автентифікацію з використанням тестового облікового запису. Успішний логін підтверджує, що сервер обробляє запити, коректно працює з бекендом зберігання пошти та не блокує доступ через перевантаження або помилки конфігурації.

Окрему роль відіграє перевірка TLS-з'єднання. У сучасних поштових системах доступ до скриньок майже завжди здійснюється через захищені канали, а проблеми з сертифікатами або параметрами шифрування можуть повністю заблокувати роботу клієнтів. Моніторинг на цьому рівні дозволяє виявляти прострочені сертифікати, помилки в ланцюгу довіри або несумісність криптографічних налаштувань ще до того, як користувачі масово втратять доступ до пошти.

Важливим показником є також час відповіді сервісу. Навіть якщо логін виконується успішно, збільшення затримок при автентифікації або отриманні списку повідомлень часто свідчить про проблеми зі сховищем, перевантаження дискової підсистеми або деградацію продуктивності бекенд-сервісів. Для користувача такі проблеми виглядають як "повільна пошта", що нерідко сприймається не менш критично, ніж повна недоступність сервісу.

Водночас IMAP / POP3-моніторинг має суттєві обмеження, які важливо чітко усвідомлювати. Успішний логін і доступ до скриньки не гарантують, що пошта коректно надходить на сервер або що листи не губляться на етапі доставки. Сервер може бути повністю доступним для клієнтів, але при цьому мати проблеми з SMTP-чергами, репутацією IP або зовнішніми блокуваннями, які не проявляються на рівні IMAP чи POP3.

Таким чином, моніторинг IMAP / POP3 є важливим індикатором користувацького досвіду та стану внутрішніх компонентів поштової системи, але не може розглядатися як повноцінний контроль доставки повідомлень. Він ефективно доповнює SMTP-моніторинг, дозволяючи охопити обидві сторони поштового сервісу — передачу повідомлень і доступ користувачів до їхнього вмісту.

- ***End-to-End email monitoring***

End-to-End email monitoring є найбільш комплексним і наближеним до реального користувацького досвіду підходом до контролю поштових сервісів. Його ключова ідея полягає у тому, щоб відтворити повний життєвий цикл поштового повідомлення — від моменту відправлення до фактичного отримання листа кінцевим адресатом. На відміну від протокольних перевірок, цей метод дозволяє оцінити не окремі компоненти інфраструктури, а результат їхньої спільної роботи.

Основою такого моніторингу є надсилання тестового листа з контрольного відправника на одну або декілька тестових поштових скриньок. Ці скриньки можуть знаходитися як у межах власної інфраструктури, так і у зовнішніх поштових провайдерів. Сам факт успішного встановлення SMTP-з'єднання при цьому не є достатнім — ключовим є те, що лист був прийнятий, доставлений та доступний для читання.

Під час End-to-End моніторингу вимірюється час доставки повідомлення, який охоплює весь шлях листа: від виходу з відправляючого сервера, проходження черг, фільтрації та зовнішніх перевірок до появи у поштовій скриньці одержувача. Збільшення цього часу часто сигналізує про проблеми, які не проявляються на рівні доступності сервісів, наприклад про тимчасові обмеження з боку зовнішніх поштових систем або внутрішні затримки у чергах.

Ще одним важливим показником є виявлення втрат повідомлень. У деяких сценаріях лист може бути прийнятий сервером, але так і не з'явитися у скриньці одержувача через внутрішні помилки, некоректну фільтрацію або відмови зовнішніх сервісів. End-to-End моніторинг дозволяє фіксувати такі ситуації як повноцінні інциденти, навіть якщо всі окремі компоненти інфраструктури формально працюють.

Окрему увагу приділяють контролю спам-фільтрації. Тестовий лист може бути доставлений, але потрапити до папки "Спам", що з точки зору бізнесу часто рівнозначно його втраті. Моніторинг цього аспекту дозволяє оцінювати репутацію відправника, коректність SPF, DKIM та DMARC, а також вплив змін у конфігурації або зовнішніх політиках поштових провайдерів.

На практиці End-to-End підхід часто реалізується у вигляді synthetic email monitoring — автоматизованого сценарію, який періодично надсилає тестові повідомлення, відстежує їхній шлях і аналізує результат доставки. Такий підхід дозволяє виявляти "тихі" проблеми, які не супроводжуються явними помилками на рівні серверів або протоколів, але безпосередньо впливають на ефективність комунікацій.

Водночас End-to-End email monitoring має і свої обмеження. Він складніший в реалізації, потребує підтримки тестових скриньок та облікових даних, а результати можуть залежати від зовнішніх факторів, що не піддаються прямому контролю. Проте саме цей метод дає найбільш повну відповідь на головне питання поштового моніторингу: чи доходять листи до адресатів так, як очікує бізнес.

Таблиця 7.01

Що показує і чого не показує моніторинг поштових сервісів

Метод моніторингу	**Що бачить**	**Чого НЕ бачить**
Port / Network check	Доступність сервісу	Логіку SMTP, доставку листів
SMTP monitoring	Протокол, коди відповіді	Чи лист дійшов до одержувача
IMAP / POP3 monitoring	Доступ користувача	Проблеми доставки, репутацію, черги
End-to-End email monitoring	Реальну доставку	Причину проблеми на рівні компонентів

Різні методи моніторингу поштових сервісів відображають різні рівні спостереження за однією і тією ж системою. Протокольні перевірки дозволяють переконатися у доступності та коректній поведінці сервісів, тоді як перевірки доступу до скриньок дають уявлення про фактичний користувацький досвід. End-to-End підхід, у свою чергу, фокусується не на окремих компонентах, а на результаті їхньої спільної роботи.

Практична цінність цього розділу полягає у розумінні того, що надійний поштовий моніторинг не може базуватися на одному індикаторі. Лише поєднання різних методів дозволяє виявляти як очевидні відмови, так і приховані проблеми, пов'язані з затримками доставки, фільтрацією або зовнішніми обмеженнями.

Таким чином, поштові сервіси слід розглядати як багаторівневу систему, для якої моніторинг має бути не лише технічно коректним, а й орієнтованим на реальний вплив на комунікації та бізнес-процеси.

Рис. 7.03. Методи моніторингу поштових сервісів

DNS як об'єкт моніторингу

Система доменних імен є одним із найбільш критичних, але водночас найменш помітних компонентів сучасної IT-інфраструктури. DNS не виконує прикладних функцій і не обробляє бізнес-логіку, проте без його коректної роботи більшість сервісів стають недоступними незалежно від стану серверів, мережі чи додатків. Саме тому DNS часто називають "невидимим фундаментом" усіх мережевих і прикладних сервісів.

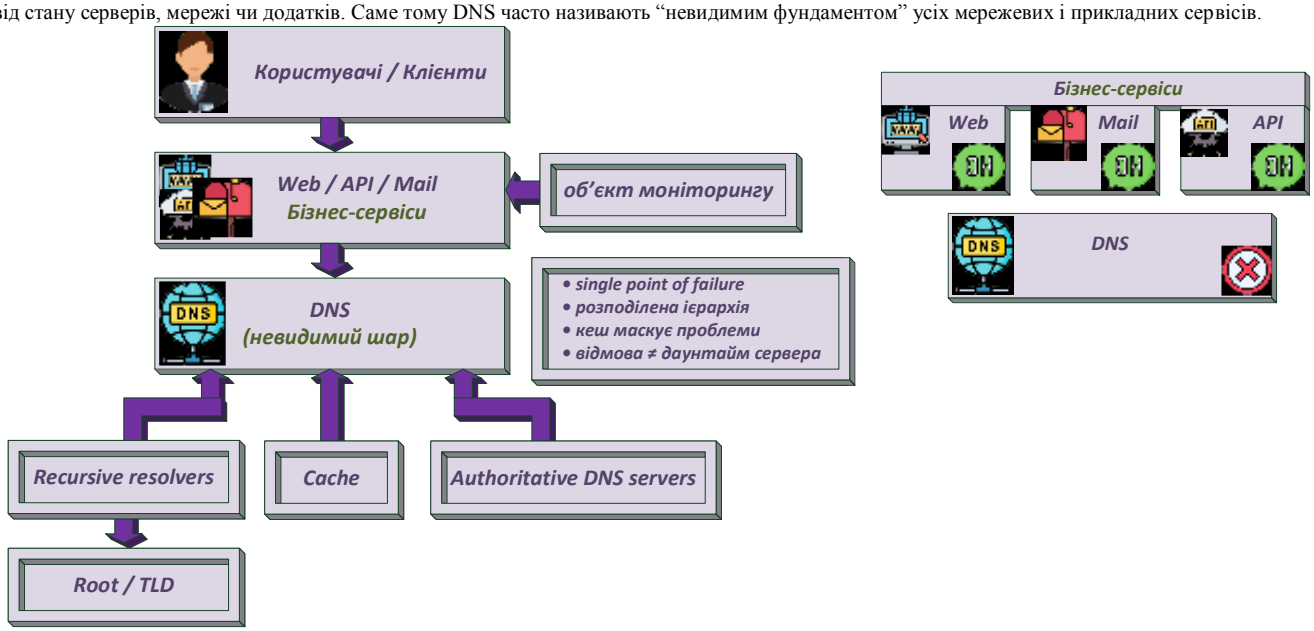

Рис. 7.04. Сервіси можуть працювати, але без DNS вони недоступні

З точки зору користувача відмова DNS виглядає як повна недоступність сервісу, хоча всі сервери можуть працювати штатно. У цьому сенсі DNS виступає single point of failure, який здатен паралізувати роботу веб-додатків, поштових систем, API та внутрішніх корпоративних сервісів без жодних ознак класичного даунтайму. Для системного моніторингу це означає необхідність окремого і цілеспрямованого контролю DNS, а не сприйняття його як "частини мережі за замовчуванням".

Архітектурно DNS є розподіленою ієрархічною системою, що складається з кількох ключових компонентів. Recursive resolvers відповідають за пошук і отримання відповідей на DNS-запити від клієнтів, використовуючи кеш і звернення до інших серверів. Authoritative servers зберігають достовірну інформацію про домени та відповідають за конкретні зони. Над ними розташовується глобальна інфраструктура root та TLD-серверів, де TLD (Top-Level Domain) — це сервери, що обслуговують домени верхнього рівня, такі як .com, .org, .net, .ua та інші, і визначають, які authoritative-сервери відповідають за конкретні доменні зони. Окрему роль відіграє кешування, яке з одного боку підвищує продуктивність і знижує навантаження, а з іншого — ускладнює діагностику проблем та відкладено проявляє помилки конфігурації.

З погляду моніторингу важливо розуміти, що відмова або деградація може відбуватися на будь-якому з цих рівнів. Проблема може бути не у власному authoritative DNS-сервері, а у рекурсивному резолвері провайдера або у некоректній роботі кешу, що призводить до вибіркової недоступності сервісів для окремих груп користувачів.

Окремим аспектом є контроль типів DNS-записів, які безпосередньо впливають на роботу сервісів. Записи **A** та **AAAA** визначають відповідність доменних імен IPv4 та IPv6-адресам і є критичними для доступності веб-ресурсів та API.

MX-записи відповідають за маршрутизацію електронної пошти і визначають, на які поштові сервери має доставлятися пошта для певного домену. Важливо підкреслити, що MX не є "поштовою адресою" або окремим видом пошти — це лише механізм вказівки серверів-приймачів із відповідними пріоритетами. Фактична робота поштових сервісів при цьому залежить від цілої групи DNS-записів, які використовуються разом із MX.

CNAME-записи застосовуються для логічної абстракції сервісів і часто використовуються у хмарних, SaaS та CDN-рішеннях, зокрема і в поштових інфраструктурах.

TXT-записи відіграють важливу роль у безпеці та репутації поштових сервісів, оскільки саме через них реалізуються механізми SPF (Sender Policy Framework — визначає, які сервери мають право надсилати пошту від імені домену), DKIM (DomainKeys Identified Mail —

забезпечує криптографічну перевірку цілісності повідомлення), DMARC (Domain-based Message Authentication, Reporting and Conformance — політика узгодженого контролю автентифікації та обробки пошти), а також інші політики захисту від підміни та зловживань.

SRV-записи застосовуються для сервісів, де важливими є не лише адреси, а й порти, пріоритети та вага підключення, зокрема у корпоративних та сервісно-орієнтованих середовищах.

Таким чином, коректна робота поштових, веб- та API-сервісів визначається не одним типом DNS-запису, а узгодженою конфігурацією кількох типів записів, кожен з яких відповідає за свою роль у загальному ланцюгу доступності та доставки.

У сучасних інфраструктурах DNS тісно пов'язаний з усіма ключовими сервісами. Веб-додатки залежать від коректного резолвінгу доменів і балансування навантаження. Поштові сервіси критично залежать від MX та TXT-записів для доставки і перевірки легітимності листів. API та мікросервіси часто використовують DNS як механізм сервіс-дискавері. Тому проблеми на рівні DNS рідко залишаються локальними — вони швидко трансформуються у масштабні інциденти, які складно діагностувати без спеціалізованого DNS-моніторингу.

Таким чином, DNS слід розглядати не як допоміжний мережевий сервіс, а як самостійний і критичний об'єкт моніторингу, стан якого безпосередньо визначає доступність і стабільність усієї IT-інфраструктури.

Методи та підходи до моніторингу DNS

Моніторинг DNS принципово відрізняється від контролю більшості інших сервісів тим, що проблеми на цьому рівні часто мають неявний і вибірковий характер. DNS може відповідати, але робити це повільно; може повертати відповіді, які формально коректні, але фактично застарілі; або ж працювати для одних користувачів і бути недоступним для інших через кешування та географічні особливості резолвінгу.

З точки зору моніторингу DNS важливо оцінювати не лише факт наявності відповіді, а якість цієї відповіді, швидкість її отримання та відповідність очікуваній конфігурації. Саме тому підхід до DNS-моніторингу зазвичай поєднує активні перевірки, аналіз відповідей і контроль змін у зоні. Першим і базовим рівнем такого контролю є моніторинг DNS-запитів.

- ***Моніторинг DNS-запитів***

Моніторинг DNS-запитів спрямований на оцінку того, як швидко і коректно система доменних імен відповідає на запити клієнтів. Для більшості сервісів DNS-запит є першим кроком у ланцюгу взаємодії, і будь-яка затримка або помилка на цьому етапі безпосередньо впливає на загальну доступність сервісу.

Одним із ключових показників є час відповіді DNS. Навіть незначне зростання latency може призводити до помітного погіршення користувацького досвіду, особливо для веб-додатків, API або мобільних клієнтів, які виконують багато DNS-запитів. Моніторинг цього параметра дозволяє виявляти перевантаження резолверів, проблеми з мережею або деградацію роботи authoritative-серверів ще до появи повної відмови.

Не менш важливим є контроль коректності відповідей DNS. Сервер може відповідати швидко, але повертати неправильні IP-адреси, застарілі записи або неочікувані типи відповідей. Такі ситуації часто виникають після змін конфігурації, міграцій або помилок синхронізації зон і можуть проявлятися як вибіркова недоступність сервісів або перенаправлення трафіку не туди, куди очікується.

Окрему категорію проблем складають відповіді з кодами NXDOMAIN та SERVFAIL. NXDOMAIN означає, що доменне ім'я не існує з точки зору DNS, і часто є індикатором помилок у записах або некоректних запитів. SERVFAIL сигналізує про внутрішню помилку на стороні DNS-сервера або про неможливість отримати коректну відповідь з інших рівнів ієрархії. Для моніторингу важливо не лише фіксувати сам факт появи таких відповідей, а й відстежувати їхню частоту та динаміку, оскільки масові NXDOMAIN або SERVFAIL можуть повністю паралізувати роботу залежних сервісів.

Ще одним критично важливим аспектом є контроль TTL та механізмів кешування. Значення TTL визначає, як довго DNS-відповіді зберігаються у кеші резолверів і клієнтів. Занадто великі значення можуть призводити до тривалого використання застарілих записів після змін конфігурації, тоді як надто малі — створюють надмірне навантаження на DNS-сервери. Моніторинг TTL дозволяє оцінювати, наскільки швидко зміни у DNS реально доходять до користувачів, і пояснювати ситуації, коли проблема вже усунена, але ефект від цього ще не проявився.

У підсумку моніторинг DNS-запитів дає змогу виявляти як явні помилки резолвінгу, так і приховані проблеми продуктивності та узгодженості відповідей. Він є базовим рівнем контролю DNS і створює основу для більш глибокого аналізу стану зон та відмовостійкості, які розглядаються у наступних підпунктах.

- ***Моніторинг DNS-зон***

На відміну від моніторингу DNS-запитів, який фокусується на поведінці сервісу під час обробки запитів, моніторинг DNS-зон спрямований на контроль статичної, але критично важливої конфігурації, від якої залежить коректність усіх відповідей DNS. Саме на рівні зон найчастіше виникають помилки, пов'язані з людським фактором, автоматизацією або неконтрольованими змінами.

Першим базовим завданням є перевірка наявності та коректності DNS-записів. Моніторинг має підтверджувати, що всі необхідні записи існують, мають очікувані типи, значення та параметри. Відсутність одного запису або його некоректне значення може призвести до повної або часткової недоступності сервісу, при цьому DNS-сервери формально продовжуватимуть працювати без помилок. Саме тому контроль зон часто дозволяє виявляти проблеми ще до того, як вони проявляться на рівні користувачів.

Окрему увагу слід приділяти синхронізації між primary та secondary DNS-серверами. У більшості інфраструктур authoritative-зона обслуговується кількома серверами, і очікується, що всі вони мають ідентичний вміст. Помилки у механізмах реплікації або збої під час оновлення можуть призводити до ситуацій, коли різні сервери відповідають по-різному на одні й ті самі запити. Для користувачів це виглядає як нестабільна або "плаваюча" робота сервісу, а для моніторингу — як складний для діагностики інцидент без очевидного джерела.

Ще одним важливим аспектом є контроль змін зон, або так званого zone drift. Під цим терміном розуміють неконтрольовані або неочікувані зміни у DNS-зоні, які не були зафіксовані у процесах управління конфігураціями. Такі зміни можуть виникати через ручне втручання, помилки автоматизованих систем або зовнішні інтеграції з хмарними та SaaS-провайдерами. З точки зору моніторингу важливо не лише виявляти сам факт зміни, а й мати можливість порівняти поточний стан з еталонною конфігурацією та швидко визначити, які саме записи були змінені.

Моніторинг DNS-зон дозволяє перевести контроль DNS із реактивного у проактивний режим. Замість того щоб реагувати на скарги користувачів або збої сервісів, система моніторингу може виявити потенційну проблему ще на етапі конфігурації та запобігти інциденту до його фактичного прояву.

- ***Відмовостійкість DNS***

DNS є одним із базових сервісів інфраструктури, і будь-які проблеми на цьому рівні миттєво впливають на доступність усіх залежних систем. Тому питання відмовостійкості DNS мають розглядатися не як додаткова опція, а як обов'язкова складова архітектури та моніторингу.

Одним із ключових підходів до підвищення стійкості є використання Anycast DNS. У цій моделі одна й та сама IP-адреса оголошується з багатьох географічно розподілених вузлів, а клієнтський запит автоматично маршрутизується до найближчої або найкращої з точки зору мережі точки присутності. Для моніторингу це означає необхідність перевіряти не лише сам факт доступності сервісу, а й коректність маршрутизації та стабільність відповідей з різних регіонів, оскільки локальні збої можуть бути непомітними з центральної точки спостереження.

Іншим базовим елементом відмовостійкості є використання кількох authoritative name servers (Multiple NS). Наявність декількох NS зменшує ризик повної втрати доступності зони у випадку відмови одного з серверів або датацентру. Водночас для моніторингу важливо не

обмежуватися перевіркою лише одного NS, а контролювати доступність, актуальність зон та однаковість відповідей усіх серверів, які оголошені в зоні.

Окремий вимір відмовостійкості пов'язаний з географічною доступністю DNS. Навіть якщо DNS-сервіс формально працює, проблеми з мережею, міжрегіональні збої або фільтрація трафіку можуть робити його недоступним для частини користувачів. Тому ефективний моніторинг DNS передбачає перевірки з різних географічних локацій, що дозволяє виявляти регіональні інциденти, які не видно з локальної інфраструктури.

Практичним аспектом є також розмежування зовнішнього та внутрішнього DNS. Зовнішній DNS обслуговує публічні домени і напряму впливає на доступність сервісів для клієнтів та партнерів. Внутрішній DNS використовується для роботи внутрішніх сервісів, мікросервісів, кластерів і корпоративних систем. Для моніторингу це означає різні вимоги до доступності, безпеки та точок спостереження, а також необхідність розуміти, що збій внутрішнього DNS може бути не менш критичним, ніж проблеми з публічним доменом.

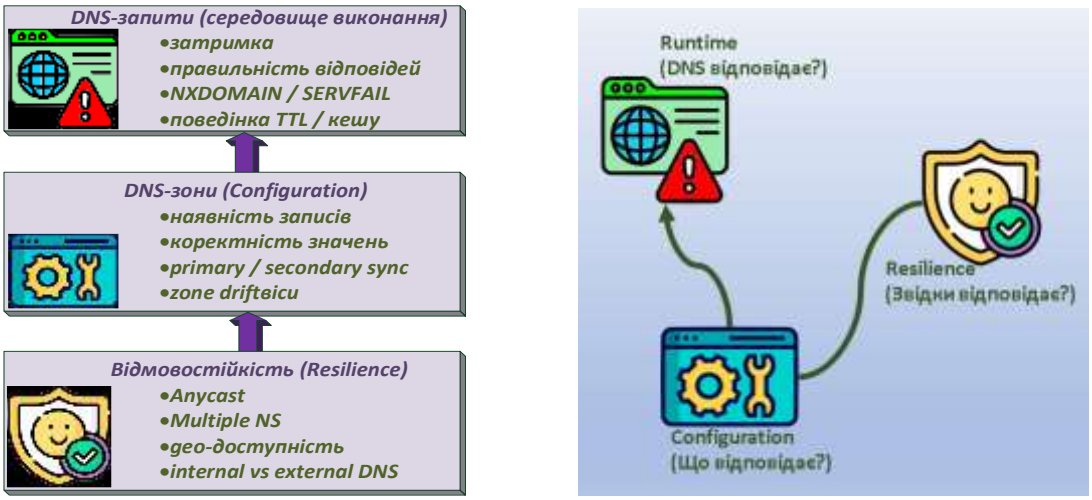

Рис. 7.05. DNS потрібно моніторити не в одному місці, а з трьох різних боків одночасно.

DNS є фундаментальною залежністю для більшості сучасних сервісів, але його проблеми часто проявляються опосередковано — через збої пошти, вебу або API. Саме тому моніторинг DNS потребує поєднання кількох підходів: контролю поведінки сервісу, перевірки коректності конфігурації та оцінки стійкості архітектури. Лише комплексний погляд на DNS дозволяє виявляти як явні збої, так і приховані ризики, що можуть перерости у масштабні інциденти під час навантаження або змін в інфраструктурі.

Безпека поштових сервісів: SPF, DKIM, DMARC

Поштова інфраструктура є одним з найбільш уразливих елементів IT-ландшафту з точки зору зловживань, підміни та репутаційних атак. На відміну від багатьох інших сервісів, електронна пошта історично проєктувалася як відкрита система, що значно ускладнює забезпечення її автентичності та довіри між сторонами. Саме тому сучасна безпека поштових сервісів базується не стільки на класичних механізмах захисту периметра, скільки на репутаційних та криптографічних механізмах перевірки відправника.

Ключову роль у цьому відіграють три взаємопов'язані технології — SPF, DKIM та DMARC. Усі вони тісно пов'язані з DNS і працюють як політики, які приймаюча сторона застосовує під час обробки листів. З точки зору моніторингу ці механізми цікаві тим, що вони дозволяють не лише підвищувати рівень захисту, а й отримувати цінну інформацію про стан поштового трафіку, помилки конфігурації та спроби підміни домену.

У цьому розділі ми розглядаємо не стільки криптографічні або протокольні деталі, скільки те, як ці механізми працюють на практиці, як вони ламаються і що саме може та має бачити моніторинг.

- ***SPF***

SPF (Sender Policy Framework) — це механізм перевірки, який дозволяє домену визначити, які сервери мають право надсилати електронну пошту від його імені. Його основна мета — зменшити кількість підроблених листів та ускладнити spoofing, коли зловмисник відправляє повідомлення з підробленою адресою відправника.

Принцип роботи SPF досить простий з концептуальної точки зору. Домен публікує у DNS спеціальний TXT-запис, у якому перелічує дозволені джерела відправки пошти: IP-адреси, діапазони, інші домени або сервіси третіх сторін. Коли приймаючий поштовий сервер отримує лист, він перевіряє IP-адресу відправника та звіряє її з SPF-політикою домену, вказаного у MAIL FROM або Return-Path.

Таким чином, SPF не підтверджує особу конкретного користувача і не шифрує повідомлення, а виконує перевірку відповідності інфраструктури відправки задекларованій політиці домену.

Технічно SPF реалізується через DNS TXT-записи, що робить його повністю залежним від коректної роботи DNS. Будь-які помилки у цих записах — неправильні механізми, відсутні include, перевищення DNS-lookup лімітів — безпосередньо впливають на результати перевірки і, як наслідок, на доставку листів.

Важливим аспектом SPF є інтерпретація результатів перевірки, зокрема різниця між SoftFail та HardFail. SoftFail зазвичай означає, що домен повідомляє: "цей сервер, ймовірно, не має права надсилати пошту, але рішення залишається за приймаючою стороною". На практиці такі листи часто доставляються, але з підвищеним рівнем недовіри або потрапляють до спаму. HardFail, навпаки, є жорсткою забороною і сигналізує, що лист з такого джерела не повинен прийматися. Багато поштових систем у цьому випадку відхиляють повідомлення ще на етапі SMTP.

З точки зору експлуатації та моніторингу SPF часто стає джерелом проблем через типові помилки конфігурації. Серед них — забуті сторонні сервіси розсилок, некоректні include-записи, конфлікти між кількома TXT-записами SPF для одного домену, а також надмірно м'які політики, які формально існують, але не виконують захисної функції. Окремим ризиком є зміни інфраструктури або провайдерів, після яких SPF-запис не оновлюється і починає блокувати легітимну пошту.

Для моніторингу SPF важливо розуміти, що сам механізм не генерує активних подій у класичному сенсі. Його стан проявляється через результати SMTP-відповідей, антиспам-фільтрацію та, пізніше, через звіти DMARC. Тому SPF є прикладом механізму безпеки, який потрібно контролювати опосередковано, через аналіз поведінки поштового потоку та DNS-конфігурації.

- ***DKIM***

DKIM (DomainKeys Identified Mail) — це механізм автентифікації електронної пошти, який використовує криптографічний цифровий підпис для підтвердження того, що лист був відправлений уповноваженим доменом і не був змінений під час транспортування. На відміну від SPF, який перевіряє інфраструктуру відправника, DKIM працює безпосередньо з вмістом повідомлення.

Принцип роботи DKIM полягає в тому, що поштовий сервер відправника підписує частину заголовків та тіло листа приватним криптографічним ключем. Цей підпис додається до листа у вигляді спеціального заголовка DKIM-Signature. Приймаюча сторона, отримавши повідомлення, витягує з нього інформацію про домен та селектор, звертається до DNS і отримує відповідний публічний ключ, після чого перевіряє коректність підпису.

Таким чином, DKIM забезпечує цілісність повідомлення і підтверджує, що лист дійсно був відправлений системою, яка володіє приватним ключем домену, вказаного у підписі.

Ключовим елементом DKIM є перевірка ключів, яка повністю залежить від доступності та коректності DNS. Публічні ключі зберігаються у DNS у вигляді TXT-записів, і будь-яка проблема з їх наявністю, форматом або TTL безпосередньо призводить до помилки перевірки підпису. З точки зору моніторингу це означає необхідність контролювати не лише сам факт існування запису, а й його відповідність очікуваному формату, актуальність і доступність з різних точок мережі.

Окремої уваги потребує ротація ключів DKIM. З міркувань безпеки криптографічні ключі мають періодично змінюватися, але на практиці цей процес часто стає джерелом інцидентів. Типовими проблемами є видалення старого ключа до того, як всі відправлені листи з ним будуть доставлені, або публікація нового ключа без оновлення конфігурації поштових серверів. Для моніторингу це означає необхідність відстежувати одночасну наявність кількох ключів, коректність їх використання та результати перевірки підписів у реальному трафіку.

На відміну від SPF, DKIM чутливий до змін вмісту листа після його підписання. Саме тому однією з поширених категорій інцидентів є проблеми сумісності з проміжними системами обробки пошти. Антиспам-фільтри, системи шифрування, поштові шлюзи або навіть некоректно налаштовані MTA можуть змінювати заголовки або тіло листа, що призводить до порушення підпису і, як наслідок, до DKIM-fail. Такі проблеми часто важко діагностувати, оскільки сам факт доставки може зберігатися, але репутація домену при цьому поступово погіршується.

З точки зору моніторингу DKIM є прикладом механізму, де формальна наявність конфігурації не гарантує її ефективності. Реальний стан DKIM проявляється через результати перевірок на приймаючій стороні, аналітику антиспам-систем та звіти DMARC. Саме тому контроль DKIM повинен поєднувати перевірку DNS-записів, аналіз заголовків тестових листів і кореляцію з подальшими рішеннями поштових сервісів щодо доставки або фільтрації.

- ***DMARC***

DMARC (Domain-based Message Authentication, Reporting and Conformance) — це політика доменного рівня, яка об’єднує результати перевірок SPF та DKIM і дозволяє власнику домену визначити, як приймаюча сторона повинна поводитися з листами, що не проходять ці перевірки. Якщо SPF і DKIM відповідають на питання «що ми бачимо», то DMARC відповідає на питання «що з цим робити».

На відміну від SPF та DKIM, які можуть існувати незалежно, DMARC працює лише за умови наявності принаймні одного з цих механізмів і вводить поняття узгодженості (alignment) — відповідності доменів, що використовуються у заголовках листа, політиці домену-відправника.

Ключовим елементом DMARC є політики обробки пошти, які визначаються у DNS TXT-записі домену. Політика none використовується для спостереження і збору статистики: листи не блокуються, але інформація про перевірки надсилається власнику домену. Політика quarantine рекомендує приймаючій стороні ізолювати підозрілі листи, зазвичай шляхом поміщення їх у спам. Політика reject є найбільш жорсткою і передбачає відхилення листів, які не відповідають вимогам DMARC, ще на етапі приймання.

З практичної точки зору вибір політики — це компроміс між безпекою та ризиком втрати легітимної пошти. Саме тому DMARC часто впроваджується поступово, починаючи з none і переходячи до більш строгих режимів після стабілізації SPF та DKIM.

Особливу цінність DMARC має завдяки механізму звітів. Звіти типу rua (Reporting URI for Aggregate reports) містять агреговану статистику про перевірки SPF і DKIM: джерела відправки, результати автентифікації та застосовані політики. Вони надходять регулярно і є основним джерелом даних для довготривалого аналізу. Звіти типу ruf (Reporting URI for Forensic reports), які інколи називають forensic-звітами, можуть містити детальні дані про окремі повідомлення, що не пройшли перевірку, але їх використання обмежене з міркувань конфіденційності та підтримується не всіма поштовими провайдерами.

З точки зору моніторингу DMARC фактично перетворює поштову автентифікацію на спостережувану систему. Замість непрямих ознак проблем, адміністратор отримує структуровані дані про те, хто і як надсилає пошту від імені домену, які механізми спрацьовують, а де виникають збої або підозрілі сценарії.

Окремо варто відзначити роль DMARC у виявленні spoofing-атак. Навіть у режимі none DMARC дозволяє побачити спроби масової підміни домену, використання несанкціонованих серверів або помилки конфігурації сторонніх сервісів розсилок. Таким чином DMARC стає не лише інструментом захисту, а й важливим елементом безпекового моніторингу, який надає видимість туди, де раніше існувала лише непрозора поведінка поштового трафіку.

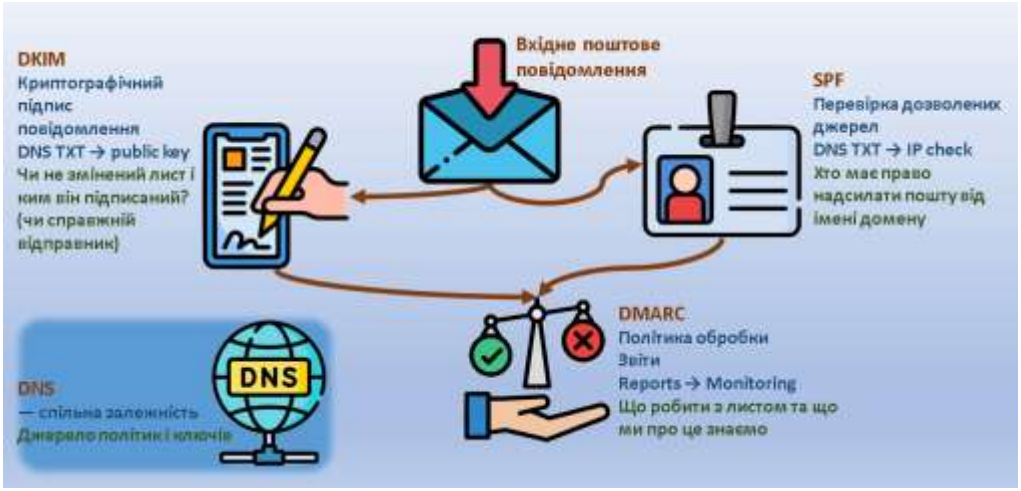

Рис. 7.06. SPF, DKIM, DMARC: рівні перевірки поштової довіри

Завершуючи розгляд механізмів SPF, DKIM та DMARC, важливо підкреслити, що безпека поштових сервісів у сучасних інфраструктурах базується не на одному окремому технічному рішенні, а на узгодженій роботі кількох взаємопов'язаних механізмів. SPF визначає допустимі джерела відправлення пошти, DKIM забезпечує криптографічну цілісність і автентичність повідомлень, а DMARC поєднує результати цих перевірок у єдину політику та надає інструменти контролю і спостереження.

З точки зору моніторингу ці механізми важливі не лише як засоби захисту, але і як джерело діагностичної інформації. Вони дозволяють виявляти проблеми конфігурації, помилки інтеграції із зовнішніми сервісами, а також спроби зловмисної підміни домену ще до того, як інцидент стане помітним користувачам або призведе до репутаційних втрат. Таким чином SPF, DKIM і DMARC органічно вписуються у загальну систему спостережуваності поштових сервісів і формують міст між технічним моніторингом, інформаційною безпекою та управлінням ризиками.

Маршрутизація як об'єкт моніторингу

Маршрутизація є фундаментальним елементом мережевої інфраструктури, від якого безпосередньо залежить доступність практично всіх IT-сервісів. Саме вона визначає, якими шляхами передається трафік між користувачами, серверами, датацентрами та зовнішніми мережами. При цьому маршрутизація зазвичай не асоціюється з конкретним сервісом або застосунком, але будь-яка помилка на цьому рівні миттєво відображається на їхній роботі.

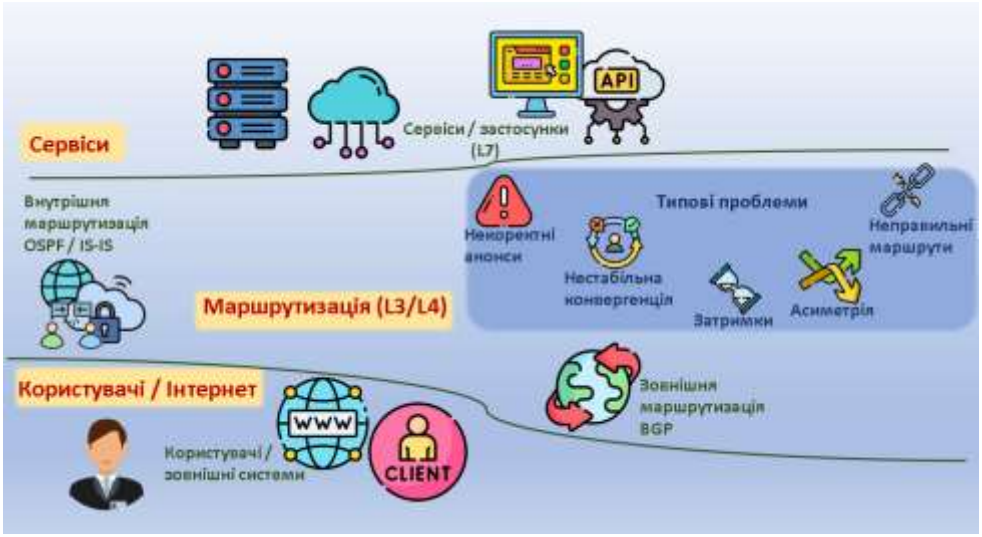

Рис. 7.07. Маршрутизація — це "невидимий шар" між сервісами і користувачем.

Однією з ключових особливостей маршрутизації як об'єкта моніторингу є те, що більшість проблем виникає на рівнях L3 та L4 моделі OSI (Open Systems Interconnection), тобто на мережевому та транспортному рівнях. Ці рівні відповідають за доставку пакетів та встановлення з'єднань, але залишаються «невидимими» для прикладного моніторингу. У результаті сервери можуть працювати коректно, сервіси бути запущеними, але користувачі стикатися з тайм-аутами, нестабільними з'єднаннями або частковою недоступністю.

З точки зору доступності сервісів маршрутизація відіграє критичну роль у формуванні затримок, стабільності маршрутів та відмовостійкості мережі. Проблеми з маршрутами часто проявляються не у вигляді повного падіння сервісу, а як деградація якості роботи, вибіркові збої або залежність проблеми від географії чи конкретних мережевих сегментів. Саме тому без моніторингу маршрутизації такі інциденти складно корелювати з подіями на прикладному або серверному рівні.

Залежно від масштабу та архітектури мережі використовуються різні типи маршрутизації. Статична маршрутизація базується на заздалегідь визначених маршрутах, які налаштовуються вручну і не змінюються автоматично. Вона є простою, передбачуваною та зручною для невеликих або ізольованих сегментів, але погано адаптується до змін топології та відмов мережевих вузлів.

Динамічна маршрутизація використовує спеціалізовані протоколи, які автоматично обмінюються інформацією про доступні маршрути та перебудовують шляхи у разі змін у мережі. У внутрішніх мережах організацій найчастіше застосовуються протоколи OSPF (Open Shortest Path First) та IS-IS (Intermediate System to Intermediate System), які забезпечують швидку збіжність і ефективну маршрутизацію в межах однієї адміністративної домени. Для обміну маршрутною інформацією між різними автономними системами в Інтернеті використовується BGP (Border Gateway Protocol), який визначає, якими шляхами трафік надходить до мережі організації та виходить з неї.

Хоча динамічна маршрутизація значно підвищує гнучкість і відмовостійкість мережі, вона також створює нові ризики. Проблеми збіжності маршрутів, помилки конфігурації або некоректні анонси можуть призводити до петльового трафіку, часткової недоступності сервісів або асиметричних маршрутів, які складно виявити без спеціалізованих засобів моніторингу.

Важливою з точки зору спостережуваності є також різниця між внутрішньою та зовнішньою маршрутизацією. Внутрішня маршрутизація визначає доступність сервісів усередині корпоративної мережі або між датацентрами, тоді як зовнішня маршрутизація відповідає за зв'язок з Інтернетом і зовнішніми провайдерами. Проблеми на зовнішньому рівні часто знаходяться поза прямим контролем організації, але безпосередньо впливають на доступність сервісів для кінцевих користувачів і тому мають бути враховані в системі моніторингу.

Таким чином маршрутизація є критичним, але непрямим об'єктом моніторингу, який поєднує мережеву інфраструктуру з прикладними сервісами. Ефективне спостереження за маршрутизацією дозволяє заповнити розрив між мережевим та сервісним рівнями і значно підвищує здатність оперативно виявляти та аналізувати складні інциденти доступності.

Методи моніторингу маршрутів і мережевих шляхів

Після розгляду маршрутизації як об'єкта спостереження логічним наступним кроком є аналіз практичних методів, які дозволяють бачити реальні мережеві шляхи, якими проходить трафік між вузлами. На відміну від моніторингу окремих пристроїв або інтерфейсів, моніторинг маршрутів зосереджується на поведінці мережі як цілісної системи, де важливими є не лише окремі компоненти, а й взаємодія між ними.

Методи моніторингу мережевих шляхів дозволяють виявляти приховані проблеми, пов'язані із затримками, втратами пакетів, асиметрією маршрутів або нестабільною роботою окремих сегментів. Саме ці методи часто використовуються для діагностики інцидентів, коли прикладні сервіси працюють нестабільно, але традиційний інфраструктурний моніторинг не показує очевидних збоїв.

Рис. 7.08. Маршрутизаційні події — це ранні індикатори проблем доступності сервісів.

Найбільш базовим і водночас універсальним інструментом такого аналізу є traceroute.

- ***Traceroute***

Traceroute — це діагностичний метод і відповідна утиліта, яка дозволяє визначити послідовність мережевих вузлів (хопів), через які проходить трафік від джерела до цільового вузла. Його робота ґрунтується на використанні поля TTL (Time To Live) у заголовку IP-пакета, яке обмежує кількість переходів пакета через маршрутизатори.

Поступово збільшуючи значення TTL і аналізуючи відповіді проміжних вузлів, traceroute дозволяє побачити реальний маршрут проходження пакетів у мережі. З точки зору моніторингу це дає уявлення про топологію шляху, наявність проміжних сегментів і точки, де можуть виникати проблеми.

Одним із ключових застосувань traceroute є аналіз затримок. Для кожного хопа зазвичай вимірюється час відповіді, що дозволяє оцінити, на якому етапі маршруту з'являються підвищені затримки. Це особливо корисно у випадках, коли сервіс повільно відповідає лише для певних користувачів або регіонів.

Окрім затримок, traceroute може допомогти у виявленні втрат пакетів або нестабільності з'єднання. Непослідовні відповіді, пропуски хопів або різкі коливання часу відповіді можуть вказувати на перевантажені маршрутизатори, проблемні канали зв'язку або нестабільну маршрутизацію.

Водночас traceroute має низку обмежень, які важливо враховувати у контексті моніторингу. По-перше, він показує лише шлях тестових пакетів, який не завжди повністю відповідає шляху реального прикладного трафіку, особливо в умовах асиметричної маршрутизації. По-друге, деякі мережеві пристрої можуть блокувати або обмежувати ICMP-відповіді, що призводить до «невидимих» хопів або помилкових висновків. По-третє, traceroute не дає прямої інформації про причину проблеми — він лише вказує на місце, де проблема може виникати.

Таким чином traceroute є потужним інструментом первинної діагностики мережевих шляхів і широко використовується як у ручному аналізі інцидентів, так і в автоматизованих системах моніторингу. Однак для повноцінної спостережуваності маршрутизації його зазвичай доповнюють іншими методами, зокрема моніторингом протоколів маршрутизації та зовнішніх маршрутних подій.

- ***BGP-моніторинг***

BGP (Border Gateway Protocol) є ключовим протоколом зовнішньої маршрутизації в Інтернеті. Саме він визначає, якими шляхами трафік між автономними системами передається у глобальній мережі. На відміну від внутрішніх протоколів маршрутизації, BGP безпосередньо впливає на те, чи буде сервіс досяжним з Інтернету, з яких регіонів і через яких провайдерів.

У контексті моніторингу важливо розуміти, що проблеми BGP часто не проявляються як повна недоступність сервісу. Натомість вони можуть призводити до часткової втрати доступності, підвищених затримок, змін географії доступу або нестабільної роботи для окремих мереж.

Одним із базових об'єктів спостереження є BGP-сесії — логічні з'єднання між маршрутизаторами, які обмінюються маршрутною інформацією. Стан BGP-сесій (встановлена, розірвана, нестабільна) є критично важливим показником здоров'я зовнішньої маршрутизації. Часті розриви або перезапуски сесій можуть свідчити про проблеми зв'язку, перевантаження маршрутизаторів або помилки конфігурації.

Поширеною проблемою, яку виявляє BGP-моніторинг, є route flapping — ситуація, коли маршрути до певних мереж постійно з'являються і зникають. Такі коливання призводять до повторної збіжності маршрутів у мережі Інтернет, що може викликати короткочасні, але регулярні збої доступності сервісів. Для прикладного рівня це виглядає як нестабільна робота або періодичні тайм-аути без очевидної причини.

Ще більш критичним сценарієм є prefix hijacking — захоплення префікса. У цьому випадку стороння автономна система помилково або навмисно анонсує IP-префікс, який їй не належить. У результаті частина трафіку може перенаправлятися до неправильного отримувача або просто втрачатися. Такі інциденти можуть призводити до серйозних порушень доступності, витоків даних або повної недоступності сервісу з окремих регіонів.

Через розподілений характер BGP більшість подій цього рівня знаходяться поза межами прямого контролю окремої організації. Саме тому важливу роль відіграють зовнішні сервіси моніторингу BGP, які збирають маршрутну інформацію з великої кількості точок Інтернету. Такі сервіси дозволяють відстежувати зміни анонсів, появу неочікуваних маршрутів, флапінг та потенційні захоплення префіксів у глобальному масштабі.

З точки зору системного моніторингу BGP виступає інструментом спостереження за «периметром» інфраструктури. Він дозволяє зрозуміти, чи проблема з доступністю сервісу викликана внутрішніми збоями, чи знаходиться на рівні міжмережевої взаємодії, і тим самим суттєво скорочує час локалізації інцидентів.

- ***IGP-моніторинг (OSPF / IS-IS)***

IGP (Interior Gateway Protocol) — це клас протоколів внутрішньої маршрутизації, які використовуються для побудови маршрутів усередині однієї адміністративної домени. Найпоширенішими представниками цього класу є OSPF (Open Shortest Path First) та IS-IS (Intermediate System to

Intermediate System). На відміну від BGP, ці протоколи працюють з повною інформацією про топологію мережі та забезпечують швидку перебудову маршрутів у разі змін.

Одним із ключових об'єктів моніторингу в IGP є стан сусідства між маршрутизаторами (Neighbor state). Протоколи OSPF та IS-IS встановлюють логічні відносини між сусідніми вузлами і постійно обмінюються службовими повідомленнями. Розрив або нестабільність такого сусідства часто є першою ознакою проблем з каналами зв'язку, інтерфейсами або перевантаженням мережевих пристроїв. Простими словами: чи "бачать" маршрутизатори один одного і чи довіряють вони інформації один одного.

Іншим важливим аспектом є моніторинг LSA (Link-State Advertisements) та змін топології. LSA — це повідомлення, за допомогою яких маршрутизатори інформують один одного про стан лінків і вузлів у мережі. Зміни у топології, такі як падіння інтерфейсів, зникнення маршрутів або поява нових шляхів, супроводжуються генерацією нових LSA та запуском процесу збіжності маршрутів. Часті або масові топологічні зміни можуть свідчити про нестабільність мережі і призводити до короткочасних, але повторюваних збоїв.

З точки зору сервісів IGP-події мають безпосередній вплив на доступність та продуктивність. Під час перебудови маршрутів можливі затримки, тимчасові втрати пакетів або зміна шляхів передачі трафіку. Ключовим фактором тут є convergence (збіжність маршрутів) — тобто час, який потрібен мережі, щоб виявити зміну (наприклад, падіння лінку або вузла), перерахувати маршрути та почати стабільно передавати трафік новим шляхом. Саме в період конвергенції найчастіше виникають втрати пакетів, тайм-аути та розриви TCP-з'єднань. Навіть якщо з точки зору мережі «все відновилось за секунду», для прикладного рівня це може бути критично і призвести до збоїв у роботі сервісів, навіть коли всі сервери залишаються працездатними. Саме тому моніторинг convergence дозволяє контролювати так звані «невидимі» мікровідмови та корелювати внутрішні мережеві події з поведінкою сервісів, точніше визначаючи першопричини інцидентів.

Методи моніторингу маршрутів і мережевих шляхів доповнюють класичний інфраструктурний і сервісний моніторинг, надаючи видимість того, як саме трафік рухається мережею. Traceroute дозволяє аналізувати фактичні шляхи пакетів і виявляти проблемні сегменти, BGP-моніторинг відкриває глобальний контекст доступності сервісів з Інтернету, а IGP-моніторинг забезпечує контроль внутрішньої стабільності мережі. У сукупності ці підходи формують основу для розуміння складних мережевих інцидентів, де причина збою лежить не в окремому компоненті, а у взаємодії маршрутів, топології та протоколів.

Ключові метрики моніторингу пошти, DNS та маршрутизації

Ефективний моніторинг інфраструктури неможливий без правильно підібраних метрик. Саме метрики перетворюють «сирі» технічні події на вимірювані показники стабільності, якості та доступності сервісів. Важливо, що для різних компонентів — пошти, DNS та маршрутизації — релевантні різні групи метрик, однак усі вони зрештою мають відповідати на одне ключове питання: чи отримує користувач сервіс у межах очікуваної якості.

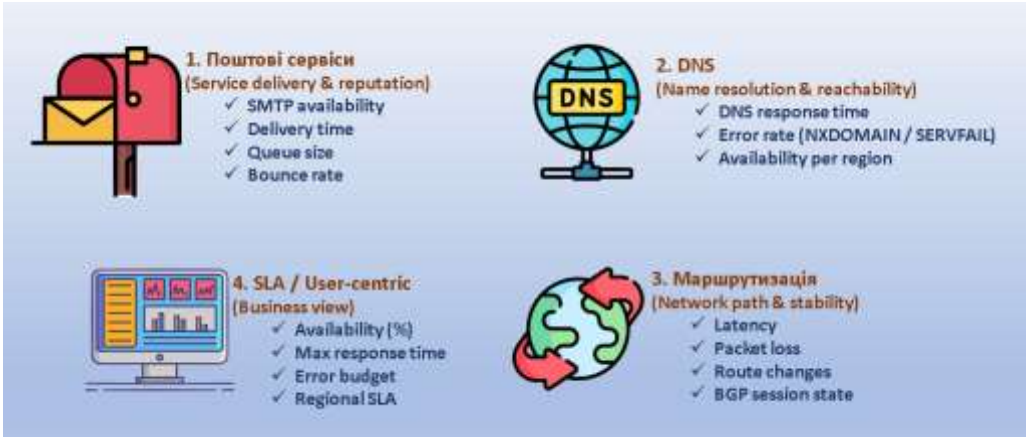

Рис. 7.09. Не всі метрики рівнозначні — важливі ті, що впливають на сервіс.

- ***Метрики моніторингу поштових сервісів***

Для поштової інфраструктури важливо контролювати не лише доступність сервісів, а й фактичну доставку повідомлень:

SMTP availability відображає доступність SMTP-серверів та їх здатність приймати пошту. Втрата цієї метрики часто є першою ознакою серйозного інциденту.

Delivery time показує час доставки листа від моменту прийому до потрапляння у поштову скриньку одержувача. Зростання цього показника сигналізує про проблеми з чергами, маршрутизацією або зовнішніми поштовими провайдерами.

Queue size характеризує обсяг повідомлень у поштових чергах. Стабільне або різке зростання черг зазвичай свідчить про деградацію доставки або блокування на стороні отримувачів.

Bounce rate (частка недоставлених листів) є важливою метрикою якості та репутації. Її підвищення може вказувати на проблеми з конфігурацією, репутацією домену або антиспам-політиками.

- ***Метрики моніторингу DNS***

DNS є фундаментальним сервісом, тому його метрики напряму впливають на всі залежні системи:

DNS response time вимірює час отримання відповіді на DNS-запит. Навіть невелике зростання цього показника може призводити до помітних затримок на рівні вебу, API або пошти.

Error rate відображає частку помилкових відповідей, таких як NXDOMAIN або SERVFAIL. Зростання цього показника часто сигналізує про проблеми з зонами, авторитетними серверами або рекурсивною інфраструктурою.

Availability per region дозволяє оцінити географічну доступність DNS-сервісу. Особливо критично для глобальних сервісів, CDN та Anycast-інфраструктур, де проблема може проявлятись лише в окремих регіонах.

Метрики моніторингу маршрутизації

Маршрутизація формує «шлях» трафіку між сервісами, і її проблеми часто мають непрямий, але відчутний вплив:

Latency показує затримку передачі пакетів і є ключовим індикатором продуктивності мережевого шляху.

Packet loss відображає втрати пакетів, які безпосередньо впливають на стабільність TCP-з'єднань і чутливі до цього сервіси.

Route changes фіксують зміни маршрутів або перебудову топології. Часті зміни можуть бути ознакою нестабільності або проблем з IGP/BGP.

BGP session state показує стан BGP-сесій між автономними системами. Їх падіння або флапінг часто призводять до втрати доступності сервісів для частини Інтернету.

- ***SLA-орієнтовані метрики***

Окрему категорію становлять **SLA-орієнтовані метрики**, які поєднують технічні показники з бізнес-вимогами. Вони не завжди відображають окремий компонент, але дозволяють оцінити сервіс у цілому: доступність у відсотках, максимальний час відповіді, допустимий рівень втрат або затримок. Саме такі метрики є основою для звітності, прийняття управлінських рішень та комунікації між технічними і бізнес-командами.

Інструменти моніторингу

Вибір інструментів моніторингу визначає не лише глибину спостереження за інфраструктурою, а й швидкість реагування, зручність аналізу та масштабованість рішення. У реальних середовищах зазвичай використовується комбінація універсальних систем моніторингу та спеціалізованих сервісів, кожен з яких закриває свою зону відповідальності: пошту, DNS, маршрутизацію або зовнішню доступність.

У курсі ми детально розглядали кожен із цих інструментів окремо. На практиці ж вони майже ніколи не використовуються ізольовано. Саме комбінація універсальних систем, метрик, перевірок і зовнішніх сервісів дає реальну видимість стану інфраструктури

Рис. 7.10. Різні задачі потребують різних підходів до спостереження.

- ***Zabbix***

Zabbix є однією з найпопулярніших універсальних систем моніторингу для on-prem та гібридних середовищ. Він добре підходить для комплексного контролю інфраструктури, включно з поштовими та DNS-сервісами.

SMTP / DNS checks дозволяють перевіряти доступність сервісів на мережевому та прикладному рівнях: відкриття порту, коректність відповіді SMTP, отримання DNS-записів.

External scripts розширюють стандартні можливості Zabbix і дають змогу реалізувати складні перевірки, наприклад end-to-end email monitoring або перевірку DNS-зон.

Low-level discovery (LLD) використовується для автоматичного виявлення об'єктів моніторингу: поштових черг, DNS-записів, інтерфейсів або BGP-сесій, що особливо корисно у динамічних середовищах.

Zabbix добре підходить для глибокої технічної діагностики, але потребує налаштування та підтримки з боку команди.

- ***Prometheus + exporters***

Prometheus є системою збору метрик, орієнтованою на **time series** та сучасні хмарні архітектури.

Exporters — це спеціалізовані агенти, які збирають метрики з конкретних сервісів або компонентів (DNS, SMTP, мережеві пристрої, BGP).

Prometheus ефективний для збору великої кількості метрик і побудови аналітики, особливо у поєднанні з Grafana.

Основний фокус — **кількісні метрики**, а не перевірка логіки протоколів, тому його часто доповнюють іншими інструментами.

- ***Nagios / Icinga***

Nagios та Icinga представляють класичний підхід до моніторингу на основі перевірок стану (check-based monitoring). Добре підходять для контролю доступності сервісів і базових протокольних перевірок.Мають велику кількість готових плагінів для SMTP, DNS та мережевих сервісів. Менш зручні для масштабування та складної кореляції подій порівняно з сучасними метрик-орієнтованими системами.

- ***Спеціалізовані сервіси***

Окрему категорію становлять вузькоспеціалізовані платформи, які зосереджуються на конкретних аспектах інфраструктури:

MXToolbox використовується для перевірки поштової конфігурації, репутації, DNS-записів, RBL та безпекових механізмів.

DNS monitoring SaaS дозволяють контролювати доступність, швидкість та коректність DNS з різних регіонів світу без розгортання власної інфраструктури.

BGP monitoring platforms (наприклад, сервіси спостереження за маршрутами) дають змогу виявляти route leaks, prefix hijacking та глобальні проблеми маршрутизації, які неможливо побачити з локального середовища.

Такі сервіси особливо цінні для виявлення зовнішніх проблем, які не проявляються всередині власної мережі.

- ***On-prem vs Cloud***

Підхід до розгортання інструментів моніторингу залежить від архітектури та вимог організації:

On-prem моніторинг забезпечує повний контроль над даними та глибоку інтеграцію з внутрішньою інфраструктурою, але потребує ресурсів на підтримку.

Cloud-рішення швидко впроваджуються, надають глобальну видимість і зручні для моніторингу зовнішньої доступності, але обмежують контроль і можуть мати залежність від сторонніх провайдерів.

На практиці найефективнішим є гібридний підхід, коли внутрішні інструменти відповідають за детальну діагностику, а хмарні сервіси — за зовнішню перспективу та незалежну перевірку доступності.

Побудова системи моніторингу базових мережевих сервісів

На цьому етапі важливо відійти від окремих перевірок пошти, DNS чи маршрутизації та подивитися на моніторинг як на цілісну систему спостереження за фундаментальними сервісами інфраструктури. Саме ці сервіси рідко є бізнес-функціями самі по собі, але від їх стабільності залежить робота практично всіх прикладних систем.

- ***Визначення критичних сервісів***

Побудова системи моніторингу починається не з інструментів, а з визначення того, що саме є критичним для організації. Для різних середовищ це можуть бути різні компоненти: для одних — outbound SMTP і репутація домену, для інших — внутрішній DNS або стабільність маршрутизації між датацентрами.

Ключовим є розуміння не лише технічної важливості сервісу, а й його ролі у ланцюжку залежностей. DNS, пошта чи маршрутизація часто не сприймаються як «бізнес-сервіси», проте саме вони можуть стати єдиною точкою відмови для десятків або сотень систем.

- ***Частота перевірок***

Для базових мережевих сервісів частота перевірок має особливе значення. Занадто рідкі перевірки не дозволяють виявити короткочасні, але критичні збої, тоді як надто часті можуть створювати зайве навантаження або шум у системі алертингу.

Оптимальна частота залежить від типу сервісу: для DNS і маршрутизації важливі швидкі реакції на зміни, тоді як для поштових сервісів критичними можуть бути тренди — зростання часу доставки або накопичення черг. У результаті система моніторингу зазвичай поєднує часті легкі перевірки та рідші, але глибші контрольні сценарії.

- ***Географічні точки моніторингу***

Базові мережеві сервіси мають чітко виражений географічний вимір. DNS, маршрути та пошта можуть працювати коректно з однієї локації і водночас бути недоступними або деградованими з іншої.

Тому ефективна система моніторингу передбачає використання кількох точок спостереження — як внутрішніх, так і зовнішніх. Це дозволяє відрізнити локальну проблему від глобальної, а також виявити регіональні інциденти, які часто залишаються непоміченими у централізованому моніторингу.

- ***Кореляція подій***

Ключовою відмінністю зрілої системи моніторингу є кореляція, а не ізольовані перевірки. Саме на рівні базових сервісів кореляція дає найбільшу цінність.

Збій DNS може проявлятися як недоступність веб-сервісу, хоча сам веб-сервер працює коректно. Проблеми з маршрутизацією можуть виглядати як падіння доступності або зростання затримок без жодних помилок на серверах. У поштових системах деградація репутації або блокування на зовнішніх сервісах доставки часто виглядає як «нормальна робота SMTP», але з різким падінням успішної доставки.

Кореляція між DNS і вебом, маршрутами і доступністю, поштою і репутацією дозволяє переходити від симптомів до першопричин інцидентів.

- ***Алертинг: багаторівневий та context-aware***

Алертинг для базових мережевих сервісів не може бути примітивним, оскільки прості правила на кшталт «порт недоступний → алерт» швидко призводять або до перевантаження сповіщеннями, або до втрати чутливості до реальних інцидентів. Ефективний підхід базується на поєднанні багаторівневого та context-aware алертингу, де події розрізняються за ступенем впливу — від незначних технічних відхилень і деградацій до критичних відмов, що безпосередньо впливають на доступність сервісів. Водночас оцінка кожної події відбувається з урахуванням контексту: географії виникнення проблеми, типу сервісу, наявності паралельних симптомів у суміжних компонентах та часових патернів роботи інфраструктури. Такий підхід дозволяє зменшити шум у сповіщеннях і водночас швидше виявляти справді значущі інциденти, характерні для пошти, DNS та маршрутизації.

У результаті система моніторингу перестає бути просто джерелом тривог і перетворюється на інструмент підтримки прийняття рішень, який допомагає швидше і точніше реагувати на інциденти.

Рис. 7.11. Моніторинг — це система спостереження, а не набір окремих перевірок.

Типові проблеми та помилки у моніторингу пошти, DNS та маршрутизації

Однією з ключових складностей моніторингу базових мережевих сервісів є те, що формальна працездатність окремих компонентів не гарантує коректної роботи сервісу в цілому. Саме тому багато інцидентів залишаються «невидимими» для класичних перевірок і виявляються лише через скарги користувачів або бізнес-показники.

- ***«SMTP працює, але листи не доходять».***

Це одна з найпоширеніших ситуацій у поштових системах. З технічної точки зору SMTP-сервіс може бути доступним: порт відкритий, handshake проходить, сервер коректно приймає листи. Проте реальна доставка може блокуватися на інших етапах — через проблеми з SPF, DKIM або DMARC, негативну IP-репутацію, потрапляння в RBL або політики приймаючої сторони. Класичний SMTP-моніторинг у такому випадку показує «зелений» статус, тоді як для користувача сервіс фактично не працює. Типова помилка — відсутність end-to-end моніторингу та ігнорування репутаційних і зовнішніх факторів доставки.

- ***DNS відповідає, але сервіс недоступний.***

DNS-сервери можуть успішно відповідати на запити, повертати записи A або AAAA, і при цьому сервіс залишатись недоступним. Причинами можуть бути застарілі записи у кеші, неправильні IP-адреси, некоректні CNAME-ланцюги або розбіжності між різними DNS-регіонами. З точки зору простого DNS-check усе виглядає нормально, однак клієнти підключаються не до того ресурсу або взагалі не можуть встановити з'єднання. Помилка моніторингу полягає в перевірці лише факту відповіді DNS без аналізу коректності та актуальності отриманих даних.

- ***Маршрут є, але з великою затримкою.***

Наявність маршруту між клієнтом і сервісом не означає прийнятної якості з'єднання. Трафік може проходити обхідними шляхами через перевантажені або географічно віддалені сегменти мережі, що призводить до значних затримок або втрат пакетів. Для прикладних сервісів це проявляється у вигляді повільної роботи, тайм-аутів або нестабільних сесій. Типова помилка — зосередження лише на доступності маршрутів без контролю latency, packet loss та змін шляхів передачі трафіку.

- ***False positive при DNS-кешуванні.***

Кешування у DNS може створювати хибне відчуття стабільності або, навпаки, породжувати помилкові алерти. Наприклад, після виправлення помилки в зоні моніторингові перевірки можуть продовжувати отримувати старі відповіді з кешу, сигналізуючи про проблему, якої вже не існує. Або навпаки — кеш маскує некоректні записи на authoritative-серверах до моменту закінчення TTL. Помилка полягає у відсутності контролю TTL і нерозумінні різниці між кешованою та авторитетною відповіддю.

- ***Ігнорування зовнішніх залежностей.***

Пошта, DNS і маршрутизація за своєю природою залежать від зовнішніх систем: провайдерів зв'язку, хмарних платформ, глобальних DNS-інфраструктур, поштових сервісів та BGP-оточення. Моніторинг, зосереджений виключно на внутрішніх компонентах, не дозволяє виявити проблеми, що виникають поза межами організації, але безпосередньо впливають на доступність сервісів. Типова помилка — відсутність зовнішніх точок спостереження і кореляції з глобальним контекстом мережі та інтернету в цілому.

Рис. 7.12. Формальна доступність не дорівнює реальній працездатності сервісу.

Практичні сценарії та кейси

Практичні сценарії дозволяють побачити, як моніторинг пошти, DNS та маршрутизації працює у реальних умовах, де проблеми рідко проявляються ізольовано. У більшості випадків інциденти мають комплексний характер і потребують кореляції даних з різних рівнів інфраструктури.

Рис. 7.13. Моніторинг має цінність лише тоді, коли дозволяє знайти першопричину інциденту.

- ***Моніторинг корпоративної пошти.***

У корпоративному середовищі електронна пошта є критичним сервісом для внутрішніх та зовнішніх комунікацій. Моніторинг у цьому випадку охоплює доступність SMTP-сервісів для прийому та відправлення листів, стабільність IMAP або POP3-доступу користувачів, а також стан поштових черг. Окрему увагу приділяють часу доставки повідомлень і зростанню черг, що часто є першими індикаторами проблем з маршрутизацією, фільтрацією або зовнішніми сервісами доставки. Практика показує, що поєднання протокольних перевірок і end-to-end тестів дозволяє виявляти проблеми ще до масових скарг користувачів.

- ***Контроль SPF, DKIM та DMARC.***

SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) та DMARC (Domain-based Message Authentication, Reporting and Conformance) є базовими механізмами захисту поштових доменів від підміни та зловживань. Практичний моніторинг включає перевірку наявності та коректності відповідних DNS TXT-записів, контроль змін політик і аналіз звітів DMARC. У реальних кейсах саме помилки в цих налаштуваннях часто призводять до зниження доставлюваності листів або потрапляння їх у спам, при тому що сам поштовий сервер працює без збоїв.

- ***Виявлення DNS-проблем у мульти-регіоні.***

Мульти-регіональна інфраструктура передбачає доступ до сервісів з різних географічних локацій. У такому середовищі DNS може поводитись по-різному залежно від регіону через кешування, Anycast або використання локальних recursive resolver'ів. Практичний сценарій моніторингу полягає у порівнянні відповідей DNS з різних точок спостереження, контролі часу відповіді та виявленні розбіжностей у записах. Це дозволяє знайти ситуації, коли сервіс працює коректно в одному регіоні і недоступний в іншому.

- ***Аналіз деградації через зміну маршрутів.***

Зміни мережевих маршрутів не завжди призводять до повної недоступності сервісу, але можуть істотно погіршувати його якість. Практичні кейси включають аналіз traceroute-даних, затримок та втрат пакетів після змін у BGP або внутрішніх протоколах маршрутизації. Такі інциденти часто супроводжуються короткочасною конвергенцією маршрутів, що проявляється у вигляді тайм-аутів або розривів з'єднань на прикладному рівні.

- ***Кореляція з веб-моніторингом.***

Остаточна цінність моніторингу базових мережевих сервісів проявляється під час кореляції з веб-моніторингом. Наприклад, зростання часу відповіді веб-додатку може співпадати з DNS-затримками або змінами маршрутів, а помилки доставки листів — з проблемами SPF або DNS. У практичних сценаріях саме зіставлення даних з різних шарів дозволяє швидко відокремити прикладні проблеми від інфраструктурних і визначити справжню першопричину інциденту.

Місце теми у загальній системі моніторингу та спостережуваності

Пошта, DNS та маршрутизація формують базовий, але часто недооцінений рівень доступності сучасних IT-систем. Саме ці сервіси забезпечують можливість з'єднання між компонентами інфраструктури і виступають фундаментом, на якому працюють веб-додатки, API, бази даних та користувацькі сервіси. За своєю природою вони рідко є кінцевою точкою взаємодії з користувачем, але будь-які проблеми на цьому рівні миттєво відображаються на роботі прикладних систем.

Однією з особливостей DNS, пошти та маршрутизації є те, що вони часто стають джерелом складних і неочевидних інцидентів. Формально сервіси можуть залишатися «працездатними», проте через кешування, репутаційні механізми, затримки або зміни маршрутів виникають часткові відмови, деградації або регіональні проблеми. Такі інциденти складно виявити без цілеспрямованого моніторингу і кореляції подій між різними рівнями інфраструктури.

У загальній системі спостережуваності ці сервіси тісно пов'язані з іншими напрямами моніторингу. Веб-моніторинг залежить від DNS та якості мережевих маршрутів, а проблеми з доступністю веб-додатків часто мають першопричини саме на рівні базових мережевих сервісів. Бази даних, у свою чергу, чутливі до мережевих затримок і нестабільності, що може проявлятися як зниження продуктивності або збої транзакцій. Логування та SIEM-системи дозволяють доповнити картину подіями безпеки, поштовими відмовами, DNS-помилками та мережевими аномаліями, забезпечуючи єдиний контекст для аналізу інцидентів.

Таким чином, моніторинг пошти, DNS та маршрутизації займає проміжне, але критично важливе місце між інфраструктурним і прикладним рівнями спостережуваності. Розуміння цих сервісів і підходів до їх контролю створює основу для наступної теми курсу — моніторингу баз даних та систем логування, де акцент зміщується від мережевої доступності до продуктивності, цілісності даних та аналізу подій у масштабах усієї IT-інфраструктури.