SENTINET

Overview

SENTINET 3.0

Nevatech

Contents

Introduction

Nevatech Sentinet™ platform is a software middleware infrastructure that manages heterogeneous SOA and API services and application deployed on-premises, in the cloud, or in hybrid environments. Sentinet provides customers' SOA architectures with design-time and run-time SOA governance and automated management.

All enterprise service applications face the same common infrastructural challenges – services' availability and accessibility, discovery, security, monitoring, auditing, service agreements and service level objectives management, alerting and many others. These common infrastructural challenges are typically not part of an organization's core business and can be addressed by middleware infrastructure tools and products that save time and resources. Development teams are enabled with faster time-to-market delivery of their business solutions, while operations teams are equipped with tools and procedures to manage and maintain production systems in a consistent and predictable environment.

The most effective and popular means of addressing common SOA infrastructural challenges is based on the concept of services virtualization or services brokerage. Services virtualization introduces the notion of software agents or brokers that mediate communication between consumer and provider applications and implement dynamic, remote and non-invasive management of common infrastructural and operational tasks. Services virtualization is the only concept that enables SOA and API solutions with non-intrusive management and provides them with the real agility to adapt to continuous changes.

Nevatech Sentinet™ software platform is the only market implementation of the services virtualization concept that is built entirely on the Microsoft platform and fully integrates with, and extends, Microsoft SOA offerings. Sentinet software platform is certified for ***Works for Windows 2008 R2 Server***, ***Certified for Windows Server 2012*** and ***Powered by Windows Azure*****.** Sentinet supports and leverages industry standards and manages common infrastructural challenges for any heterogeneous SOA and API solutions, whether they are developed on the Microsoft platform or not.

Sentinet is most beneficial to organizations that leverage a Microsoft platform to develop and operate their SOA and API solutions, and those organizations that have to integrate and mediate Microsoft and non-Microsoft technologies as part of their SOA architectures. Sentinet is a unified middleware software infrastructure solution for on-premises, cloud and hybrid environments. It can operate in any of these diverse network configurations, and it can manage an organization's SOA and API solutions deployed and operated on-premises, in the cloud or in hybrid environments. Sentinet is the only middleware infrastructure that fully integrates with, and extends capabilities of the Microsoft Windows Azure cloud platform.

Sentinet provides organizations with connectivity and integrations across enterprise and cloud applications by enriching them with dynamic and remote manageability of security, access control, monitoring, alerting, SLAs management and automated testing. Sentinet provides organizations with

design-time and run-time SOA governance and automation. Using Sentinet, enterprises implementing service-based applications can realize the full potential of their flexible, standards-based systems.

Sentinet is:

- Powerful – provides complete visibility and manageability of services, discovers problems and provides solutions.
- Non-intrusive – no code or deployment configuration modifications are required for business services.
- Platform-independent – fully supports Microsoft and non-Microsoft based architectures.
- Microsoft focused - runs natively on, fully integrates with, and extends Microsoft on-premises and Windows Azure cloud platforms; provides powerful mediation capabilities between Microsoft and non-Microsoft services and applications.
- Versatile – can operate on-premises, in the cloud or in the hybrid environments; can manage on-premises or cloud business services.
- Flexible – can be configured to perform a multitude of tasks for each system, service, or request.
- Secure – supports various security standards and custom authentication/authorization schemes; fully supports interoperable and Microsoft-specific protocols and security standards.
- Extensible – provides interoperable Web Services-based public API with multiple extensibility points; integrates with third party or custom management tools and products; customizable through standard Microsoft .NET extensibility points .
- Easy To Use – Rich Internet Application graphical user interface is both powerful and intuitive.
- Supports variety of industry standards and protocols such as SOAP, REST, JSON, XML, WS-* specifications, HTTP, HTTPS, NET.TCP, MSMQ, Windows Azure Service Bus binary exchange.

Customer Benefits

Customer benefits span across all stages of customers' SOA and API solutions' life-cycle.

Development and Test

Sentinet enables development teams with faster time-to-market delivery of their SOA and API solutions by providing:

- Central SOA and APIs Repository with discoverable and reusable services and their metadata.
- Standardized and centralized policies enforcement that ensures developers adhere to policies and security models adapted for their projects and solutions.
- Effective and non-intrusive security policies models implementations.
- Effective and non-intrusive identities management.
- Effective and non-intrusive access control management.
- Effective and non-intrusive performance testing and performance impact analysis.

- Powerful and non-intrusive monitoring and message exchanges recording, auditing and troubleshooting.
- Consumer and provider applications parallel development enablement.
- Services and consumer applications automated testing.
- PKI keys and certificates management infrastructure.
- Extensibility at multiple levels and across a variety of management aspects.

Production and Operations

Sentinet enables operations team with tools and procedures to operate and maintain production systems in a consistent, reliable and predictable environment by providing:

- Better understanding of system behaviors.
- Services accessibility and high-availability management.
- Policies implementations that automate performance management.
- Security policies provisioning and security uphold.
- Remedy for exceptional conditions.
- Visibility and control without system reconfigurations or redeployments.
- Identities management and non-invasive access control.
- Integration with third party identity systems and Federated Security environments.
- Real-time monitoring that keeps enterprises appraised of applications behavior and their constituent components.
- Performance and impact analysis.
- Performance patterns and trends analysis.
- Service consumption patterns and trends analysis.
- Active and pro-active alerting.
- Root-cause analysis and auditing.
- Service Level Agreements and Service Level Objectives management.

Architecture

Sentinet platform consists of four major components:

1. **Sentinet SOA Repository**, an on-premises or cloud based MS SQL server database that provides centralized, hierarchical and secure storage for all SOA managed software assets, such as services, virtual services, security policies, metadata, authentication/authorization and access control rules, service agreements, identities and identity systems configurations, monitoring

data and auditing trails. Access to SOA Repository is subject to strict security that includes data confidentiality, integrity, authentication and authorization control, and role-based access. Sentinet Repository is enabled with a multi-tenancy that allows partitioning of its content, its visibility and accessibility per specific Sentinet users and user groups.

2. **Sentinet Management Services** is an API of secure and interoperable Web services that provide secure access to the Sentinet Repository. Sentinet Management Services application is used by the Sentinet users and administrators to remotely control the content of the SOA Repository and to drive behavior of all their managed SOA services.
3. **Sentinet Nodes** are high-performance, low-latency, scalable intermediary brokers that host dynamic virtual services designed and managed by Sentinet administrators using interactive Sentinet Administrative Console. Sentinet Nodes mediate communication between service consumers and service providers, and through that brokerage they enable SOA solutions with multi-dimensional run-time management capabilities. Sentinet Nodes make outbound asynchronous connections to the Sentinet Management Services to dynamically configure themselves via light-weight heartbeat calls. Sentinet Nodes can be deployed as secure gateway proxies or as the agents embedded into application servers. Sentinet Nodes can be deployed within enterprise EAI internal infrastructure, or they can be distributed across on-premises and cloud environments forming a light-way ESB, a ***Virtual Service Bus*** of on-premises *and* ***Cloud Service Brokers***. Sentinet Nodes enable managed SOA services with agility and control of connectivity, security, monitoring and auditing - all in a non-intrusive way. Sentinet virtual services hosted on the Sentinet Nodes create an “SOA software reuse” environment by allowing aggregation of multiple business services and APIs in a single service with fine-grained control of the aggregate service structure and accessibility.
4. **Sentinet Administrative Console** is a Microsoft Silverlight-based, Rich Internet Application that enables Sentinet users and administrators with highly interactive and intuitive remote control of all the aspects of their SOA solutions’ management.

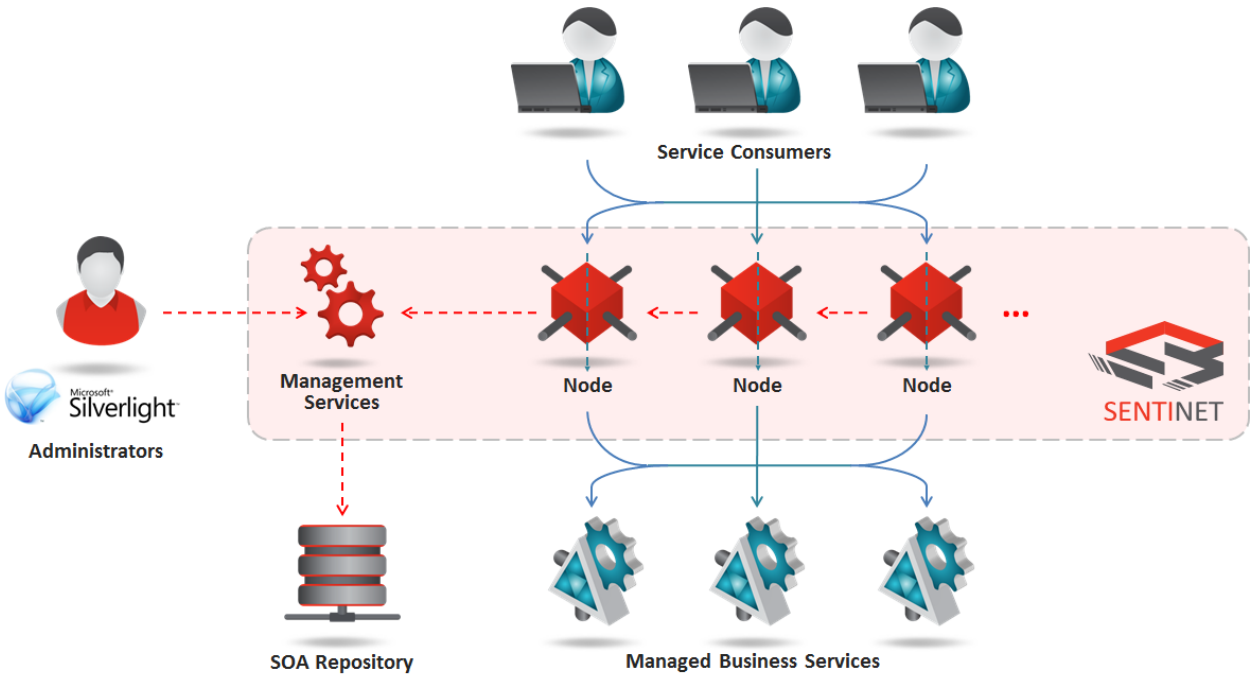

Figure 1. Sentinet Architecture overview.

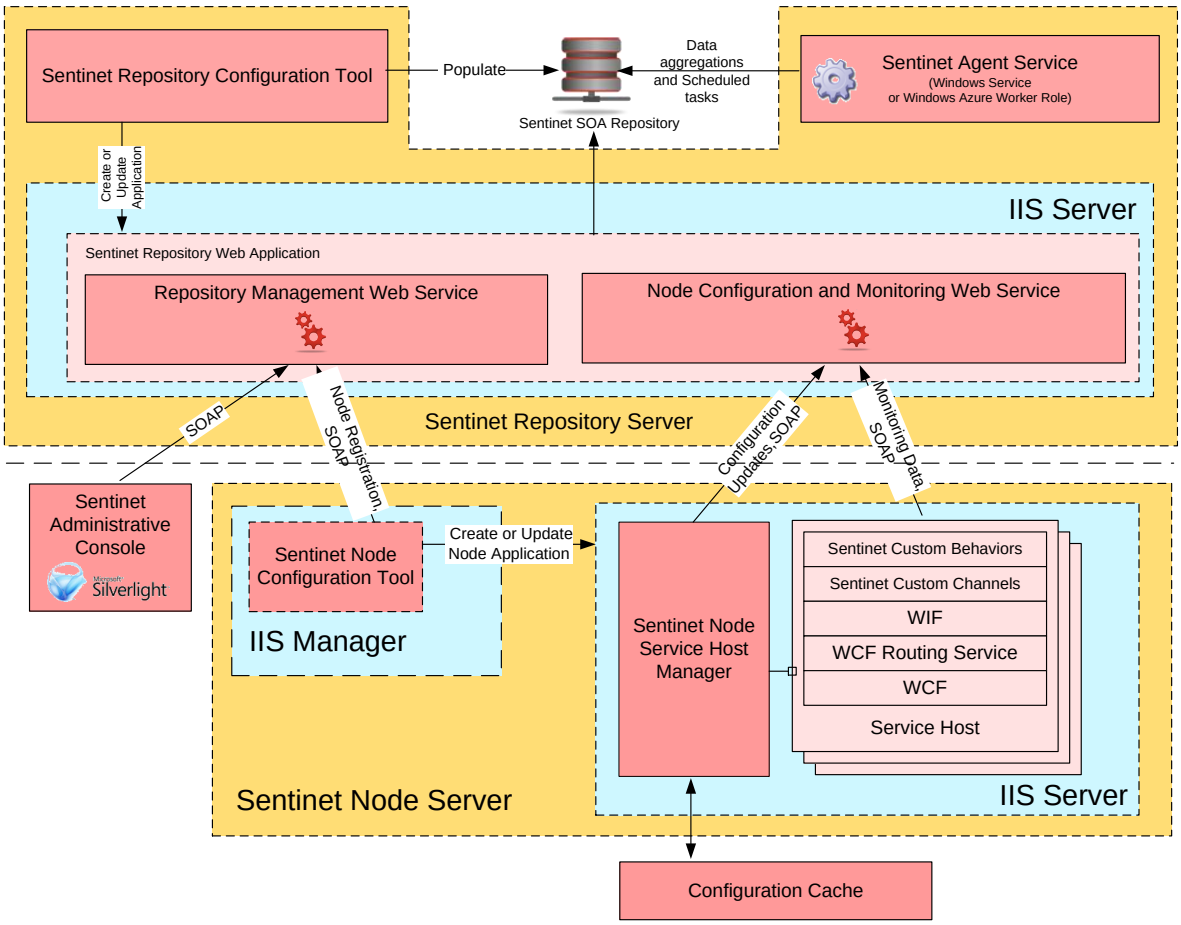

Figure 2. Sentinet components overview.

Technology Stack

Even though Sentinet is designed and built to manage heterogeneous services and applications, it is best suited for environments that host Microsoft services, or those that have to integrate Microsoft and non-Microsoft applications. Sentinet is built on top of Microsoft technology stacks and extends its capabilities.

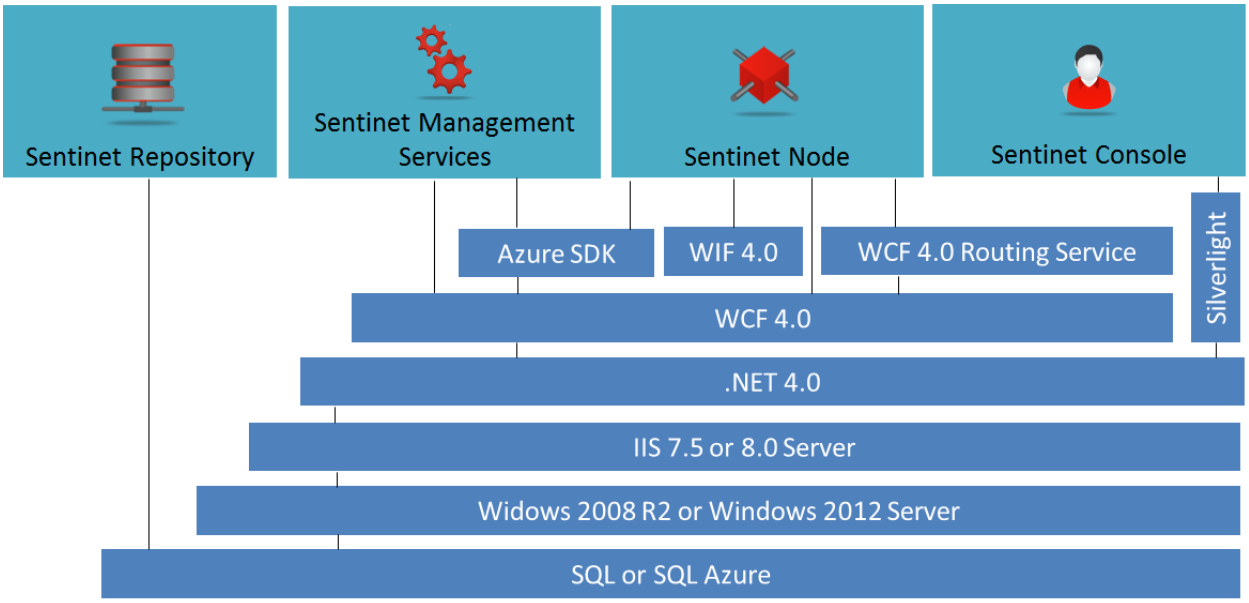

Figure 3. Sentinet technology and run-time platform stack.

Sentinet is highly extendable through standard Microsoft .NET, WCF and WIF extensibility points, and also via Sentinet interoperable Web Services and .NET API interfaces.

Features Summary

Sentinet Repository and design-time Governance

1. Services discovery and secure access to services metadata.
   Unlike most of the UDDI-type of registries that provide only references to external metadata or incomplete services metadata, Sentinet Repository stores and provides access to the actual metadata with all associated attributes and artifacts. External links or entire documents can be attached to service description elements.
2. Dynamic metadata updates. Changes made to service definitions and artifacts automatically update relevant metadata by keeping it synchronized with real environment updates.
3. Secure Repository access. Only authenticated and authorized users can access Repository.
4. Role-based Repository access. Sentinet Repository includes multi-tenancy and role-based access.
5. Support for standards-based policies and all Microsoft specific policies.
6. Policies automatic synchronization, implementation and enforcement. Sentinet Repository is an “active” repository. Changes made to the service definitions automatically propagate to the run-time environment ensuring automatic updates and no downtime of the production systems.
7. Service and consumer identities management and governance.
8. Built-in PKI and X.509 Certificates management infrastructure.

9. Sentinet Repository is a centralized storage for the runtime information such as real-time and historical monitoring, alerting, and SLA violations management.
10. Support for services and APIs versioning at design-time and run-time.
11. Services and Service Agreements life-cycle management.
12. Services and APIs access control and access rules management.
13. Systems' state, compliance, and operational metrics reporting.
14. Repository export/import capabilities to automate services and APIs migration from development to staging and production environments.

Sentinet Runtime Management

Protocols and Standards support

Sentinet supports a wide range if standards, protocols and message formats.

1. SOAP and REST.
2. All WS-* standards supported by Microsoft WCF technology.
3. XML, JSON, text, binary.
4. HTTP, HTTPS, NET.TCP, NET.MSMQ, MSMQ.FORMATNAME, NET.PIPE, SB (Windows Azure Service Bus).

Virtualization and Mediation

1. Services virtualization using drag-and-drop graphical interface.
2. Mediation of transports, policies, message protocols, versions, and encodings.
3. Identities mapping and transformation.
4. Fine-grained virtualization. Virtualization of all or only selected business service or API operations.
5. Aggregate virtualization. Aggregation of multiple business services and APIs by a single virtual service with fine grained control of the virtual API operations, endpoints and policies.
6. Bridging interoperable and non-interoperable communication protocols and security models.
7. Messages transformation.
8. Support for interoperable and all Microsoft-specific communication transports.

Security

1. Support for industry standard interoperable and all Microsoft-specific, non-interoperable security models.
2. Support for industry standard and custom security tokens.
3. Support for security Federation and Single-Sign-On scenarios.
4. Support for and integration with industry standard and custom Security Token Services (STS). For example: Windows Azure Access Control Service or Microsoft ADFS 2.0 server.
5. Support for industry standard and custom authentication schemes.
6. Support for Claims based authentication/authorization and claims aware applications.
7. Support for Identities transformation and Identities pass-through.
8. Sentinet Authorization Engine that provides services and APIs with fine-grained and non-invasive run-time authorization at different service scopes such as service, service interface, service operation, or service endpoint.
9. Access Rules Graphical Designer with extensibility for custom Access Rules.

Routing

1. Dynamic messages routing to different business services, service versions APIs and service endpoints.
2. Built-in load-balancer with fault tolerance.
3. Priority-based routing.
4. Multicast and publish/subscribe routing.
5. Custom routing (content-based, schedule-based, identity-based, geography-based, etc.).

Monitoring

1. Real-time and historical transactions monitoring.
2. Messages recording at different message-processing stages such as wire-level monitoring, message transformation monitoring, encrypted and decrypted messages monitoring, protocol bridging monitoring.
3. Exceptions monitoring.
4. Search for message exchanges by date, time and transaction status.
5. Service and API traffic volume monitoring, performance and other execution metrics monitoring.
6. Monitoring by access rules, consumer identities and consumer addresses.
7. Service Level Agreements and Service Level Objectives violation monitoring.

Service Level Agreements Management

1. Service Level Agreements can cover multiple services and APIs.
2. Service Level Agreements can cover multiple service and API scopes such as service, interface, operation or endpoint.
3. Service Level Agreements per consumer or consumer groups.
4. Service Level Agreements monitored against multiple service metrics such as traffic volume, service availability and performance metrics.
5. Service Level Agreements per specific service access rules.
6. Service Level Agreements per specific time schedules.

Alerting

1. Alerts on expiring consumer and service applications' X.509 certificates.
2. Alerts on SLA violations, service traffic volumes, service availability and performance metrics.
3. Built-in alert notification targets such as user emails and custom Windows Events.
4. Alerts extensibility via custom alert handlers. For example, send alerts to Microsoft System Center Operations Manager or send SMS messages.

Testing

1. Virtual services testing.
2. Security models testing.
3. Performance implications testing.
4. Auto-generated test responses and fault messages.
5. Service response patterns testing.
6. Pro-active development testing.
7. On-premises and cloud testing.

Reporting

8. Reports of the most active, most failed, or least performing services within different time intervals.
9. Reports of the service consumption, performance and availability details.
10. Reports extensibility via Sentinet interoperable Web Service API.

Integration with Windows Azure cloud platform

1. Integrates with and extends Windows Azure Service Bus relay capabilities.
2. Integrates with Windows Azure Service Bus asynchronous messaging with support for Queues, Topics and Subscriptions.
3. Integrates with and extends Windows Azure Access Control service capabilities.

Deployment Topologies

1. Sentinet Nodes can be deployed as security gateway proxies or stand-alone intermediaries.
2. Sentinet Nodes can be deployed as the agents embedded into application servers.
3. Sentinet fully supports high-availability redundant deployment topologies.
4. Sentinet Nodes can be deployed within internal EAI infrastructure and in the cloud environment.
5. Microsoft Windows Azure deployment topologies include Sentinet Node deployments as native Windows Azure Cloud Services Web Roles and Windows Azure Virtual Machines.

System Requirements

1. Windows Server 2012, Windows Server 2008 R2 or 2008.
2. Can be installed on Windows 7 and Windows 8 for non-production environments.
3. .NET 4.0 or 4.5 Framework
4. IIS Server 8.0, 7.5 or 7.0.
5. Microsoft SQL Server 2012, 2008, 2005 or SQL Azure Database.

Services Virtualization and Mediation

When business services are exposed through Sentinet Nodes, they become more accessible to consumer applications. Business services can be developed and deployed with the unified and most effective communications and security implementations, while ultimately exposed to consumer applications using requirements driven by the service's external accessibilities and security models.

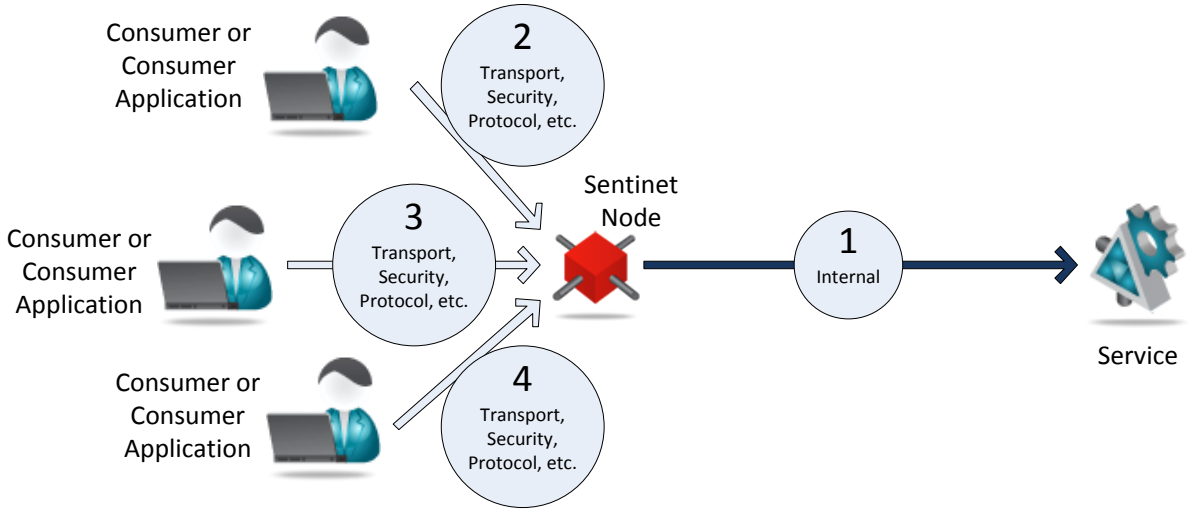

Figure 4. Service virtualization.

Figure 4 shows a business service that is developed, tested and deployed with a unified and optimized internal communications and security implementation (1). Once the service is virtualized through the Sentinet Node, it is exposed to consumer applications through dynamic endpoints hosted on the Sentinet Node using variety of managed communication and security models (2), (3), (4), etc. Consumer applications are decoupled from the business service endpoints location and internal communication and security requirements. Consumers can retrieve virtual service metadata using Sentinet Administrative console or from the optional metadata endpoints that can be remotely opened on the Sentinet Node.

Communication and Security Mediation

In this sample scenario Microsoft WCF service is deployed with performance-optimized *net.tcp* transport. WCF *binary message encoder* is used to provide the smallest message sizes payloads during messages transmission. Windows integrated security is used for optimal performance and strong authentication (1). Both *net.tcp* transport and *binary message encoder* are not interoperable and cannot be used by external consumer application that can only support interoperable *http(s)* transport with standard *text message encoder* and interoperable transport level security (2), figure 5.

A virtual service hosted on the Sentinet Node enables consumer application with the service accessibility by mediating transport and security requirement.

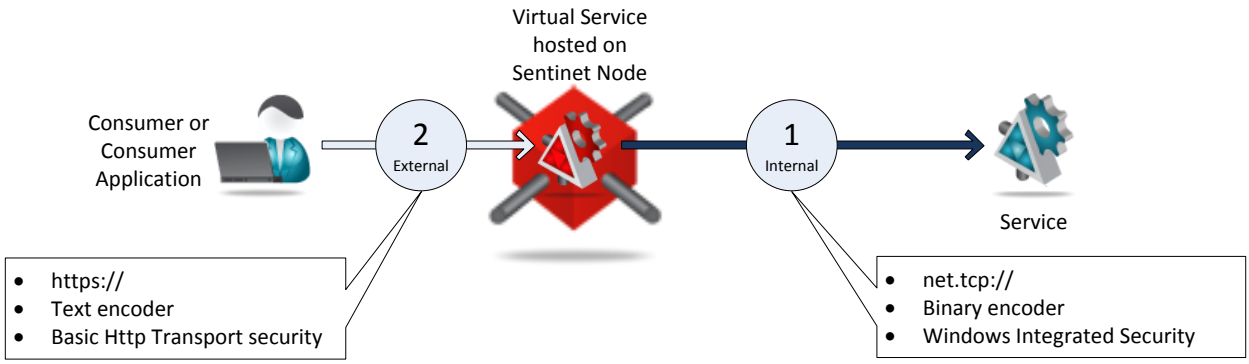

Figure 5. Communication and Security Mediation.

If a new consumer application needs to access business service, and that new consumer application has different supported transport and security capabilities, then Sentinet Node is dynamically configured with additional virtual service endpoints to mediate new transport and security requirements to the same business service implementation.

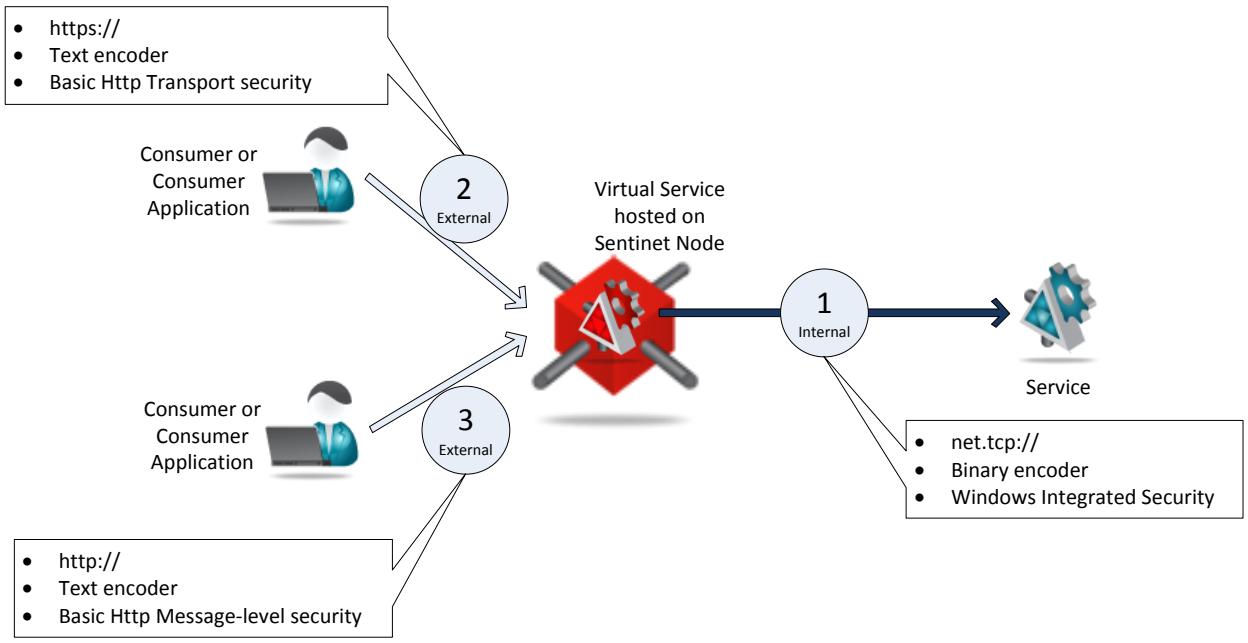

Figure 6. Multiple virtual endpoints.

Consider another hypothetical scenario, when a customer organization makes its mobile application available for its consumers' community. Mobile application is designed to make calls to a customer proprietary REST API, as well as it makes use of the public Microsoft Bing Search API. Sentinet will manage both APIs, but most importantly it will leverage organization's private account with Microsoft Bing service to give its mobile applications access to Microsoft Bing Search API. Each mobile application consumer will use his own personal security key that is issued to him by the mobile application provider. Sentinet will authenticate consumers based on their personal security keys and authorize application's access to Microsoft Bing Search API by using privately held Microsoft Bing Primary Account Key.

Note that Microsoft Bing Primary Account Key will be securely stored with the Sentinet Node, while it is not known to, or even distributed to thousands of mobile application installations.

Mobile applications do not have dependency on the public Bing API location and even syntax requirements. If public API endpoints or API syntax changes, Sentinet will mediate these changes without affecting existing mobile applications.

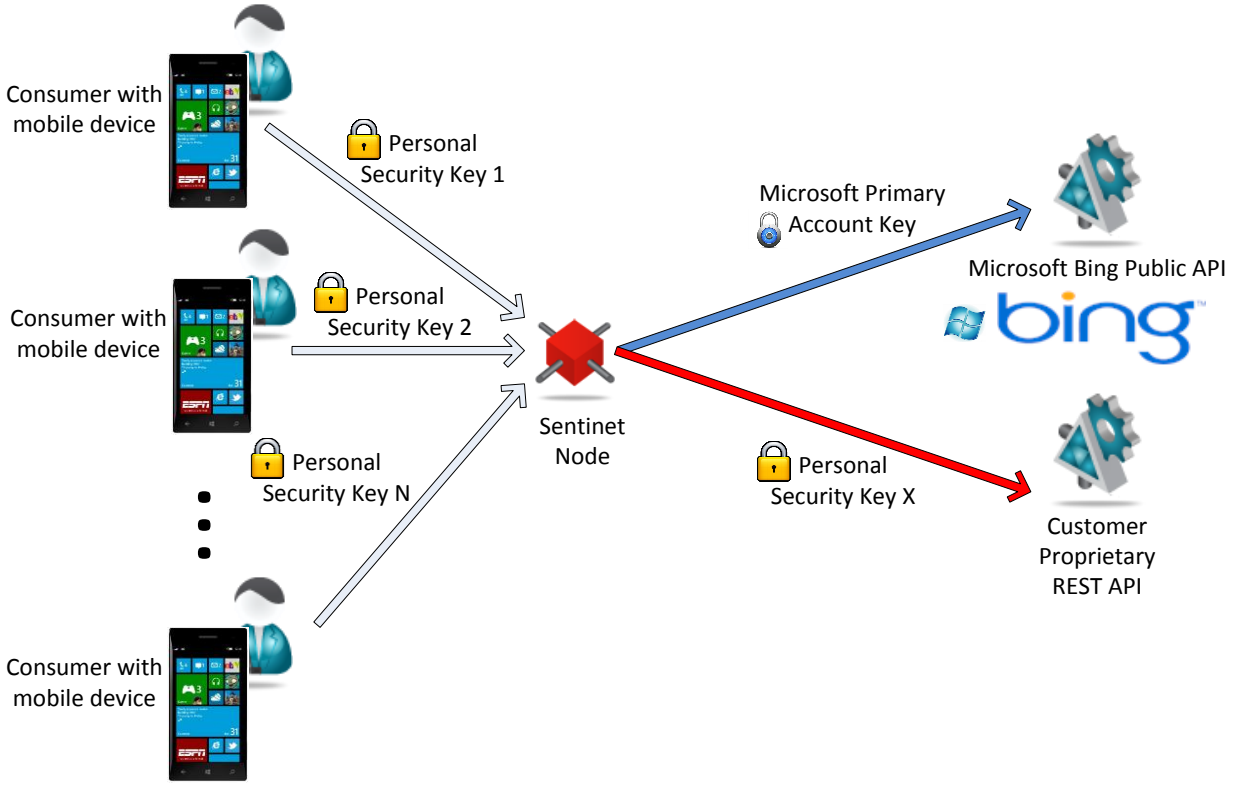

Figure 7. Mediating security and aggregating REST APIs.

Authorization and Federated Security

Service authorization logic is often hardcoded in the business service implementation which makes it difficult to scale authorization rules through services, and to promote services through different life cycles and environments. Sentinet provides a highly flexible run-time Authorization Engine and an interactive design-time Access Rules Designer. The Authorization Engine executes at the Sentinet Nodes where it enforces custom authorizations rules designed by the Sentinet administrators. Business services can now delegate ultimate authentication and authorization decisions to the Sentinet virtual services, while authenticating and authorizing only trusted Sentinet Nodes.

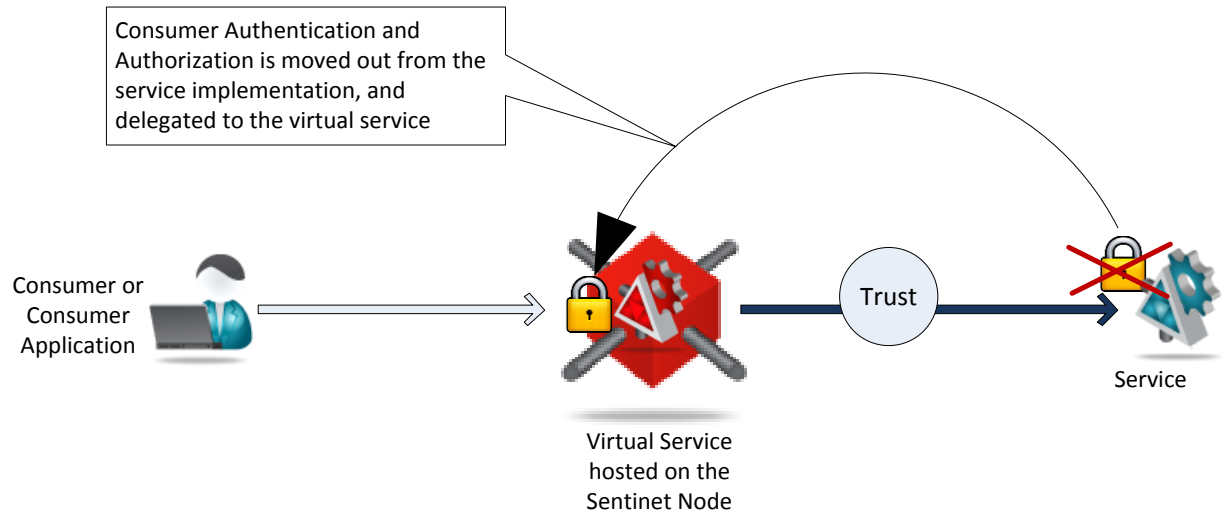

Figure 8. Scalable and non-invasive authorization rules and access control.

Sentinet Authorization and Access Control rules are managed declaratively using rich graphical user interface and Access Control Designer. Administrators can control authorized identities, access time schedules, allowed throughput, and content-based access rules. Developers can extend Sentinet Authorization Engine with custom Access Control rules and integrate them in the Sentinet Administrative Console application.

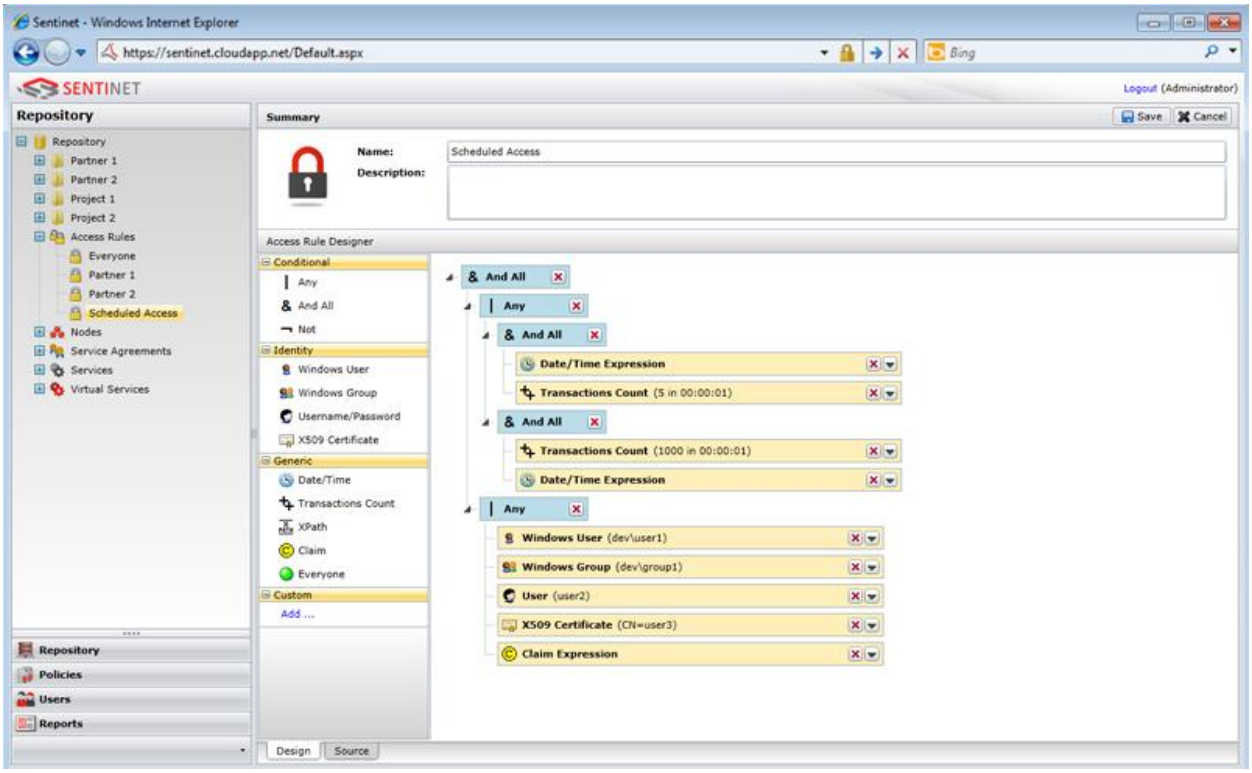

Figure 9. Graphical Access Rule Designer.

Sentinet Authorization Engine supports and extends industry standard Security Token Services (STS), including native support and integration with Microsoft Active Directory Federation Services (ADFS) and Windows Azure Access Control Service (ACS).

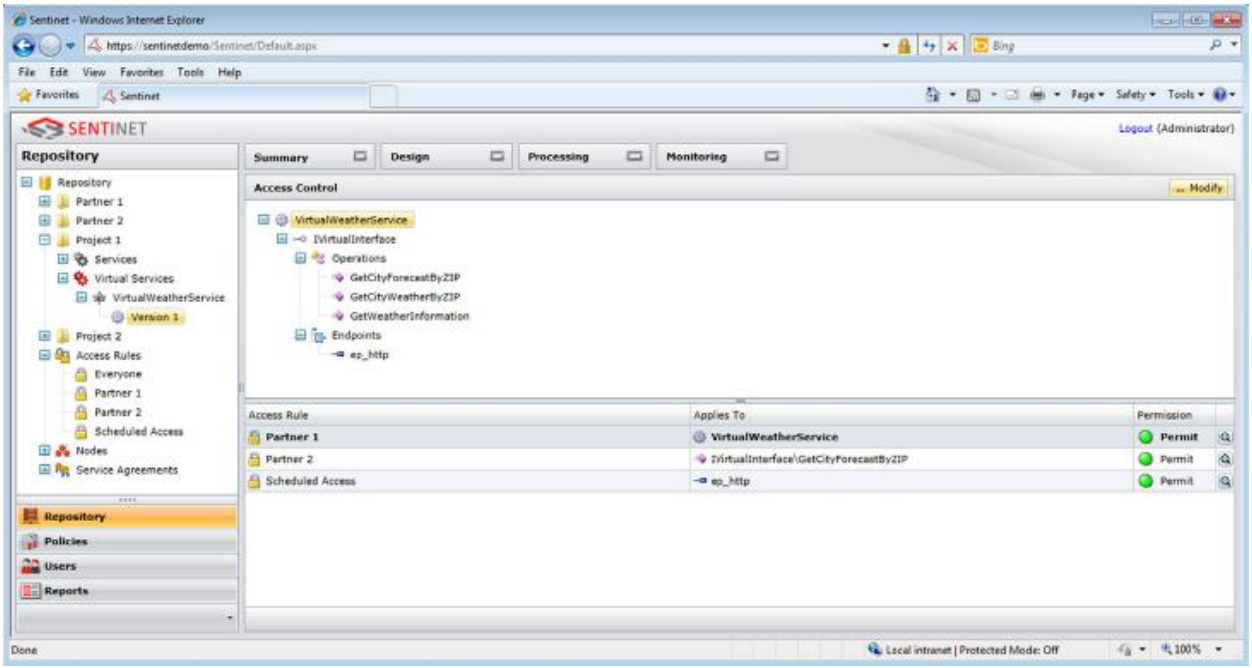

Figure 10. Access Control Designer.

Routing and Versioning

Sentinet provides flexible support for messages routing and services versioning. Not only can Sentinet Nodes be clustered and load-balanced, but they can also execute as load-balancers by routing messages to different business service deployments. Messages can be routed based on a variety of routing rules and criteria such as weighted round-robin, fail-over priority based routing, multi-cast, content based, schedule-based, identity-based or any other custom routing rule. Sentinet Nodes can route messages to different service versions using either endpoints-based or content-based mapping rules.

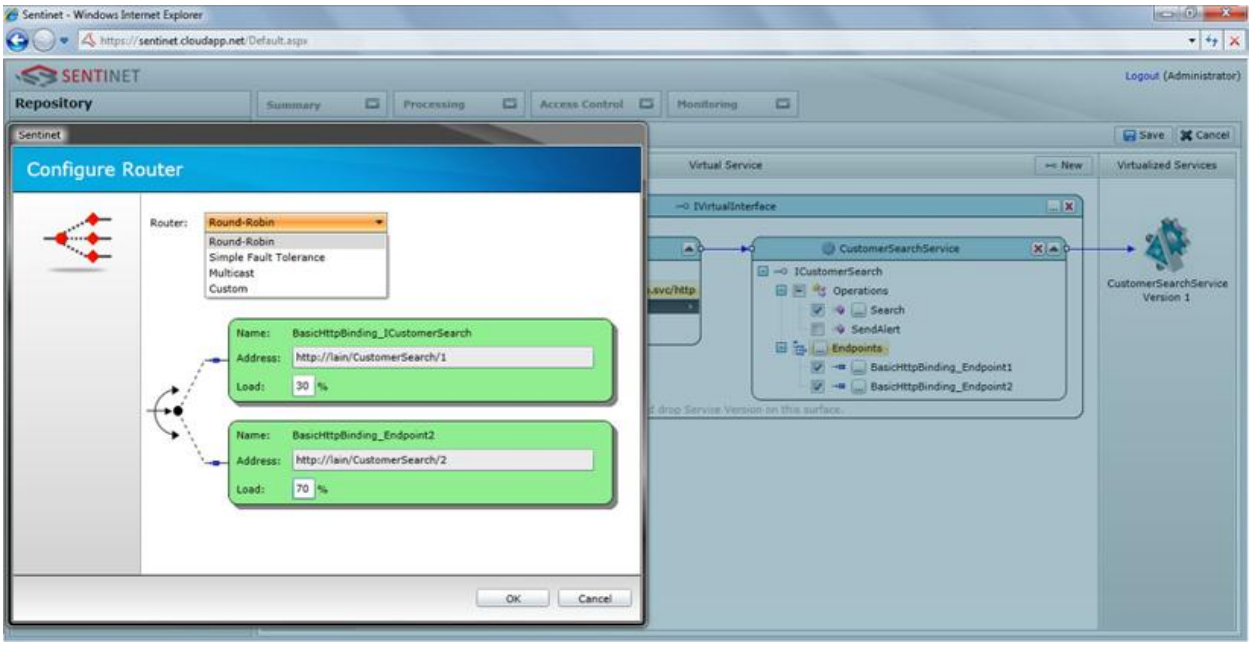

Figure 11. Sentinet messages Router configuration.

Services Aggregation

Sentinet allows easy aggregation of multiple business services and APIs within a single virtual service. Services aggregation gives the benefit of software assets reuse. Services implemented as different APIs with different locations, communications and policy requirements, can be exposed to the ultimate consumer applications via unified and standard communication protocols and policies. Sentinet Virtual Service Designer helps to build aggregated virtual services using intuitive drag-and-drop user interface and graphical wizards.

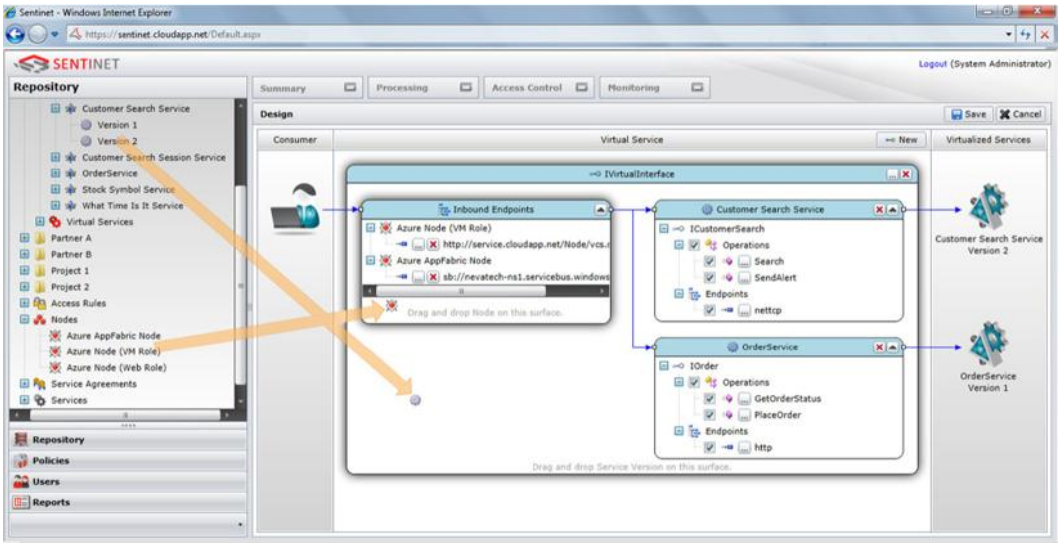

Figure 12. Virtual service Designer. Drag-and-drop services to construct an aggregate virtual service.

Monitoring

Monitoring APIs and services is not a second-level concern. There is no management and cost control without visibility. Sentinet Administrators can see who is using their business services, when, and how. Sentinet provides extensive message exchanges monitoring, tracking, recording and aggregated statistics that help administrators to analyze current systems states and trends. Using real-time and historical monitoring users can predict services future use, scalability, and performance degradations so that service level agreements are continuously maintained.

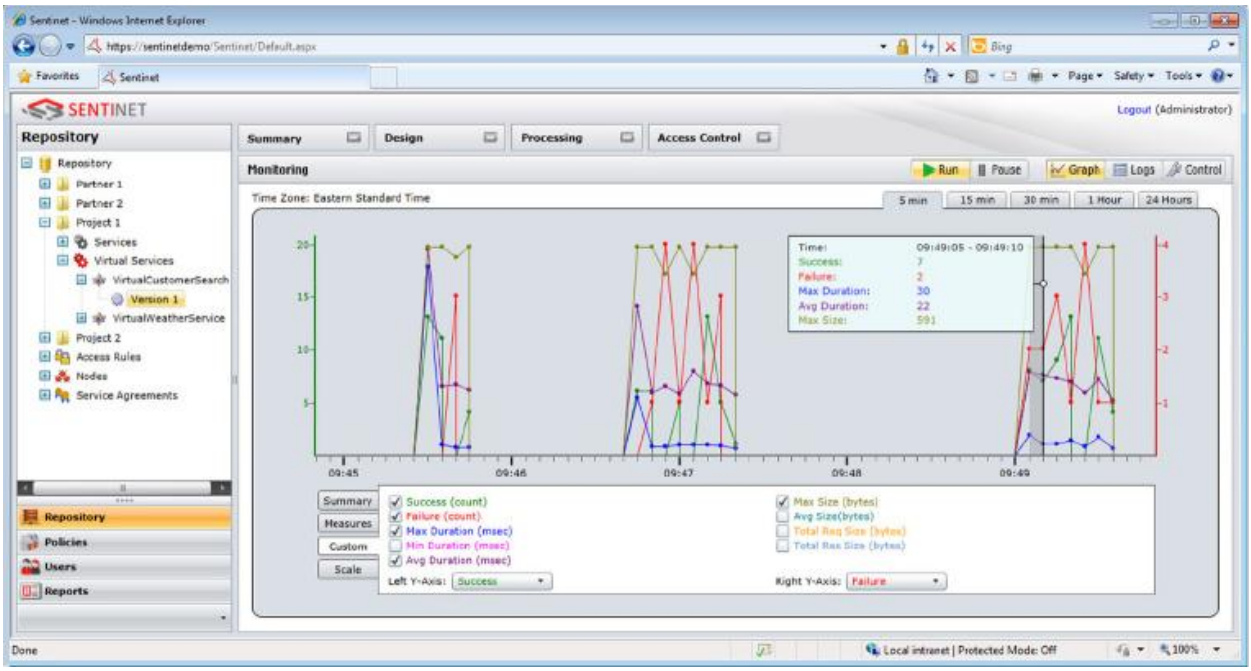

Figure 13. Real-time monitoring.

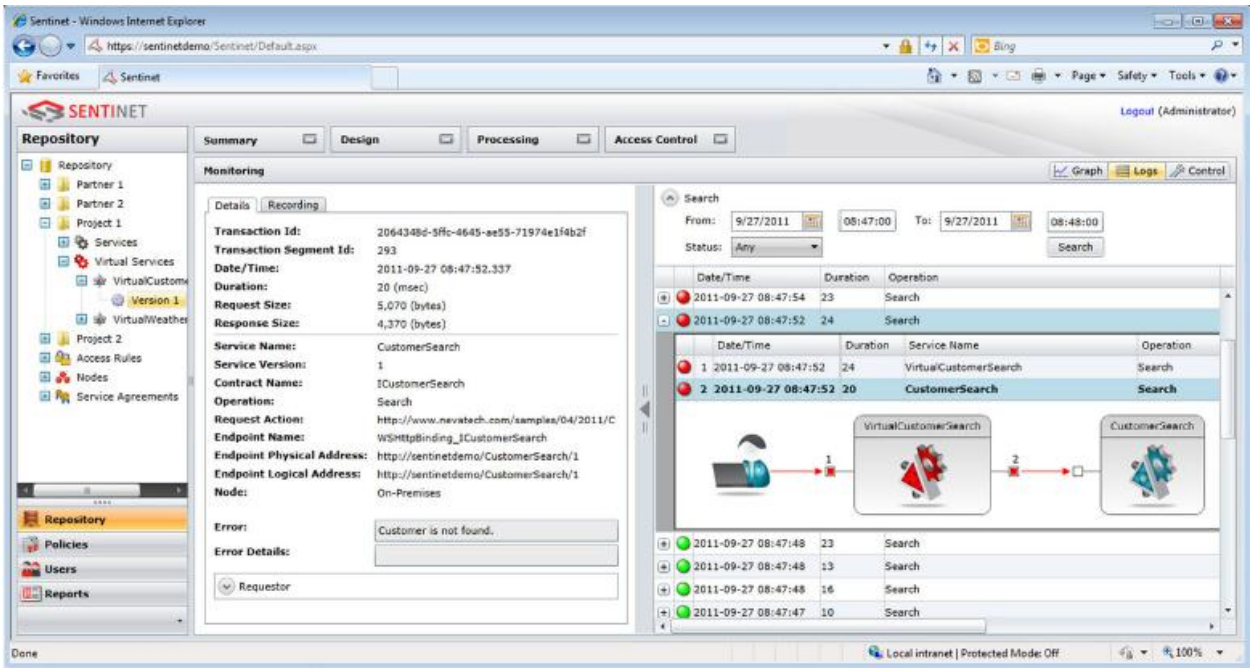

Figure 14. Individual Messages Monitoring and Tracking.

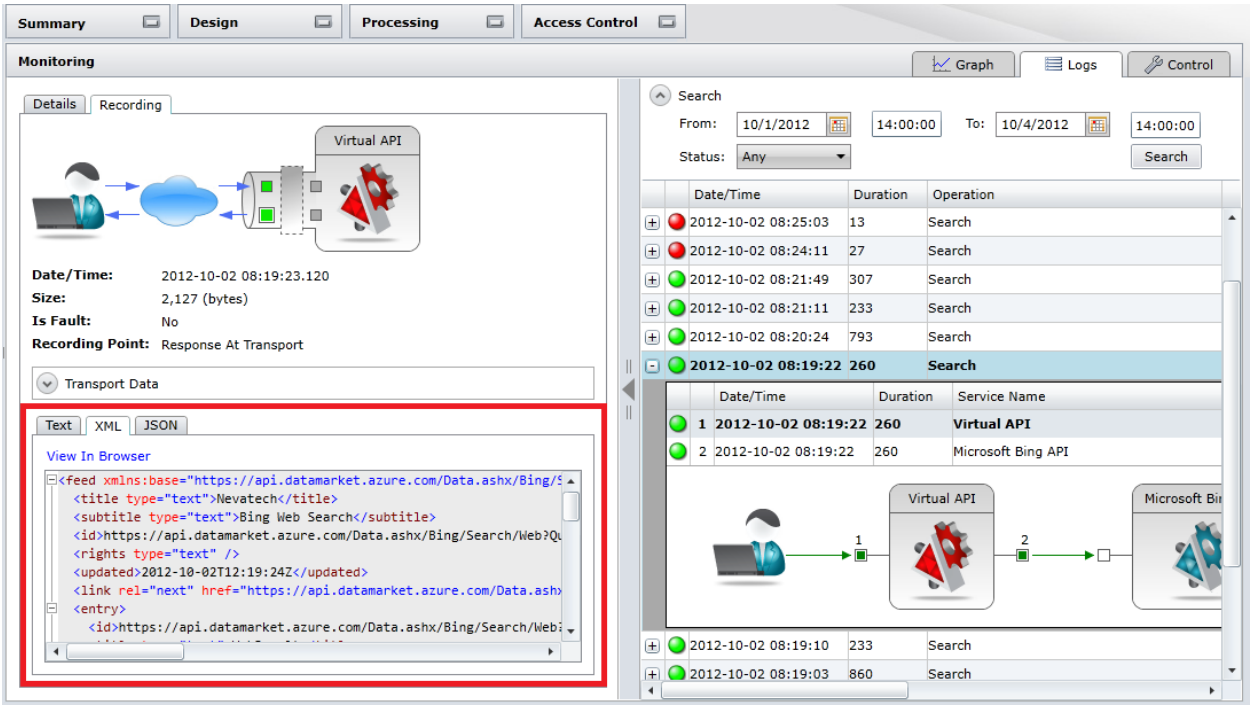

Figure 15. XML messages recording.

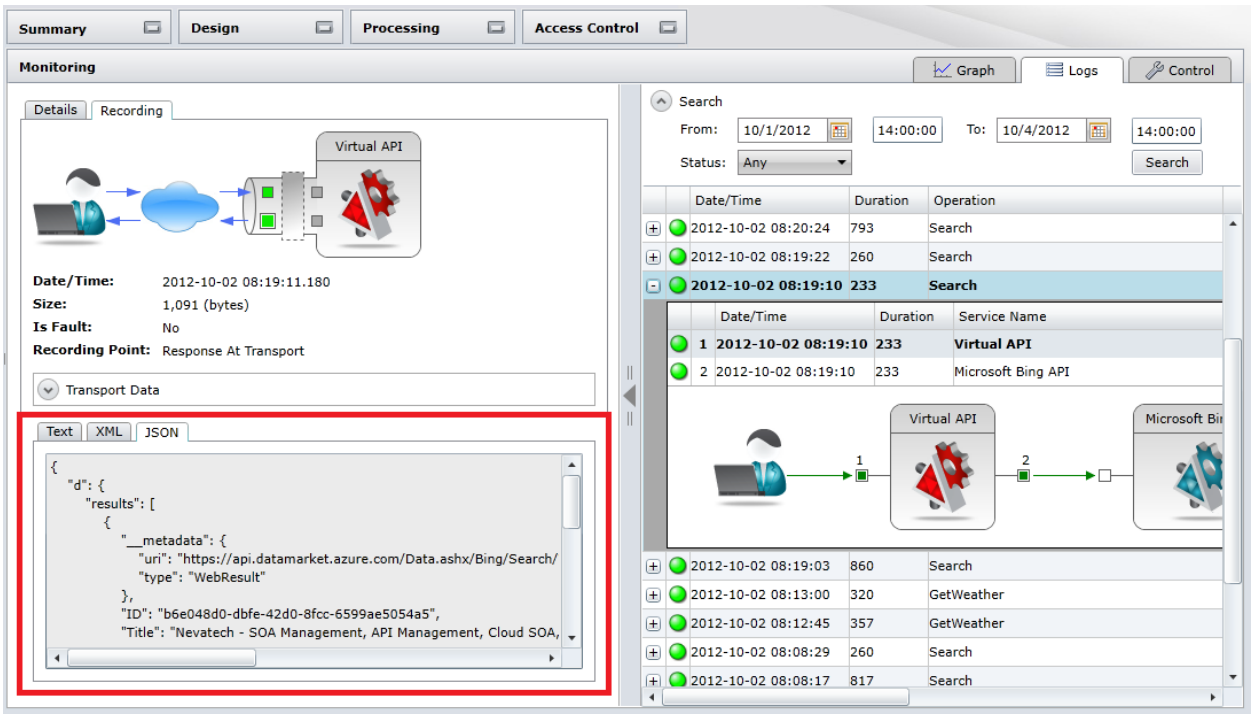

Figure 16. JSON messages recording.

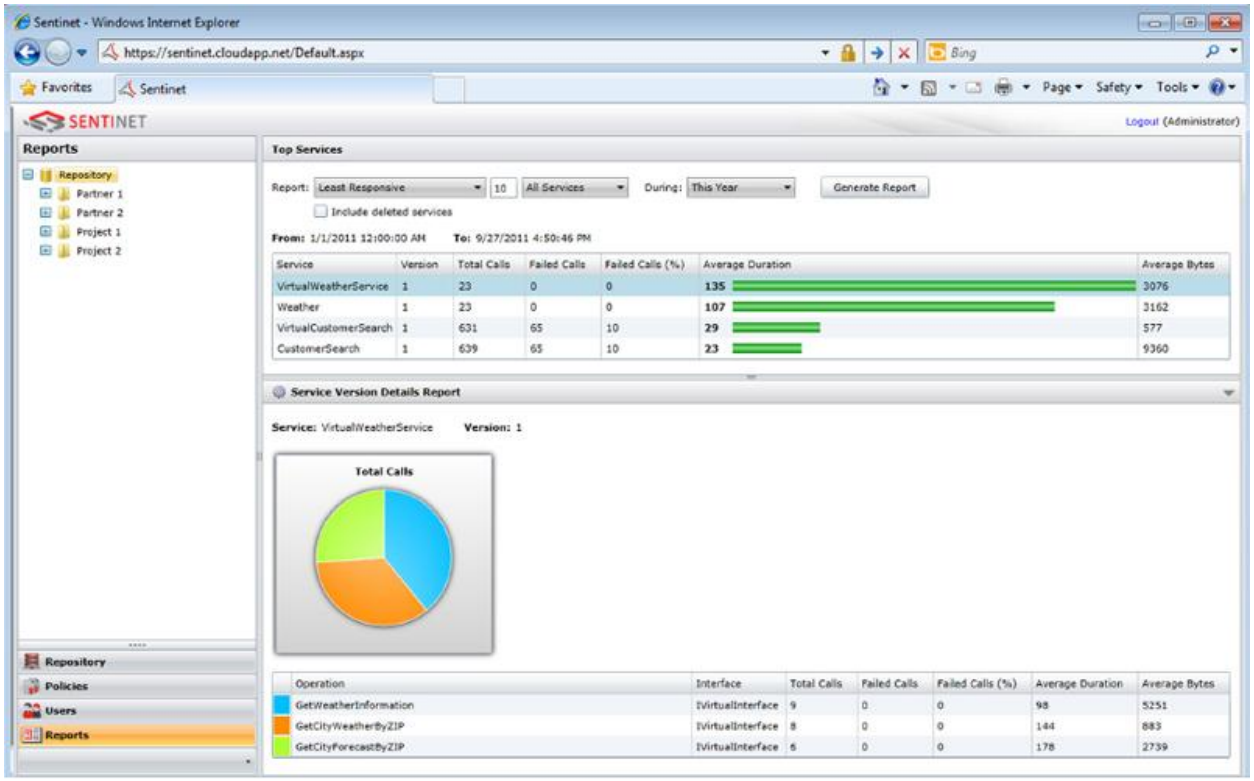

Figure 17. Historical Monitoring and Reporting.

Service Agreements Management

Sentinet Service Level Agreements (SLA) and Service Level Objectives (SLO) management helps organizations and IT operations to understand and implement best practices for monitoring, diagnostics and reporting in order to maintain reliable and scalable applications. Degradations in IT Service delivery can be costly and damaging to business. Organizations are implementing strict Service Level Agreements to ensure high standards of IT service.

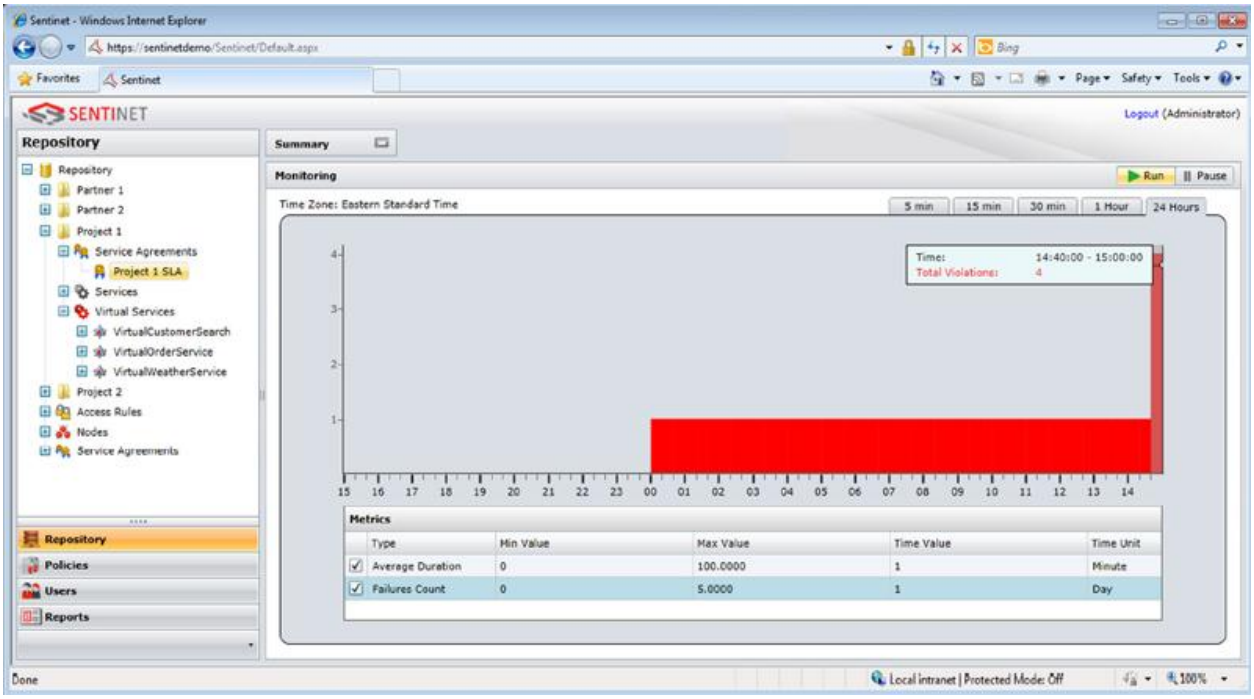

Figure 18. Monitoring Service Agreement Violations.

Sentinet SLA management infrastructure helps organizations to create, monitor and respond actively and pro-actively on SLAs and operational requirements violations in any type of on-premises or cloud environment. Service Agreements can be validated against multiple performance, service availability and traffic volume metrics, and can cover multiple services at different service scopes filtered by access control rules. Sentinet SLAs manage relationships between service consumers and service providers, and enable administrators with complete visibility and operational performance of their services. SOA administrators can define different SLAs for the same service or group of services, and monitor and alert on SLA violations per individual consumer or group of consumers.

Alerting

Sentinet provides a powerful and extendable Alerting System that can generate and handle alerts for expiring X.509 certificates, SLAs and operational metrics violations. Alerts can be configured against individual SLAs, with individual frequency generation and more than one Alert Action. Each Alert Action can handle generated alerts differently (for example: Send email, or Send SMS or Text Message). Sentinet Alerting System can be integrated with third party and industry standard Operations Management Systems (for example: Microsoft SCOM).

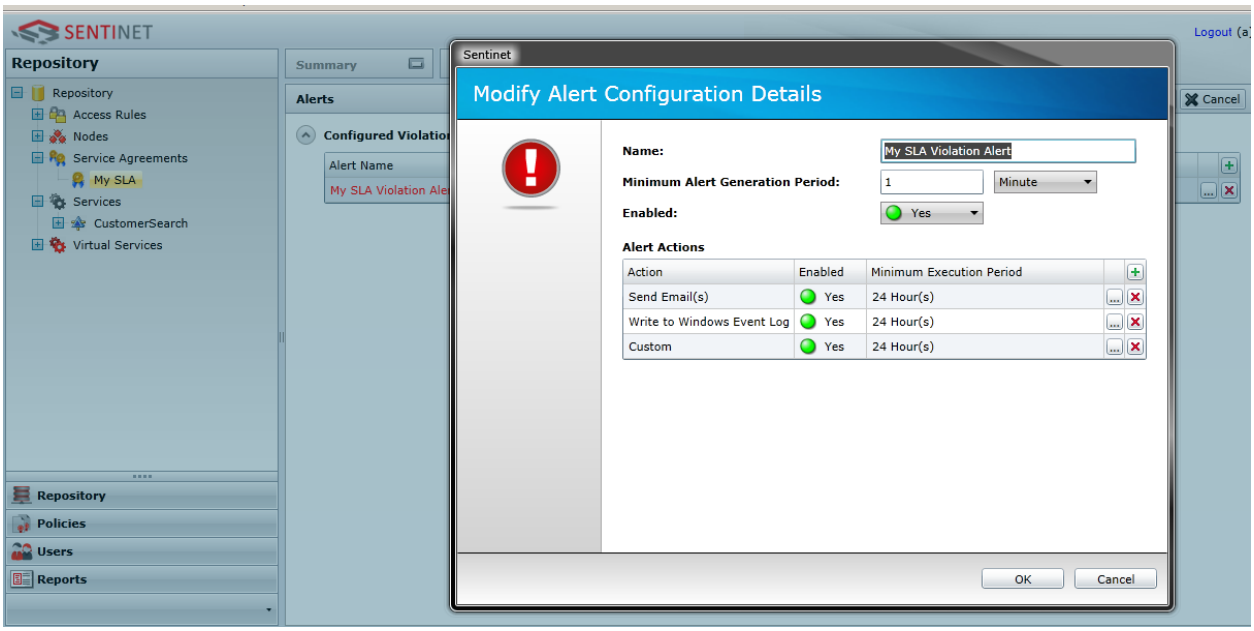

Figure 19. Sample SLA Alert Configuration.

Testing

Sentinet provides non-intrusive automated testing and service-mockup capabilities. These features make developers more productive by allowing them to create both parallel and isolated development and test processes. Developers and administrators can test their services performance and security even before services concrete implementations are available. Sentinet helps to simulate and predict production systems behaviors before they are deployed in real environments.

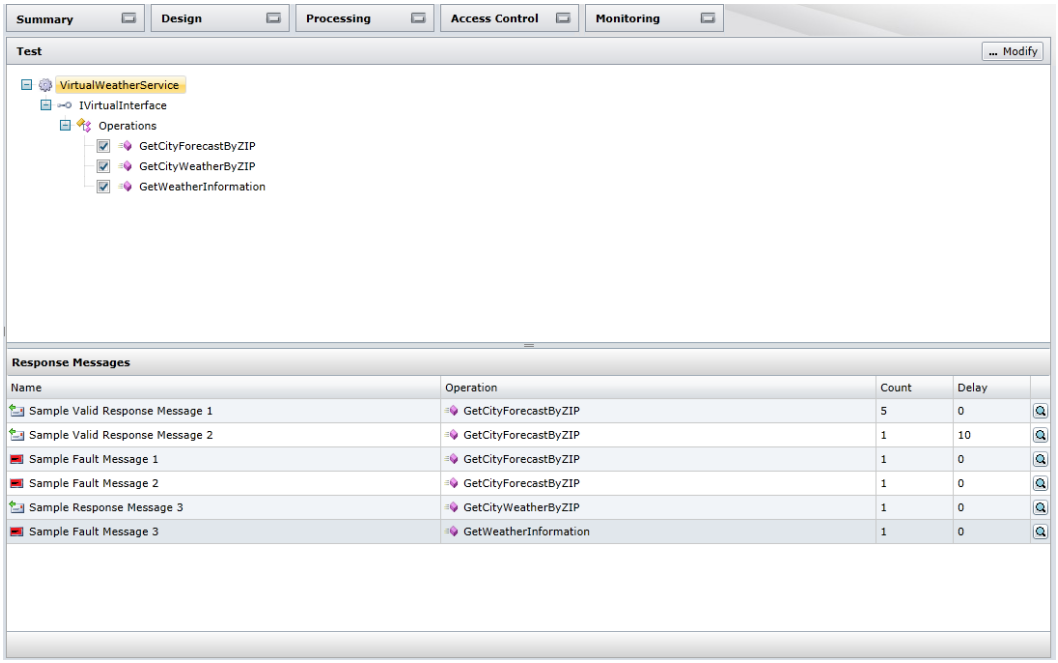

Figure 20. Sample Response Test Messages.