SOLARWINDS WHITEPAPER

IT Management System Scalability for the Enterprise

Author: Vinod Mohan

Follow SolarWinds:

solarwinds

Introduction

Your IT infrastructure is constantly evolving and growing and with that, you need to ensure that your monitoring system has the capability to scale along with your environment. Considering the dependency of the business on network infrastructure, it's the responsibility of the network, systems, and IT teams to work toward providing uninterrupted business services by ensuring availability and performance of the network and IT infrastructure. Regardless of what type of business you are running—small, mid-sized, or large enterprises; whether you are an MSP or a federal or state agency—infrastructure expansion means more IT expenditure, more network devices, servers and applications to manage, more issues to fix, and more staff personnel for support. This is definitely not an easy challenge to tackle, especially when you haven't prepared for growth. Taking all of these factors into account, it's easy to see how critical it is for IT administration teams to proactively plan for and accommodate the various aspects of growth without impacting business services and causing network implications for the end-users.

As your environment grows, it becomes more and more important that you have a monitoring and management system that can scale alongside this growth. Monitoring and management scalability means preparing your implementation to support IT infrastructure monitoring of your growing network devices, applications, servers and other aspects of network growth.

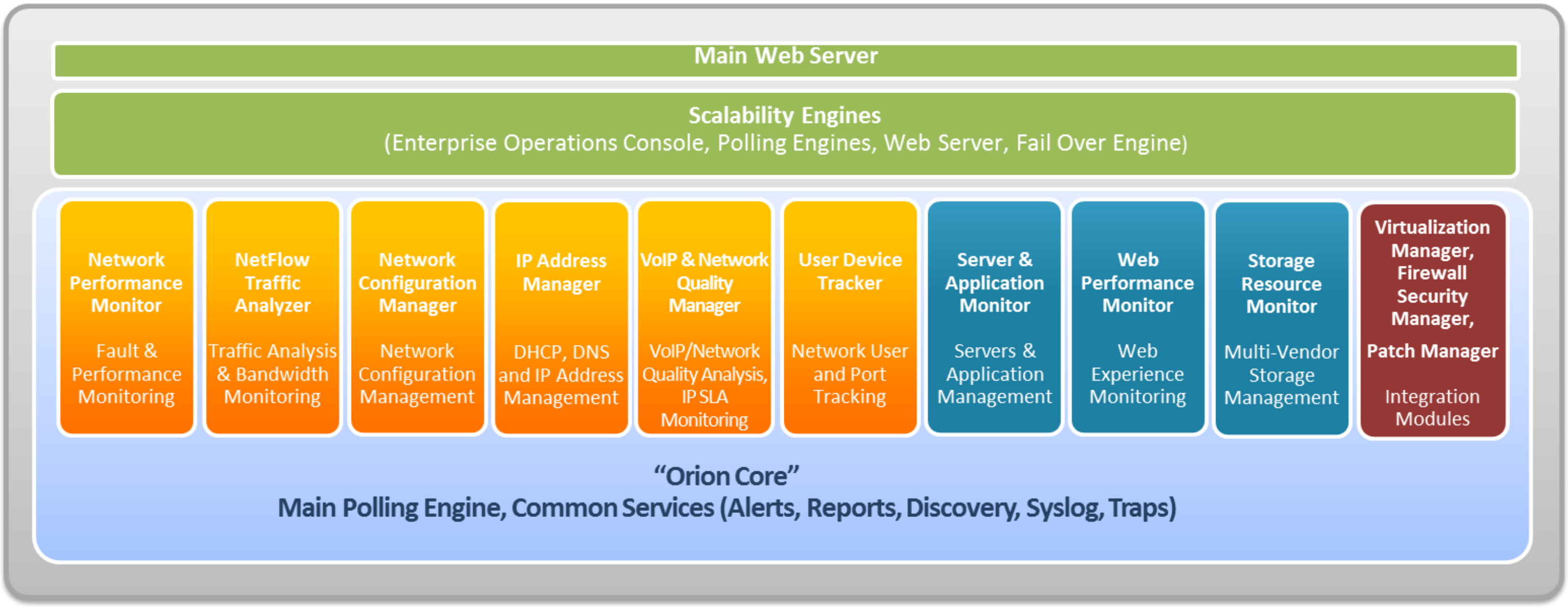
What to Expect from this White Paper?

If you are a user of SolarWinds® Network Performance Monitor (NPM), or other network management and application & server management software from SolarWinds, this white paper will provide you information on various types of SolarWinds Orion® deployments for different network requirements and scalability options.

If you're evaluating IT management solutions for your enterprise and are considering the aspects of scalability, this paper will help you understand how SolarWinds will support your growth and ensure you are prepared to meet different architectural and infrastructural requirements and monitoring system failover scenarios.

Before We Discuss Scalability, What Is the SolarWinds Orion® Platform?

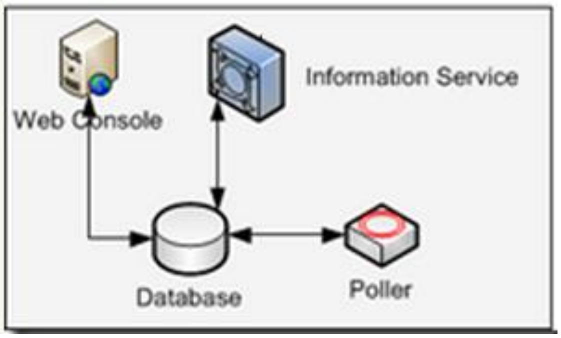
SolarWinds Orion is a suite of IT management products sharing common services such as alerting, reporting, intuitive dashboards and charts, Web interface, and database. The architecture diagram below lists all Orion platform modules and some other modules that are not part for Orion, but still integrate with the platform for comprehensive IT management.


Main Web Server
Scalability Engines
(Enterprise Operations Console, Polling Engines, Web Server, Fail Over Engine)
Network Performance Monitor
Fault & Performance Monitoring
NetFlow Traffic Analyzer
Traffic Analysis & Bandwidth Monitoring
Network Configuration Manager
Network Configuration Management
IP Address Manager
DHCP, DNS and IP Address Management
VoIP & Network Quality Manager
VoIP/Network Quality Analysis, IP SLA Monitoring
User Device Tracker
Network User and Port Tracking
Server & Application Monitor
Servers & Application Management
Web Performance Monitor
Web Experience Monitoring
Storage Resource Monitor
Multi-Vendor Storage Management
Virtualization Manager, Firewall Security Manager,
Patch Manager
Integration Modules
"Orion Core"
Main Polling Engine, Common Services (Alerts, Reports, Discovery, Syslog, Traps)

What Comprises IT Management Scalability?

The Orion platform is based around:

- A server that hosts the monitoring product and polls for status and performance
- A database where the polled information is stored for historical data access and reporting
- An information service (IS) which will provide a single point of communication and query the servers
- A Web console for software management and data visualization and reporting



SolarWinds Network Performance Monitor (NPM) Architecture

Three Primary Variables that Affect IT Management System Scalability

1. **Infrastructure size**: The most important factor is the number of monitored elements (where an element is defined as a single, identifiable node, interface, or volume) or the number of servers and applications to be monitored
2. **Polling frequency**: This defines the interval in which the monitoring system polls for information. For example, if you are collecting statistics every few minutes, the system will have to work harder and system requirements will increase.
3. **Number of simultaneous users accessing the monitoring system:** This directly impacts system performance.

Additional Polling Engine for Load Balancing

The number of network elements monitored and the data polling frequency are some key determinants of the polling capacity of a monitoring system. Additional polling engines will help distribute the polling load for your monitoring system between multiple servers to provide scalability for large networks. Having additional polling engines will also reduce the impact on monitoring system's core poller performance due to rapid growth within your network infrastructure.

You can add Additional Polling Engine to a centralized single SolarWinds instance, or add pollers for a geographically distributed Orion deployment with either a single Orion server instance or multiple instances.

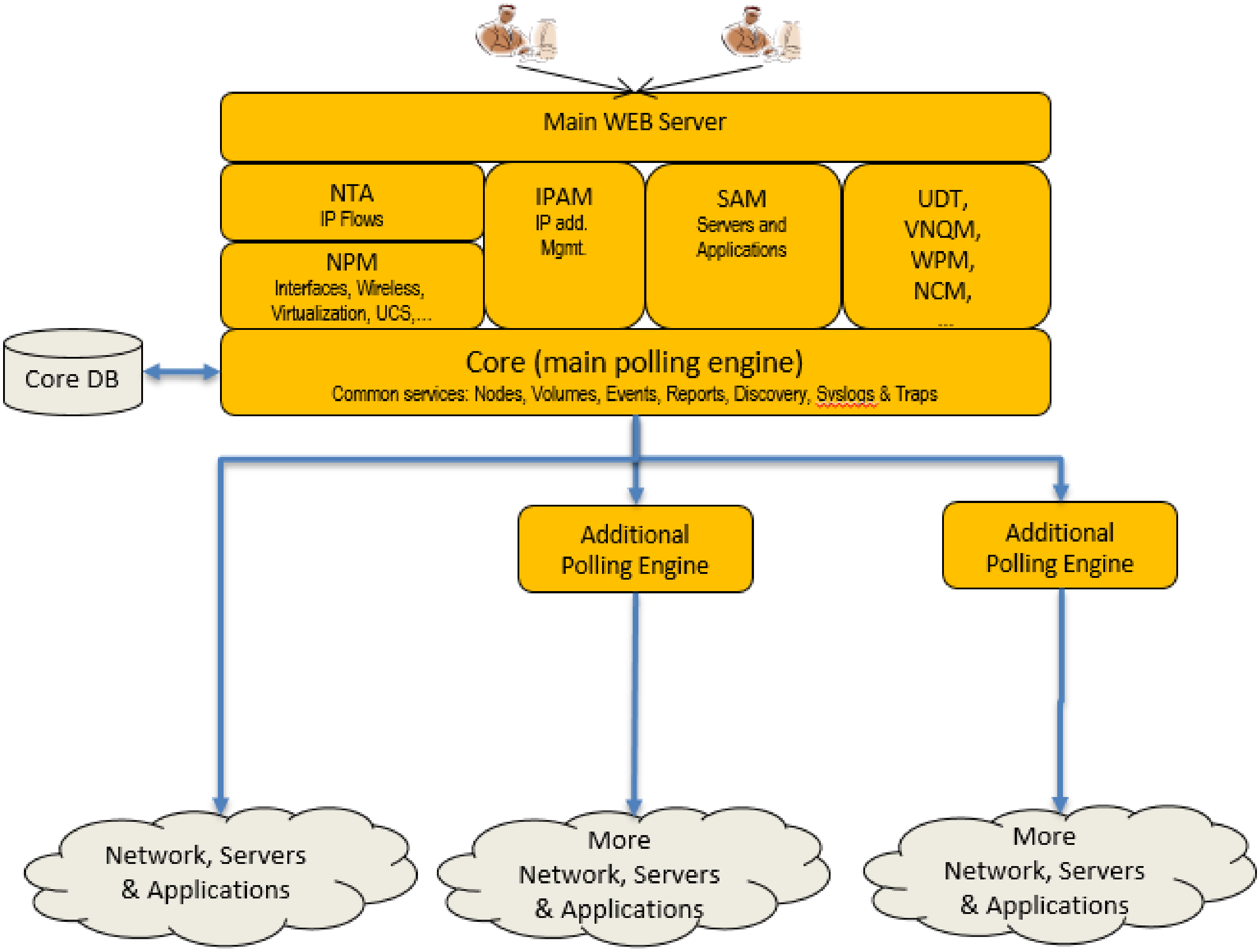
Web Access Scalability

The number of simultaneous users accessing the monitoring system can degrade performance if your Web server deployment is not able to handle the load. You need to be certain you can support the growing number of concurrent sessions by adding additional Web Servers. This will ensure uninterrupted Web access and control to more users to concurrently manage and work with your network monitoring software.

Let's now discuss the various deployment options available with SolarWinds IT management software that will help you scale up according to your the needs of your network expansion.

Growing a Single SolarWinds Instance to Support Larger Networks

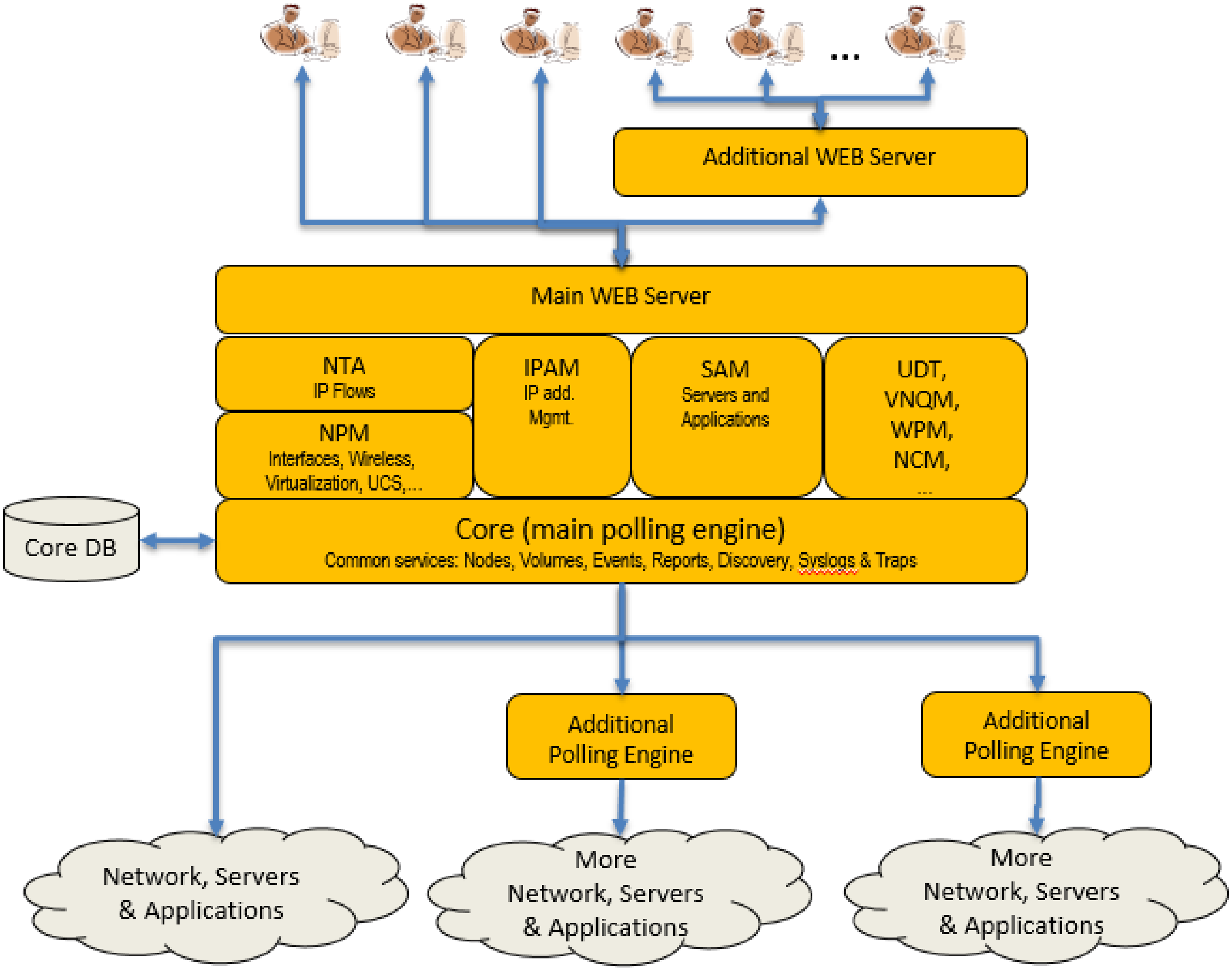
Most deployments are based on a single product instance that monitors the infrastructure or applications. As your IT environment grows, you may find that you are no longer able to monitor everything you would like at your desired polling frequency. In this case, you can deploy an Additional Polling Engine (APE) to reduce the load on the main polling engine. The data polled by the APE will be stored in the core database along with the data from the main polling engine.


Main WEB Server
NTA
IP Flows
IPAM
IP add. Mgmt.
SAM
Servers and Applications
UDT, VNQM, WPM, NCM, ...
NPM
Interfaces, Wireless, Virtualization, UCS,...
Core DB
Core (main polling engine)
Common services: Nodes, Volumes, Events, Reports, Discovery, Syslogs & Traps
Additional Polling Engine
Additional Polling Engine
Network, Servers & Applications
More Network, Servers & Applications
More Network, Servers & Applications

This type of installation allows you to have a centralized deployment of your monitoring software and combines the data polled from different APEs with the core database for centralized data access.

Scalability to Support User Growth

As mentioned earlier in the paper, the number of simultaneous users accessing the Web console can have a direct impact on the performance of the system. If you have more than 20 users accessing the Web console simultaneously, then SolarWinds recommends the installation of an additional Web server that will load balance the number of concurrent users.

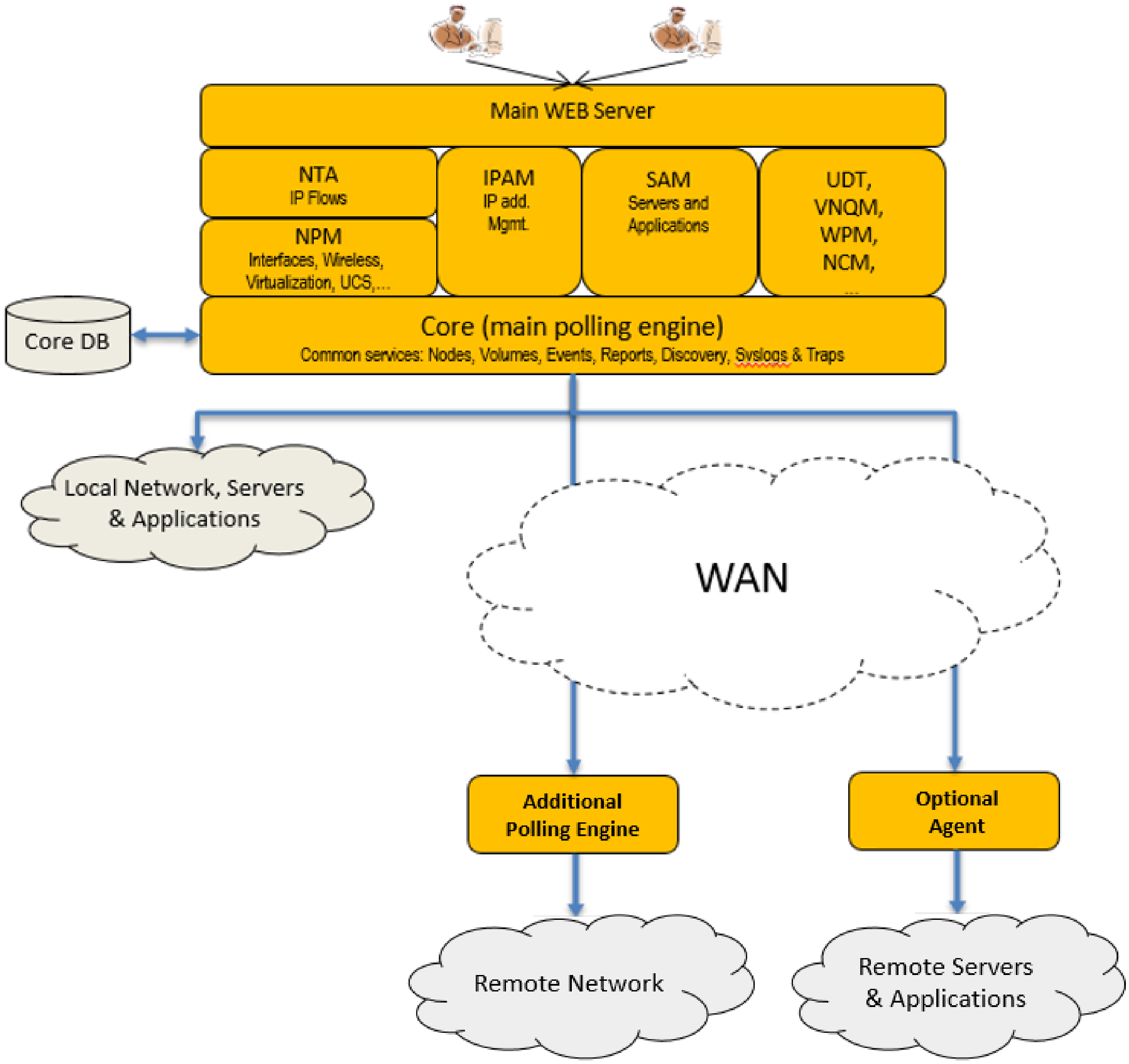


...
Additional WEB Server
Main WEB Server
NTA
IP Flows
NPM
Interfaces, Wireless, Virtualization, UCS,...
IPAM
IP add. Mgmt.
SAM
Servers and Applications
UDT, VNQM, WPM, NCM, ...
Core DB
Core (main polling engine)
Common services: Nodes, Volumes, Events, Reports, Discovery, Syslogs & Traps
Additional Polling Engine
Additional Polling Engine
Network, Servers & Applications
More Network, Servers & Applications
More Network, Servers & Applications

Monitoring Geographically Distributed Environments with a Single SolarWinds Instance

This is similar to the previous scalability scenario with the difference being that the SolarWinds product is deployed in the primary location, and Additional Polling Engines are deployed in the geographically distributed regions. This type of deployment helps to cover monitoring a distributed network with just a single SolarWinds Orion instance.

This scalability option is well suited for environments where most of the monitored nodes or applications are located in a single primary region and where other remote offices are much smaller. Here, all the additional Polling Engines are connected to the single centralized SolarWinds instance.


Main WEB Server
NTA
IP Flows
NPM
Interfaces, Wireless, Virtualization, UCS,...
IPAM
IP add. Mgmt.
SAM
Servers and Applications
UDT, VNQM, WPM, NCM,
...
Core DB
Core (main polling engine)
Common services: Nodes, Volumes, Events, Reports, Discovery, Syslogs & Traps
Local Network, Servers & Applications
WAN
Additional Polling Engine
Optional Agent
Remote Network
Remote Servers & Applications

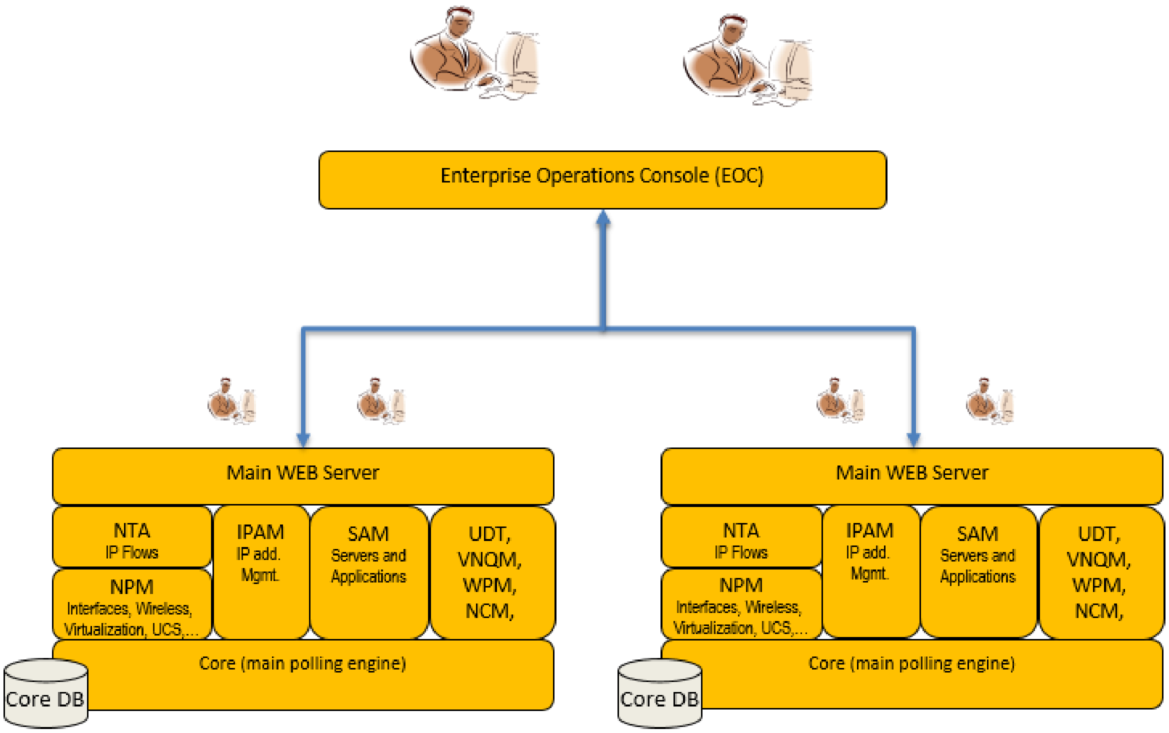
Monitoring Geographically Distributed Environments with Multiple SolarWinds Instances

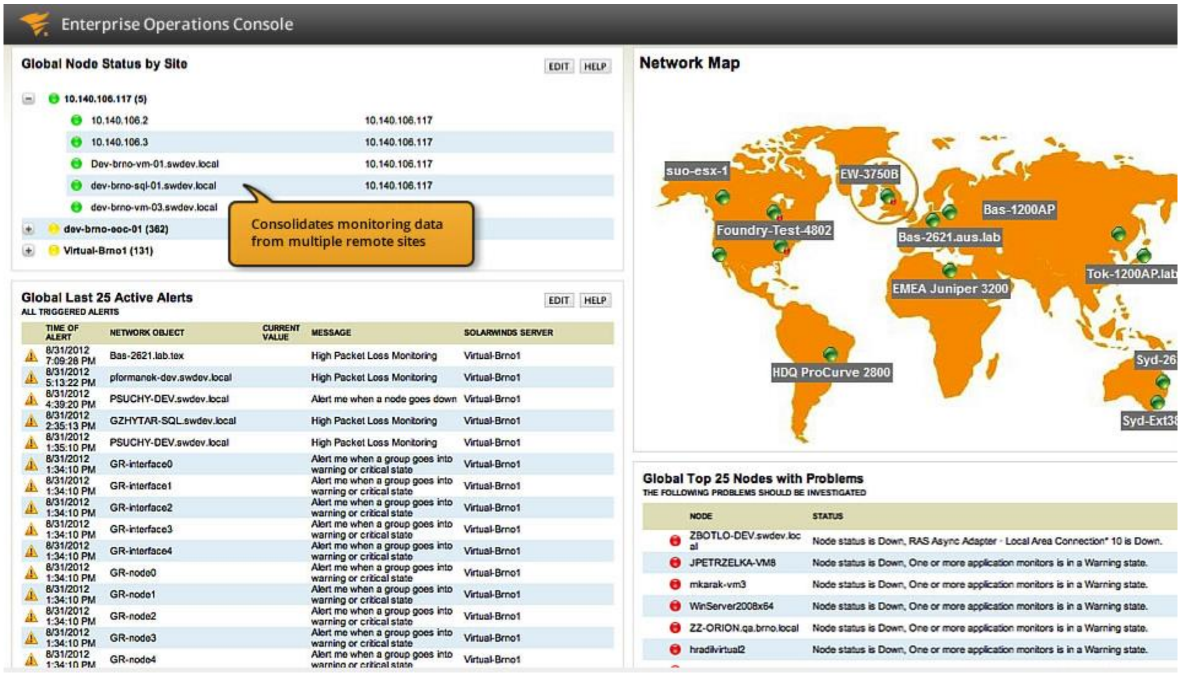
It's possible to have multiple instances of SolarWinds deployed in different geographical locations and rolled up into a single view. Though the polling operations and database storage of each instance would be different, SolarWinds provides a solution to centralize and simplify data management in a single consolidate view with SolarWinds Enterprise Operations Console (EOC).

This type of deployment option is well suited to organizations with multiple regions or sites where the quantity of nodes to be monitored in each region would warrant both localized data collection and storage. It works well when there are regional teams responsible for their own environments and when regional teams need autonomy over their monitoring platform, preferring not to share a single Orion instance. This option gives regional operators autonomy as well as the ability to have different modules and license sizes installed in each region to match individual requirements. While the systems are segregated between regions, all data can still be accessed from the centrally located SolarWinds EOC.

What is SolarWinds Enterprise Operations Console?

SolarWinds EOC delivers a command center for monitoring your enterprise-wide network health, providing a single interactive screen that aggregates data from multiple SolarWinds Orion-based deployments. This simplifies the management of large, distributed networks by providing a unified view into the performance of your network and also accelerates your ability to identify and resolve issues.





Global Node Status by Site

- 10.140.106.117 (5)
  - 10.140.106.2 — 10.140.106.117
  - 10.140.106.3 — 10.140.106.117
  - Dev-brno-vm-01.swdev.local — 10.140.106.117
  - dev-brno-sql-01.swdev.local — 10.140.106.117
  - dev-brno-vm-03.swdev.local
- dev-brno-eoc-01 (362)
- Virtual-Brno1 (131)

Consolidates monitoring data from multiple remote sites

Global Last 25 Active Alerts
ALL TRIGGERED ALERTS

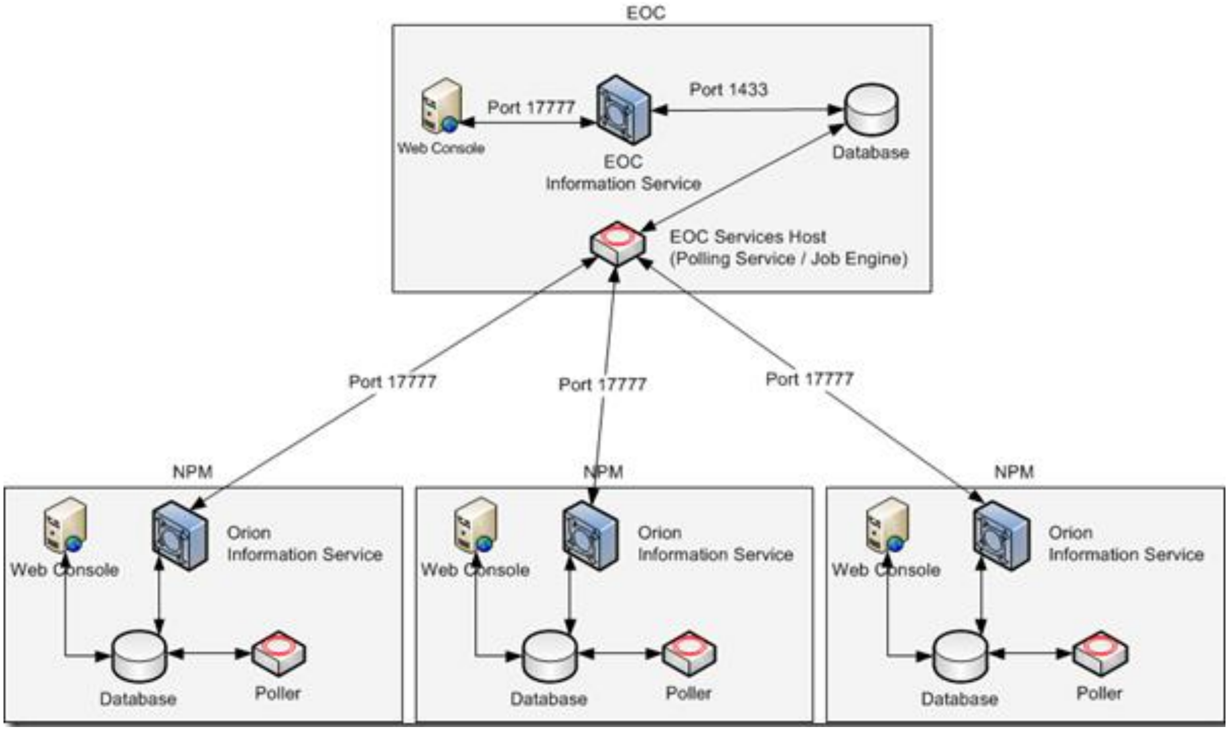
	TIME OF ALERT	NETWORK OBJECT	CURRENT VALUE	MESSAGE	SOLARWINDS SERVER
⚠	8/31/2012 7:09:28 PM	Bas-2621.lab.tex		High Packet Loss Monitoring	Virtual-Brno1
⚠	8/31/2012 5:13:22 PM	pformanek-dev.swdev.local		High Packet Loss Monitoring	Virtual-Brno1
⚠	8/31/2012 4:39:20 PM	PSUCHY-DEV.swdev.local		Alert me when a node goes down	Virtual-Brno1
⚠	8/31/2012 2:35:13 PM	GZHYTAR-SQL.swdev.local		High Packet Loss Monitoring	Virtual-Brno1
⚠	8/31/2012 1:35:10 PM	PSUCHY-DEV.swdev.local		High Packet Loss Monitoring	Virtual-Brno1
⚠	8/31/2012 1:34:10 PM	GR-interface0		Alert me when a group goes into warning or critical state	Virtual-Brno1
⚠	8/31/2012 1:34:10 PM	GR-interface1		Alert me when a group goes into warning or critical state	Virtual-Brno1
⚠	8/31/2012 1:34:10 PM	GR-interface2		Alert me when a group goes into warning or critical state	Virtual-Brno1
⚠	8/31/2012 1:34:10 PM	GR-interface3		Alert me when a group goes into warning or critical state	Virtual-Brno1
⚠	8/31/2012 1:34:10 PM	GR-interface4		Alert me when a group goes into warning or critical state	Virtual-Brno1
⚠	8/31/2012 1:34:10 PM	GR-node0		Alert me when a group goes into warning or critical state	Virtual-Brno1
⚠	8/31/2012 1:34:10 PM	GR-node1		Alert me when a group goes into warning or critical state	Virtual-Brno1
⚠	8/31/2012 1:34:10 PM	GR-node2		Alert me when a group goes into warning or critical state	Virtual-Brno1
⚠	8/31/2012 1:34:10 PM	GR-node3		Alert me when a group goes into warning or critical state	Virtual-Brno1
⚠	8/31/2012 1:34:10 PM	GR-node4		Alert me when a group goes into warning or critical state	Virtual-Brno1

Global Top 25 Nodes with Problems
THE FOLLOWING PROBLEMS SHOULD BE INVESTIGATED

	NODE	STATUS
●	ZBOTLO-DEV.swdev.local	Node status is Down, RAS Async Adapter - Local Area Connection* 10 is Down.
●	JPETRZELKA-VM8	Node status is Down, One or more application monitors is in a Warning state.
●	mkarak-vm3	Node status is Down, One or more application monitors is in a Warning state.
●	WinServer2008x64	Node status is Down, One or more application monitors is in a Warning state.
●	ZZ-ORION.qa.brno.local	Node status is Down, One or more application monitors is in a Warning state.
●	hradilvirtual2	Node status is Down, One or more application monitors is in a Warning state.

How Does SolarWinds EOC Collect Network Polling Data?

SolarWinds EOC securely collects Orion-based server data directly from each of the regional SQL databases. WAN performance is not impacted because Orion-based servers poll network devices locally and EOC only periodically pulls updates from each Orion-based server database.

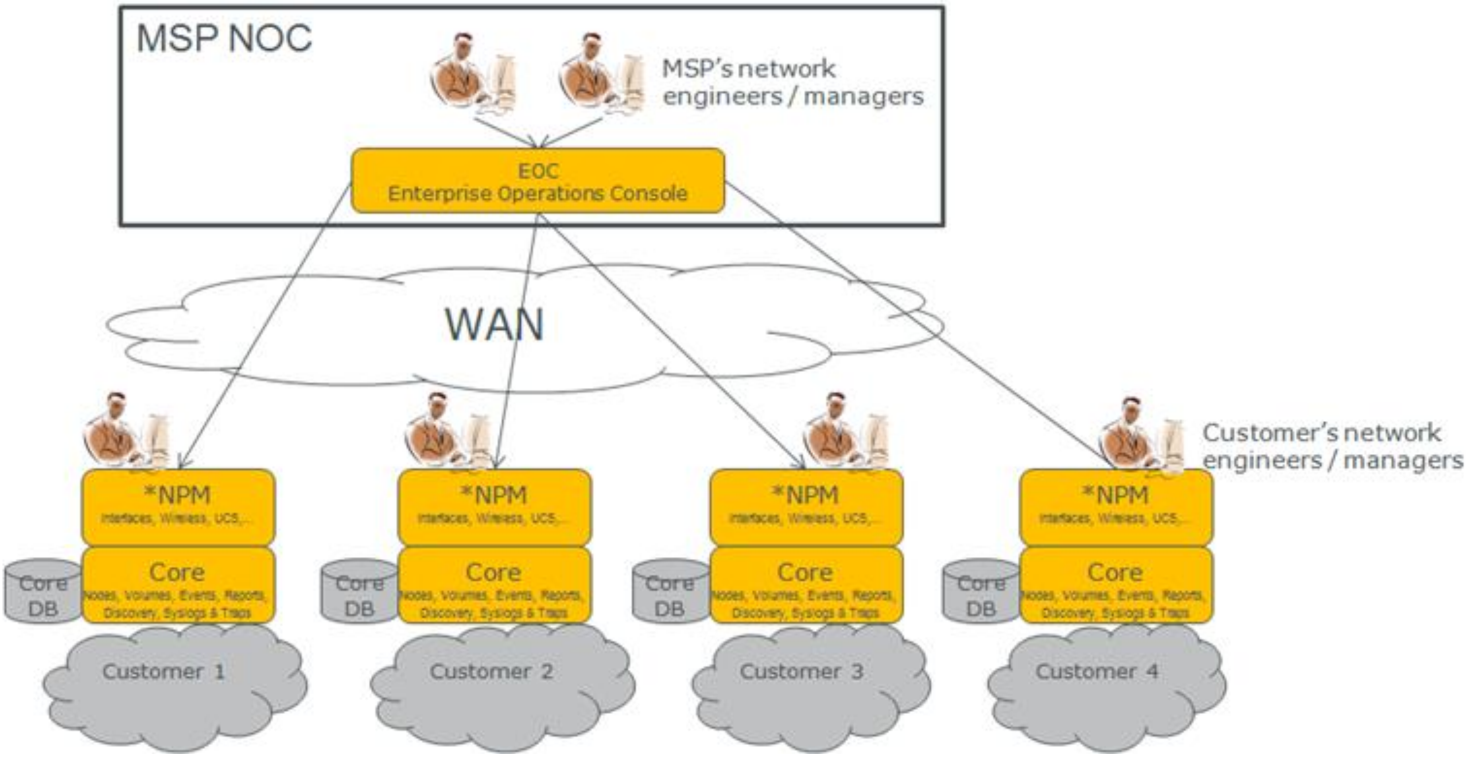


This WAN-optimized architecture ensures that WAN traffic is minimized and that, even if the WAN link temporarily goes down, regional Orion-based servers will continue polling without disruption. Once the WAN link is restored, SolarWinds Enterprise Operations Console automatically reconnects to the Orion-based servers, ensuring you never lose important information about network health.

MSP-friendly Architecture & Multi-Tenant Deployment

SolarWinds allows you to maintain a cost-effective network management plan for your managed customer networks. This is accomplished by deploying a full instance of SolarWinds Orion per customer or customer site, and consolidating them at the MSP-level onto a single screen by using SolarWinds Enterprise Operations Console.

This type of MSP deployment gives you multi-tenancy and provides your customers with full network management capabilities based on their individual SolarWinds Orion instances, which are then rolled up into an MSP-level NOC view using SolarWinds Enterprise Operations Console.


MSP NOC
MSP's network engineers / managers
EOC
Enterprise Operations Console
WAN
Customer's network engineers / managers
*NPM
Interfaces, Wireless, UCS,...
Core
Nodes, Volumes, Events, Reports, Discovery, Syslogs & Traps
Core DB
Customer 1
Customer 2
Customer 3
Customer 4

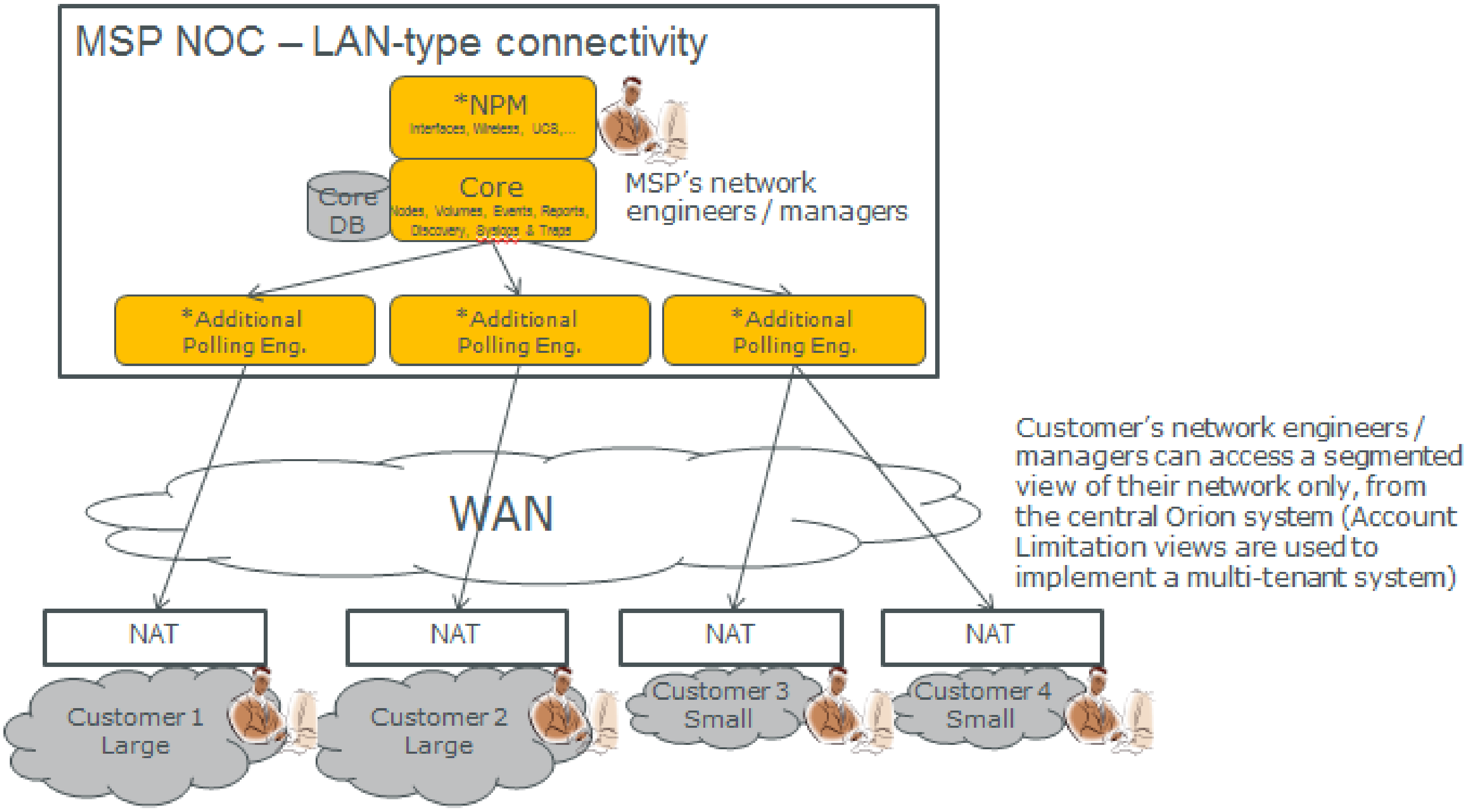
SolarWinds Orion modules are robust and flexible to suit the needs of managed service provider (MSP) environments. Two additional deployment scenarios give you the necessary network operations center (NOC) view and control over your SolarWinds Orion deployment for customer networks across multiple geographies.

#1 NAT-based MSP Deployment

When you have customer networks that have potentially overlapping IP addresses you can have a NAT-based deployment so that Network Address Translators (NAT) translate the customer domain addresses. This allows all domain addresses to be unique from an Orion perspective, thereby eliminating overlapping IP addresses issues.

If it becomes difficult to identify managed devices because the translated IPs don't make sense to report readers, you can populate the Orion custom properties with IPs or Names that will not be affected by any translation.

In this type of deployment, all Additional Polling Engines are deployed only on the MSP side, and customers do not get any visibility into the network management data.


MSP NOC – LAN-type connectivity
*NPM
Interfaces, Wireless, UCS,...
Core DB
Core
Nodes, Volumes, Events, Reports, Discovery, Syslogs & Traps
MSP's network engineers / managers
*Additional Polling Eng.
*Additional Polling Eng.
*Additional Polling Eng.
WAN
Customer's network engineers / managers can access a segmented view of their network only, from the central Orion system (Account Limitation views are used to implement a multi-tenant system)
NAT
NAT
NAT
NAT
Customer 1 Large
Customer 2 Large
Customer 3 Small
Customer 4 Small

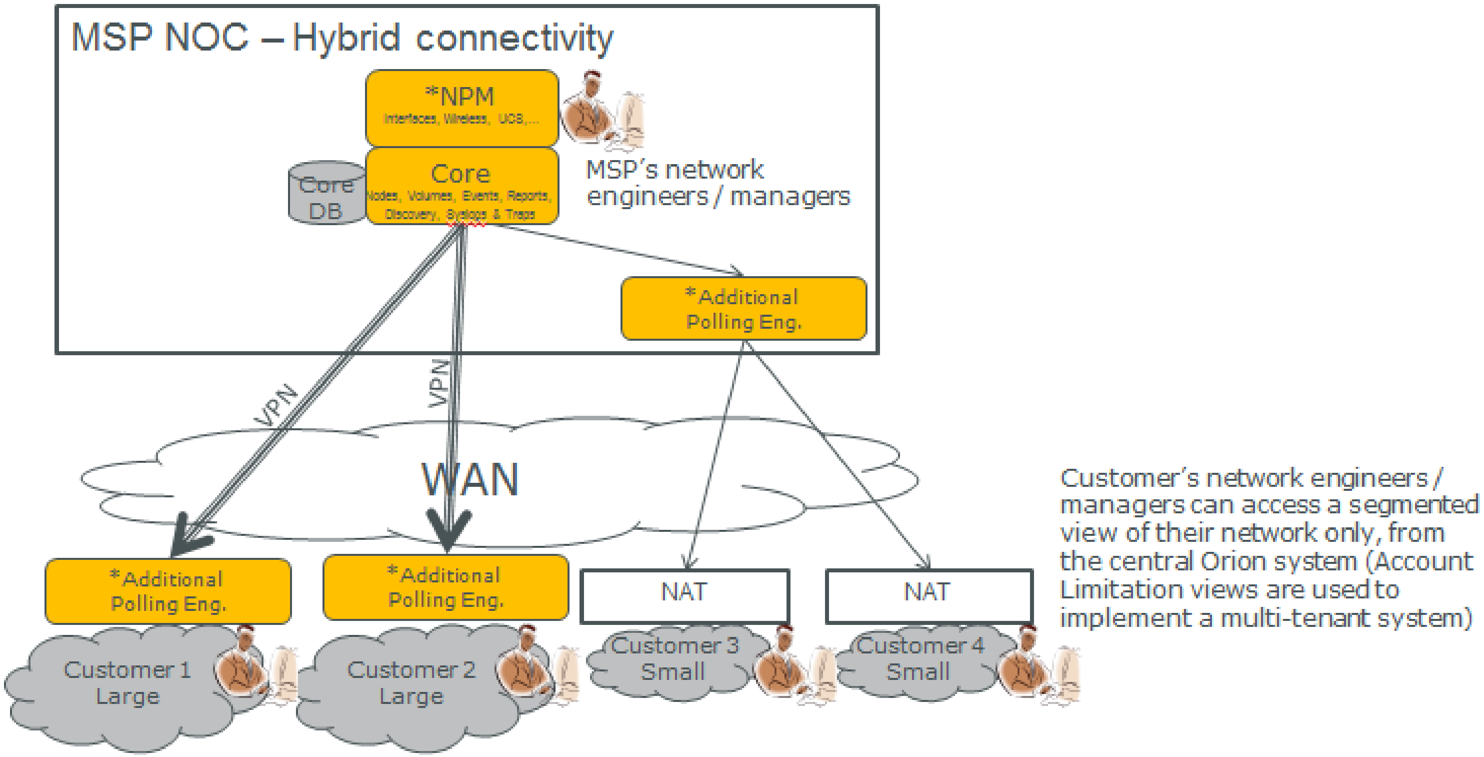
#2 Hybrid MSP Deployment

This type of SolarWinds Orion deployment combines the best of both worlds of Additional Polling Engine deployment. You can have a combination of Additional Polling Engines:

- Installed on the central Orion core managed by MSP NOC

- Remotely installed on customer networks (especially large customers) who have network administration teams that want to view their network management data

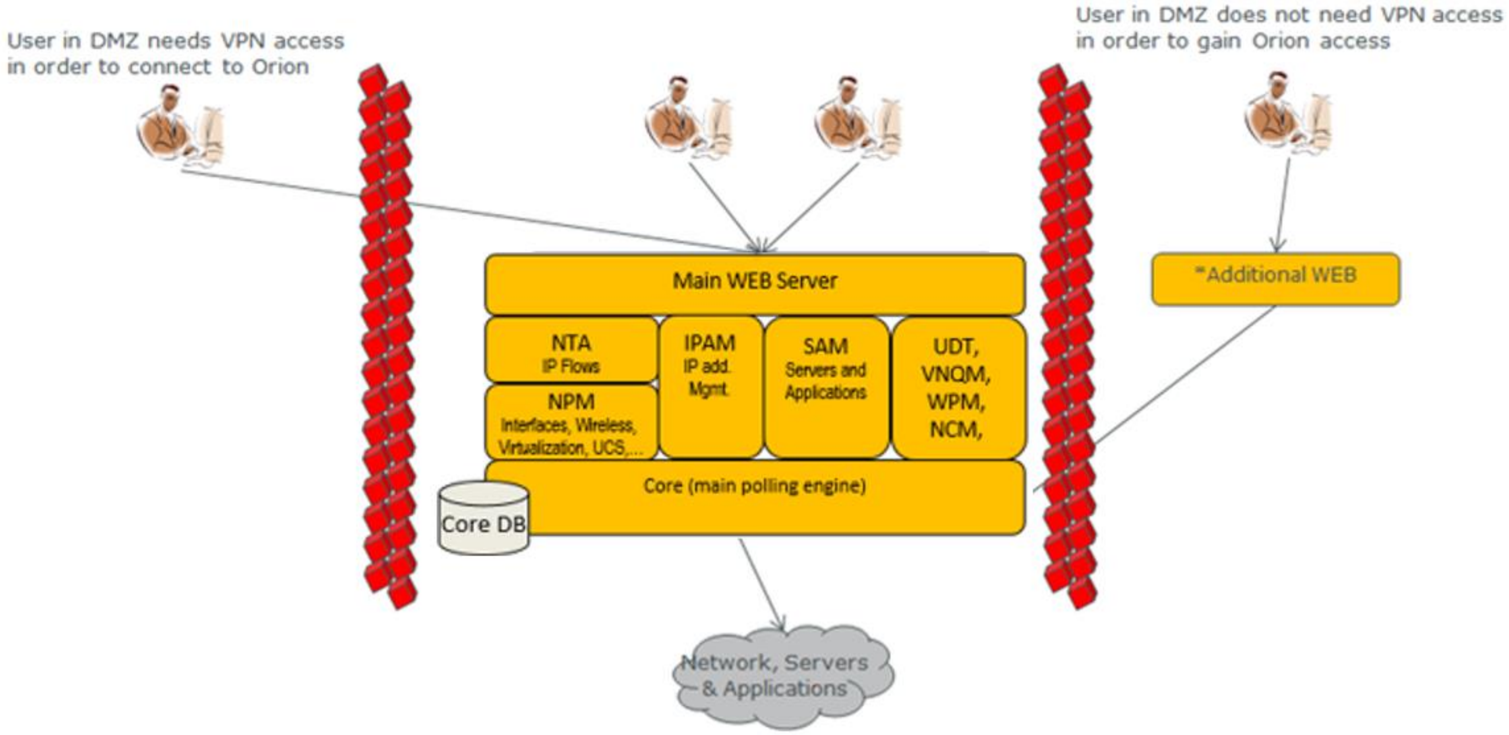
This is a cost-effective method of Orion deployment for MSPs managing large customer networks. Use of VPN is also recommended for this approach.



Customer's network engineers / managers can access a segmented view of their network only, from the central Orion system (Account Limitation views are used to implement a multi-tenant system)

SolarWinds Deployment over Secure DMZ Networks

SolarWinds Network Performance Monitor (NPM) and other Orion modules can be deployed over secure DMZ networks. When users connect from DMZ areas to the deployed SolarWinds Orion instance, they can either use VPN to gain secure access to the Orion Web console, or choose to install an additional Web Server Engine in the DMZ and gain secure access via that Web server to Orion core server. The optional agent in SolarWinds Server & Application Monitor (SAM) enables remote monitoring of servers and applications in DMZ segments. No additional polling engine is required in this case for SAM.


User in DMZ needs VPN access in order to connect to Orion
User in DMZ does not need VPN access in order to gain Orion access
Main WEB Server
*Additional WEB
NTA
IP Flows
IPAM
IP add. Mgmt
SAM
Servers and Applications
UDT, VNQM, WPM, NCM,
NPM
Interfaces, Wireless, Virtualization, UCS,...
Core (main polling engine)
Core DB
Network, Servers & Applications

Creating High Availability and Fault Tolerant Monitoring Environments

Every network should have a fault tolerance and failover plan for its monitoring system deployment. It's possible that your NMS installation can fail due to faulty hardware on the server, link issues, interrupted power supply, etc. To ensure the monitoring system is always available, it's important to lay out a failover mechanism that will switch over the monitoring system operation to secondary server if the primary server should fail. Recovery time objective (RTO) is the accepted time of experiencing monitoring system downtime before it's switched over to another instance. If your impact analysis determines that your production system can comfortably withstand 30 minutes of downtime, then 30 minutes becomes your RTO. Everything you do by way of keeping your systems operational implicitly occurs against that RTO.

The shorter the RTO, the quicker the monitoring system will be available after failover. Since very few systems are capable of an entirely automatic response to an operational issue, recovery strategy most likely involves IT engineers performing triage based on alerts. SolarWinds Orion modules can be switched over to another failover server using SolarWinds Failover Engine (FoE).

Monitoring Servers & Applications on the Cloud

All SolarWinds products on the Orion platform are agentless solutions that comprehensively monitor on-premises and private cloud infrastructure**.** SolarWinds Server & Application Monitor (SAM) is the first Orion module to introduce an optional agent for monitoring applications on the public cloud, where it is normally difficult to use agentless technologies for monitoring due to firewall issues, network bandwidth, latency and other security concerns. SolarWinds SAM supports the installation of an optional agent on the cloud server to monitor the health of the applications and the server itself. Agents are used as an alternative to WMI or SNMP to provide information about key devices and applications that you specify. This can be beneficial in the following situations:

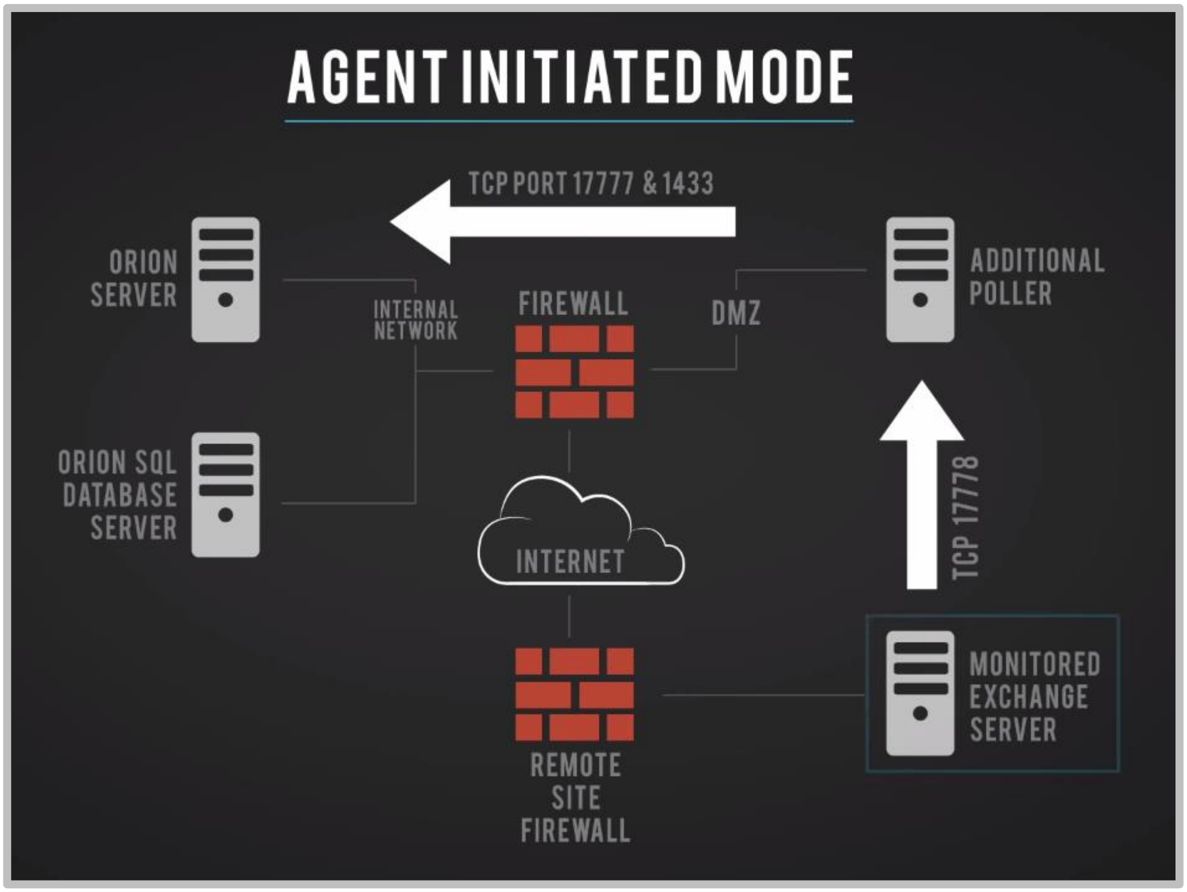
- Polling host and applications behind firewall NAT or proxies
- Polling node and applications across multiple discrete networks that have overlapping IP address space
- Secure encrypted polling over a single port
- Support for low bandwidth, high latency connections
- Polling nodes across domains where no domain trusts have been established
- End-to-end encryption between the monitored host and the Orion server (or additional poller)
- During a network outage, the agent continues monitoring the server and its applications, regardless of whether or not it can communicate with the Orion server/poller. Once connectivity to the server is restored, the agent then forwards the results of its monitoring during the outage to the server for processing. All gaps in the data will be filled with the data collected by the agent.
- Monitoring servers in DMZ, in addition to satellite, remote, and branch offices located anywhere on the globe.

SolarWinds SAM agents can be deployed in one of the following methods—**Agent Initiated Mode** and **Server Initiated Mode**. Each agent can be configured independently to operate in the mode that best suits your needs. For example, you may want to use Server Initiated mode for servers hosted on Amazon® EC2 because they have publicly routable IP addresses. Conversely, you may want to use Agent Initiated mode for servers you're hosting in Azure™ because those servers are using private address space behind a NAT.

#1 Agent Initiated Mode

In Agent Initiated Mode, all communications between the Orion server (or additional poller) and the agent is initiated by the agent.

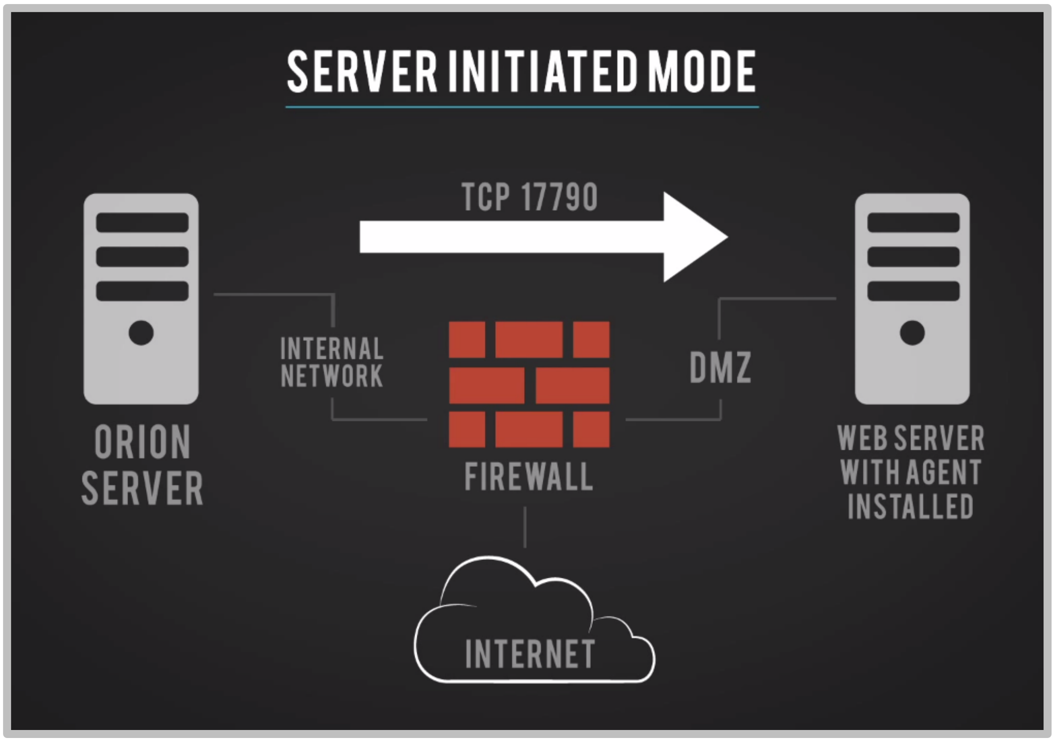
No direct route from the Orion server or additional poller to the monitored host is required. No port forwarding needs to be configured at the remote site, nor do you need a pool of public routable IP addresses at each remote site for 1:1 address translation.



#2 Server Initiated Mode

In Server Initiated Mode, the agent waits for requests from the server on the default port of 17790. This port must be opened on the agent computer's firewall so the server can connect. No change to the server firewall is required.

The difference in "Server Initiated" mode is that the Orion server polls information from the agent in a similar fashion to SNMP or RPC. No ports need to be opened inbound to the internal network from the DMZ, and all communication is done across a single port.



In either method, the agent is very secure and fully encrypted utilizing FIPS compatible 2048 bit TLS encryption to ensure all communication between the Agent and the Orion Server (or additional Poller) are safe from cybercriminals.

What is SolarWinds Failover Engine?

SolarWinds FoE monitors the health of the server hosting the Orion module(s) to ensure you never lose visibility. If something should happen to your primary Orion platform server, FoE automatically fails over to a remote server. The passive failover server assumes the full identity of the primary server and assumes all monitoring, alerting, reporting, and data collection. FoE's switchover is an automatic, seamless, and transparent process that ensures data collection continuity. FoE is an ideal disaster recovery solution for networks that demand high availability and performance

How Does SolarWinds Failover Engine Work?

SolarWinds Failover Engine is installed in a secondary server. Each server is assigned both an *Identity* (*Primary* or *Secondary*) and a *Role* (*Active* or *Passive*).

- *Identity* is used to describe the physical instance of the server
- *Role* is used to describe what the server is doing.

When the *Identity* is assigned to a server it normally will not change over the life of the server whereas the *Role* of the server is subject to change as a result of the operations the server is performing.

When SolarWinds FoE is deployed on a pair of servers, it can provide five levels of protection to the server, and can be deployed for High Availability in a Local Area Network (LAN) or Disaster Recovery over a Wide Area Network (WAN). The five levels of protection are:

1. Server Protection
2. Network Protection
3. Application Protection
4. Performance Protection
5. Data Protection

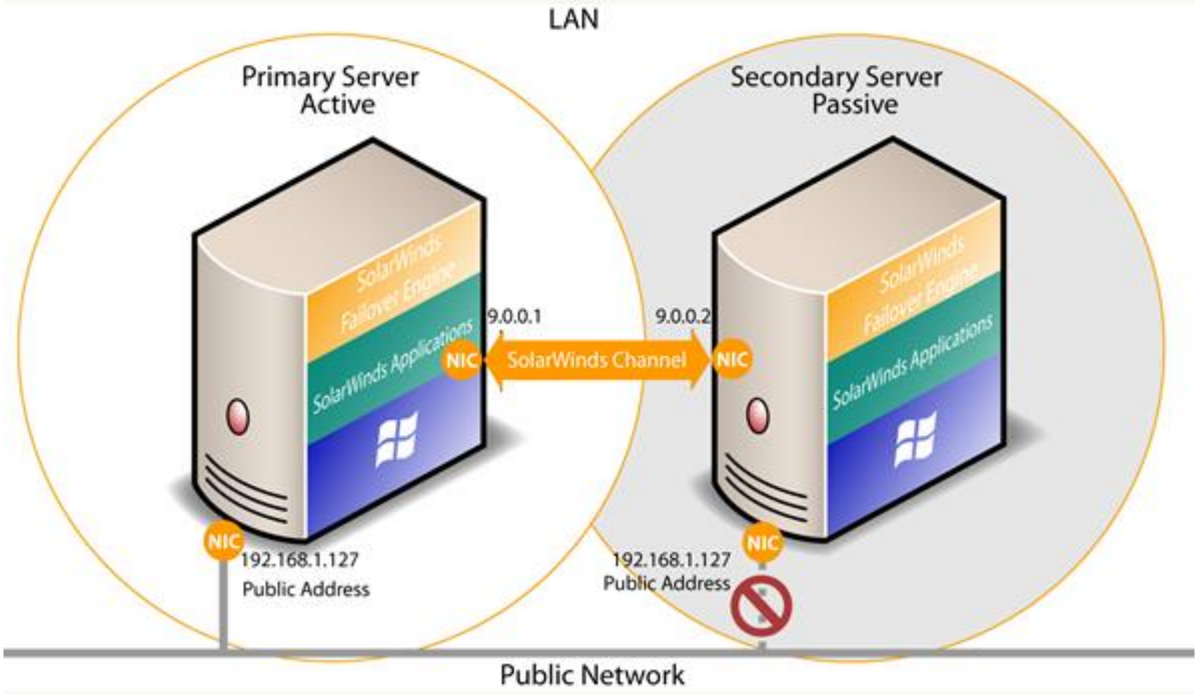
Note:

FoE works in an *Active-Passive* setup, meaning only one server has the SolarWinds services started and running. FoE is NOT an *Active-Active* solution, meaning both servers have the SolarWinds services started and running

#1 High Availability with SolarWinds Failover Engine

High Availability (HA) role is normally deployed in a LAN where communications are configured with the Public IP address being shared by both the active/primary and passive/secondary servers.

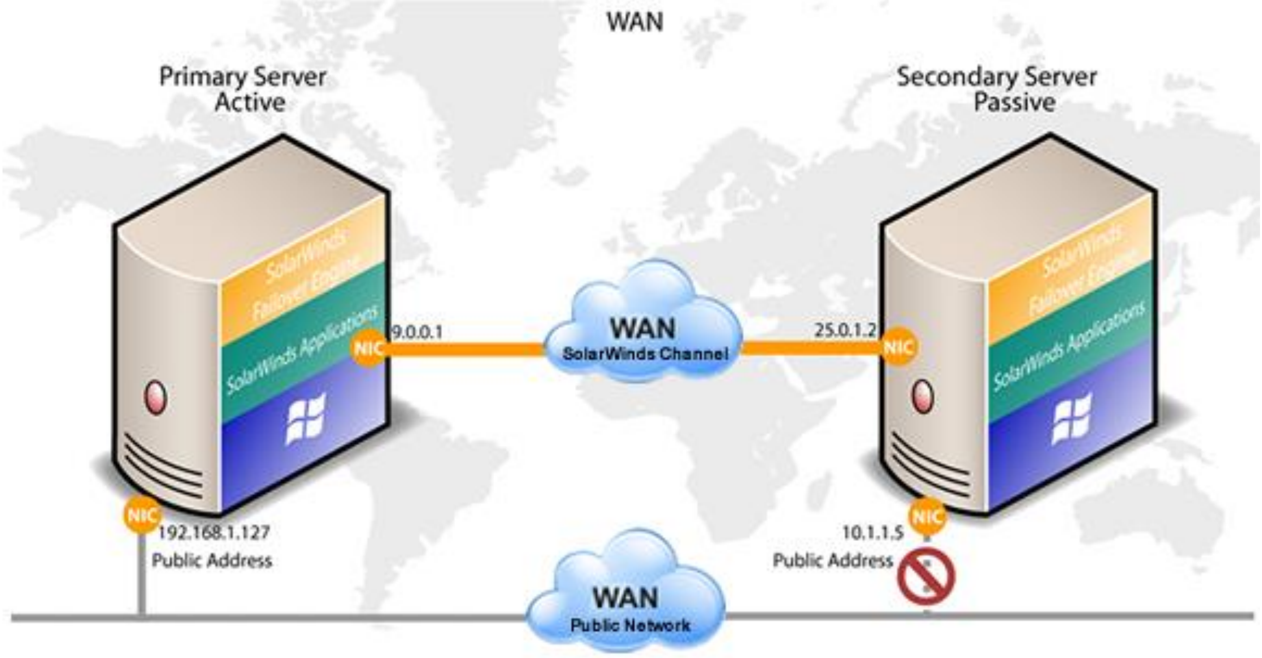
In the event of a failure on the **active/primary server**, the packet filter is removed from the **passive/secondary server** making it now assume the role as the active/primary server. Simultaneously the packet filter gets added to the server that was originally the **active/primary server** making it the **passive/secondary server**. Since both servers are sharing the Public IP address, DNS updating is not required.



#2 Disaster Recovery with SolarWinds Failover Engine

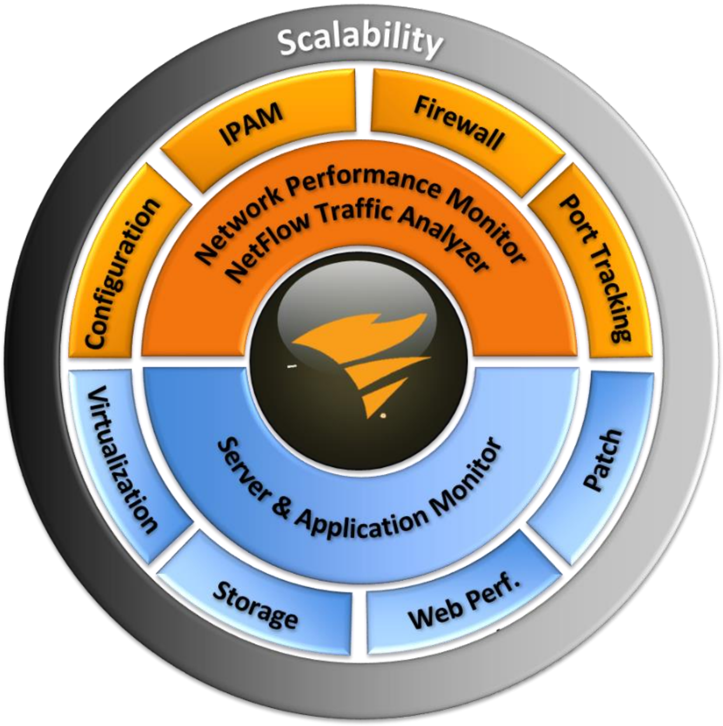
When deployed in a Disaster Recovery role, the active/primary server and the passive/secondary server operates over a Wide Area Network (WAN) in different subnets. As a result, the active/primary and passive/secondary servers are configured with different Public IP addresses.

In the event of a failover, the Failover Engine automatically updates DNS with the IP address of passive/secondary, so end users continue to access the SolarWinds server with the same DNS name they always use.



SolarWinds Scalability for Growing Enterprise Networks

SolarWinds offers a wide portfolio of IT management products to meet the needs of enterprises. Each one of the SolarWinds products:



- Are purpose-built to make the IT professional's job easier
- Eliminate the complexity found in traditional enterprise software—making it easier to find, buy, deploy, and maintain
- Connect with our community to guide product development
- Deliver increasing value over their lifetime by constantly evolving to users' needs

SolarWinds offers IT management solutions across the network management, servers and applications, storage and virtualization management, help desk, remote and mobile IT administration, and network security areas. The goal is to help enterprises build a scalable architecture that provides then with high operational efficiency and measurable ROI. SolarWinds Orion platform products include:

Product	Functionality
Network Performance Monitor (NPM)	For network fault, availability and performance monitoring
Server & Application Monitor (SAM)	For application performance and server health monitoring
NetFlow Traffic Analyzer (NTA)	For network traffic analysis and bandwidth monitoring
Network Configuration Manager (NCM)	For network configuration, change and compliance management
VoIP & Network Quality Manager (VNQM)	For VoIP and WAN performance monitoring
IP Address Manager (IPAM)	For centralized DHCP, DNS and IP address management
User Device Tracker (UDT)	For network user and device tracking & switch port capacity planning
Web Performance Monitor (WPM)	For website performance and synthetic end-user monitoring
Storage Resource Monitor (SRM)	For multi-vendor storage performance and capacity monitoring

These IT management solutions are used by all types of businesses (trusted by over 425 of the Fortune 500 companies) ranging from large enterprises to small business, from federal government agencies to managed service providers (MSP), and everyone else in between.

Watch this webinar to know more about scalability limits for Orion platform products.

About SolarWinds

SolarWinds (NYSE: SWI) provides powerful and affordable IT management software to customers worldwide. Focused exclusively on IT Pros, we strive to eliminate the complexity in IT management software that many have been forced to accept from traditional enterprise software vendors. SolarWinds delivers on this commitment with unexpected simplicity through products that are easy to find, buy, use, and maintain, while providing the power to address any IT management problem on any scale. Our solutions are rooted in our deep connection to our user base, which interacts in our online community, thwack®, to solve problems, share technology and best practices, and directly participate in our product development process. Learn more at http://www.solarwinds.com.