SENTINET

Sentinet for BizTalk Server

VERSION 2.2

Nevatech

Contents

Introduction

BizTalk Server is Microsoft's Integration and connectivity server solution. BizTalk Server provides a solution that allows organizations to more easily connect disparate systems. Including over 25 multi-platform adapters and a robust messaging infrastructure, BizTalk Server provides connectivity between core systems both inside and outside your organization. In addition to integration functionality, BizTalk also provides strong durable messaging, a rules engine, EDI connectivity, Business Activity Monitoring (BAM), RFID capabilities and IBM Host/Mainframe connectivity.

Nevatech's Sentinet™ platform, a generic SOA Management Infrastructure and services virtualization middleware software solution, helps organizations to manage SOA solutions during their entire life-cycle. Sentinet is the only SOA management Infrastructure that is non-invasive and developed entirely on a Microsoft platform. It is certified for ***Works for Windows 2008 R2 Server***, ***Certified for Windows Server 2012*** and ***Powered by Windows Azure***. Sentinet fully integrates with Microsoft technologies and server products, extends their capabilities, and simplifies SOA solutions' development and operational processes and procedures.

Sentinet provides particular benefits to SOA solutions built on, or integrated with, the Microsoft BizTalk Server platform. Most of the BizTalk integration solutions are based on communication protocols that utilize BizTalk Server SOAP, WCF and WCF LOB web service Adapters. Sentinet provides these solutions with dynamic and remote management of security, monitoring, auditing, service agreements management, alerting and other vital SOA management features via non-invasive services virtualization. Developers benefit from using Sentinet platform by ensuring their BizTalk services are implemented, debugged and tested according to specified security and performance requirements. Sentinet decouples development and deployment efforts from common infrastructural challenges such as security, authentication, authorization and monitoring. Sentinet provides the BizTalk application with agility to adapt to changing deployment requirements without reconfigurations or redeployments of the actual BizTalk applications or application artifacts. Operations team benefit from the Sentinet platform by ensuring BizTalk production services and applications are secured, monitored, audited, alerted on, and satisfy performance and availability metrics defined by the Sentinet SLAs. Sentinet extends BizTalk capabilities to communicate with interoperable and non-interoperable external and internal systems more effectively.

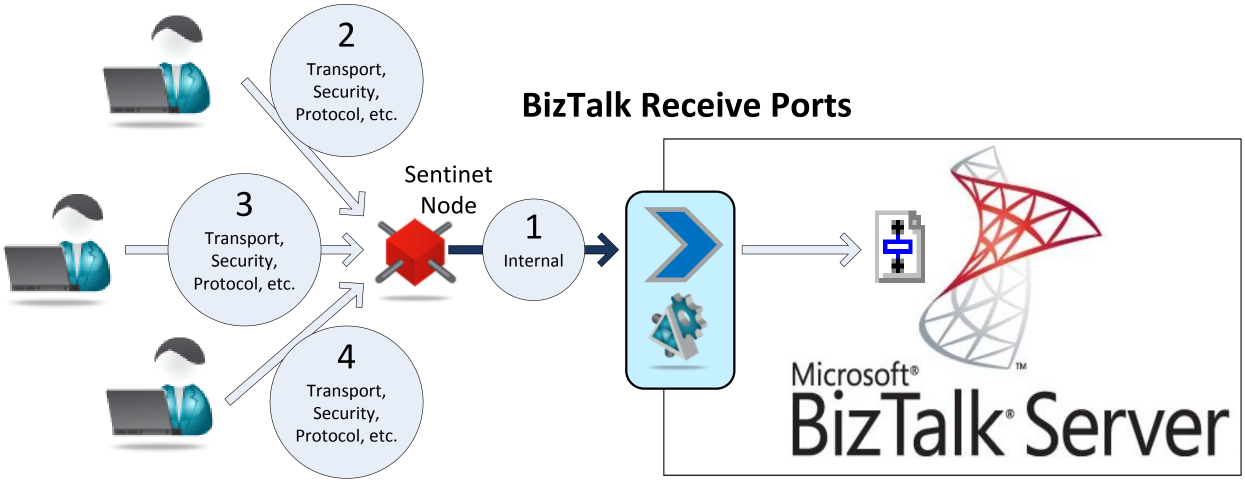
SOA Repository

Sentinet extends BizTalk solutions with generic SOA Repository that provides centralized, hierarchical and secure storage for all SOA software assets, such as services, security policies, metadata, authentication/authorization and access control rules, service agreements definitions, 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. Sentinet administrators access SOA Repository by using Sentinet Administrative Console to discover and manage BizTalk services and their metadata, BizTalk security and access rules, and to monitor the real-time operational environment. BizTalk applications and those that integrate with BizTalk Server, can access Sentinet Repository programmatically by leveraging the interoperable Sentinet Web Service API.

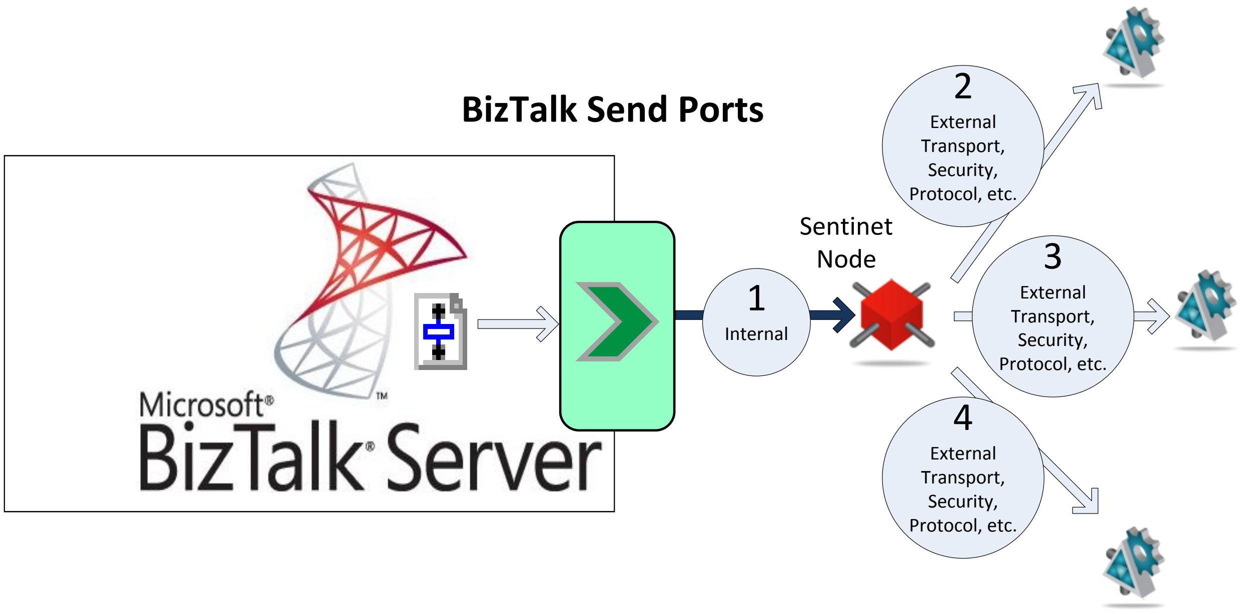
Security

Mediation and Virtualization

BizTalk services and applications leverage Sentinet Nodes to mediate and implement managed security. BizTalk Server receive ports can be configured with a unified and standardized WCF adapter configuration, and then exposed to consumer applications as Sentinet dynamic virtual services by using transport and security models that satisfy the ultimate security and communication requirements. For example, all BizTalk application's ports can be configured with *WCF-NetTcp* or *WCF-WSHttp* adapter with Windows Integrated ("internal") security, and then they can be exposed to consumer applications via Sentinet virtual endpoints that may require a Username/Password, X.509 or SAML based authentication (or all of the above at the same time) using variety of transport and message-level security models. Administrators use Sentinet Administrative Console, a browser-based Silverlight application, to create and remotely manage virtual services hosted on Sentinet Nodes. Effectively, BizTalk applications deployed in development, test and production environments are decoupled from specific knowledge of the ultimate communication and security requirements.


2
Transport, Security, Protocol, etc.
BizTalk Receive Ports
Sentinet Node
3
Transport, Security, Protocol, etc.
1
Internal
4
Transport, Security, Protocol, etc.
Microsoft® BizTalk® Server™

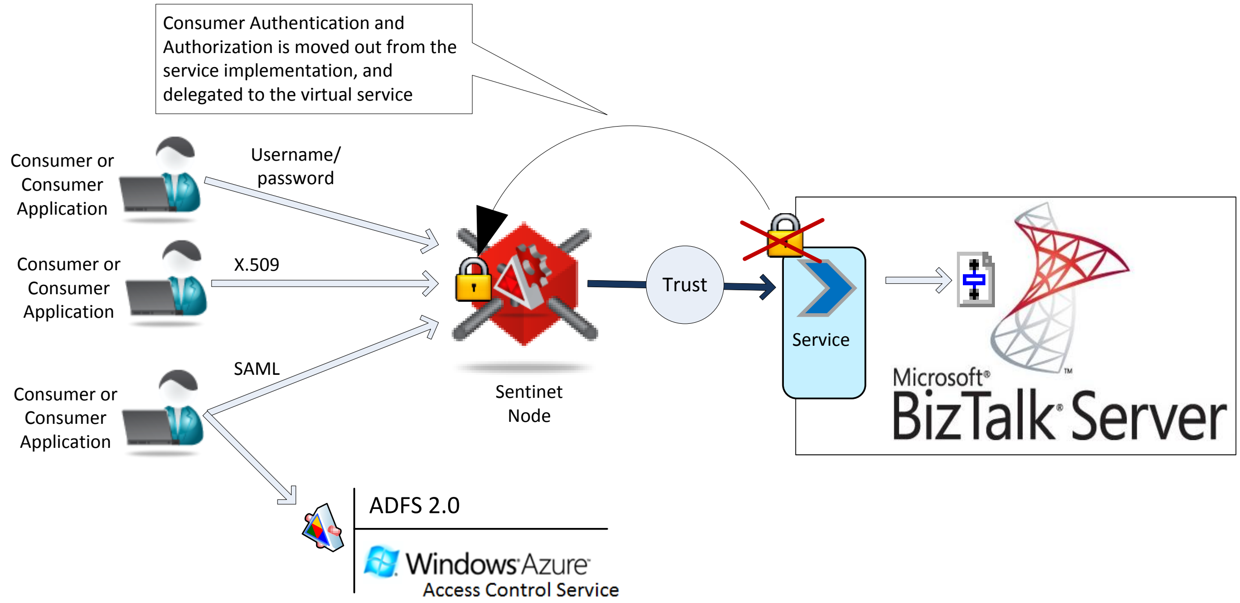
Similar benefits apply to BizTalk applications that consume external services. BizTalk Send ports do not have to be enabled with the knowledge of specific communication and security requirements imposed by external services. BizTalk Send ports no longer have to be configured with specific consumer identities that are expected by the external services. All of these infrastructural challenges are fully delegated to the Sentinet Nodes that mediate and route messages to external services.


BizTalk Send Ports
Microsoft® BizTalk® Server™
Sentinet Node
1
Internal
2
External Transport, Security, Protocol, etc.
3
External Transport, Security, Protocol, etc.
4
External Transport, Security, Protocol, etc.

Sentinet software platform supports the industry standard and all Microsoft-specific communication and security protocols, and can mediate between interoperable and Microsoft-specific message exchanges.

Authentication and Authorization

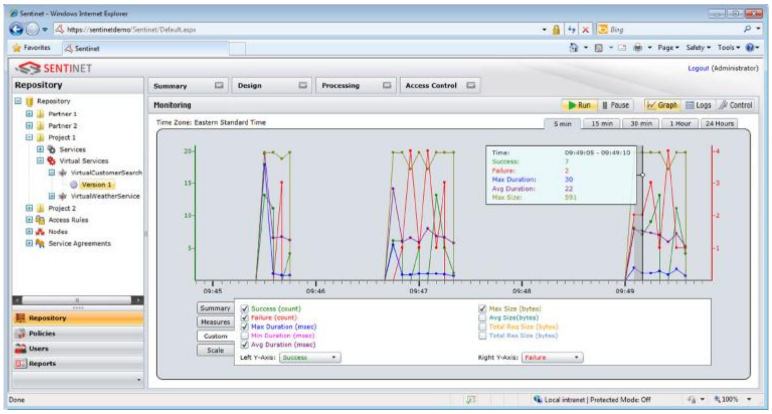
BizTalk applications can be decoupled from authentication and authorization decisions by delegating these tasks to Sentinet Nodes. An explicit trust relationship can be established between BizTalk Server and Sentinet Nodes where all messages pre-authenticated and pre-authorized by a Sentinet Node will be automatically trusted by the BizTalk Server application. BizTalk Server application and services can be deployed with the unified security and identity requirements that only authorized and authenticated Sentinet Nodes can satisfy. By leveraging Sentinet, BizTalk services can be enabled to understand and process SAML claims in Federated Security scenarios.


Consumer Authentication and Authorization is moved out from the service implementation, and delegated to the virtual service
Consumer or Consumer Application
Username/ password
Consumer or Consumer Application
X.509
Consumer or Consumer Application
SAML
Sentinet Node
Trust
Service
Microsoft® BizTalk® Server™
ADFS 2.0
Windows Azure Access Control Service

Implementing Authorization rules within BizTalk application is a very challenging task that does not scale well with the growing number of services and applications. Sentinet absorbs critical authorization challenges. Administrators can create, modify and apply sophisticated and extendable authorization rules dynamically and remotely, without reconfiguring or redeploying BizTalk Server applications and artifacts. Sentinet Authorization Engine executes at the Sentinet Nodes where it enforces custom authorization rules designed by the Sentinet administrators.

Monitoring, Recording and Service Agreements Management

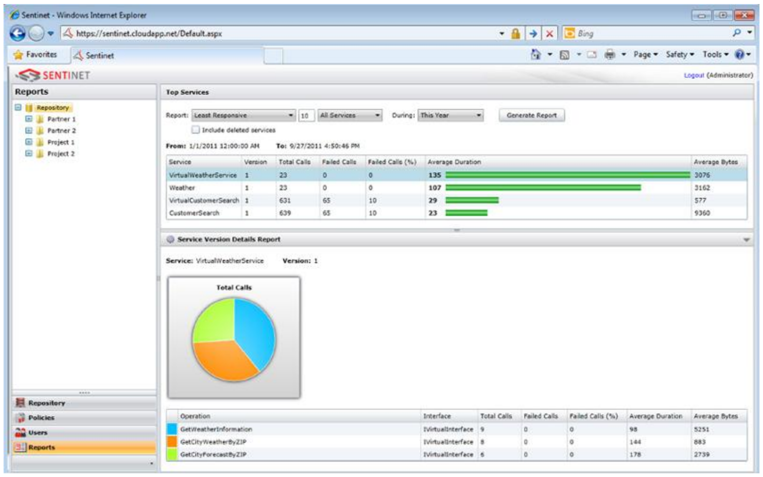
In addition to virtualization, Sentinet provides BizTalk applications with a wide array of non-invasive enabling capabilities including monitoring, recording and auditing, dynamic alerts, SLAs management, real-time and historical reporting. Sentinet enables BizTalk solutions with full visibility and analysis of who is using BizTalk services, when, and how. Sentinet SLAs can be created per individual consumer identity or consumer application, and validated against configurable performance, traffic volume and service availability metrics. Multiple services can be covered by a single SLA.



Time: 09:49:05 - 09:49:10
Success: 7
Failure: 2
Max Duration: 30
Avg Duration: 22
Max Size: 591

☑ Success (count)
☑ Failure (count)
☑ Max Duration (msec)
☐ Min Duration (msec)
☑ Avg Duration (msec)
☑ Max Size (bytes)
☐ Avg Size(bytes)
☐ Total Req Size (bytes)
☐ Total Res Size (bytes)

Left Y-Axis: Success
Right Y-Axis: Failure



Top Services

Report: Least Responsive 10 All Services During: This Year

☐ Include deleted services

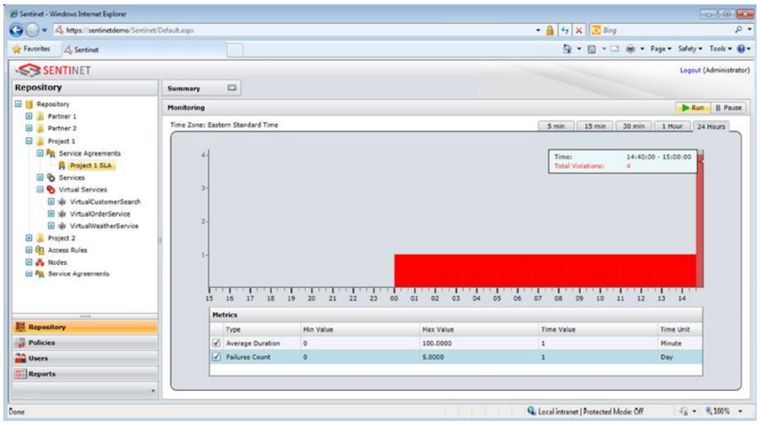
From: 1/1/2011 12:00:00 AM To: 9/27/2011 4:50:46 PM

Service	Version	Total Calls	Failed Calls	Failed Calls (%)	Average Duration	Average Bytes
VirtualWeatherService	1	23	0	0	135	3076
Weather	1	23	0	0	107	3162
VirtualCustomerSearch	1	631	65	10	29	577
CustomerSearch	1	639	65	10	23	9360

Service Version Details Report

Service: VirtualWeatherService Version: 1

	Operation	Interface	Total Calls	Failed Calls	Failed Calls (%)	Average Duration	Average Bytes
🟦	GetWeatherInformation	IVirtualInterface	9	0	0	98	5251
🟧	GetCityWeatherByZIP	IVirtualInterface	8	0	0	144	883
🟩	GetCityForecastByZIP	IVirtualInterface	6	0	0	178	2739



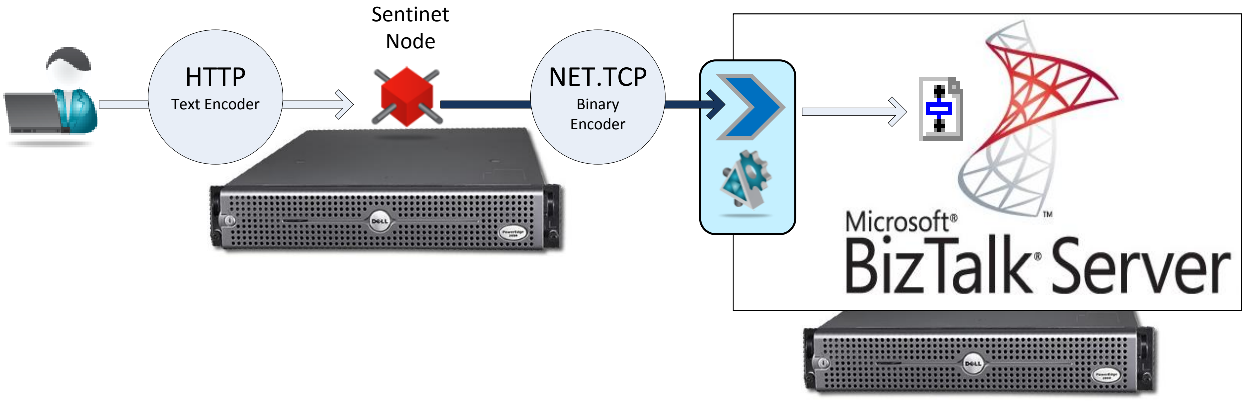
Metrics

	Type	Min Value	Max Value	Time Value	Time Unit
☑	Average Duration	0	100.0000	1	Minute
☑	Failures Count	0	5.0000	1	Day

Deployment Topologies

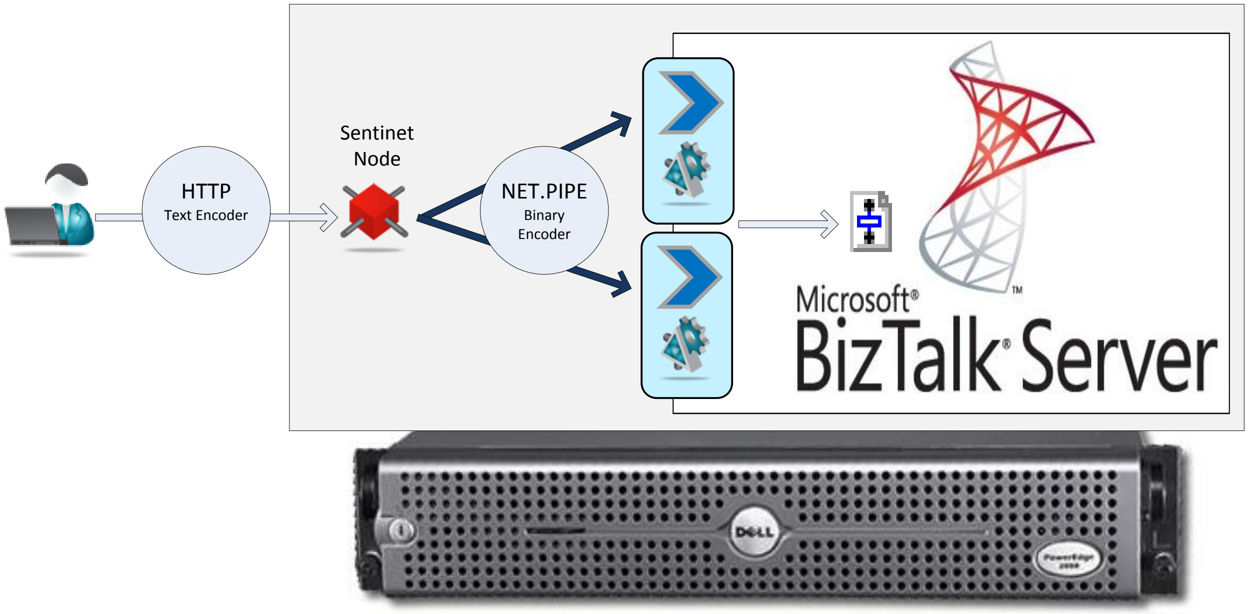
Isolated Deployment

Sentinet Nodes are typically deployed as security gateways (or stand-alone network intermediaries). Additional network latencies introduced by a network intermediary are negligible compared to BizTalk Server persistent messaging delivery. Latencies can be further minimized by leveraging optimized network communication protocols, for example *net.tcp* transport with binary encoder.

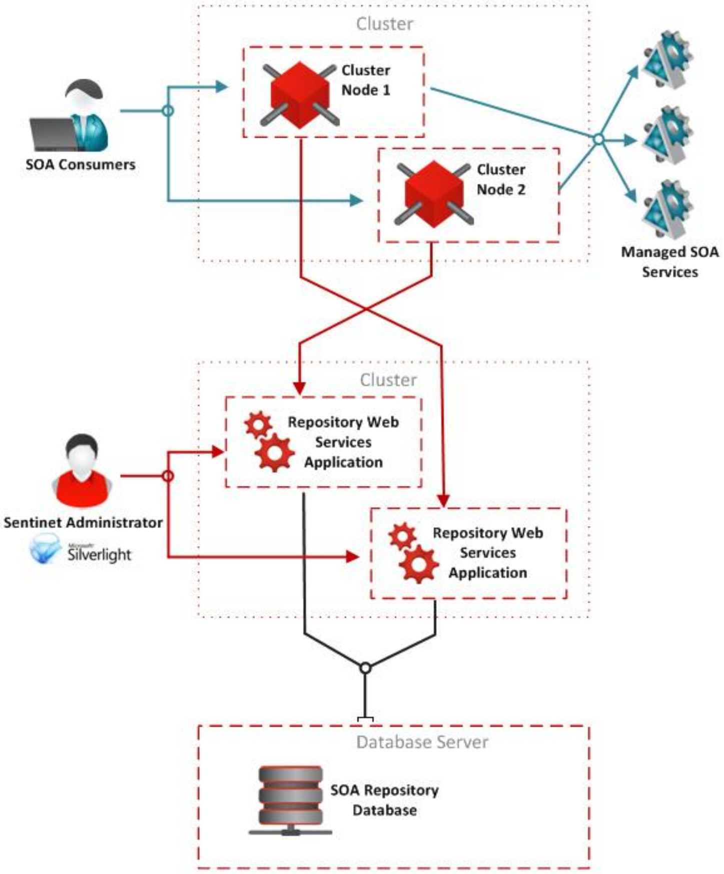


Collocated Deployment

Sentinet Node is particularly effective when it is deployed side-by-side with BizTalk IIS Server isolated hosts. In this case BizTalk ports and locations can be configured with inter-process communication via *WCF-NetNamedPipe* adapter, where Sentinet Node routes messages to local BizTalk services via *net.pipe* transport. By using *net.pipe* transport BizTalk applications are guaranteed to be secure (services cannot be accessed from other computers, unless they are accessed through a Sentinet Node), and there are no additional network latencies because *net.pipe* transport is the most effective local cross-process communication.



Sentinet fully supports high-availability redundant deployment topologies.



BizTalk Server and Windows Azure Cloud Platform

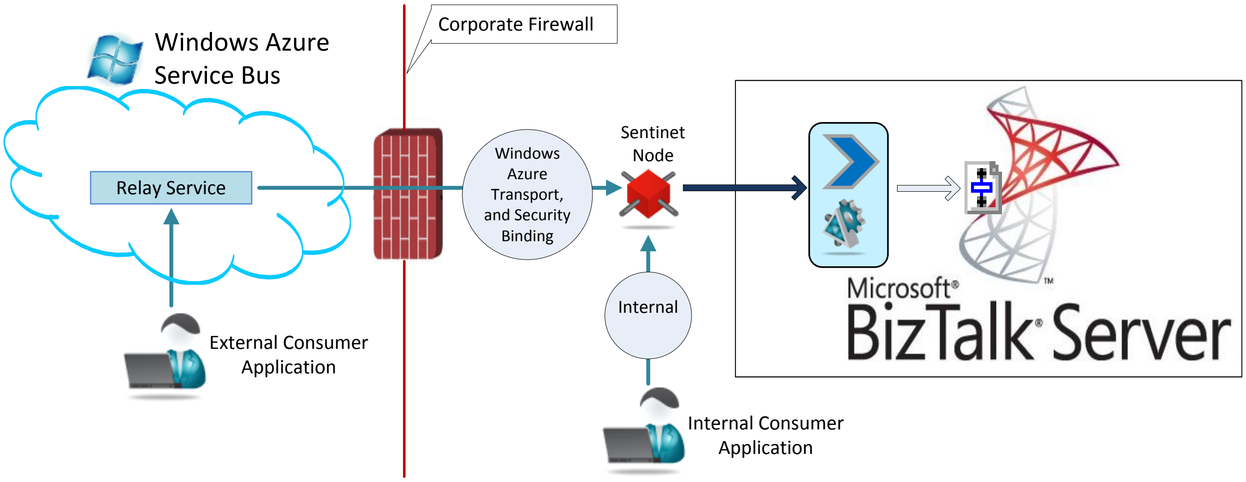
Integration with Windows Azure Service Bus Relay

Sentinet platform extends BizTalk Server capabilities through the Windows Azure cloud platform. Sentinet provides BizTalk with easy interactions to external parties you need to integrate with, without needing complex firewall and security infrastructure. Sentinet Nodes are designed to natively integrate with Windows Azure Service Bus and Windows Azure Access Control Service. Sentinet Nodes can be dynamically and remotely configured with Azure Service Bus endpoints, encapsulating Service Bus non-interoperable protocols and Windows Azure ACS security identities.

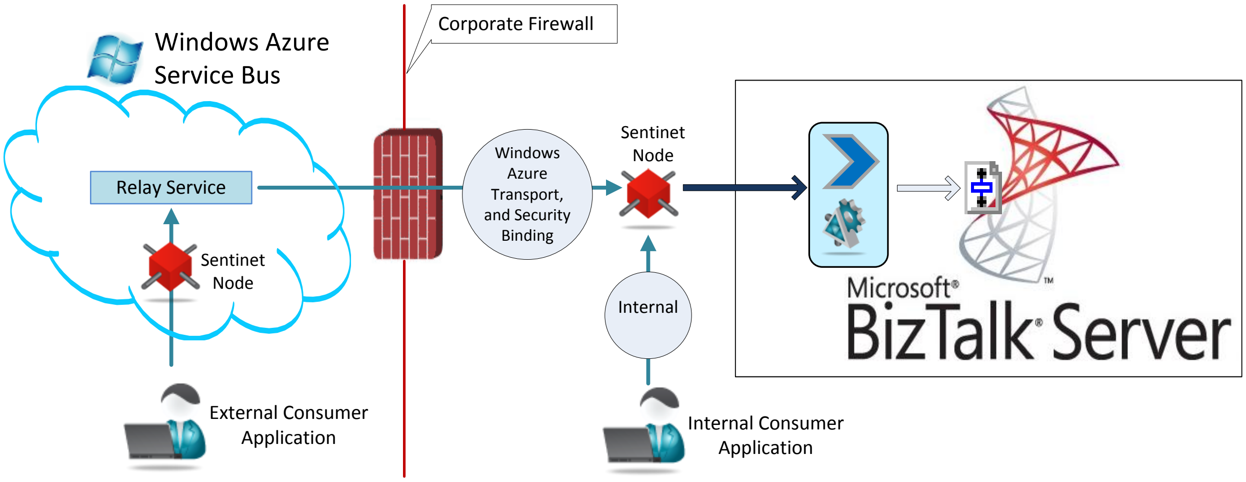
In order to join Windows Azure Service Bus infrastructure, BizTalk services have to be reconfigured to use special WCF bindings (via *WCF-Custom* or *WCF-CustomIsolated* adapters' configurations), and configured with Windows Azure subscription's security keys, which is neither a scalable deployment model nor sufficiently secure (all ports have to be given knowledge of all the subscription security keys).

As stated by Microsoft Customer Advisory team (http://windowsazurecat.com/2010/08/leveraging-wcf-extensibility-to-simplify-secure-integration-of-biztalk-server-with-windows-azure-service-bus/), the challenge is that "in a complex composite application that involves both a BizTalk and a Cloud element of the solution architecture, the number of friction points that define how these solution elements interoperate with each other can be substantial. For example, there may well be a large number of Receive Ports configured in the BizTalk environment, each servicing different needs and exposing distinct service contracts. In addition, the on-premise BizTalk solution may be communicating through the Service Bus with a number of services each requiring a dedicated Send Port configured with WCF-Custom adapter and appropriate Service Bus WCF binding."

By using Sentinet software platform, any service (including BizTalk service), can be on-boarded onto Windows Azure Service Bus infrastructure without any reconfigurations, redeployments or potential security keys compromises. Sentinet administrators can remotely configure Sentinet Nodes to dynamically open and manage Windows Azure Service Bus endpoints and authenticate virtual services with the Windows Azure ACS service. Service Bus security keys are stored in the central Sentinet SOA Repository and securely delivered to the Sentinet Nodes when they have to open Windows Azure Service Bus endpoints. Moreover, Sentinet Nodes can be configured side-by-side with Windows Azure Service Bus endpoints and additional internal endpoints, for testing and staging. Sentinet Administrators get full visibility and control over endpoints exposed via Windows Azure Service Bus, and can remotely and dynamically take Service Bus endpoints offline or reconfigure them with new or additional security, access rules, monitoring and SLAs.

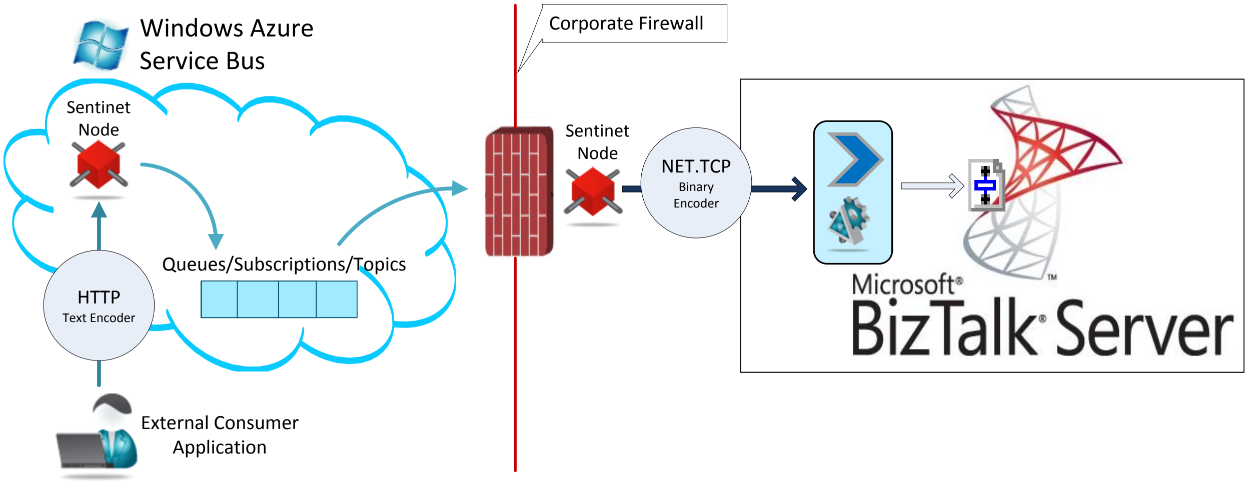

Windows Azure Service Bus
Corporate Firewall
Relay Service
Windows Azure Transport, and Security Binding
Sentinet Node
Internal
External Consumer Application
Internal Consumer Application
Microsoft® BizTalk® Server™

Sentinet Nodes can also be deployed in the hybrid deployment scenarios, where some Nodes are deployed on-premises while others are in the cloud. Both consumer and service applications can be fully decoupled from Windows Azure Service Bus specific APIs and security configurations.


Windows Azure Service Bus
Corporate Firewall
Relay Service
Sentinet Node
Windows Azure Transport, and Security Binding
Sentinet Node
Internal
External Consumer Application
Internal Consumer Application
Microsoft® BizTalk® Server™

Integration with Windows Azure Asynchronous Queuing

Sentinet provides BizTalk SOA solutions with asynchronous messaging with automatic load-leveling by tightly integrating with Windows Azure Queues, Topics and Subscriptions. Consumer applications and BizTalk Server applications can be completely decoupled from the knowledge and mechanics of Windows Azure queuing while staying enabled to handle load-leveling with asynchnonous messages delivery.


Windows Azure
Service Bus
Sentinet
Node
Queues/Subscriptions/Topics
HTTP
Text Encoder
External Consumer
Application
Corporate Firewall
Sentinet
Node
NET.TCP
Binary
Encoder
Microsoft®
BizTalk® Server™