

# **SolarWinds Orion**

# **Failover Engine**

## Quick Start Guide

Copyright© 1995-2012 SolarWinds, Inc., all rights reserved worldwide. No part of this document may be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the written consent of SolarWinds. All right, title and interest in and to the software and documentation are and shall remain the exclusive property of SolarWinds and its licensors. SolarWinds®, the SolarWinds logo, ipMonitor®, LANsurveyor®, and Orion® are among the trademarks or registered trademarks of the company in the United States and/or other countries. All other trademarks contained in this document and in the Software are the property of their respective owners.

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON SOFTWARE AND DOCUMENTATION FURNISHED HEREUNDER INCLUDING WITHOUT LIMITATION THE WARRANTIES OF DESIGN, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS OR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Microsoft®, Windows 2000 Server®, Windows 2003 Server®, and Windows 2008 Server® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Graph Layout Toolkit and Graph Editor Toolkit © 1992 - 2001 Tom Sawyer Software, Oakland, California. All Rights Reserved.

Portions Copyright © ComponentOne, LLC 1991-2002. All Rights Reserved.

Fluent is a trademark of Microsoft Corporation and the Fluent user interface is licensed from Microsoft Corporation.

SolarWinds Orion Failover Engine version 6.4.1 [Build 5984] 1.24.2012

## **About SolarWinds**

SolarWinds, Inc develops and markets an array of network management, monitoring, and discovery tools to meet the diverse requirements of today's network management and consulting professionals. SolarWinds products continue to set benchmarks for quality and performance and have positioned the company as the leader in network management and discovery technology. The SolarWinds customer base includes over 45 percent of the Fortune 500 and customers from over 90 countries. Our global business partner distributor network exceeds 100 distributors and resellers.

## **Contacting SolarWinds**

You can contact SolarWinds in a number of ways, including the following:

<b>Team</b>	<b>Contact Information</b>
Sales	1.866.530.8100 www.solarwinds.com
Technical Support	<a href="http://www.solarwinds.com/support">http://www.solarwinds.com/support</a>
User Forums	support.solarwinds.net/support <b>Note:</b> You need a customer account to access the Customer Support area of the website.

# SolarWinds Orion Failover Engine Documentation Library

The following documents are included in the SolarWinds Orion Failover Engine documentation library:

Document	Purpose
Administrator Guide	Provides configuration and conceptual information.
Installation Guide	Provides detailed setup information.
Page Help	Provides help for every window in the Orion Failover Engine user interface
Quick Start Guide	Provides installation, setup, and common scenarios for which Orion Failover Engine provides a simple, yet powerful, solution.
Release Notes	Provides late-breaking information, known issues, and updates. The latest Release Notes can be found at <a href="http://www.solarwinds.com/">http://www.solarwinds.com/</a> .

## Conventions

The documentation uses consistent conventions to help you identify items throughout the printed and online library.

Convention	Specifying
<b>Bold</b>	Window items, including buttons and fields.
<i>Italics</i>	Book and CD titles, variable names, new terms
Fixed font	File and directory names, commands and code examples, text typed by you
Straight brackets, as in [value]	Optional command parameters
Curly braces, as in {value}	Required command parameters
Logical OR, as in value1 value2	Exclusive command parameters where only one of the options can be specified

## **Contents**

<i>About SolarWinds</i> .....	<i>iii</i>
<i>Contacting SolarWinds</i> .....	<i>iii</i>
<i>SolarWinds Orion Failover Engine Documentation Library</i> .....	<i>iv</i>
<i>Conventions</i> .....	<i>iv</i>

### Chapter 1

<b>Introduction</b> .....	<b>1</b>
<i>Orion Failover Engine Protection</i> .....	<i>1</i>
<i>Server Protection</i> .....	<i>1</i>
<i>Application Protection</i> .....	<i>2</i>
<i>Network Protection</i> .....	<i>3</i>
<i>Performance Protection</i> .....	<i>3</i>
<i>Data Protection</i> .....	<i>3</i>
<i>Communications</i> .....	<i>4</i>

### Chapter 2

<b>SolarWinds Orion Failover Engine Installation</b> .....	<b>7</b>
<i>Installation Requirements</i> .....	<i>7</i>
<i>Additional Requirements</i> .....	<i>8</i>
<i>Server Architecture Options</i> .....	<i>8</i>
<i>Virtual to Virtual (V2V)</i> .....	<i>8</i>
<i>Physical to Virtual (P2V)</i> .....	<i>9</i>
<i>Physical to Physical (P2P)</i> .....	<i>9</i>
<i>Cloning Technology Options</i> .....	<i>10</i>
<i>Supported Pre-Clone Technologies</i> .....	<i>10</i>
<i>Supported Install Clone Technologies</i> .....	<i>11</i>
<i>Application Component Options</i> .....	<i>11</i>
<i>Network Options</i> .....	<i>11</i>
<i>LAN</i> .....	<i>11</i>
<i>WAN</i> .....	<i>12</i>
<i>Installation Process</i> .....	<i>14</i>
<i>Installation on the Primary Server</i> .....	<i>15</i>
<i>Installation on the Secondary Server</i> .....	<i>16</i>

<i>Actions Required After an Installation</i> .....	17
<i>Configure actions to take upon failure of a service</i> .....	17
<i>When Additional Pollers (AP)s are not installed, create an Exclusion Filter to reduce replication traffic</i> .....	19
<i>When IPAM 2.0 is installed, create an Inclusion Filter to replicate the IPAM.attributes.xml file</i> .....	19

**Chapter 3**

<b>Installation Verification</b> .....	<b>21</b>
<i>Failover Simulation Exercise</i> .....	21
<i>Data Replication Exercise</i> .....	22
<i>Switchover Exercise</i> .....	23

---

## Chapter 1

# Introduction

This chapter introduces the Orion Failover Engine, providing an overview of general concepts related to the protection Orion Failover Engine provides.

## ***Orion Failover Engine Protection***

The Orion Failover Engine (Orion Failover Engine) is a Windows-based service specifically designed to provide high availability protection for SolarWinds Orion installations without requiring any specialized hardware. The following sections describe the various ways Orion Failover Engine protects your SolarWinds Orion installation:

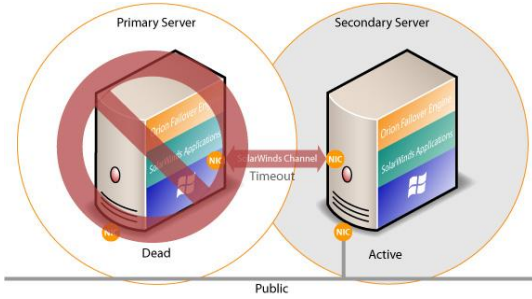
- Server Protection
- Application Protection
- Network Protection
- Performance Protection
- Data Protection

## **Server Protection**

The Orion Failover Engine provides continuous availability to end users should a hardware failure or operating system crash occur. Additionally, Orion Failover Engine protects the network identity of the production server, ensuring users are provided with a replica server including server name and IP address should the production server fail.

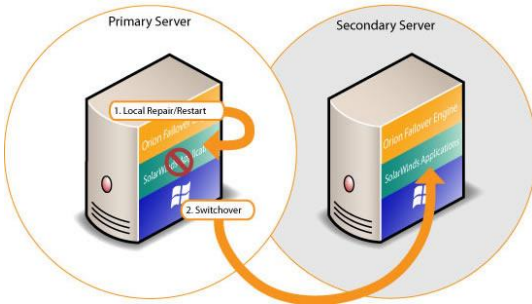
The Orion Failover Engine software is installed on both a primary server and a secondary server. These names refer to the physical hardware (identity) of the servers. The secondary server has the same name, file and data structure, and network address as the primary server, and runs the same applications and services as the primary server. Under normal operating conditions in a non-failover state the primary server functions as the “active” server, and the secondary server functions as the “passive” server. These two Orion Failover Engine instances regularly send “I’m alive” messages and acknowledgments to one another over a network connection referred to as the SolarWinds Channel to detect interruptions in responsiveness. If the passive server detects that the monitoring process has failed, it initiates a failover. The Orion Failover Engine is symmetrical in almost all respects, and either server—primary or secondary—can take the active role, providing protected applications and services to users.

A failover is used in more urgent situations, such as when the passive server detects that the active server is no longer responding. The active server can become non-responsive due to hardware failure, loss of network connectivity, or other communication failure. In a failover situation, the passive server determines that the active server has failed and then immediately assumes the active server role, as illustrated in the following figure:



## Application Protection

The Orion Failover Engine enables you to maintain your application environment by ensuring that network applications and services stay alive. The Orion Failover Engine on the active server uses plug-ins to monitor the applications and services it has been configured to protect. If a protected application fails, the Orion Failover Engine first tries to restart the application on the active server (1). If restarting the application fails, then the Orion Failover Engine can initiate a switchover (2) as illustrated in the following figure.



A switchover gracefully closes any protected applications running on the active server, and then restarts all of them on the passive server, including the service or application that initially caused the failure, as illustrated in the figure above.

## Network Protection

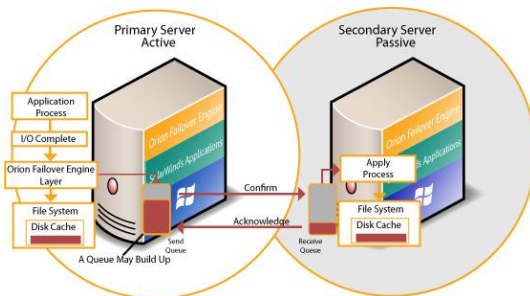
The Orion Failover Engine proactively monitors the network by polling up to three nodes to ensure that the active server is visible on the network. The Orion Failover Engine polls defined nodes around the network, including the default gateway, the primary DNS server, and the global catalog server, at regular intervals. If all three nodes fail to respond, for example, in the case of a network card or a local switch failure, the Orion Failover Engine can initiate a switchover, allowing the secondary server to assume a network identity identical to that of the primary server.

## Performance Protection

The Orion Failover Engine proactively monitors system performance attributes to ensure that the system administrator is notified of problems and can take preemptive action to prevent an outage. In addition to monitoring application services, the Orion Failover Engine can monitor specific application attributes to ensure they remain within normal operating ranges. Similar to application monitoring, various rules can be configured to trigger specific corrective actions when these attributes fall outside of their respective ranges.

## Data Protection

The Orion Failover Engine intercepts all data written by users and applications, and it maintains a copy of this data on the passive server that can be used in the event of a failure. The Orion Failover Engine configures itself to protect files, folders, and even the registry settings on the active server by mirroring these in realtime to the passive server. If a failover occurs, all files protected on the failed server are available after the failover, hosted on the secondary server.

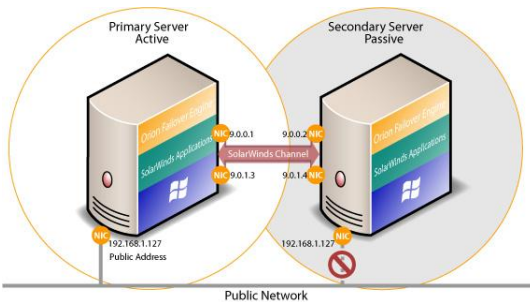


Orion Failover Engine continuously provides all five protection levels, ensuring all facets of the user environment are maintained at all times, and that the principal network continues to operate through as many failure scenarios as possible.

# Communications

The SolarWinds Channel is a crucial component of an Orion Failover Engine installation, and it can be configured in a number of ways, provided the following conditions are met:

- Both the primary and the secondary servers must have two or more network interface connections (NICs).
- The principal (public) network requires one NIC. The SolarWinds Channel uses a separate NIC for the private connection between the protected servers that is used for control and data transfer.
- A second pair of NICs can be used to provide a degree of redundancy for the SolarWinds Channel. In this configuration, the SolarWinds Channel has a dual channel if more than one dedicated NIC is provided for the SolarWinds Channel on each server. To provide added resilience, the communications for the second channel must be completely independent from the first channel. They must not share any switches, virtual switches, routers or the same WAN connection.



The IP address a client uses to connect to the active server—the principal IP address—must be configured as a static IP address that is not DHCP-enabled (Dynamic Host Configuration Protocol). In the figure above, the IP address is configured as 192.168.1.127.

The principal NICs on the passive server are configured to use the same IP address as the active server, but they are prevented from communicating with the live network through an IP packet filtering system installed with the Orion Failover Engine. This packet filter prevents traffic using the principal address from being committed to the wire. It also prevents NetBIOS traffic using other IP addresses on the NIC from being sent to prevent NetBIOS name resolution conflicts. Following restore and after the Orion Failover Engine installation completes (runtime), NetBIOS is disabled across the SolarWinds Channel. This occurs during installation to prevent name conflicts that occur when both servers have the same name.

The NICs on the active and passive servers that support connectivity across the SolarWinds Channel can be standard 100BaseT Ethernet cards providing a throughput of 100Mbps per second across standard Cat-5 cabling, and are configured so their IP addresses are outside the subnet range of the principal network. These addresses are referred to as SolarWinds Channel addresses.

**Note:** Firewalls protecting the SolarWinds Channel network connections must be disabled to allow uninterrupted communications between the primary and secondary servers.

When configured for a WAN deployment, the SolarWinds Channel uses static routes over switches and routers to maintain continuous communications independent from corporate or public traffic.

Only one server name and network address can be visible on the same network at any one time. One of these two servers is live on the principal network and serves the protected applications; this is the active server. The other server, referred to as the passive server, is hidden from the principal network, remaining as a ready standby server.



## Chapter 2

# SolarWinds Orion Failover Engine Installation

Prior to installing the Orion Failover Engine, select the deployment options you intend to use. The installation process prompts you to select options throughout the procedure to create the configuration you want.

## *Installation Requirements*

The following table lists minimum requirements for the SolarWinds Orion Failover Engine.

**Note:** These requirements are in addition to any other requirements for the operating system or installed applications.

Orion Failover Engine Requirements	
Supported SolarWinds Orion Modules	SolarWinds Orion NPM MP v10.0 SP1 and higher SolarWinds Orion IPAM v1.7.1 and higher SolarWinds Orion APM v3.5 and higher SolarWinds Orion APM MP v4.0.1 and higher SolarWinds Orion IPSLA Manager v3.5 and higher SolarWinds Orion NTA v3.6 and higher SolarWinds Orion NCM v6.0 and higher <b>Note:</b> NCM v7.0 is supported, but it must be updated to NCM v7.0.1 if additional polling engines or additional web sites are in use. SolarWinds Orion SEUM v1.0 and higher SolarWinds Orion UDT v1.0 and higher SolarWinds Orion EOC v1.2 and higher
Supported Operating Systems	Windows Server 2003 x86 Standard or Enterprise, SP1 and SP2 Windows Server 2003 x64 Enterprise SP2 Windows Server 2003 R2 x86 Standard or Enterprise Windows Server 2003 R2 x64 Standard or Enterprise Windows Server 2008 x86 or x64, SP1 and SP2 Standard or Enterprise Windows Server 2008 R2 Standard or Enterprise <b>Note:</b> SolarWinds recommends installing all Microsoft security updates.
Memory	1 GB (2 GB is recommended) <b>Note:</b> During setup, Orion Failover Engine verifies that a minimum of 1GB RAM is available. To ensure proper operation, 2GB is recommended in addition to any other memory requirements for the operating system or SolarWinds Orion modules.
Disk Space	2 GB of available disk space on the installation drive for Orion Failover Engine.

## ***Additional Requirements***

The following additional requirements also apply:

- The Orion Failover Engine cannot protect any server configured as a domain controller, global catalog, or domain name server.
- You must use an account with local administrator rights to complete an Orion Failover Engine installation.
- All applications you intend to protect must be installed and configured on the primary server prior to installing an Orion Failover Engine.
- Verify that both primary and secondary servers have identical system date, time, and time zone settings. Once configured, do not change the time zone.
- Verify that the principal network adapter is listed as the first network adapter in the network connections bind order. (**Network Connections > Advanced > Advanced Settings**).
- Firewalls protecting the SolarWinds Channel network connections must be disabled to allow uninterrupted communications between the primary and secondary servers. Consult the SolarWinds Knowledge Base for additional information.
- SQL Server should not be installed on the same machine as Orion Failover Engine.

## ***Server Architecture Options***

The server architecture you select affects both hardware requirements and the technique used to clone the primary server. The following server architecture options are available:

- Virtual to Virtual (V2V)
- Physical to Virtual (P2V)
- Physical to Physical (P2P)

### **Virtual to Virtual (V2V)**

The V2V architecture is supported if the Orion Failover Engine is already installed on a primary production server running on a virtual machine. The secondary virtual machine must also meet the minimum requirements. For more information about minimum Orion Failover Engine requirements, see “Installation Requirements” on page 7.

- The specifications of the secondary virtual machine must match the specifications of the primary virtual machine as follows:
  - Similar CPU (including resource management settings)
  - Appropriate resource pool priorities
  - Same memory configuration, operating system version, and service pack (including resource management settings)
- Each virtual machine used in the V2V pair must be on a separate host to guard against failure at the host level.
- Each virtual NIC must use a separate virtual switch.

## Physical to Virtual (P2V)

The P2V architecture is used when the environment requires a mix of physical and virtual machines. The secondary virtual machine must meet the minimum requirements.

- The specifications of the secondary virtual machine must match the primary physical server as follows:
  - Similar CPU
  - Identical Memory
  - Operating system version and service pack
- The secondary virtual machine must have priority in resource management settings to ensure that other virtual machines do not impact its performance.
- Each virtual NIC must use a separate virtual switch.

## Physical to Physical (P2P)

P2P architecture is used in environments where both the primary and secondary servers are physical servers.

**Note:** Using P2P limits installation options as it requires using the Install Clone technique. This architecture requires attention to detail when preparing for installation as both hardware and software must meet specific prerequisites. For more information about the Install Clone technique, see “Cloning Technology Options” on page 10.

### Primary Server

The primary server must meet the hardware and software requirements specified in “Installation Requirements” on page 7.

## **Secondary Server**

The secondary server operates as a near-clone of the primary server and must meet the following requirements.

- Secondary server hardware must meet the following requirements:
  - Similar CPU and memory.
  - Identical number of NICs as the primary server.
  - Drive letters must match those on the primary server.
  - Available disk space must be greater than or equal to the space available on the primary server.
  - Advanced Configuration and Power Interface (ACPI) compliance must match the primary server. If not, contact SolarWinds support for further information.
- Software on the secondary server must meet the following requirements:
  - Operating system version and service pack version must match the primary server.
  - The operating system must be installed to the same driver letter and directory as on the primary server.
  - The machine name must be different from the primary server prior to installing the Orion Failover Engine.
  - The secondary server must be configured in a workgroup.
  - System date, time, and time zone settings must be consistent with the primary server.

## ***Cloning Technology Options***

Cloning the primary server to create a near identical secondary server involves different techniques depending on the selected server architecture.

## **Supported Pre-Clone Technologies**

Orion Failover Engine supports most third-party cloning technologies for creating pre-cloned images for use as a secondary server in the following configurations:

- Physical to virtual. For more information, see “Physical to Virtual (P2V)” on page 9.
- Virtual to virtual. For more information, see “Virtual to Virtual (V2V)” on page 8.

## Supported Install Clone Technologies

The Orion Failover Engine provides support for NTBackup on Windows 2003 and Wbadmin on Windows Server 2008 for automated install cloning. This process is automated, but it requires that all prerequisites for a Physical to Physical architecture are met. For more information, see “Physical to Physical (P2P)” on page 9.

## Application Component Options

The Orion Failover Engine can accommodate any supported SolarWinds Orion installation with the following SolarWinds Orion modules:

- SolarWinds Orion NPM MP v10.0 SP1 and higher
- SolarWinds Orion IPAM v1.7.1 and higher
- SolarWinds Orion APM v3.5 and higher
- SolarWinds Orion APM MP v4.0.1 and higher
- SolarWinds Orion IPSLA Manager v3.5 and higher
- SolarWinds Orion NTA v3.6 and higher
- SolarWinds Orion NCM v6.0 and higher  
**Note:** NCM v7.0 is supported, but it must be updated to NCM v7.0.1 if additional polling engines or additional web sites are in use.
- SolarWinds Orion SEUM v1.0 and higher
- SolarWinds Orion UDT v1.0 and higher
- SolarWinds Orion EOC v1.2 and higher
- Tomcat v5.5.6

## Network Options

Networking requirements are contingent upon how your Orion Failover Engine is deployed. To deploy an Orion Failover Engine as a high availability solution, a LAN configuration is required. For more information, see “LAN” on page 11. To deploy an Orion Failover Engine for Disaster Recovery (DR), a WAN configuration is required. For more information, see “WAN” on page 12.

### LAN

When deployed in a LAN environment, the Orion Failover Engine requires that both servers use the same principal IP address. Each server also requires a separate SolarWinds Channel IP address on a separate dedicated subnet.

## **Primary Server**

Three NICs (1 x principal; 2 x channel) are recommended for redundancy in the event that any single channel fails. A minimum of two NICs (one for the SolarWinds Channel, and one for the principal connection) are required in this configuration. Split-brain avoidance should be configured.

- The principal network connection is configured with the following:
  - Static IP address
  - Correct network mask
  - Correct Gateway and preferred and secondary DNS server addresses
  - NetBIOS enabled
- Channel network connections are configured with the following:
  - Static IP address in a different subnet than the principal network with a different IP address than the secondary server channel NIC
  - Correct network mask
  - No Gateway IP address or DNS server address
  - NetBIOS enabled (disabled during the installation process)

## **Secondary Server**

Networking components on the secondary server must be configured as follows:

- Same number of NICs as the primary server
- Principal network connection configured with temporary network settings
- Channel network connection(s) configured with the following:
  - Static IP address in a different subnet than the principal network with a different IP address than the primary server channel NIC.
  - Correct network mask
  - No Gateway or DNS IP address
  - NetBIOS enabled (disabled during the installation process)
  - File and print sharing enabled

## **WAN**

Deploying an Orion Failover Engine in a WAN environment requires additional considerations as indicated in the following section.

## **WAN Requirements**

When deploying an Orion Failover Engine in a WAN environment, the following components must be configured:

- Persistent static routing configured for the channel connection(s) where routing is required
- Two NICs (1 x principal; 1 x SolarWinds Channel) recommended
- At least one domain controller at the disaster recovery site
- If the primary and disaster recovery site use the same subnet:
  - During install, follow the steps for a LAN or VLAN on the same subnet
  - Both servers in the Orion Failover Engine pair use the same principal IP address
- If the primary and disaster recovery site use different subnets:
  - During install, follow the steps for a WAN
  - Both servers in the Orion Failover Engine pair require a unique principal, public IP address in a subnet separate from the SolarWinds Channel
  - Additionally, each server requires separate NIC with a SolarWinds Channel IP address assigned and static routing configured between the primary and secondary servers
  - Provide a user account with rights to update DNS using the DNSUpdate utility provided as a component of the Orion Failover Engine when prompted during the setup process
  - Recommend integrating Microsoft DNS into AD so that DNSUpdate can identify all DNS Servers that require updating
  - At least one domain controller at the disaster recovery site
  - Refer to the following articles in the SolarWinds Knowledge Base:
    - “Configuring DNS with Orion Failover Engine in a WAN Environment”. Search `SWREFID 1425` in the SolarWinds Knowledge Base.
    - “Configuring Orion Failover Engine to Update BIND9 DNS Servers Deployed in a WAN”. Search `SWREFID 1599` in the SolarWinds Knowledge Base.

## **Bandwidth**

Determine the available bandwidth and estimate the volume of data throughput to determine acceptable latency for the throughput. Available bandwidth can affect the queue size required to accommodate the estimated volume of data. SolarWinds recommends making a minimum of 1Mbit of spare bandwidth available to the Orion Failover Engine.

The Orion Failover Engine offers automatic bandwidth optimization in WAN environments. This feature compresses data transferred over the SolarWinds Channel, optimizing the traffic for low bandwidth connections while placing some additional CPU load on the active server.

## **Latency**

Latency has a direct effect on data throughput. Latency on the link must not fall below the standard defined for a T1 connection.

## ***Installation Process***

After selecting implementation options, begin the installation process. The installation process for all scenarios follows the same basic procedure.

### **Notes:**

- ***If the primary and secondary site subnet is the same***, an IP address is required for this subnet.
- ***If Active Directory-integrated DNS is enabled***, a domain account with rights to update DNS is required.
- ***If Active Directory-integrated DNS is not enabled***, see the following knowledge base articles:
  - “Configuring DNS with Orion Failover Engine in a WAN Environment”. Search `SWREFID 1425` in the SolarWinds Knowledge Base.
  - “Configuring Orion Failover Engine to Update BIND9 DNS Servers Deployed in a WAN”. Search `SWREFID 1599` in the SolarWinds Knowledge Base.
- For more detailed information about Orion Failover Engine installation, see the *Orion Failover Engine Administrator Guide*.

## Installation on the Primary Server

After reviewing the setup prerequisites to ensure the servers in the pair (either physical or virtual) meet the minimum requirements and completing the pre-installation tasks (Pre-Cloning for V2V and P2V environments and configuring the SolarWinds Channel), you can begin the setup process.

### Notes:

- For more information about minimum installation requirements, see “Installation Requirements” on page 7.
- If you need help during the setup process, the left panel of the setup window explains each step or option.
- When installing on Windows Server 2008, you must specify a universal naming convention (UNC) path to the backup file location.

### To set up the primary server

1. Double-click the WinZip Self-Extracting file on the primary server.
2. The Setup Introduction dialog is displayed. Click **OK**.
3. The WinZip Self-Extractor dialog is displayed. Click **Setup** to open the Install SolarWinds Orion Failover Engine window.
4. The first installation option to configure is the **Setup Type**. Select **Install SolarWinds Orion Failover Engine**.
5. On the following step, select **Primary** as the Server Identity.

During the setup process, you have the opportunity to identify the following:

- The program Installation location
- SolarWinds Channel IP addresses
- The principal IP addresses
  - A single IP for a LAN installation
  - Two IPs for a WAN installation
- The location to store the clone files

Setup runs a pre-install check to verify that the server meets the minimum requirements before installing Orion Failover Engine.

The next option to configure is the cloning technique. When you select the cloning option, the subsequent setup screens display the setup process for the selected cloning technology.

When using the Install Clone technique, setup makes a backup. When using the Pre-Clone setup, setup copies two small files to the storage location configured on the secondary server.

A Packet Filter is installed on the principal NIC and the setup process completes on the primary server.

## Installation on the Secondary Server

After reviewing the setup prerequisites to ensure the servers in the pair (either physical or virtual) meet the minimum requirements and completing the pre-installation tasks (Pre-Cloning for V2V and P2V environments and configuring the SolarWinds Channel), you can begin the setup process.

### Notes:

- **If the primary and secondary site subnet is the same**, an IP address is required for this subnet.
- **If Active Directory-integrated DNS is enabled**, a domain account with rights to update DNS is required.
- **If Active Directory-integrated DNS is not enabled**, see the following knowledge base articles:
  - “Configuring DNS with Orion Failover Engine in a WAN Environment”. Search `SWREFID 1425` in the SolarWinds Knowledge Base.
  - “Configuring Orion Failover Engine to Update BIND9 DNS Servers Deployed in a WAN”. Search `SWREFID 1599` in the SolarWinds Knowledge Base.
- For more detailed information about Orion Failover Engine installation, see the *Orion Failover Engine Administrator Guide*.

### To set up the secondary server

1. Double-click the WinZip Self-Extracting file to start the setup process for the secondary server (physical or virtual).
2. The Setup Introduction dialog is displayed. Click **OK**.
3. The WinZip Self-Extractor dialog is displayed. Click **Setup** to open the Install SolarWinds Orion Failover Engine window.
4. The first installation option to select is the **Setup Type**. Select **Install SolarWinds Orion Failover Engine**.
5. Select **Secondary** for the Server Identity option.

6. Specify the location of the folder containing the backup file from the primary server. Type the location path in the text box or click **Browse** and locate the folder.
7. Click **Next**.
8. Setup identifies the backup file location and runs pre-install checks before installing Orion Failover Engine on the secondary server.
9. The next step installs the Packet Filter and identifies the SolarWinds Channel and principal NICs.
10. When using an Install Clone setup in a LAN environment, configure the principal NIC with the same IP address as the primary server.
11. After reconfiguring the principal NIC, if necessary, start the restore process.
12. Following completion of the restore process, if the secondary server is a physical server, Windows Plug and Play might run multiple times to detect hardware differences. As a result, one or more system restarts may be required.
13. After Plug and Play completes detection, the setup process displays the **Finish** window.

## ***Actions Required After an Installation***

After a successful installation of the Orion Failover Engine, complete the following tasks:

1. Activate the Orion Failover Engine license.
2. Ensure that the Orion Failover Engine is shut down.
3. Verify that the date, time, and time zone on the secondary server are identical to the same on the primary server.
4. Start the Orion Failover Engine on the primary server.
5. Start the Orion Failover Engine on the secondary server.
6. Right-click the System Tray icon and select **About SolarWinds Orion Failover Engine** to verify v6.4 (5984) is displayed.

## **Configure actions to take upon failure of a service**

Orion Failover Engine assigns three sequential tasks to perform in the event a monitored service fails. Task options include Recover Service, Application Restart, Log Warning, Switchover, and any additional user-defined tasks previously created. By default, Orion Failover Engine assigns Recover Service to each of the three actions. To cause a switchover in the event of service failure, configure the 3<sup>rd</sup> option to *Switchover*.

## To configure tasks to perform upon service failure:

1. Navigate to **Applications: Services**.
2. Select the intended service.
3. Click **Edit** and assign a task to each of the three failure options, and then click **OK**.

**Important:** For dependent services, failure actions must match the failure actions for any protected service on which those services depend, in both type and order. For example:

- Service X is automatically protected by Orion Failover Engine
- Service Y is automatically protected by Orion Failover Engine and has a dependency on service X
- The system administrator sets custom recovery actions for service X as follows:
  - First Failure = Recover Service
  - Second Failure = Application Restart
  - Third Failure = Switchover

In this situation, the system administrator should also set the service recovery actions for service Y to:

- First Failure = Recover Service
- Second Failure = Application Restart
- Third Failure = Switchover

Note that if service X fails, the dependent service Y must also fail. If the service recovery actions for service Y are different to those for service X, they may take precedence, for example service X requires a switchover but the failure of service Y has already triggered a service restart action.

This advice applies only to services which are automatically protected by Orion Failover Engine and dependent upon one another. These dependencies may be examined via the Windows Service Control Manager, under **Properties > Dependencies**.

For services which are shown in the *Protected services depend on:* pane of the Orion Failover Manager **Applications: Services** page, this advice is *not* applicable, because:

1. These services do not depend on protected services; rather, protected services are dependent upon them; and

2. These services are not directly managed by Failover Engine and therefore have no configurable recovery actions.

**Note:** If an application with the failure option set to Application Restart fails, only the services that have failed are restarted. Dependent services do not stop and restart as a result of the failure.

## When Additional Pollers (AP)s are not installed, create an Exclusion Filter to reduce replication traffic

To prevent needless replication of temporary files created when Additional Pollers are not used, create an Exclusion Filter.

### To create the Exclusion Filter:

1. Launch SolarWinds Orion Failover Manager.
2. Navigate to the **Data: File Filters** pane, and click **Add Exclusion Filter** to open the *Add Exclusion Filter* dialog.
3. Type the complete path to or browse to locate the file at the following locations:

```
Windows Server 2003: C:\Documents and Settings\All
Users\Application Data\SolarWinds\JobEngine\*.sdf
```

or

```
Windows Server 2008: C:\ProgramData\Application
Data\SolarWinds\JobEngine\*.sdf
```

4. click **OK**.

## When IPAM 2.0 is installed, create an Inclusion Filter to replicate the `IPAM.attributes.xml` file

To create the Inclusion Filter:

1. Launch the Orion Failover Manager on the active server.
2. Navigate to **Data: File Filters**.
3. Click **Add Inclusion Filter**.
4. Type the path below or browse to the file location.

```
<installation_dir>\Orion\Information
Service\2.0\Schemas\IPAM.attributes.xml
```

5. Click **OK**.



## Chapter 3

# Installation Verification

Installation verification tests and validates your installation. The following exercises are examples that must be performed in order. SolarWinds recommends performing a switchover rather than a failover to test the operation of the passive server.

**Warning:** SolarWinds does not recommend attempting to test a failover on a properly operating server pair using methods such as unplugging a power cord. When power is lost, any data not written to the passive server is lost.

## *Failover Simulation Exercise*

This exercise demonstrates that the secondary server can function as the primary server without the test data being immediately replicated back to the original server. During the exercise, you will stop the primary server from providing service and hide it from the network, then introduce the secondary server to the network and allow it to provide service.

**Note:** Using the System Tray icon, verify that the primary server displays **P/A** indicating that it is the active server. On the secondary server, repeat the process and verify that the secondary server displays **S/—** indicating that it is passive.

Using the SolarWinds Orion Failover Manager, navigate to the **Data: Replication** tab. Verify that both the *File System* and the *Registry* status display as *Synchronized*.

Notify any local users that the service will be unavailable for the duration of the exercise.

Machine	Activity	Result
Primary	Shut down the Orion Failover Engine. Select <b>Stop SolarWinds Orion Failover Engine and all protected applications</b> , and then click <b>OK</b> .	Orion Failover Engine stops all monitored services and exits.
	With Orion Failover Engine shut down, on the primary server, click <b>Start &gt; All Programs &gt; SolarWinds Orion &gt; Orion Failover Engine &gt; Configure Server</b> to launch the <b>Configure Server</b> wizard. In the wizard, change the primary server's role to passive.	Primary server becomes passive
	Start Orion Failover Engine, and then shut it down. Select <b>Stop Orion Failover Engine and all protected applications</b> , and then click <b>OK</b> .	This activates the network filter hiding the primary server from the network.

Machine	Activity	Result
Secondary	Click <b>Start &gt; All Programs &gt; SolarWinds Orion &gt; Orion Failover Engine &gt; Configure Server</b> to launch the <b>Configure Server</b> wizard. In the wizard, change the secondary server role to active, and then start the Orion Failover Engine.	The secondary server starts as the active server.
Client	Compare application functional status to defined criteria for availability and performance.	The secondary server acts as the primary.

## Data Replication Exercise

The Data Replication exercise follows the Failover Simulation exercise performed previously. The objective is to take a working active server (the secondary server) and synchronize it with the passive (primary server). This exercise also demonstrates that all the correct services stopped when the primary server became passive.

### Notes:

- Orion Failover Engine is running on the secondary active server. Using the System Tray icon, verify that the server status displays S/A. Orion Failover Engine is not running on the primary server which is set to passive. Using the System Tray icon, verify that the server status displays —/— to indicate that Orion Failover Engine is not running.
- Notify any local users that the service will be unavailable for the duration of the exercise.

Machine	Activity	Result
Primary	Start Orion Failover Engine.	Orion Failover Engine starts. The Orion Failover Engine shows the connection between the secondary (active) and primary (passive) servers.
	Wait for both the Registry and the File System to become Synchronized. Access the Orion Failover Engine logs and confirm that no exception errors occurred during synchronization.	Data replication resumes from the secondary server back to the primary server. Both the File System & Registry become Synchronized.

Both machines are resynchronized. All data changed on the secondary machine while the primary was running Orion Failover Engine is updated onto the primary machine. The secondary (active) machine continues to provide service.

## Switchover Exercise

This exercise demonstrates the ability to switch the functionality and operations of the active server on command to the other server in the pair using SolarWinds Orion Failover Manager. Perform this exercise only after successfully completing the Failover Simulation and Data Replication Exercises.

Notify any local users that the service will be unavailable for the duration of this exercise.

**Notes:** Using the System Tray icon, verify that the secondary server is active (**S/A**) and servicing clients. On the primary server, verify that the server is passive using the System Tray icon status (**P/—**). On the secondary server, launch SolarWinds Orion Failover Manager and select the **Data: Replication** tab. Verify that both the *File System* and *Registry* status are *Synchronized*.

Machine	Activity	Result
Orion Failover Engine	Click <b>Make Active</b> and confirm.	The Orion Failover Engine displays the services stopping on the active server. Once all services are stopped, the active server becomes passive and the passive server becomes active. The Orion Failover Engine shows the services starting on the newly active server. Both the File System and the Registry are Synchronized.
Any	Confirm application performance and availability meets previously defined criteria. Verify that client applications are running as expected after the switchover process.	Service as usual. You might have to refresh or restart some client applications as a result of a switchover.

Application service transferred from the originally active machine to the originally passive machine. Document the application-client behavior for future reference.