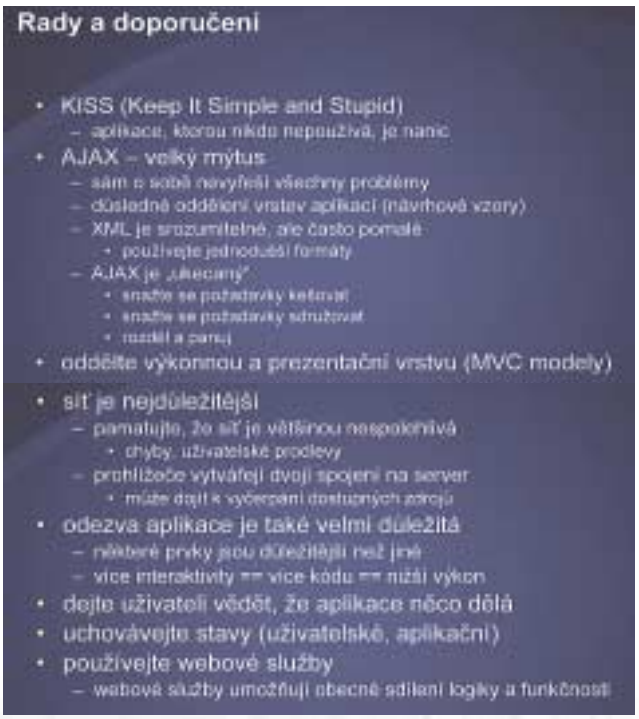


Web ADF vytvářet i vlastní. Takto vytvořené komponenty pak lze snadno integrovat do webových aplikací.

Na závěr je třeba dodat, že vývojové prostředí ArcGIS Server ADF je i ve verzi pro mobilní zařízení. Jedná se o Mobile ADF, které poskytuje mobilní ovládací prvky usnadňující vývoj aplikací pro mobilní zařízení, jakými jsou např. PocketPC a Smartphone.

ArcGIS Server 9.2 představuje komplexní GIS serverové řešení pro různě velké organizace. Služby, které ArcGIS Server poskytuje, mají funkcionalitu srovnatelnou s produkty ArcGIS Desktop a lze je využívat v nejrozličnějších typech klientů – od lehkých webových aplikací přes mobilní aplikace až po desktopová řešení.

ArcGIS Server nabízí vývojové prostředí (ADF), které umožňuje vyvíjet vlastní aplikace využívající GIS služeb. Pomocí nástrojů vývojového prostředí ArcGIS Server ADF lze GIS služby integrovat do stávající informační infrastruktury podniku. ArcGIS Server tak představuje jednotnou a otevřenou serverovou platformu ESRI.

Mgr. Matej Vrtich, ARCDATA PRAHA, s.r.o.

David Ondřich

ArcIMS a bezpečnost

Část druhá.

Ve druhém pokračování seriálu, které bude více technicky zaměřené než první část, se ještě jednou podrobně zaměříme na architekturu ArcIMS a popíšeme si pro a proti různých konfigurací jednotlivých komponent. Podíváme se také na problematiku komunikačních protokolů, síťových portů a sledování probíhajícího provozu. Úvodem připomeňme, co jsme si v minulém dílu připravili pro povídání o bezpečnosti. ArcIMS je z pohledu tohoto seriálu složeno z pěti vrstev, z nichž každá pracuje nezávisle na ostatních a komunikuje s nimi prostřednictvím standardních síťových protokolů známým jazykem (ArcXML) a jedním směrem předává ke zpracování klientský požadavek (v našem schématu směrem shora dolů) a opačným směrem předává odpověď na tento požadavek. Těchto pět vrstev je 1) webový server, 2) (servlet) konektor, 3) aplikační server (AS), 4) výkonná vrstva (Spatial Server, SpS) a 5) datové zdroje.

Sborka, rozborka

Ještě než se pustíme do uvažování, jaké rozmístění komponent je z hlediska bezpečnosti nejvhodnější, je na místě připomenout důležitou zásadu uvedenou v prvním dílu: obecné nejlepší řešení neexistuje. Vždy je třeba brát v úvahu souvislosti, které s ArcIMS nemají přímou spojitost, např. strukturu sítě, požadavky na intranetovou bezpečnost, umístění dat, ale i věci, které se ArcIMS přímo týkají, např. struktura dat, povaha předpokládaných klientů nebo očekávané zatížení a využití serveru.

Je možné uvažovat různá rozmístění komponent, říkejme jim v tomto článku scénáře, právě podle základních charakteristik, které jsou ArcIMS serveru „vtištěny“ povahou okolí nebo dat. Obvykle se uvažují scénáře podle rozmístění jednotlivých vrstev ArcIMS (architektura sítě, bezpečnost dat), podle umístění datových zdrojů (bezpečnost dat, sdílení dat v rámci organizace) nebo podle typů klientů (internetoví uživatelé, pokročilí uživatelé s desktopovým GIS klientem). V tomto dílu seriálu se zaměříme hlavně na scénáře prvního typu, tedy podle rozmístění vrstev ArcIMS, na druhé dva typy scénářů se dostane v dílu příštím.

Ačkoliv jsem v prvním dílu zmínil, že není bezpodmínečně nutné použít pro ArcIMS dedikovaný server, na kterém neběží žádné jiné služby ani úlohy, budeme pro další úvahy v tomto dílu brát tuto zásadu jako splněnou (s drobnou výjimkou popsanou níže).

Kam s ním?

Poslední věc, kterou je třeba určit, aby popis jednotlivých scénářů dával smysl, jsou základní předpoklady, které budou pro všechny popisované varianty shodné. Vezměme typickou situaci, která se předpokládá u budovaného ArcIMS: organizace chce ArcIMS použít k publikování mapových služeb prostřednictvím Internetu (ať už zcela veřejnému, nebo omezenému), zároveň chce ovšem část služeb poskytovat pouze svým zaměstnancům v rámci intranetu. Předpokládáme tedy, že existuje nějaká veřejná síť (Internet), která je od neveřejné vnitřní sítě oddělena demilitarizovanou zónou (DMZ). Podrobnosti schématu sítí, DMZ, ani dalšího uspořádání jednotlivých síťových „prostorů“ nejsou v tuto chvíli důležité, pokud pro některý scénář bude některá z vlastností důležitá, neopomenu to zdůraznit. Pod pojmem DMZ si představme jakékoliv uspořádání, které umožňuje, aby ArcIMS byl přístupný jak z vnější, tak z vnitřní sítě. Pod pojmem firewall se dále rozumí aktivní síťový prvek, který slouží k oddělování provozu mezi jednotlivými sítěmi a blokuje nežádoucí požadavky. V následujících odstavcích se podíváme na možné scénáře podle počtu vrstev ArcIMS, které budou umístěné v rámci DMZ, u ostatních vrstev se předpokládá umístění na jiném serveru (jiných serverech) ve vnitřní síti.

All Inclusive

Nejjednodušším scénářem je kompletní instalace všech vrstev ArcIMS na jednom serveru. Ačkoliv se na první pohled zdá, že s bezpečností toto uspořádání nemá nic společného, pravý opak může být pravdou. Velmi záleží na tom, jak osamocený ve skutečnosti server v DMZ je a jaké povahy jsou (mají být) poskytovaná data.

Na exponovaném serveru zůstávají všechny vrstvy 1–5.

Pro:

- minimální komunikace mezi ArcIMS a vnitřní sítí, tedy minimální riziko průlomu do vnitřní sítě po napadení ArcIMS;
- jednoduchost instalace, možnost snadné a rychlé reinstalace v případě bezpečnostního incidentu nebo selhání serveru;
- možnost použít standardizovaný server;
- možnost omezit komunikaci na serveru na jeden jediný otevřený port.

Proti:

- obtížná správa serveru (pravidelné záplaty), monitorování, aktualizace dat;
- nízká kontrola nad daty (zejména pokud jde o jejich zneužití);
- nízký výkon (buď je nutné mít data v souborovém systému, nebo na stejném hardwaru provozovat ještě [geo]databázi) v případě většího objemu dat.

Zatímco nevýhody tohoto scénáře jsou na první pohled patrné, výhody úplně zřejmé být nemusí. Pro situaci, kdy je třeba poskytovat víceméně statická data (která se aktualizují s periodou větší než rok), není jich mnoho a nikdo ze správců sítě nebo GIS odborníků nemá příliš času, aby se o ArcIMS mohl starat, se jedná o téměř ideální řešení. Možnost vytvořit obraz hotové instalace, který se dá v případě potřeby rychle a snadno nahrát místo poškozeného ArcIMS, může být také velké plus.

Naopak se tento scénář vůbec nehodí, pokud je třeba systém vyladit na vysoký výkon, je třeba monitorovat chování uživatelů, datové zdroje se často aktualizují, nebo je dat velké množství na to, aby se dala umístit do souborového systému. Instalace (geo)databáze na stejný server sice je částečné řešení, ale jednak snižuje výkon celého systému, jednak se tím otevírá další potenciální skulina k napadení. Další nevýhodou je, že jediný způsob škálování (většinou tedy zvýšení výkonu) je možný pouze použitím výkonnějšího hardwaru (zato však postačí výměna jednoho serveru).

Data uvnitř

Pokud scénář poněkud pozměníme v tom smyslu, že skutečné vrstvy ArcIMS ponecháme v DMZ a do vnitřní sítě přesuneme nejnižší vrstvu, tedy samotná data, snížíme sice poněkud bezpečnost celého systému, ale můžeme zvýšit bezpečnost dat.

Na exponovaném serveru zůstávají vrstvy 1–4.

Pro:

- snadná instalace ArcIMS (zůstává shodná s předchozím scénářem);
- možnost větší kontroly nad daty, snadnější správa dat, možnost pravidelných aktualizací i využití sdílení dat;
- možnost použít standardizovaný server;
- snadná škálovatelnost datových zdrojů.

Proti:

- je nutné otevřít kanál mezi DMZ a vnitřní sítí, tzn. zvyšuje se riziko průlomu do vnitřní sítě (viz dále);
- výkon samotného ArcIMS zůstává obtížně škálovatelný;
- potřeba dalšího serveru pro poskytování dat;
- stejně tak správa ArcIMS, instalace záplat a oprav se musí provádět ručně.

Nejslabším místem tohoto scénáře je bezesporu otevření komunikace mezi DMZ a vnitřní sítí. Datovým zdrojem pro ArcIMS

mohou být jednak data umístěná v distribuovaném souborovém systému, jednak data umístěná v (geo)databázi. Zatímco pro popsaný scénář je možné doporučit druhý uvedený způsob, první doporučuji použít jen v krajním případě, kdy opravdu není jiná možnost. Síťové souborové systémy (pro Microsoft Windows se používá tzv. CFS [Common File System], známý jako sdílení disků, pro UNIXové operační systémy je obvyklý NFS [Network File System]) jsou známé svou nízkou spolehlivostí vůči bezpečnostním útokům (např. i při použití zabezpečených variant je možné, že se po síti posílají nezašifrovaná hesla). Toto riziko lze částečně omezit vhodným nastavením komunikačních pravidel mezi DMZ a vnitřní sítí a DMZ a vnější sítí, nicméně distribuovaný síťový systém se poměrně špatně monitoruje, pro některé situace je dokonce nemožné určit, na kterých portech spolu budou obě strany komunikovat. Když už není možné použít jinou variantu, snažte se použít nejmodernější a co možná nejvíce zabezpečený síťový souborový systém.

Je také možné data umístit na speciální server, který bude umístěn také v DMZ (dokonce může být i ve své vlastní), ArcIMS k němu pak přistupuje prostřednictvím firewallu stejně jako by data byla ve vnitřní síti, ale v případě průlomu do datového serveru se útočník nedostane do vnitřní sítě. Uživatelé z vnitřní sítě k datům také přistupují prostřednictvím firewallu. Tím je možné bezpečnost vnitřní sítě opět zvýšit.

Naopak velkou výhodou přesunutí datových zdrojů mimo ArcIMS (ať už do vnitřní sítě nebo jen na jiný server v DMZ), je oddělení ostatních vrstev od dat. To má důsledky jednak výkonnostní (datový server se může škálovat nezávisle na samotném ArcIMS), jednak bezpečnostní (datovou vrstvu je možné zdvojit, nebo vytvořit záložní server, který se spustí v okamžiku výpadku).

Zaměřeno na výkon

Při postupném přesunování jednotlivých vrstev ArcIMS do vnitřní sítě (nebo do vlastní oddělené DMZ) se nezastavíme pouze u výkonné vrstvy, ale posoudíme současně dva případy, kdy z exponovaného serveru odsuneme a) výkonnou vrstvu (SpS) a b) SpS a aplikační server (AS).

Rozdíl v obou případech není velký, abychom si jej trochu osvětlili, připomeňme si, co vlastně AS dělá: jedná se o „manažera“, který rozděluje práci jednotlivým výkonným jednotkám a který se stará o odevzdání výsledků jejich práce. Pokud do vnitřní sítě umístíme pouze výkonné jednotky a AS ponecháme v DMZ, je nutné pro každý SpS ve firewallu nastavit pravidla komunikace mezi DMZ a vnitřní sítí. Naproti tomu při přesunutí AS mimo DMZ stačí definovat tato pravidla pouze pro jeden kanál (za předpokladu, že AS je pouze jeden). Tato varianta je obecně vhodnější, proto dále budeme uvažovat právě ji.

Na exponovaném serveru zůstávají vrstvy 1, 2 a volitelně 3.

Pro:

- možnost velké kontroly chování prakticky celého ArcIMS (monitorování, ladění výkonu atd.) ve vnitřní síti;
- nižší nároky na hardware exponovaného serveru;
- možnost vytvořit vlastní konektor.

Proti:

- nutnost správy oddělených komponent (vyšší nároky na správce, více potenciálních problémů);
- při rozdělení komponent mohou být zvýšené licenční nároky na ArcIMS;
- nutnost investice do dalšího hardwaru;
- nutnost komunikace mezi AS a konektorem (předávání výstupů), otevřený kanál mezi DMZ a vnitřní sítí.

Obrovskou slabinou tohoto uspořádání, která není na první pohled patrná, je nutnost propojení SpS s webovým serverem. Jedná se o chybu v návrhu architektury ArcIMS, která u většiny scénářů nevadí, ovšem v tomto případě vyžaduje poněkud nesmyslné otevření spojení mezi vrstvou 4 a vrstvou 1. Když totiž SpS vygeneruje mapový výstup, který typicky uloží do obrázku na harddisku do určeného *output* adresáře, jediný způsob, kterým se k němu může webový server dostat, je prostřednictvím síťového souborového systému (viz výše). To samozřejmě představuje velké bezpečnostní riziko, které ovšem může být vyváženo přínosy tohoto scénáře.

V obou modelech situace se totiž jedná o výrazné zvýšení škálovatelnosti celého systému, které souvisí s prostým rozdělením jednotlivých vrstev ArcIMS. Je naprosto logické, že čím rozprostřenější systém je, tím jednodušší je nahradit kteroukoliv z jeho vrstev výkonnější variantou. Tento postřeh je možné uplatnit na všechny scénáře.

Přesunutí AS a výkonné vrstvy mimo exponovaný server dovoluje kontrolovat skutečnou práci ArcIMS v mnohem větší míře, na serveru v DMZ zůstává pouze samotný konektor (a případně webová aplikace postavená nad konektorem). Při použití vlastního naprogramovaného konektoru (např. Java, .NET ad.) je možné implementovat velmi snadno další bezpečnostní mechanizmy, stejně tak je možné snadno filtrovat provoz mezi exponovaným serverem a AS (znovu připomínám, že komunikace probíhá v nešifrované podobě v jazyce ArcXML).

Úměrně možnostem, které tato dvě uspořádání poskytují, ovšem také vzrůstá prostor ke vzniku problémů nejrůznějšího druhu, od komunikačních potíží na úrovni síťových protokolů, po velmi obtížné ladění maximálního výkonu takového systému. Také řešení kritických situací vyžaduje dobrou znalost ArcIMS a síťových technologií, proto tyto scénáře lze doporučit pouze tam, kde správce serveru a systémový administrátor mají dostatek zkušeností jak s ArcIMS, tak s distribuovanými systémy.

Když jde hlavně o web

Hlavní nevýhodu předchozího scénáře je možné odstranit, pokud mimo exponovaný server přesuneme také vrstvu 2 a webový server zdvojíme tak, že na exponovaném serveru z něj vytvoříme tzv. transparentní proxy server. Jeho úloha spočívá v jakémsi maskování skutečného stavu věcí, neboť funguje jako normální

webový server, pouze místo toho, aby příchozí požadavek sám vyřídil, přepošle jej jinému webovému serveru, od něhož pak převezme odpověď a vrátí ji klientovi, jako by to byla jeho vlastní odpověď. Pokud je proxy server správně nakonfigurován, klient nemá možnost zjistit, že ve skutečnosti komunikuje s proxy serverem a ne přímo s ArcIMS. ArcIMS pak může být umístěn úplně kdekoliv a na proxy serveru je zcela nezávislý.

Na exponovaném serveru nezůstává žádná z vrstev, resp. speciální varianta 1. vrstvy.

Pro:

- celý ArcIMS ve vnitřní síti (snadný monitoring, ladění, správa, přístup do vlastních databází atd.);
- snadná kontrola provozu mezi proxy serverem a ArcIMS (filtrování);
- nejvyšší zabezpečení dat;
- velmi snadné škálování ArcIMS i datových zdrojů (vše nezávislé na exponovaném serveru);
- minimální hardwarové nároky na proxy server, možnost provozovat proxy jako službu existujícího webového serveru (minimální zátěž);
- hardwarová náročnost úměrná požadovanému výkonu ArcIMS.

Proti:

- nutno otevřít kanál mezi DMZ a vnitřní sítí (ovšem v tomto případě pouze na jednom portu);
- nutnost správy proxy serveru, ať už v rámci existujícího webového serveru nebo samostatně;
- proxy server poněkud zpomaluje provoz.

Výhody tohoto scénáře jsou poměrně dobře patrné a sahají od úplné kontroly ArcIMS ve vnitřní síti přes prakticky neomezenou škálovatelnost ArcIMS nezávisle na exponovaném serveru až po nejvyšší dosažitelnou míru zabezpečení dat. Velkým přínosem také může být možnost odladění systému ve vnitřní síti a teprve následné zveřejnění. Jednoduchost komunikace mezi proxy serverem a skutečnou 1. vrstvou ArcIMS navíc umožňuje implementovat další mechanizmy nebo filtrování na úrovni firewallu mezi DMZ a vnitřní sítí. Možnosti rozšíření tohoto scénáře jsou velmi velké a záleží hlavně na potřebách a schopnostech tvůrců systému, jak bude výsledné uspořádání vypadat.

Nevýhod tohoto uspořádání je poměrně málo nebo nejsou příliš velké. Jediná vážná námitka se týká zpomalování komunikace mezi klientem a ArcIMS, která je oprávněná a byť je možné zpomalování minimalizovat vhodným nastavením síťových prvků, zcela odstranit je možné není. Scénář se proto nehodí v situaci, kdy se předpokládá, že vytížení ArcIMS bude velké, nebo např. při předpokládaném velkém přenosu dat prostřednictvím nadstavby Data Delivery.

Závěrem přehledu scénářů znovu připomínám, že neexistuje univerzální řešení, které by bylo vhodné pro jakoukoliv situaci. Ačkoliv se z prostého popisu může zdát, že poslední uvedený scénář je pro většinu obvyklých požadavků na uspořádání nejlepší, nemusí to být pravda.

Díry, škvíry, dvířka, dveře a vrata

Dále se v tomto díle podíváme na přehled používaných portů a komunikačních protokolů, které jednotlivé vrstvy ArcIMS používají ke komunikaci mezi sebou. Opět to vezmeme popořádku, tak jak požadavek prochází jednotlivými vrstvami. Opět je třeba něco předpokládat, neboť není možné vyjmenovat všechny myslitelné požadavky a všechny typy možných odpovědí na ně. Tentokrát předpokládejme, že na ArcIMS vyšleme požadavek od standardního (dejme tomu) HTML klienta ArcIMS (nebo ekvivalentní požadavek např. od aplikace ArcMap), na který ArcIMS odpoví vygenerováním obrázku s mapou a odesláním odpovědi, která obsahuje URL, na níž bude vygenerovaný soubor s obrázkem dostupný.

1. klient ➡ webový server

Klient se připojí na port webového serveru (standardní port pro HTTP protokol má číslo 80, ale webový server může obecně naslouchat na kterémkoliv portu) a požadavkem typu POST odešle požadavek obsahující ArcXML, ve kterém jsou určeny rozměry požadovaného obrázku, název služby, rozsah zobrazeného území, zobrazené vrstvy, případně způsob jejich vykreslení.

Je-li webový server v DMZ (což bylo splněno ve všech uvedených scénářích), je potřeba povolit na firewallu přístup z vnější sítě na port 80 exponovaného serveru (nebo odpovídající port, na kterém webový server naslouchá).

2. webový server ➡ (servlet) konektor

Webový server z konfiguračních souborů a z URL předaného požadavku pozná, že má požadavek předat konektoru, který zpravidla běží jako servlet nebo jako služba nějakého kontejneru nebo skriptovacího jazyka. Detaily v tomto případě záleží na konkrétním použitém konektoru a jeho konfiguraci, ale pro nejpoužívanější (výchozí) servlet konektor běžící v rámci kontejneru Apache Tomcat se jedná o port 8009 (i to je možné v konfiguračním souboru `$TOMCAT/conf/server.xml` změnit).

Webový server a kontejner s konektorem zpravidla běží na jednom serveru, obvykle není nutné v DMZ nastavovat speciální pravidla (připojení serveru na sebe sama na jiném portu je obvykle povolené), nicméně pokud je potřeba oddělit i tyto dvě vrstvy, je nutné povolit připojení na port 8009 (nebo ekvivalentní) serveru s konektorem ze serveru s webovým serverem (zdrojový port obvykle přidělí operační systém jako první volný).

3. konektor ➡ aplikační server

Konektor se stará o posouzení vlastností požadavku – např. autentizace, kontrola přítomnosti zakázaných direktiv ArcXML, rozlišení obrázků, požadovaný rozsah dat, typ požadavku apod., což jsou všechno záležitosti, které je možné upravit příslušnou konfigurací konektoru (případně jeho naprogramováním). Pokud požadavek projde touto vstupní kontrolou a pokud konektor neumí požadavek vyřídit sám (např. zmíněnou autentizaci), připojí se na aplikační server ArcIMS.

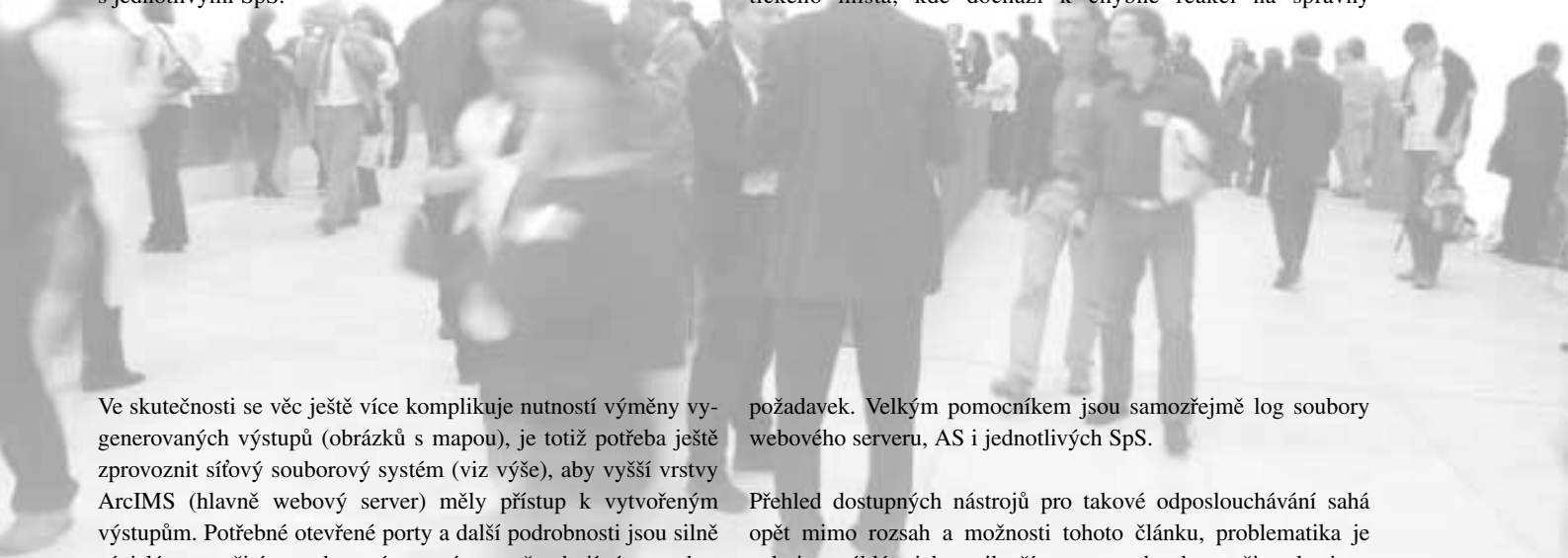
Aplikační server ve výchozí konfiguraci „poslouchá“ na portu 5300, tato hodnota se nastavuje v konfiguračním souboru `$AIMSHOME/Middleware/Application_Server/App`

`Server.properties` jako vlastnost `connectorPort`. Při přesunutí AS do vnitřní sítě je tedy potřeba povolit přístup na port 5300 (zdrojový port konektoru opět přiděluje operační systém exponovaného serveru).

4. aplikační server ➞ výkonná vrstva

V případě SpS je situace zkomplikovaná mezivrstvou, která se jmenuje ArcIMS Monitor a stará se právě o komunikaci mezi SpS a AS. Každý SpS má k dispozici „svůj" Monitor (jeden Monitor ale může sloužit pro více SpS běžících na stejném serveru), ke kterému se po spuštění připojí a ohlásí se mu. AS se nepřipojuje přímo k jednotlivým SpS, dokonce ani k jednotlivým Monitorům, ale naopak jednotlivé Monitory registrují „svoje" SpS pro použití s AS.

Monitor musí vědět, ke kterému AS a na jaký jeho port se má připojit, to se nastavuje v souboru `$AIMSHOME/Monitor/Monitor.properties` v klíčích `registryHost` a `registryPort` (výchozí hodnota portu je 5353). Monitor naopak naslouchá na portu určeném vlastností `listenerPort`, která má výchozí hodnotu 5050. Pokud je tedy AS v DMZ a SpS ve vnitřní síti, musí být možné se z vnitřní sítě připojit na port 5353 exponovaného serveru, zatímco z exponovaného serveru musí být otevřený kanál na port 5050 všech serverů s jednotlivými SpS.



Ve skutečnosti se věc ještě více komplikuje nutností výměny vygenerovaných výstupů (obrázků s mapou), je totiž potřeba ještě zprovoznit síťový souborový systém (viz výše), aby vyšší vrstvy ArcIMS (hlavně webový server) měly přístup k vytvořeným výstupům. Potřebné otevřené porty a další podrobnosti jsou silně závislé na použitém souborovém systému a přesahují rámec tohoto článku. Prostřednictvím vyhledávačů je možné na internetu najít řadu informací týkajících se této problematiky a tématu se věnuje i velká část odborné literatury z oblasti počítačových sítí.

5. výkonná vrstva ➞ data

Jednotlivé SpS se k datovým zdrojům připojují velmi rozdílně podle jejich povahy. Pokud jsou data umístěná v (geo)databázi, připojují se k databázi, pokud se používají data ze souborů, musejí být dostupná v rámci souborových systémů daného serveru (ať už lokálně nebo prostřednictvím sítí, viz výše).

Pro vcelku obvyklý případ, kdy data jsou umístěna v ArcSDE, platí jednoduché pravidlo: mezi serverem, kde běží SpS, a ArcSDE musí být povolena komunikace na port 5151 (nebo ekvivalentní, na kterém poslouchá ArcSDE). V případě použití jiné databáze je třeba povolit přístup na příslušný port, na kterém databáze komunikuje.

Pokud je požadavek správný a ArcIMS má k dispozici data, SpS vygeneruje výstupní obrázek, uloží ho do souboru a vytvoří odpověď v jazyce ArcXML, kterou vyšle AS, který ji předá konektoru a ten ji podle vlastností původního požadavku případně upraví (např. přidá HTML formulář pro HTML klienta) a dodá webovému serveru, který ji vrátí klientovi. Odpověď obsahuje URL obrázku s vytvořenou mapou, který si klient musí stáhnout samostatným HTTP požadavkem, který už vyřídí pouze webový server, zbytek ArcIMS se o samotné stažení hotového výstupu nijak nestará.

Když síť není záchranná

Protože se veškerá komunikace jednotlivých vrstev (až na samotné získávání dat) odehrává v jazyce ArcXML, je velmi snadné monitorovat výměnu informací mezi jednotlivými vrstvami ArcIMS. Je k tomu potřeba pouze nástroj pro odchytávání paketů, trpělivost a znalost vnitřních pochodů ArcIMS, z nichž ty důležité byly nastíněny výše. Při rozdělení jednotlivých vrstev je někdy takové „odposlouchávání" důležité pro určení problematického místa, kde dochází k chybné reakci na správný požadavek. Velkým pomocníkem jsou samozřejmě log soubory webového serveru, AS i jednotlivých SpS.

Přehled dostupných nástrojů pro takové odposlouchávání sahá opět mimo rozsah a možnosti tohoto článku, problematika je velmi rozsáhlá a jako nejlepší postup mohu doporučit pokusit se v okolí najít někoho, kdo počítačovým sítím rozumí a případný problém s ním konzultovat. Mnoho firem, které se sítěmi zabývají, také nabízí konzultační služby. Spolupráce s odborníkem se v tomto případě většinou vyplatí, protože ušetří spoustu času (a v důsledku peněz), byť se na první pohled může zdát drahá.

Pokračování

V příští části se budeme věnovat bezpečnosti dat, řízení přístupu k datům a podíváme se na některé scénáře z hlediska poskytování dat. Povíme si více o možnostech použití jiných konektorů, úpravách a programování a budeme se také věnovat popisu možných útoků, který se do tohoto dílu již nevešel.

Mgr. David Ondřich, ARCDATA PRAHA, s.r.o.