Eseményalapú IT infrastruktúra felderítés

Önálló laboratórium feladat kiírása

Farkas Tamás (V9TI8U)
Konzulens: Szombath István
BME Méréstechnika és Információs Rendszerek Tanszék
Rendszertervezés ágazat, 2008/2009. II. félév

A nagyvállalati rendszerekben jobbára egységes eseménykezelő rendszereket használnak. Ezek feladata az érkező eseményekre a megfelelő akciók végrehajtása. Minden esemény információt hordoz a rendszer struktúrájáról, mely adott esetben frissebb lehet, mint az informatikai infrastruktúráról tárolt rendszermodell. A félév során a feladatom ezeknek az eseményeknek és kezelésüknek a megismerése, valamint egy tesztrendszeren kipróbálása.

A félév első felében irodalomkutatással foglalkoztam, megismertem a konfigurációkezelés alapjait, az ITIL ajánlásait a CMDB alkalmazására, valamint a CIM szabványban leírt sémákat. Létrehoztam egy a CIM szabványban lévő konfiguráció modellel kompatibilis, azonban célirányosan egyszerűsített infrastruktúra metamodellt. A metamodell főleg hálózati eszközök és számítógépek kapcsolatát, valamint az ezeken futó szoftverek, operációs rendszerek és ezek függőségeinek kapcsolatát jeleníti meg.

Ezután az eseménykezeléssel foglalkoztam, hogyan lehet a beérkező eseményekből a modellt felépíteni. Az új események alapján a már meglévő modellt inkrementálisan építem tovább, nem kell mindig elölről kezdeni, mint egy felderítési folyamat esetén. Az általam használt események mintájául a Cisco Netflow rekordok szolgáltak. Az események feldolgozása érkezési sorrendben történik, feldolgozáskor két kérdést kell megválaszolni, hogy az üzenetben lévő elemeket tartalmazza-e már a modellünk és, hogy az esemény alapján kell-e még tartalmaznia továbbra is. A beérkező esemény mindig tartalmazza a modellelem valamilyen azonosítóját (általában IP cím, vagy alkalmazásnál a neve), ami alapján a tartalmazás könnyen eldönthető. A második kérdésre a válasz az eseményből jön, majd a két válasz birtokában eldönthető, hogy létrehozni, módosítani, vagy törölni kell a modellből az azonosított elemet.

A következő részben ismerkedtem az Eclipse Modeling Framework-kel (EMF), létrehoztam a modellem Ecore reprezentációját. Az Ecore modellből ezután generáltattam egy editor plug-in-t Eclipse alá. A későbbiekben ezt kiegészítettem egy eseményeket fogadó (jelenleg socket kommunikációt használó), és feldolgozó osztállyal. A kapott szöveges esemény feldolgozása után azt, hogy résztvevő elemeket tartalmazza-e már a modellünk az EMF Query plug-in használatával, SQL-szerű lekérdezésekkel döntöm el. A létrehozást, törlést és módosítást az EMF Edit API Command-jai segítségével oldottam meg. Az esemény-feldolgozó szál a háttérben fut, a modellben elvégzett változtatások az EMF Editor nézetén azonnal megjelennek.

A félév végén az elkészített infrastruktúra-modell változásainak követésével foglalkoztam. Létrehoztam egy metamodellt, ami a változásokat, és azok típusát tárolja (ún. trace modell). Minden változáshoz eltárol egy időbélyeget, és a változott elem azonosítóját, mint hivatkozást az eredeti modellelemre. A változások eltárolását kezdetben manuálisan oldottam meg, ez később még automatizálható lesz, EMF Resource Notifier-ek segítségével.

Ezt a trace modellt arra szeretném majd a későbbiekben felhasználni, hogy konfigurációs elemekről olyan információkat nyerjek ki a tárolt modellből, amikhez egyébként aktív hozzáférésre volna szükség az adott eszközökhöz. Ennek a megvalósítására a következő félévben kerül sor.