

1 Produktová řada Progress Actional

Produktová řada Progress Actional řeší úsporně, výkonně a na celopodnikové úrovni úlohy spojené se správou, řízením, bezpečností, reportingem a vizualizací heterogenní Servisně Orientované Architektury. Poskytují přehled o službách a podnikových procesech jak z provozního tak i podnikatelského hlediska.

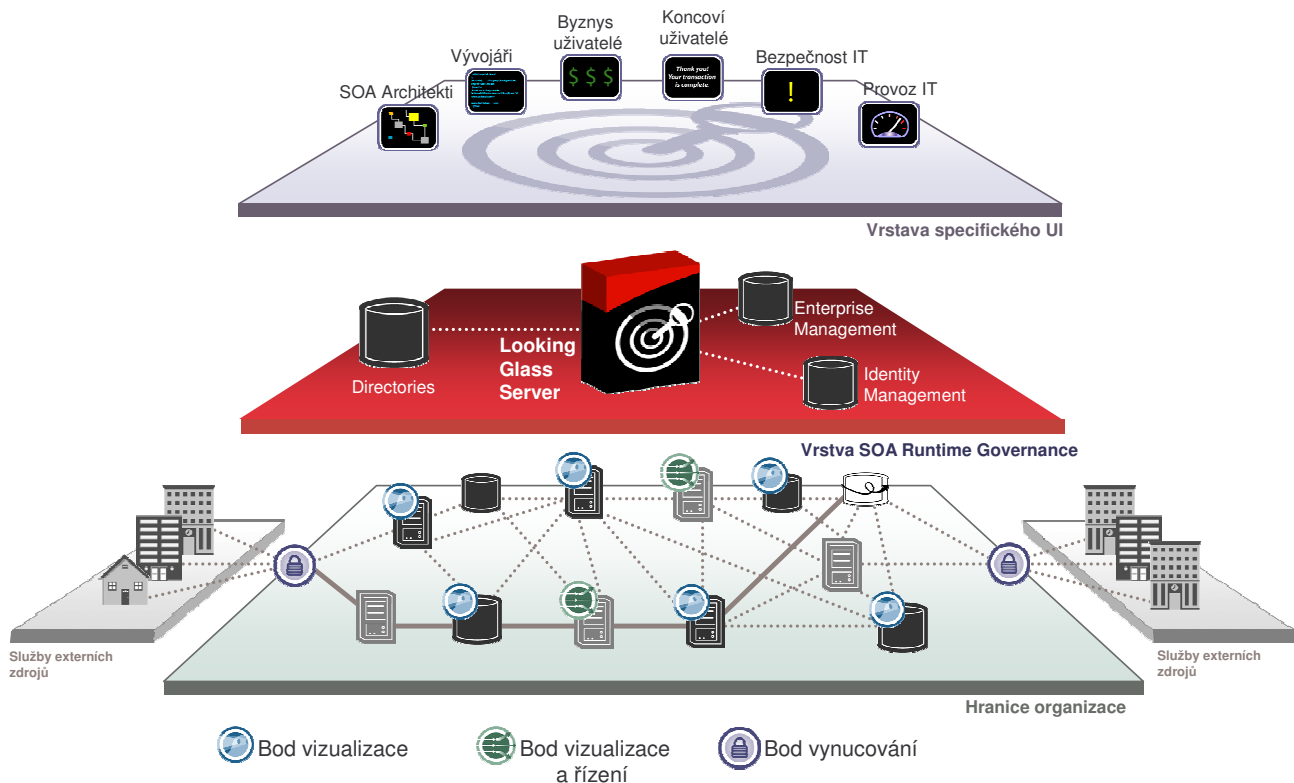
Správa a řízení služeb je založena na definovaných technických či obchodních politikách (SLA) bez nutnosti programování.

Uvádí výpočetní prostředí do souladu s politikami pro bezpečnost a do souladu s legislativou. Díky centralizovanému řízení s možností vytvoření SW klastru a možnosti konzistentního opakovaného použití politik snižuje rizika provozu SOA.

1.1 Produkty Progress Actional zahrnují:

- Actional Server
- Actional Agenty, kteří mohou vystupovat jako:
 - Bod vizualizace.
 - Bod řízení.
 - Bod aktivního vynucování politik.

Jak nastiňuje schéma níže, Actional hraje roli zastřešující vrstvy SOA jdoucí napříč celou organizací přes různé platformy, aplikace, middlewary nebo databáze.



1.1.1 Actional Server

Představuje serverovou aplikaci běžící na dodávaném vnořeném open-source aplikačním serveru (popř. běží i na omezené množině aplikačních serverů dostupných komerčně) s JMS (Java Message Service) nebo WS API (Web Service). Server v pravidelných intervalech přijímá data-zprávy od svých agentů, dává tyto zprávy do vzájemných souvislostí a agentům zpět rozepisuje politiky, na základě kterých jsou jednotlivé služby resp. celé uzly (nodes) řízeny.

Actional Server umožňuje:

- Spravovat, řídit, vizualizovat, monitorovat, reportovat a logovat SOA.
- Porozumět vzájemným závislostem a rozkrýt složitost sítě služeb, která se může v reálném čase dynamicky měnit.
- Rychle identifikovat a přesně lokalizovat příčiny vzniklých potíží a zamezit jejich dalšímu šíření sítě služeb.
- Předvídat a připravit se na možné dopady plánovaných změn.
- Nasazovat nové služby nebo jejich nové verze bez nutnosti služby odstavit.
- Vytvářet a aplikovat politiky na monitorování výkonnosti a vynucovat si SLA (Service Level Agreements).

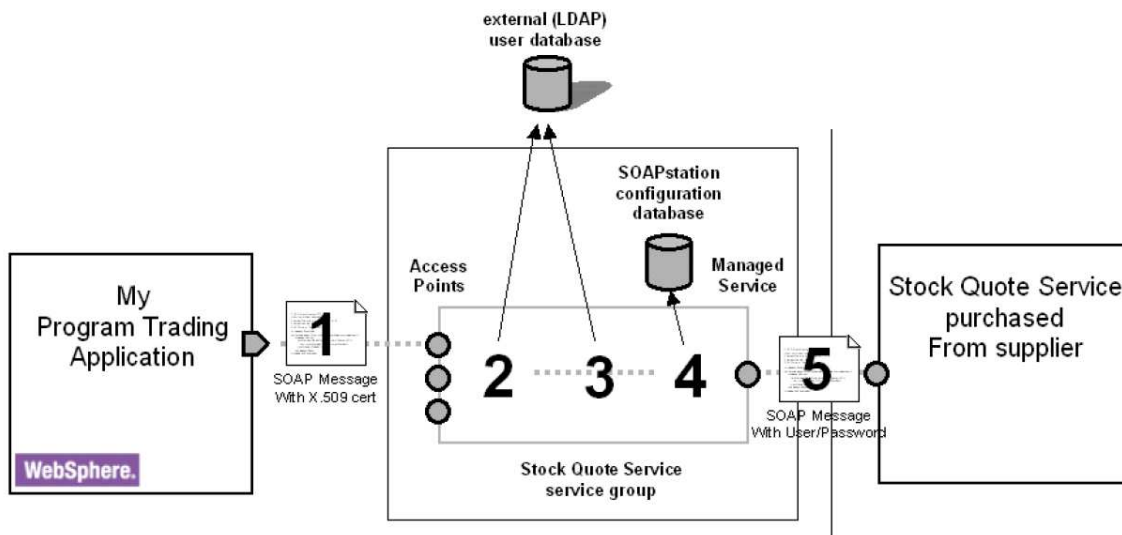
1.1.2 Actional agent

Actional agent je SW komponenta běžící nepřetržitě na každém HW uzlu, který provozuje aplikační služby (WS, JMS a další). Agent detekuje veškerý provoz, informace o něm zaznamenává do svého bufferu a v pravidelných intervalech odesílá tyto informace Actional serveru. Agent dále shromažďuje potřebné provozní statistiky, které vyhodnocuje proti definovaným politikám. Na základě vyhodnocení těchto statistik se různými kanály (eMail, log, SMS, SNMP a další) aktivuje okamžitě systém včasného upozorňování nebo varování.

Actional agent je zcela neinvazivní a neviditelný vůči dané SW platformě (aplikaci), kde běží a jejíž služby spravuje, vizualizuje, řídí a monitoruje.

1.1.3 Actional Intermediary

Actional Intermediary je bod řízení a aktivního vynucování politik, který umožňuje a zjednodušuje distribuci a zabezpečení webových služeb široké škále konzumentů. Intermediary funguje jako proxy pro webové služby, řídící interakci mezi aplikací, která poskytuje webové služby a jejich uživateli. Pomocí Intermediary se uplatňují a provádějí politiky a SLA, které jsou definovány v Actional Server konzoly.



Klíčovou úlohou Actional Intermediary je zajištění bezpečnosti mimo aplikaci, která poskytuje webové služby.

K dispozici je široká škála bezpečnostních mechanismů:

- Podepisování, šifrování a validace požadavků a odpovědí (3-DES, DES, AES128/192/256, RSA, DSA, SHA-1, MD-5 a další)
- Autentikace
 - Uživatelské jméno/Heslo
 - X509 certifikáty
 - SAML
- Autorizace uživatelů webové služby založená na rolích
- Předávání autentikačních údajů dále k poskytovateli webové služby
- Spolehlivé doručení požadavků a odpovědí (podpora standardu WS-ReliableMessaging)
- WS-Security, WS-Policy a WS-SecurityPolicy

1.1.3.1 SAML

SAML (Security Assertion Markup Language) je standard vydaný a organizací OASIS (Organization for the Advancement of Structured Information Standards).

Actional Intermediary může fungovat v těchto režimech:

- Jako poskytovatel SAML služby, která je provozována externím subjektem(např. Oracle Identity manager)
- Jako vestavěný (built-in) SAML server (SAML Identity Provider), což je kompletní řešení pro zákazníky, kteří nedisponují SAML službou určené pro rychlé nenáročné implementace.

Typický scénář SAML autorizace může například probíhat takto:

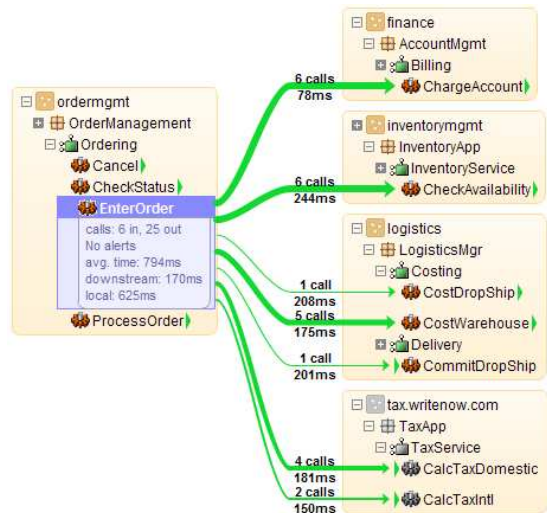
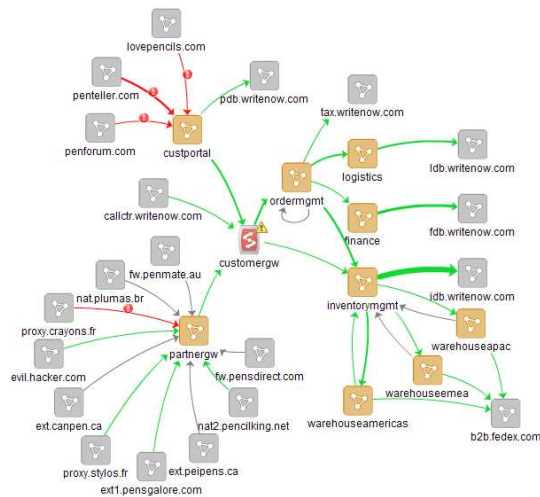
1. WS Konzument se autentikuje voláním SAML služby
2. V případě úspěchu je mu přidělen SAML token
3. WS konzument volá příslušnou službu s aplikační logikou. K požadavku přikládá SAML token, který získal v krocích 1 a 2.
4. Actional Intermediary ověří token a předává ho i s požadavkem poskytovateli příslušné webové služby.
5. Poskytovatel webové služby ověří token, zpracuje požadavek a zasílá zpět odpověď.

1.2 Terminologie

Actional Server používá následující NGSO termíny pro jednotlivé infrastrukturní komponenty-vrstvy sítě služeb. V této NGSO struktuře je pak možné v reálném čase sledovat stav vaší SOA:

- **Node.** Typický HW server-uzel reprezentující aplikační server případně jejich klastr. Node může být dále ESB nebo i webový server (např. Tomcat).
- **Group.** Příslušná aplikace, která je předmětem governance. V případě bodu vynucování je to skupina těchto agentů.
- **Services.** Příslušná sada webových služeb.
- **Operations.** Příslušná sada operací (metod), které služba/služby vystavují.

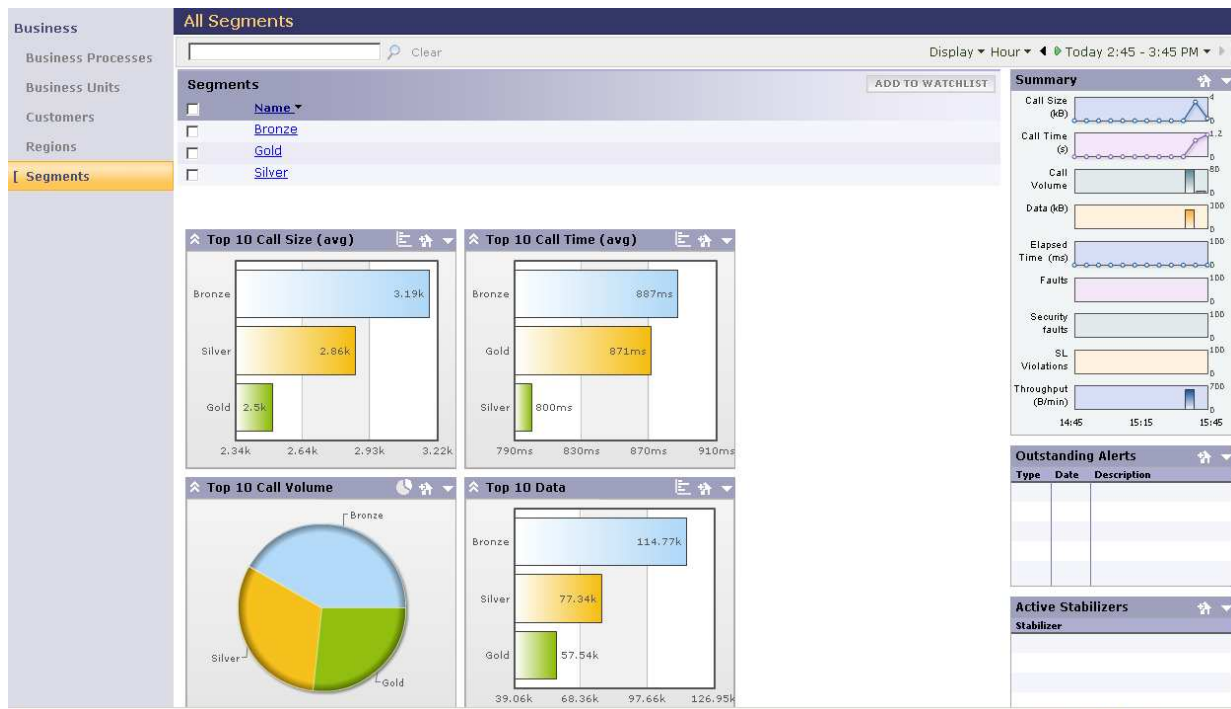
Node, kde je agent instalovaný je označen jako řízený (managed). Actional server však umožňuje řídit i nody, kde agent instalovaný není (unmanaged nodes) využitím dohledové komponenty (watchdog). Tato komponenta se typicky používá v případech, kdy pro dohled postačuje informace systém běží/neběží resp. systém komunikuje/nekommunikuje s okolím.



Příklad celkového pohledu přes jednotlivé uzly na komunikaci služeb. Tento i ostatní grafy zobrazující komunikaci vznikají zcela automaticky využitím funkce autodiscovery. Zobrazována je tak reálná skutečnost a ne její návrh nebo představa, jak by skutečnost vypadat měla.

Detailní pohled na operaci „EnterOrder“. Autodiscovery funguje i zde. Zobrazeny jsou automaticky rozpoznané služby a jejich operace se znázorněním dalšího směru volání. Posouváním se po příslušné lince volání lze takto traversovat kompletní kolečko volání od konzumenta přes všechny následné služby a zpět.

Kromě těchto infrastrukturních nabízí Actional možnost definice řady byznys pohledů a statistik této komunikace včetně podmožiny uzlů, na kterých probíhá příslušný byznys proces. Obrázek níže nastiňuje možnost pohledu a byznys i IT statistik dle rozdělení zákazníků do tří kategorií dle objemu jejich objednávek (Zlatí, Stříbrní, Bronzoví). Grafy mohou být tabulkové, sloupcové či koláčové. Každé okno s těmito grafy je implementováno jako portlet s unikátním URL. Je tedy velice snadné integrovat tyto pohledy do vašeho stávajícího intranetu.

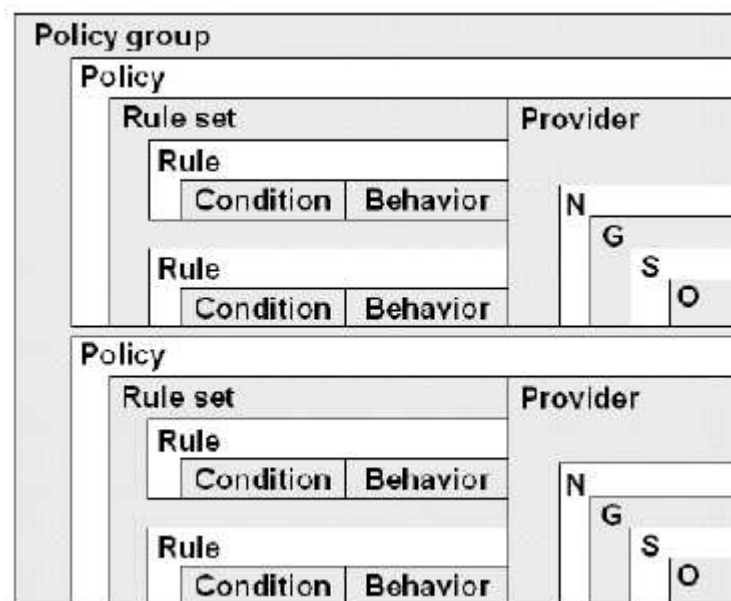


1.3 Politiky

Politiky – jejich centrální definice na Actional Serveru, decentralizované nasazení a vyhodnocování agenty – představují stěžejní funkcionalitu SOA Runtime Governance.

Politiky představují množinu pravidel (obchodních či IT), které Actional server může uplatnit vůči NGSO struktuře včetně identifikovaných byznys procesů. V rámci různých kombinací je jedna politika opakovatelně v NGSO použitelná nebo naopak jednu politiku lze uplatnit i napříč celou NGSO strukturou např. pro určitou skupinu uzlů.

Aby se politika stala použitelná, je nutné ji začlenit do hierarchicky strukturovaného úložiště politik jak nastiňuje schéma níže:



Při vyhodnocování politik se používá dvoustupňový resp. dvouprahový systém upozorňování. Po překročení první prahové hodnoty dojde pouze k varování, při překročení druhé prahové hodnoty již dojde k alarmu. Tento způsob vyhodnocování umožňuje předcházet nežádoucím jevům.

Vyhodnocení určité podmínky politiky bývá zpravidla i důležitou informací pro samotnou aplikaci vystavující dané služby. Actional dokáže tuto zpětnou vazbu této aplikaci doručit pomocí tzv. stabilizátorů a jejich zdokumentovaného API. Stabilizátor může nabývat boolean hodnot (true/false) – podmínka nastala/nenastala.

***** Konec tohoto dokumentu *****