***Система мониторинга Zenoss***

Системи моніторингу спостерігають за станом пристроїв в мережі і дозволяють попередити проблеми ще до їх появи. Zenoss дасть фору багатьом пропрієтарним продуктам.

У мережах навіть невеликих організацій налічується не один десяток пристроїв, самого різного призначення. Деякі з них мають бути доступні 24 години 7 днів на тиждень, інші час від часу. Але вихід з ладу або проблеми з будь-яким з них означає переривання бізнес-процесів, втрату або невдоволення клієнтів, а значить втрачений прибуток. Постійний моніторинг сервісів і ресурсів дозволяє визначити велику частину проблем і зреагувати ще до того як відбудеться збій. Якщо ж аварійна ситуація сталася, то подібні системи автоматично сповістять адміністратора, який може зреагувати раніше, а значить і незадоволених буде менше.

Zenoss (Zenoss Core) - програма з відкритим кодом, платформа управління мережею, створена на основі сервера застосунків Zope. Випущена під ліценією GNU General Public License (GPL) version 2, Zenoss Core надає веб інтерфейс що дозволяє системним адміністраторам моніторити доступність, конфігурацію, продуктивність та різноманітні події в пристроях мережі. Розробка Zenoss Core почалась в 2002, а в серпні 2005 було засновано корпорацію що займається цим проектом — Zenoss, Inc. Вона спонсорує розробку Zenoss Core та продає промислову версію системи побудовану на основі базової версії.

Динаміка обслуговування Zenoss:

* Ресурсний менеджер
* Дослідження та моделювання
* Повний моніторинг
* Повідомлення та контроль
* Вплив та управління подіями
* Картографічне обслуговування
* Аналіз та розв'язання основних причин
* Аналітика та оптимізація
* Склад даних операцій
* Аналіз та звітність

Глобальний операційний директор Zenoss:

* Згадує події з декількох примірників Зеноса

Zenoss Core:

* Вільне, відкрите джерело
* Спільнота підтримується
* Одна і та ж платформа моніторингу як менеджер ресурсів
* Не включає:
* Покращена функціональність масштабованості та доступності диспетчера ресурсів
* Контроль "поза коробки" (“Out of the box”) для деяких типів пристроїв
* Підтримка Zenoss

Zenoss Core надає наступні можливості:

* Контроль доступності мережевих пристроїв за допомогою SNMP, SSH, WMI
* Моніторинг мережевих послуг (HTTP, POP3, NNTP, SNMP, FTP)
* Моніторинг ресурсів хоста (процесор, використання диска) в більшості мережевих операційних систем.
* Контроль часу роботи пристроїв
* Розширений моніторинг Microsoft Windows за допомогою розширень з відкритим вихідним кодом WS-Management та Zenoss
* Інструменти керування подіями для анотації системних сповіщень
* Автоматично виявляє мережеві ресурси та зміни конфігурації мережі
* Система оповіщення забезпечує сповіщення на основі наборів правил та нарахованих календарів
* Підтримує формат плагіна Nagios

1. Функціональні компоненти:
2. За замовчуванням всі компоненти встановлюються на одному сервері
3. Кожен компонент складається з набору процесів демонів, конфігураційних файлів і т. д.
4. Додаткові сервери можуть бути додані для розміщення окремих компонентів
5. Додаткові колектори та концентратори можуть бути додані для масштабованості
6. Сервер Zenoss ("Майстер"):
7. Включає веб-сервери додатків Zope
8. Балансу завантаження веб-сервера (Nginx)
9. Процесує події
10. Брокери спілкуються з БД подій
11. ZenDS
12. Брендований сервер MySQL
13. Може бути перенесено з Master Server
14. Колектор:
15. Модеювання та моніторинг пристроїв
16. Зберігає дані про продуктивність у файлах RRD, відображає графіки ефективності
17. Додаткові екземпляри можуть бути розгорнуті для масштабованості
18. Xаб:
19. Брокери спілкуються між колекторами та майстер-сервером
20. Зберігає дані ZODB
21. Кількість робочих серверів-концентраторів може бути налаштована
22. Можна додати додаткові серверні концентратори

-----------------------------------------------------------------------------------------------

Меню навігації дозволяє отримати доступ до основних функцій системи. На додаток до інформаційної панелі, меню розділено на декілька функціональних областей:

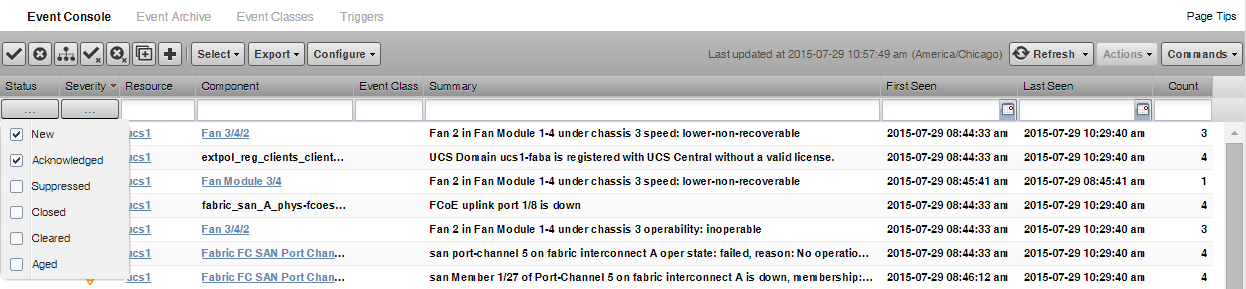
* ПОДІЇ - надає вам інформацію про область управління події, де ви можете відстежувати статус події, активацію та перетворення подій. Ви також можете відстежувати зміни, внесені до подій.
* ІНФРАСТРУКТУРА - пропонує доступ до мережевої інфраструктури, включаючи пристрої, мережі, процеси та послуги.
* ЗВІТИ - Дозволяє отримувати доступ до попередньо визначених та налаштовуваних звітів.
* ADVANCED- Надає доступ до шаблонів моніторингу, колекторів, MIB, налаштування системи та настроювання.

Основний вміст панелі інструментів містить портлети, які надають інформацію про систему та вашу інфраструктуру. Портлети можуть відображати:

* Випробування пристрою. Відображає список пристроїв, пов'язаних із кольоровими подіями критичних, помилкових або рівень важкості попередження. Натисніть назву пристрою, щоб переглянути деталі, або натисніть подію, щоб перейти на консоль події для пристрою. ***Figure 7. Device Issues Portlet***
* Карти Google (місцезнаходження пристроїв) - показує налаштовані місцезнаходження та налаштовані мережеві з'єднання.
* Daemon Processes Down - містить інформацію про систему самоконтролю.
* Стан виробництва - показує пристрої, призначені для певного виробничого стану. Якщо необхідно, ви можете визначити декілька станів виробництва для відображення.
* Вікно сайту - Спочатку надається посилання на ресурси, такі як посібники з продуктів, форуми та тренінги.
* Ви можете налаштувати портлет вікна сайту для відображення вмісту з будь-якої URL-адреси; однак, Zenoss рекомендує зберегти портлет з URL-адресою за умовчанням, щоб ви могли бути в курсі останніх тренінгів та оновлень продуктів Zenoss. Ви можете мати кілька портлетів Window Site, визначених на панелі інструментів.
* Діаграма пристроїв. Дозволяє відображати графік декількох точок даних для вибраного класу пристроїв.
* Event View - Відображення списку подій, подібних до перегляду на консолі подій.
* HTML Portlet-Відображення вмісту HTML. Ви повинні використовувати розмітку HTML у цьому портлеті. Якщо ви хочете заповнити портлет вмістом з певної URL-адреси, використовуйте портлет вікна сайту.
* Network Map - відображає мережеву карту для певної мережі, яка підлягає моніторингу. Ви можете визначити інтервал оновлення та рівень глибини вашої карти.
* Відкрита діаграма подій - відображає діаграму кількості відкритих подій, згрупованих за ступенем тяжкості. Ви можете визначити клас події для використання, а також кількість останніх днів, для яких потрібно показувати події.
* Список спостережень - Дозволяє відображати клаци, групи, системи, класи подій та вибрані розташування пристроїв стану високого рівня.

Консоль подій - це система центральної нервової системи, яка дозволяє переглядати та керувати подіями. Він відображає сховище всіх подій, які виявляються системою.

Щоб отримати доступ до консолі подій, натисніть "Події" в меню навігації. Відображається Консоль подій.

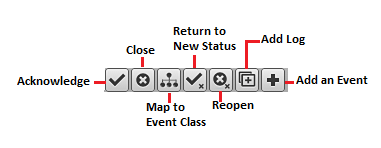
***Figure 13. Event Console Filter Options***

Ви можете відфільтрувати події, що з'являються у списку, різними способами залежно від типу поля:

* Ресурс - введіть значення відповідності, щоб обмежити список.
* Компонент. Введіть значення відповідності, щоб обмежити список.
* Клас події - введіть значення відповідності, щоб обмежити список.
* Резюме - Введіть значення відповідності, щоб обмежити список.
* First seen - Введіть значення або скористайтеся інструментом вибору дати, щоб обмежити список.
* Останнє сеанс - введіть значення або скористайтеся інструментом вибору дати, щоб обмежити список.
* Count - Введіть значення, щоб відфільтрувати список, як показано нижче:
* N - відображає події з числом, рівним N.
* : N - відображає події з кількістю, меншим чи рівним N.
* M: N - відображає події з підрахунком між М і N (включно).
* M: - Відображає події, кількість яких більше або дорівнює М.

Ви можете керувати подіями з консолі подій. Після вибору, натиснувши рядок події, ви можете:

* Підтвердити подію
* Закрити подію
* Перекласифікуйте подію, пов'язуючи її з певним класом події
* Повернути подію в Новий стан (скасувати його статус підтвердження)
* Повторне відкриття події
* Додайте нотатку до журналу
* Ви також можете додати подію з консолі події. Ця функція корисна для тестування конкретного стану шляхом імітації події.

***Figure 17. Event Management Options***

**Робота з тригерами та сповіщеннями**

Ви можете створювати сповіщення, щоб відправляти електронні листи або сторінки, створювати пастки SNMP або виконувати довільні команди у відповідь на події. Сповіщення також можуть бути використані для повідомлення інших систем управління, а також для виконання довільних команд для керування іншими типами інтеграції. Як і коли повідомлення надсилається, визначається тригером, який вказує правило, що містить серію з одного або декількох умов.

* Щоб налаштувати сповіщення, потрібно:
* Створіть тригер, вибравши правила, які його визначають
* Створіть сповіщення, вибравши один або декілька тригерів, які викликають його запуск
* Виберіть відповідні параметри та підписки, залежно від типу сповіщення

**Робота з тригерами**

Налаштування тригера передбачає:

* Створення тригера та правила, які його визначають
* Налаштування дозволів тригера

**Створення тригера**

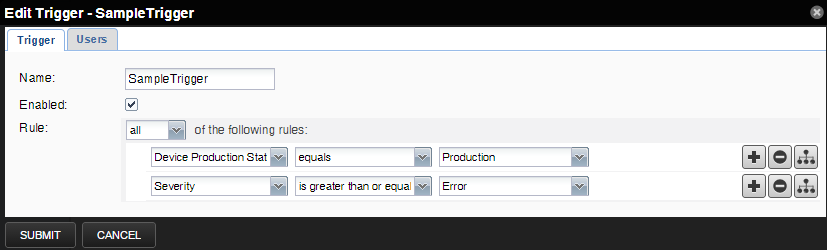
Ця процедура описує, як створити тригер.

* Виберіть EVENTS> Triggers.
* На сторінці Тригери відображаються всі визначені тригери.
* Натисніть значок "Додати".
* У діалоговому вікні «Додати тригер» введіть ім'я тригера та натисніть кнопку «Надіслати».
* У назвах тригерів дозволено використовувати лише літери верхнього та нижнього регістру, цифри та підкреслення.
* Тригер увімкнено та додано до списку.
* Щоб завершити тригер, перейдіть до наступного завдання.

**Редагування тригера**

Ця процедура описує, як відредагувати тригер.

* Виберіть EVENTS> Triggers.
* На сторінці Тригери відображаються всі визначені тригери.
* Відкрийте діалогове вікно Редагування триггера тригера для редагування.
* У таблиці тригерів двічі натисніть тригер або виберіть тригер, а потім натисніть значок дій.

***Edit Trigger dialog***

* Визначте правила для тригера, а потім натисніть SUBMIT.
* Правила тригерів об'єднують булеву логіку з значеннями подій, щоб вирішити, чи надсилати сповіщення. Тригер може використовувати будь-які або всі свої правила для прийняття рішення, і кожне правило може мати підзаконні правила чи гілки.

Примітка. Стани вироблення пристрою можуть змінюватися під час експлуатації вікон. Якщо ви хочете застосувати той самий тригер під час експлуатації вікон, обов'язково відредагуйте свій тригер для обліку всіх станів виробництва, які застосовуються до вашого тригера.

Setting Global Trigger Permissions

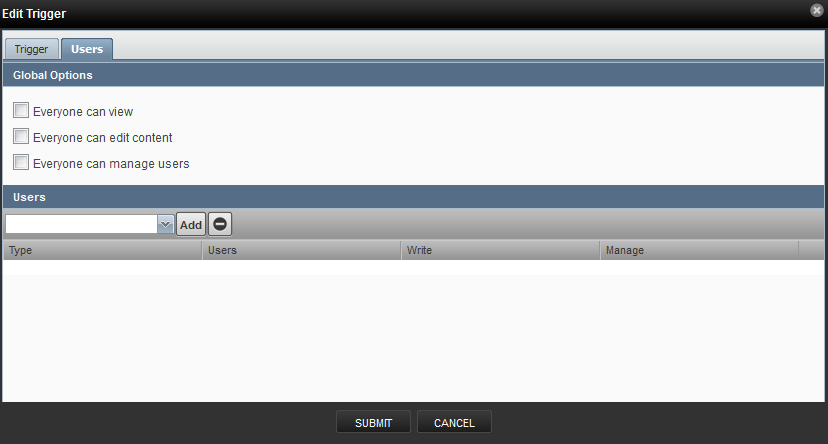
Ви можете встановити глобальні дозволи для перегляду, редагування та керування тригерами. Глобальні дозволи надаються будь-якому користувачеві з дозволом "керувати", який включає:

* Admin, Manager, and ZenManager roles
* Trigger owner

Редагування глобальних дозволів на вкладці "Користувачі" в діалоговому вікні "Редагувати тригер".

Глобальні параметри:

* Кожен може переглядати - надає дозвіл глобального перегляду.
* Кожен може редагувати вміст - надає повне дозвіл на оновлення.
* Кожен може керувати користувачами - надає глобальний дозвіл на керування.

***Edit Trigger - Users Tab***

**Встановлення індивідуальних дозволів тригерів**

Ви можете надати дозволи окремим користувачам. Для кожного доданого користувача ви можете вибрати:

* Write - виберіть цей параметр, щоб надати користувачеві дозвіл на оновлення активатора
* Керування - виберіть цей параметр, щоб надати користувачеві дозвіл на керування тригером.

Щоб встановити дозволи тригера окремого користувача:

* Виберіть користувача зі спадного списку в розділі "Користувачі" діалогового вікна редагування тригера.
* Натисніть "Додати". Користувач додається.
* Призначте дозволи, вибравши відповідні прапорці (-и).
* Необов'язково, додайте додаткові права на активацію користувача, повторюючи цю процедуру.
* Коли ви закінчите, натисніть Надіслати.

Щоб видалити дозволи тригера окремого користувача:

* Виберіть рядок дозволів користувача.
* Натисніть значок "Видалити".
* За бажанням, видаліть інші дозволи тригера користувача, повторюючи цю процедуру.
* Коли ви закінчите, натисніть Надіслати.

**Робота з сповіщеннями**

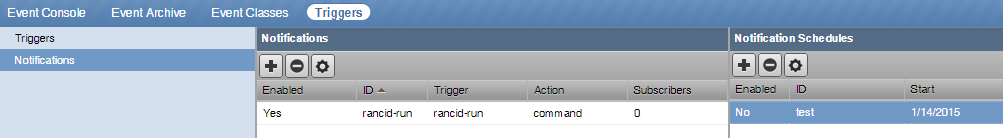
Налаштування сповіщення передбачає:

* Створення сповіщення
* Визначення вмісту сповіщення (для повідомлень електронної пошти або сторінок)
* Визначення хоста лову SNMP (для повідомлень типу ловушки SNMP)
* Визначення команд для запуску (для повідомлень типу командного типу)
* Налаштування дозволів на отримання сповіщень
* Налаштування розкладів сповіщень

**Створення сповіщення**

Ця процедура описує, як редагувати сповіщення.

* Виберіть EVENTS> Triggers.
* На панелі ліворуч виберіть «Сповіщення».

***Notifications***

У області сповіщень входить таблиця сповіщень і таблиця розкладів сповіщень.

* Натисніть значок "Додати".
* У діалоговому вікні «Додати сповіщення» введіть ім'я та вкажіть дію.
* Введіть ідентифікатор сповіщення.
* Пропускання не дозволено в ідентифікаторах сповіщень.
* Пов'яжіть дію з повідомленням.
* Щоб отримати додаткові відомості, див. Дії про сповіщення.
* Натисніть "ВІДПРАВИТИ".

Щоб завершити сповіщення, перейдіть до наступного завдання.

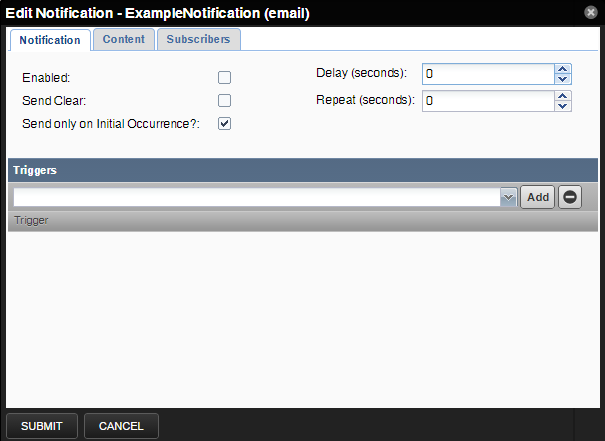
**Дії сповіщення**

|  |  |
| --- | --- |
| Action | Description |
| Command | Викликати команду оболонки, коли відбуваються події. Спільне використання цієї дії включає:   * Автоматичне відновлення подій. Ви можете використовувати ssh або wincommand для перезапуску служб на пристроях Linux та Windows. * Інтеграція з зовнішніми системами. Наприклад, відкриття квитків в системі управління інцидентами. * Розширення механізмів попередження. Менеджер ресурсів підтримує електронну пошту та пейджери як механізми оповіщення "поза вікна" за допомогою звичайних правил попередження. |
| Email | Відправляє HTML або текстовий електронний лист авторизованим підписчикам, коли подія відповідає правилу тригера. |
| Page | Pages authorized subscribers when an event matches a trigger rule. |
| Syslog | Відправляє повідомлення в системний журнал. |
| SNMP Trap | Відправляє SNMP trap, коли подія відповідає правилу тригера. |
| WinCommand | Відправляє або очищує команду Windows CMD. |

**Редагування сповіщення**

Ця процедура описує, як редагувати сповіщення.

* Виберіть EVENTS> Triggers.
* На панелі ліворуч виберіть «Сповіщення».
* Відкрийте діалогове вікно «Редагувати сповіщення» для повідомлення, яке потрібно редагувати.
* У таблиці "Сповіщення" двічі клацніть на сповіщення або виберіть сповіщення та натисніть значок дій.

***Edit Notification***

* Визначте параметри сповіщення.

**Налаштування сповіщень**

|  |  |
| --- | --- |
| Settings | Description |
| Увімкнено | Установіть прапорець, щоб увімкнути сповіщення. |
| Send Clear | Надішліть сповіщення, коли проблема вирішена очищенням. |
| Відправляти лише по початковій події | Надсилати сповіщення лише тоді, коли виникає перша подія активації. |
| Delay (seconds) | Мінімальна кількість секунд очікувати перед виконанням сповіщення. Затримка забороняє сповіщення про тимчасові проблеми та кілька сповіщень про ту ж проблему.  Наприклад, якщо п'ять подій, які відповідають тригерові, з'являються через 45 секунд, затримка в 60 секунд гарантує, що надсилається лише одне сповіщення. Також, якщо запуск спрацьовування повторюється через 15 секунд після початкової події, після чого відбувається очистка по 45 секунд, 60-секундна затримка гарантує, що не надсилатимуться сповіщення. |
| Repeat (seconds) | Інтервал між ретифікованими повідомленнями, у секундах. Повторення сповіщень триває, доки спрацьовування запуску не буде вирішено. |

**Автентифікація LDAP**

Ви можете використовувати існуючу інфраструктуру автентифікації LDAP, наприклад Active Directory або OpenLDAP, для вмикання єдиного входу в інтерфейс диспетчера ресурсів. За допомогою цієї можливості ви можете використовувати інструменти керування користувачами, з якими ви знайомі, щоб дозволити своїм користувачам Windows використовувати свої облікові дані Windows для автентифікації в інтерфейсі диспетчера ресурсів. Це заощаджує вас від необхідності вручну створювати облікові записи користувачів і окремо зберігати паролі.

Для тих властивостей LDAP, які відображені, зміни, внесені вами в LDAP, оновлюються в диспетчері ресурсів. (Ви повинні очистити кеш-пам'ять вашого браузера або вийти із системи, щоб змінити властивості, які потрібно негайно розповсюджувати.).

Перш ніж налаштувати автентифікацію LDAP, зібрати таку інформацію з вашого адміністратора LDAP або Active Directory:

* Ім'я хоста або IP-адреса каталогу глобального каталогу Active Directory (для автентифікації Active Directory)
* Ім'я хоста або IP-адреса сервера LDAP (для іншої автентифікації сервера LDAP)
* База користувача відмінне ім'я (DN)
* Менеджер DN
* Пароль менеджера
* Групи базу DN
* Необов'язково, список груп Active Directory для картування ролей Ресурсів Менеджера.

**Event management**

Events, and the graphs generated from performance monitoring, are the primary operational tools for understanding the state of your environment.

**Основні поля подій**

Щоб ввести систему керування події, подія повинна містити значення для пристрою, строки та поля підсумків. Менеджер ресурсів відхиляє події, у яких відсутні будь-які з цих полів.

*Основні поля подій:*

*Summary*

* Device
* Component
* Severity
* Event Class Key
* Event Class
* Collector

**Device field**

Поле пристрою - це текстова поле вільної форми, яка може містити до 255 символів. Менеджер ресурсів приймає будь-яке значення для цього поля. Якщо поле пристрою містить IP-адресу або ім'я хоста, система автоматично визначить і додасть подію відповідному пристрою.

Менеджер ресурсів автоматично додає інформацію до вхідних подій, які відповідають пристрою. Поле додано:

* prodState - Визначає стан поточного виробництва пристрою.
* Location - Вказує місце (якщо таке є), до якого пристрій призначено.
* DeviceClass - класифікує пристрій.
* DeviceGroups - Визначає групи (якщо такі є), до яких призначено пристрій.
* Системи - системи (якщо такі є), до яких призначено пристрій.
* DevicePriority-Priority присвоєний пристрою.

**Status field**

Поле «Статус» визначає поточний стан події. Це поле часто оновлюється після того, як подія була створена. Значення для цього числового поля 0-6, визначені наступним чином:

|  |  |  |
| --- | --- | --- |
| Number | Name | Description |
| 0 | *New* | *Стан наданий події, коли вона спочатку створюється в системі.* |
| 1 | Acknowledged (Визнано) | Стан наданий події, коли проблема вирішена очищенням. |
| 2 | Suppressed (Придушений) | Стан наданий події, яка була придушена через перетворення події. |
| 3 | Closed | Стан наданий події, яка була закрита в результаті дії користувача. |
| 4 | Cleared | Стан наданий події , яка була очищена відповідною явною подією. |
| 5 | Dropped | Стан наданий події, яка була скинута через перетворення події. Ця подія ніколи не зберігається в системі |
| 6 | Aged | Стан наданий події, яка була автоматично закрита системою відповідно до ступеня тяжкості та останнього побаченого часу події. |

**Severity field**

Поле Severity (Важкість) визначає суворість події. Значення для цього числового поля 0-5, визначені наступним чином:

0 - Ясно - Зелений

1 - Debug - сірий

2 - Інформація - синій

3 - Попередження - Жовтий

4 - Помилка - помаранчевий

5 - Критично - червоний

**Summary and message fields (Пояснення та повідомлення)**

Пояснення та повідомлення є вільними текстовими полями. Поле резюме може до 255 символів. Поле повідомлення може містити до 4096 символів. Ці поля, як правило, містять схожі дані.

Система обробляє ці поля по-різному залежно від того, присутній один або обидва вхідній події:

* Якщо є лише резюме, то система копіює свій вміст у повідомлення та скорочує вміст резюме до 128 символів.
* Якщо є лише повідомлення, то система копіює свій вміст у стислий опис та скорочує зміст резюме до 128 символів.
* Якщо узагальнення та повідомлення є присутніми, система скорочує сумарний зміст до 128 символів.

В результаті втрата даних можлива лише в тому випадку, якщо вміст повідомлення або резюме становить більше 65535 символів, або якщо обидва поля є присутніми, а загальний зміст - більше 128 символів.

Щоб переконатись, що обмеження кількості стовпців у 128 символів містять достатньо деталей, уникніть відтворення інформації в резюме, що існує в інших полях (наприклад, пристрої, компонентах або жорсткості).

*Події включають численні інші стандартні поля*. Деякі керують тим, як події накладаються та корелюються; інші надають інформацію про подію.

У наведеній нижче таблиці перелічені додаткові поля подій.

Dedupid - Динамічне створення відбитків пальців, що дозволяє системі виконувати де-дублювання при повторюванні подій, які поділяють подібні характеристики.

Component - Текстове поле вільної форми (максимум 255 символів), що дозволяє додавати додаткові контексти для подій (наприклад, назву інтерфейсу для порогової події інтерфейсу).

eventClass - Назва класу події, в якій ця подія була створена або зіставлена.

eventKey - Текстового поля вільної форми (максимум 128 символів), що дозволяє використовувати іншу ключову специфікацію для керування процесом кореляції де-дублювання та автоматичного очищення.

eventClassKey - Текстове поле вільної форми (максимум 128 символів), яке використовується як перший крок при відображенні невідомої події у класі подій.

eventGroup - Текстове поле вільної форми (максимум 64 символи), яке можна використовувати для групування подібних типів подій. Це, перш за все, розширення для налаштування. В даний час не використовується в стандартній системі.

stateChange - Останній раз, коли будь-яка інформація про події змінилася.

firstTime - Перший раз, коли подія сталася.

lastTime - Найновіше час, коли подія сталася.

Count - Кількість випадків події між першим і останнім часом.

prodState - Стан виробництва пристрою, оновлене, коли відбувається подія. Це значення не змінюється при зміні виробничого стану пристрою; це завжди відображає стан, коли подія була отримана системою.

Agent - Зазвичай ім'я демона, що генерує подію. Наприклад, порогова подія SNMP матиме zenperfsnmp як його агента.

DeviceClass - Клас пристрою пристрою, з яким пов'язана ця подія.

Location - Місцезнаходження пристрою, з яким пов'язана подія.

Systems - Список систем, до яких міститься пристрій.

DeviceGroups - Список систем, до яких міститься пристрій.

Facility - Тільки присутні на подіях, що надходять із системного журналу. Обладнання syslog.

Priority - Тільки присутні на подіях, що надходять із системного журналу. Системний пріоритет.

Ntevid - Тільки присутні на події, що надходять із журналу подій Windows. NT Event ID.

Ownerid - Ім'я користувача, який підтвердив цю подію.

Clearid - Тільки присутні на події в архіві, які були автоматично очищені. Це свідчить про подію, яка очистила це.

DevicePriority - Пріоритет пристрою, з яким пов'язана ця подія.

eventClassMapping - Якщо ця подія була узгоджена з однією з наведених відображень класів подій, містить назву цього правила відображення.

Monitor - У розподіленій установці міститься ім'я колектора, з якого виникла подія.

**Де-дублювання (De-duplication)**

Менеджер ресурсів використовує функцію "де-дублювання", засновану на концепції відбитка події. В межах системи цей відбиток є "Dedupid". Усі стандартні події, створені системою в результаті її опитування, дедублюються, без необхідності встановлення. Тим не менш, ви можете застосувати де-дублювання до подій, які надходять з інших джерел, таких як syslog, SNMP-ловушки або журнал подій Windows.

Найважливішою концепцією де-дублювання є відбиток пальців. Відбиток пальця події (або дедупуп) складається з рядка з роздільниками труб, що містить ці поля подій:

* пристрій
* компонент (може бути порожнім)
* eventClass
* eventKey (може бути порожнім)
* суворість
* резюме (пропущено з дедубупу, якщо eventKey не є порожнім)

**Event classes**

Класи подій - це проста організаційна структура для різних типів подій, які система генерує та отримує. Ця організація корисна для оповіщення та звітування. Ви можете, наприклад, створити правило сповіщення, яке надсилає вам електронний лист або сторінки, коли ви надаєте доступ до веб-сайту чи сторінки, відфільтруючи клас / Status / Web класу події.

Нижче наведено підмножина класів подій за умовчанням. Ви можете створювати додаткові класи за необхідністю.

* / App - Події, пов'язані з додатком.
* / Change - Події, створені, коли система знаходить зміни у вашому середовищі.
* / Perf - використовується для порогових подій ефективності.
* / Perf / CPU - порядок використання ЦП

/Perf/Memory - Використання пам'яті або подій для підкачки

/Perf/Interface - події для використання мережевого інтерфейсу

/Perf/Filesystem - Події з використанням файлової системи

* / Status - використовується для подій, що впливають на доступність.

/ Status / Ping - Події, що ведуть вгору / вниз

/ Status / Snmp - події SNMP вгору / вниз

/ Status / Web - події веб-сайту або сторінки вгору / вниз

* / ZenossRM - події системного менеджера ресурсів, включаючи ключові показники для вузлів у збірці показників, генерації подій та процесів моделювання

Параметри конфігурації класу подій (Event class configuration properties)

Подібно до того, як кластери пристроїв та пристрої мають властивості конфігурації, то також роблять класи подій і відображення класів подій. Властивості конфігурації застосовуються ієрархічно, при цьому застосовується найбільш конкретне властивість.

Наступні властивості конфігурації доступні для класів подій і класів.

* zEventAction - Як і де події, що постраждали, зберігаються, коли вони виникають.

статус - таблиця активних подій з оригінальним станом події

історія - таблиця активних подій із закритою подією

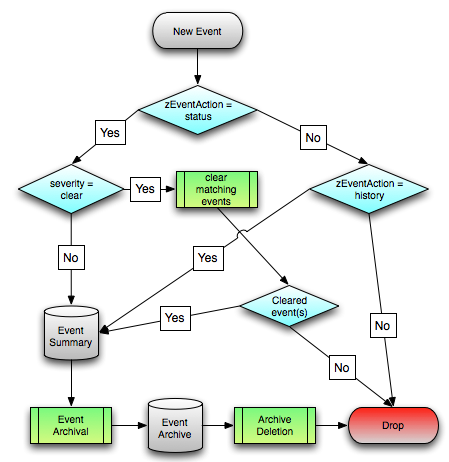
drop-Події не зберігаються

* zEventClearClasses-Необов'язковий список імен класів події, активні події яких буде очищено явними подіями, що відбуваються в цьому класі.
* zEventMaxTransformFails - погані перетворення відключені від виконання після вказаної кількості помилок. Значення за замовчуванням дорівнює 10.
* zEventSeverity - Тяжкість постраждалих подій змінюється на це значення, якщо не використовується значення за замовчуванням (-1).
* zFlappingIntervalSeconds - Визначає часовий інтервал, щоб перевірити, чи не відбувається перемикання подій (багаторазово змінюється рівень тяжкості). Значення за умовчанням становить 3600 секунд.
* zFlappingSeverity - Визначте ступінь тяжкості, щоб перевірити, чи не відбувається перегортання. Якщо рівень серйозності події змінюється від цього значення певною кількістю разів (zFlappingThreshold) протягом певного діапазону часу (zFlappingIntervalSeconds), то подія події згортає. Можливі значення включають: 5-критичний, 4-Error, 3-Warning, 2-Info, 1-Debug і 0-Clear.
* zFlappingThreshold - кількість разів, коли ступінь події повинна закриватися в межах інтервалу. Один із параметрів для визначення, щоб генерувати подібні події.

Хороший приклад того, як система використовує властивості конфігурації класу події, знаходиться в класі подій / Status. У межах властивостей конфігурації класу події / Статусу zEventAction встановлено на "історію", а zEventSeverity встановлено на "Default". Це означає, що події, що надсилаються з даним класом події, надсилаються в таблицю активних подій із початковим станом закритого, а ступінь події не змінюється.

**Життєвий цикл подій (Event life cycle)**

Окрім ручних методів отримання подій у таблиці стану або архіву подій, існують автоматичні процеси, які переміщують події зі статусу в архів. Життєвий цикл події визначається як всі способи додавання подій, їх переміщення та видалення з бази даних.

Наступна ілюстрація показує життєвий цикл події.

***Event life cycle***