Motion10

API Management Solutions

The Microsoft Way

Inhoud

Introduction

API Management solutions are not a new phenomenon, but over the recent years they have broadened their scope and become more sophisticated. From the outset API Management solutions were created to expose internal web services to external partners and customers through basic HTTP(s).

Nowadays API Management solutions meet on premise integration requirements as well. In this article I will focus on the two API Management solutions available on the Microsoft platform: Nevatech Sentinet and Azure API Management.

API Management solutions defined

API Management is bit of a fuzzy term, so let's start off by contrasting API Management with something we know: the Enterprise Service Bus or BizTalk Server if we talk Microsoft. Some vendors claim that API Management solutions can be used as a light-weight ESB. Actually that's not the case. ESBs are true message oriented middleware, whereas API Management solutions are merely an extra virtual service layer around existing business services. API Management solutions provide what we call plumbing functionality, that is: security, monitoring, routing and policy enforcement. As a result service developers can focus on providing business functionality, operators can do real-time monitoring and managers can manage service level agreements. And there's a second important characteristic. Virtual services are said to be non-intrusive. That means security, monitoring, routing and policy enforcement can be added to business services, without changing these business services.

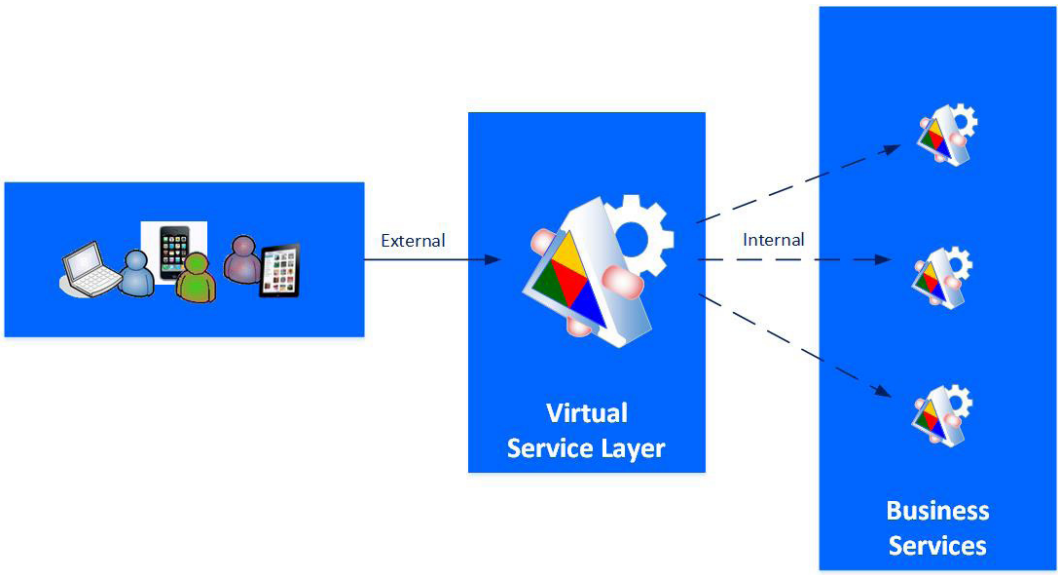

Figure 1
The service virtualization pattern.

Another angle to look at it, is the primary functionality of the two products. ESBs were originally designed to connect internal applications within the context of a service oriented architecture. That's very different for API Management solutions. They were not designed with external integration and mobile computing in mind. To be a bit more specific, API Management solutions have the following typical usage scenarios:

- Exposing corporate data and services. API Management solutions can be used to give customers, business partners and mobile employees access to corporate data and services. Of course we can already achieve this today, but with API Management we can do it in a secure way without inducing performance degradation of the exposed backend systems.

- Using SaaS services. A company cannot only expose its data and services, it also works the other way around. Companies are making more and more use of SaaS services. That sounds easy, but brings a lot of new challenges. What you need to avoid is spaghetti integration and an unmanageable application landscape. That's exactly what API Management brings to the table. Governance, but also the ability to intercept outgoing calls and add client credentials, hashing or a message signature.

- Enabling mobile access. Mobile devices are overtaking PCs as the most broadly used devices to access corporate data. Think of a homecare organization with a mobile workforce. API Management can provide a REST based service layer around existing backend systems with XML to JSON transformation if needed.

- Consolidating different queuing solutions. What if you decide to use multiple best-of-breed applications and you want to decouple those applications using a variety of queuing solutions? Instead of connecting to each of those queuing solutions directly, you can hide the interfaces behind a service façade. The technical term for this is protocol bridging. API Management solutions can provide a single REST endpoint to access different queuing solutions, like ActiveMQ, OracleAQ and/or MSMQ.

- Design time and runtime governance. One of the challenges of using SaaS services is related to governance. Governance is of paramount importance to keep oversight. At design time you need a repository to easily find the services you need and avoid duplications. At runtime, you need a central location for consistent policy enforcement and health monitoring. Again all of this can be provided by API Management solutions.

Microsoft API Management

Although Nevatech Sentinet and Azure API Management are both labeled API Management solutions, they are actually quite different products. Before looking at the differences between the two products, first a brief introduction.

Nevatech Sentinet

Nevatech positions Sentinet on the market as the only API Management solution entirely built on the Microsoft platform. With Sentinet you can configure virtual services that expose one or more business services. A virtual service has one or more endpoints and each endpoint has its own WCF binding. Think for instance of basicHttpBinding, netMsmqBinding or webHttpBinding. Note that the definition of WCF bindings does require a certain amount of developer skills, so that's a complicating factor.

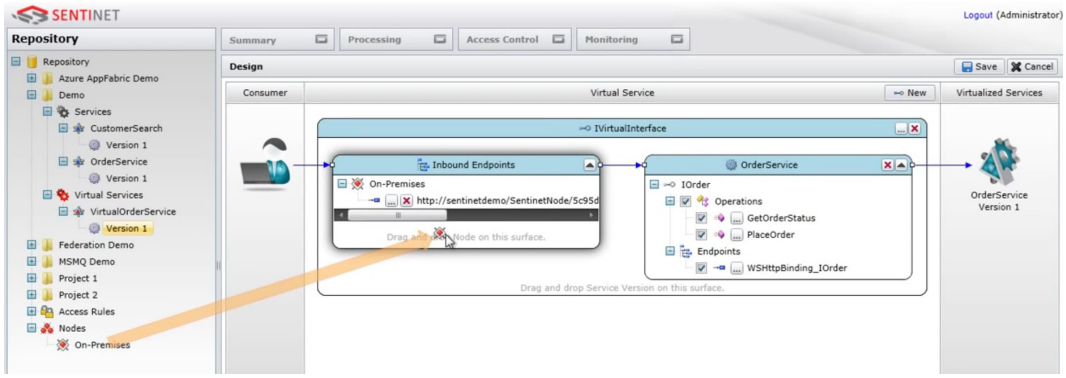

Figure 2
Designing a virtual service in Sentinet.

After defining the virtual service and its endpoints, you can set the service access rules. Access rules can be based on usernames or claims, but they can also be based on the http header, the message body or have a custom format like a rate limit (calls/min) or an IP filter. Once again realize, that the definition of custom access rules requires a certain amount of developer skills.

All virtual services are stored in the repository to allow for design time and runtime governance. Sentinet has what we call an active repository. This means virtual services and other assets are deployed automatically to the Sentinet nodes after changing the status from draft to active. At runtime you can use a dashboard for real-time monitoring and message tracking. It's also possible to define alerts, for instance if you want to monitor Service Level Agreements.
Sentinet is an expensive product. Just to give an idea, a single Sentinet node will cost around US$ 25.000 and you will definitely need more than one. License fees for Windows Server, SQL Server and Azure are not included in the price.

Azure API Management

Azure API Management is based on the like-named delivery platform from Apithany, a company acquired by Microsoft in the fall of 2013. What Microsoft stresses when it comes to Azure API Management is the ease of development. Using the Publisher Portal, developers can build their first API in five minutes. Moreover, it's easy to add metadata to further simplify service consumption. Service consumers can subscribe to the APIs and use the Developer Portal to actually call them. The Developer Portal can be customized to adhere to the look and feel of the company. At runtime, the health of your APIs can be monitored via a graphical dashboard. It's as simple as that. A strong point of Azure API Management I like to emphasize is the ease with which policies can be defined. Examples of policies include access restriction policies (usage quotas, rate limits), content transformation policies (convert XML to JSON, set HTTP header) and caching policies.

Figure 3
The Azure API Management Policy Editor.

Of course Azure API Management also offers all the typical advantages of a cloud-based solution. Think of availability, scalability, elasticity and pay for use. To elaborate on the latter. The standard version of Azure API Management uses four nodes, each of which will cost $16.80 per day. Next to this fee, Microsoft will charge the standard data transfer rates. It's difficult to put an accurate price tag on it, but Azure API Management can be interesting pricewise.

On the downside, Azure API Management has somewhat more limited functionality than Sentinet. It's important to emphasize though, that the cloud model by nature allows for seamless extension of the product.

Below is a list of functionality that is to be expected in the near future:

- Hosting Azure API Management in a private cloud.
- Enhanced security. Think of mutual authentication via certificates, OAuth 2.0, SAML and support for Windows Azure Active Directory (WAAD). Other extensions relate to role-based access and the implementation of an audit log.
- API versioning and lifecycle management.
- Support for SOAP and REST-to-SOAP mapping.
- Support of tracing and debugging.
- Access via a Management API.
- Custom C# policies.
- Usability improvements.
- Customized reports per user.

When to use Microsoft API Management?

The first question is when you should consider using a Microsoft-based API Management solution. Of course the client should have sufficient budget. API Management solutions are expensive products, so they will not be interesting for every client. Next the client should be committed to Microsoft technology. Despite the promise of open standards, it can be challenging to bridge the gap between the Java and the .Net world. That works both ways. It's a good advice to choose a Microsoft API Management solution when you have an application landscape that is predominantly Microsoft.

Third point. The client should be committed to service orientation. In general, the added value of API Management solutions dramatically increases when you have more services to expose. Finally, API Management solutions can be a good fit in situations where a client wants to integrate with business partners, cloud services and mobile apps. External integration and mobile computing are exactly what API Management solutions are good at and what they should be used for.

When to use Nevatech Sentinet?

Nevatech Sentinet is a professional, mature product. It brings all the advantages of service virtualization and service governance. That's important to stress, because it's really a valuable addition to the Microsoft stack next to the somewhat clumsy UDDI tools.

Unlike Azure API Management, Sentinet is best used on premise, especially if you have a service oriented architecture with BizTalk as the service bus. Sentinet offers support for protocols like SOAP, REST and MSMQ. It can also be used as a virtualization layer if you want to expose BizTalk orchestrations or if you want to call business services from BizTalk. Sentinet finally offers an easy to configure service endpoint resolver for routing in an ESB Toolkit scenario.

Next to its use on premise, Sentinet can also be used in hybrid scenarios. Think of a retailer with a web shop that uses SaaS solutions for distribution management, product catalogue updates and business partner management. Sentinet is a good choice in this scenario, especially because of the extensive security features of the product.

When to use Azure API Management?

Using Azure API Management is not limited to a situation where you start off from a service oriented architecture with an enterprise service bus. Under the current market conditions, one could even question the fact whether we actually need a full-fledged ESB. The world around us is changing and businesses must be able to respond quickly. There is a growing need to integrate with partners, cloud services and mobile apps. Network boundaries are blurring. Business consumers expect 24/7 access to data, not just in one way but across multiple devices and channels. We see a rise of The Internet of Things and machine-to-machine communication. All these trends urge us to think about a cloud strategy. Creating a digital platform to interact with customers and partners in new, innovative ways. Creating new revenue channels for existing on premise services. In this new economy, sometimes referred to as the API economy, Azure API Management can be a good option. Azure API Management offers a low-price, low-risk model for service virtualization. It has a short time to market and makes it easy to add security and other policies.

Key takeaways

A Microsoft-based API Management solution is a good choice if you have an application landscape that is predominantly Microsoft. The added value increases if you have a service oriented architecture or if you want to integrate with business partners, cloud services or mobile apps. Sentinet is best used for on premise scenarios and hybrid scenarios. If offers excellent service governance, integration with the BizTalk ESB and support for SaaS integration. Azure API Management is the weapon of choice in cloud scenarios. It has a short time to market with extensive policy injection and base security. To make a final choice, it's obviously a good idea to perform a proof of concept with clearly defined scenarios and evaluation criteria. In the end, the proof of the pudding is in the eating.

De auteur

Paul Baars

Paul Baars is a professional consultant with twenty years of experience in the IT industry. Paul has gained extensive project experience working as a developer, designer, architect and team lead for various companies in different industries. Paul has a strong background in Microsoft technology. He specializes in service orientation and application integration and is a certified consultant for BizTalk, WCF and C#. Paul is an enthusiastic blogger and can be followed on linkedin.com/in/paulbaars and phv-baars.wordpress.com.

Motion10 helps companies and organi-zations get greater value out of their information flows. The firm helps organizations to connect and to share. It uses the latest technology from the Microsoft Application Platform. Motion10 is the premier competence center in the Netherlands for SharePoint and BizTalk.

For more information: www.motion10.nl

Motion10

www.motion10.nl