









Last Updated: Wednesday, June 25, 2014













Overview





This document compares and contrasts the capabilities of SolarWinds Failover Engine (FoE) to that of an Active/Active Orion deployment configuration.

Both the SolarWinds Failover Engine and Active/Active Orion configurations can be used for disaster recovery and high availability within the local LAN or across the WAN. Each solution has its own distinct advantages that customers must weigh when deciding between the two.

Critical Differences

Capability	Failover Engine	Active/Active
Automatic Failover	 SolarWinds Failover engine provides transparent and near instantaneous failover of all Orion functions when application, network, or hardware failures occur	 Failover is not available in an Active/Active configuration. Users wishing to access the Orion web console must manually redirect users to the secondary Orion instance. Load balancers can be used to reduce this overhead but data may not be consistent between both Orion instances.
Zero Down Time Upgrades	 Failover Engine requires that both the primary and secondary Orion instances not be running when performing product upgrades or installing service packs and hotfixes.	 In an Active/Active configuration the secondary Orion instance continues to operate normally while the primary Orion instance is being upgraded. Once the primary Orion instance is upgraded it is brought back online and the upgrade procedure is repeated on the secondary Orion instance. Visibility into the environment is maintained at all times .
Management Overhead	 Virtually zero additional overhead associated with redundancy is incurred in an FoE configuration. As new nodes, applications, volumes, etc. are managed within the environment, that configuration is maintained across both primary and secondary instances with no additional steps.	 As new nodes are added, alerts and reports created, applications managed, etc. on the primary Orion instance, these steps must be completed again manually on the secondary Orion instance to maintain synchronization between the two instances.
Ease of deployment	 Initial setup and configuration can be somewhat time consuming, and does require the Orion server to be offline for a short period of time during the installation.	 Deployment of a secondary Orion server is as simple and straightforward as the primary Orion server.

Capability	Failover Engine	Active/Active
Domain Membership	<p> In a WAN/DR Failover Engine configuration, both primary and secondary Orion servers must use the same hostname. This precludes both primary and secondary Orion servers from both being joined to the same Active Directory domain.</p> <p><i>Note: This limitation does not exist when FoE is used in a LAN/HA configuration.</i></p>	<p> Both primary and secondary Orion servers in an Active/Active configuration can be joined to the same, or different active directory domains, and both primary and secondary Orion servers can have their own unique hostname.</p>
Alerting	<p> Because only one Orion server is active at any given time, Failover Engine provides single source alert notifications when issues occur in the environment.</p>	<p> In an Active/Active configuration both Orion instances are running simultaneously and operate independently of one another. As such, alerts are sent from both Orion instances for the same issue.</p>
Active Directory Authentication	<p> Leverage Active Directory users and groups for authenticating users to Orion In a WAN/DR FoE configuration it is not possible.</p> <p><i>Note: This limitation does not exist in a LAN/HA configuration.</i></p>	<p> Administrators can leverage existing Active Directory Users and Groups to allow users to authenticate to the Orion web interface using their existing Active Directory credentials on both active and passive Orion instances.</p>
Passive Monitoring	<p> NetFlow, Syslog and SNMP Traps are received in a seamless fashion with no additional configuration on end point devices when failovers occur in a LAN/HA FoE configuration.</p> <p><i>Note: Additional device configuration is required in a WAN/DR FoE Configuration</i></p>	<p> Endpoint devices such as routers, switches and firewalls must be configured to send NetFlow, Syslog, and SNMP Traps to both primary and secondary Orion servers to ensure they are received and processed appropriately in the event one of the Orion servers is in a failed state.</p>
Cost	<p> Cost is tied to specific individual products and is typically a lower cost option to deploy depending on environment size.</p>	<p> Pricing is tied to all products running on the primary Orion instance and their respective license tiers.</p>
NetFlow	<p> Orion Failover Engine does not as yet support high availability of NTA's NetFlow database. The NetFlow application itself is made redundant by FoE, but the database remains unprotected.</p>	<p> Active/Active configurations maintain two separate NetFlow databases and require flow capable devices to send flow data to both primary and secondary Orion instances simultaneously. This ensures that both primary and secondary Orion servers have a full redundant copy of the Netflow database.</p>

Capability	Failover Engine	Active/Active
Bandwidth	 Only one Orion server is actively polling at any given time, limiting bandwidth usage and reducing network overhead.	 Both primary and secondary Orion servers are actively polling, consuming double the normal network bandwidth associated with management and placing marginal additional load on devices managed by both Orion instances.
Maintenance	 In a LAN/HA FoE Configuration the secondary Orion server is prevented from accessing the network until it becomes the "Active" server. Once "Active" the Primary server is then prevented from accessing the network, making management and maintenance of the "passive" member a task that necessitates manual failovers to occur regularly for patching and other routine server maintenance of the "passive" cluster member.	 Primary and secondary Orion servers can be managed and maintained independently without impacting the other.