Administrator's Guide

For
Ipswitch Failover v9.5

IPSWITCH

Copyright

Contents

About This Book

The Administrator Guide provides information about configuring and performing the day-to-day management of Ipswitch Failover when deployed in a Pair over a Local Area Network (LAN) or Wide Area Network (WAN), or a Trio deployed over both a LAN for High Availability and a WAN for Disaster Recovery. Additionally, this guide provides information about configuring network protection, application protection, data protection, split-brain avoidance, and more. To help you protect your applications, this guide provides an overview of the protection offered by Ipswitch Failover and the actions that Ipswitch Failover can take in the event of a network, hardware, or application failure.

Intended Audience

This guide assumes a working knowledge of networks including the configuration of TCP/IP protocols and a sound knowledge of domain administration on the Windows™ 2008 R2, 2012, and 2012 R2 platforms, notably in Active Directory and DNS.

Using the Administrator's Guide

This guide is designed to provide information related to the daily management of your Ipswitch Failover Cluster after successful installation. To help you protect your applications, this guide provides an overview of the protection offered by Ipswitch Failover and the actions that Ipswitch Failover can take in the event of a network, hardware, or application failure. The information contained in this guide is current as of the date of printing.

Overview of Content

This guide is designed to give guidance on the configuration and administration of Ipswitch Failover, and is organized into the following sections:

Preface — About This Book (this chapter) provides an overview of this guide and the conventions used throughout.

Chapter 1 — Ipswitch Failover Concepts presents an overview of Ipswitch Failover architecture and the five levels of protection provided by Ipswitch Failover.

Chapter 2 — Status and Control describes how to connect to Ipswitch Failover using the Failover Management Service or the Ipswitch Advanced Management Client to review the status of and manage a Cluster.

Chapter 3 — Configuring Ipswitch Failover discusses how to configure Ipswitch Failover using the *Configure Server Wizard*.

Chapter 4 — Server Protection discusses how the Ipswitch Failover solution protects users from server system failure or server hardware crash.

Chapter 5 — Network Protection describes how Ipswitch Failover protects against network failure by ensuring that the network identity of the production server, IP address, etc. are provided to users.

Chapter 6 — Application Protection discusses how Ipswitch Failover maintains the protected application environment ensuring that applications and services stay alive on the network.

Chapter 7 — Data Protection discusses how Ipswitch Failover intercepts all data written by users and protected applications and maintains a copy of this data for use in case of failure.

Appendix A — Other Administrative Tasks discusses additional tasks for the administrator to configure system logging and alerting functions.

Appendix B — Troubleshooting discusses common issues that may appear and techniques to troubleshoot the issue and includes two active servers or two passive servers, application slowdown, channel drops, and MaxDiskUsage errors.

Appendix C — Ipswitch SCOPE Data Collector discusses how to use Ipswitch SCOPE to measure bandwidth, and interrogate your server environment to prepare for installation.

Document Feedback

Ipswitch welcomes your suggestions for improving our documentation and invites you to send your feedback to *docfeedback@ipswitch.com* .

Abbreviations Used in Figures

The figures in this book use the abbreviations listed in the table below.

Table 1: Abbreviations

Abbreviation	*Description*
Channel	Ipswitch Channel
NIC	Network Interface Card
P2P	Physical to Physical
P2V	Physical to Virtual
V2V	Virtual to Virtual
SAN	Storage Area Network type datastore

Technical Support and Education Resources

The following sections describe the technical support resources available to you. To access the current version of this book and other books, go to *http://www.ipswitch.com/support* .

Online and Telephone Support

Use online support to view your product and contract information, and to submit technical support requests. Go to *http://www.ipswitch.com/support* .

Support Offerings

To find out how Ipswitch Support offerings can help meet your business needs, go to *http://www.ipswitch.com/support* .

Ipswitch Professional Services

Ipswitch Professional Services courses offer extensive hands-on labs, case study examples, and course materials designed for use as on-the-job reference tools. Courses are available on site, in the classroom, and live online. For the day-to-day operations of Ipswitch Failover, Ipswitch Professional Services provides offerings to help you optimize and manage your Ipswitch Failover servers. To access information about education classes, certification programs, and consulting services, go to *http://www.ipswitch.com/support* .

Getting Started

Chapter 1

Ipswitch Failover Concepts

Overview

Ipswitch Failover is a Windows based system specifically designed to provide *High Availability (HA)* and *Disaster Recovery (DR)* to server configurations in one solution that does not require any specialized hardware. To appreciate the full capabilities of Ipswitch Failover you must understand the basic concepts under which Ipswitch Failover operates and the terminology used.

Note: *In this document, the term "Cluster" refers to an Ipswitch Failover Cluster. Refer to the Glossary for more information about Ipswitch Failover Clusters.*

Architecture

Ipswitch Failover provides a flexible solution that can be adapted to meet most business requirements for deployment and management of critical business systems. Capitalizing on VMware vCenter Server's ability to manage virtual infrastructure assets combined with Ipswitch's application-aware continuous availability technology, Ipswitch Failover brings a best in class solution for protecting critical business systems.

Ipswitch Failover consists of the Failover Management Service that is used to deploy and manage the Ipswitch Failover service that provides for application-aware continuous availability used for protecting critical business systems.

Using Failover Management Service, users can deploy and manage Ipswitch Failover with the ability to view Ipswitch Failover status and perform most routine Ipswitch Failover operations from a single pane of glass.

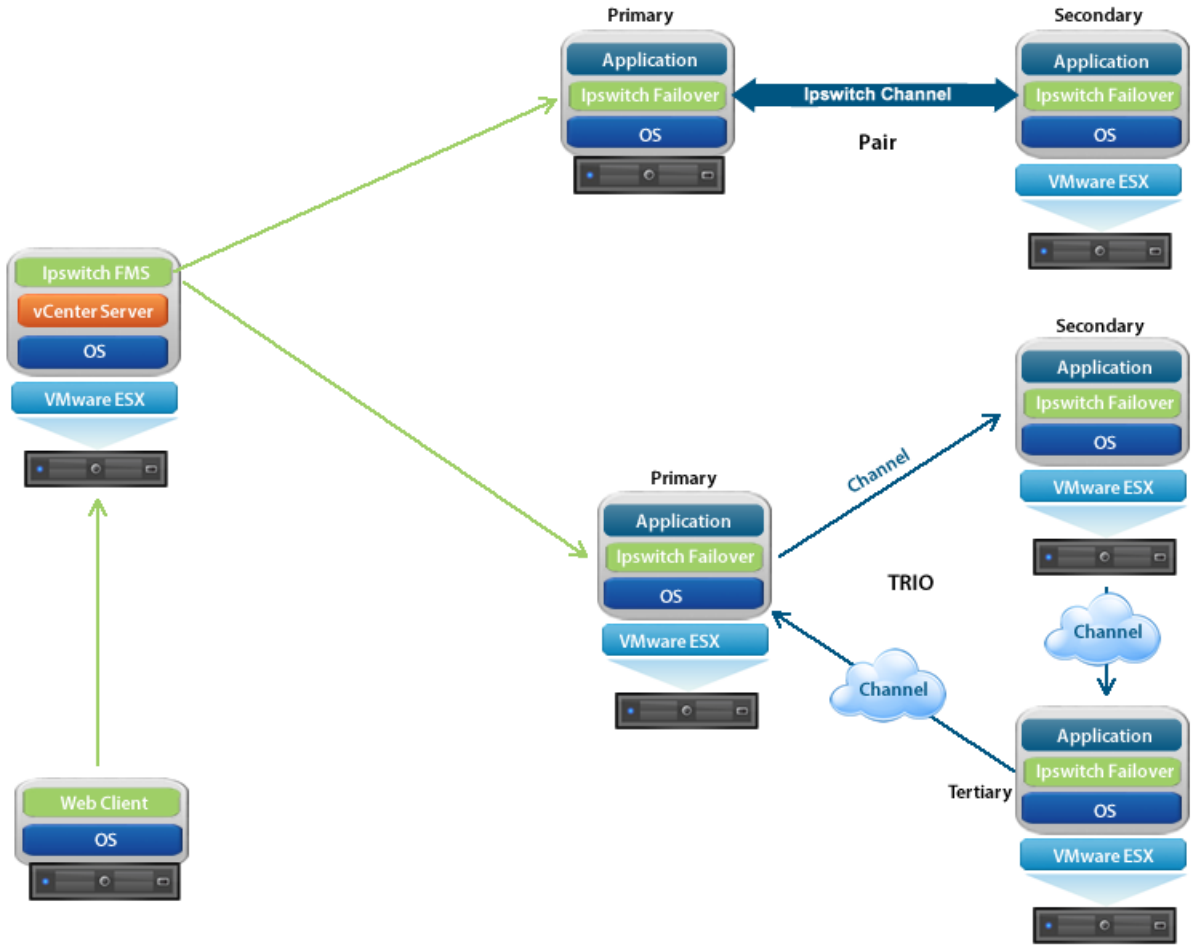

Figure 1: Deployment Architecture

Ipswitch describes the organization of Ipswitch Failover servers based upon Clusters, Cluster status, and relationships between Clusters. Ipswitch refers to a Cluster of two servers as an Ipswitch Failover Pair or three servers as an Ipswitch Failover Trio. Installing Ipswitch Failover on the servers and assigning an identity to the servers results in an Ipswitch Failover Pair or Trio.

Each server is assigned both an *Identity* (*Primary* , *Secondary* , or *Tertiary* if installed) and a *Role* (*Active* or *Passive*). Identity is used to describe the physical instance of the server while the 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 (except in the special case described below) whereas the role of the server is subject to change as a result of the operations the server is performing. When Ipswitch Failover is deployed on a Pair or Trio of servers, Ipswitch Failover can provide all five levels of protection (Server, Network, Application, Performance, and Data) and can be deployed for High Availability in a Local Area Network (LAN) or Disaster Recovery over a Wide Area Network (WAN) or both High Availability and Disaster Recovery.

Note: *The identity of an existing Disaster Recovery (DR) Secondary server can change under certain circumstances. This is when a DR pair is extended to become a Trio. In this case, the Secondary will be re-labeled as the Tertiary, so that the Tertiary is always the DR stand-by in any Trio.*

In its simplest form, Ipswitch Failover operates as an Ipswitch Failover Pair with one server performing an active role (normally the Primary server) while the other server performs a passive role (normally the Secondary server). The server in the active role provides application services to users and serves as the source for replication while

the server in the passive role serves as the standby server and target for replicated data. This configuration supports replication of data between the active and passive server over the Ipswitch Channel.

When deployed for High Availability, a LAN connection is used. Due to the speed of a LAN connection (normally 100 Mb or more) bandwidth optimization is not necessary.

When deployed in a WAN for Disaster Recovery, Ipswitch Failover can assist replication by utilizing WAN Compression with the built-in WAN Acceleration feature.

Additionally, Ipswitch Failover can be deployed as a Trio incorporating both High Availability (HA) and Disaster Recovery (DR) or can be extended from an HA or DR pair to a Trio resulting in the following scenarios:

- Primary-Secondary (HA) + Tertiary (DR)
- Primary-Secondary (HA) > extending Pair to Trio resulting in: Primary-Secondary (HA) + Tertiary (DR)
- Primary-Secondary (DR) > extending Pair to Trio resulting in: Primary-Secondary (HA) + Tertiary (DR)

Protection

Ipswitch Failover provides five levels of protection to ensure that end-user clients remain connected in the event of a failure.

- **Server Protection** — Ipswitch Failover continues to provide availability to end-user clients in the event of a hardware failure or operating system crash. When deployed, Ipswitch Failover provides the ability to monitor the active server by sending “I‘m alive” messages from the passive server to the active server which reciprocates with an acknowledgment over a network connection referred to as the Ipswitch Channel. Should the passive server detect that the process or "heartbeat" has failed, it can then initiate a failover.

  A failover occurs when the passive server detects that the active server is no longer responding. This can be because the active server’s hardware has crashed or because its network connections are lost. Rather than the active server being gracefully closed, it has been deemed to have failed and requires no further operations. In a failover, the passive server is brought up immediately to take on the role of the active server. The mechanics of failover are discussed later in this guide.
- **Network Protection** — Ipswitch Failover proactively monitors the ability of the active server to communicate with the rest of the network by polling up to three defined nodes around the network, including by default, the default gateway, primary DNS server, and the Global Catalog server at regular intervals. If all three nodes fail to respond, for example, if a network card or local switch fails, Ipswitch Failover can gracefully switch the roles of the active and passive servers (referred to as a switchover) allowing the previously passive server to assume an identical network identity to that of the previously active server. After the switchover, the newly active server then continues to service the clients.
- **Application Protection** — Ipswitch Failover running on the active server locally monitors the applications and services it has been configured to protect through the use of plug-ins. If a protected application should fail, Ipswitch Failover will first try to restart the application on the active server. If a restart of the application fails, then Ipswitch Failover can initiate a switchover.

  A switchover gracefully closes down any protected applications that are running on the active server and restarts them on the passive server along with the application or service that caused the failure. The mechanics of switchover are discussed in more detail later in this guide.
- **Performance Protection** — Ipswitch Failover proactively monitors system performance attributes to ensure that your protected applications are actually operational and providing service to your end users, and that the performance of those applications is adequate for the needs of those users.

  Ipswitch Failover Plug-ins provide these monitoring and preemptive repair capabilities. Ipswitch Failover Plug-ins monitor application services to ensure that protected applications are operational, and not in a ‘hung’ or ‘stopped’ state. In addition to monitoring application services, Ipswitch Failover can also monitor specific application attributes to ensure that they remain within normal operating ranges. Similar to application

monitoring, various rules can be set to trigger specific corrective actions whenever these attributes fall outside of their respective ranges.

- **Data Protection** — Ipswitch Failover ensures the data files that applications or users require in the application environment are made available should a failure occur. Once installed, Ipswitch Failover can be configured to protect files, folders, and even the registry settings of the active server by mirroring these protected items, in real-time, to the passive server. This means that if a failover occurs, all files that were protected on the failed server will be available to users on the server that assumes the active role after the failover.

  Updates to protected files are placed in a queue on the active server (the send queue), ready to be sent to the passive server with each request numbered to maintain its order in the queue. Once the send queue reaches a specific configured size, or the configured time duration has expired, the update is sent to the passive server, which places all the requests in an array of log files termed the receive queue. The passive server then confirms the changes have been logged by sending the active server an acknowledgment.

  The passive server's receive queue is then read in numerical order and a duplicate set of file operations are applied to the disk of the passive server.

Ipswitch Failover provides all five protection levels simultaneously ensuring that all facets of the user environment are maintained at all times and that the network (the *Public Network*) continues to operate through as many failure scenarios as possible.

Ipswitch Failover Networking Configuration

The server IP address used by a client to connect to the active server, the Public IP address, must be a static IP address (not DHCP-enabled). In the example below, the Public IP address is configured as `192.168.1.127`.

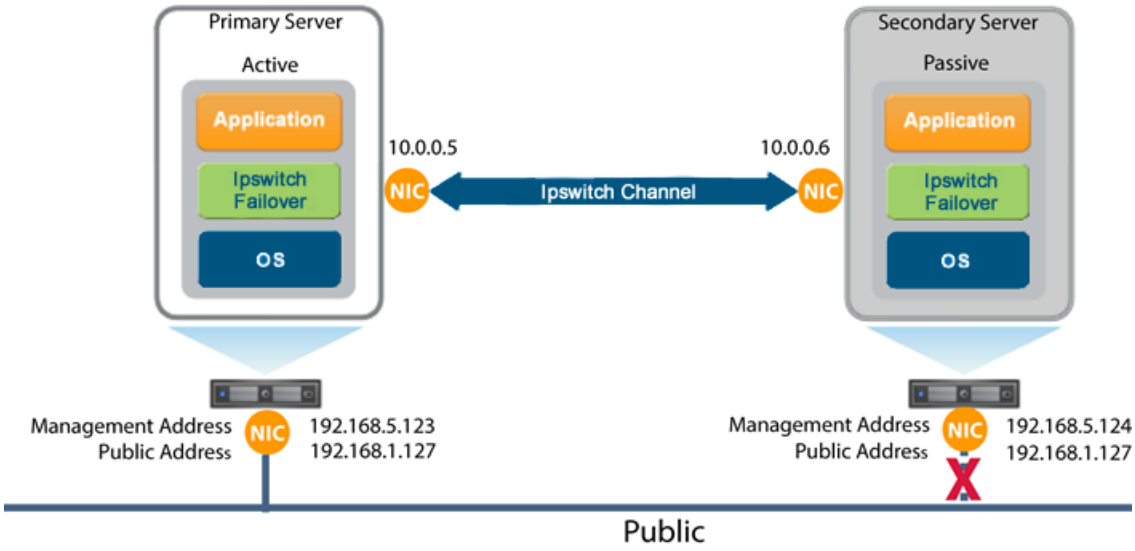

Figure 2: Ipswitch Failover Network Configuration

Note: *The IP addresses of all NICs on the server can be obtained using a Windows command prompt and typing* `ipconfig /all`.

Ipswitch Failover uses a proprietary filtering system that works with the native Windows Filter Platform to expose a set of Application Programming Interfaces (APIs) to permit, block, modify, and/or secure inbound and outbound traffic while providing enhanced performance over previous versions of the Ipswitch Packet Filter Driver.

In a High Availability configuration, the Public NIC on the passive server uses the same IP address as the active server but is prevented from communicating with the live network through a filtering system installed with Ipswitch Failover. This filter prevents traffic using the Public IP address from being committed to the wire. It also prevents NetBIOS traffic utilizing other IP addresses on the NIC from being sent to prevent NetBIOS name resolution conflicts.

When configured for Disaster Recovery (DR) to a remote site with a different subnet, Ipswitch Failover must be configured to use a different Public IP address for the Primary and Secondary servers. When a switchover is performed, the DNS server will be updated to redirect users to the new active server at the DR site. These updates are not required when the same subnet is used in the Disaster Recovery Site. Ipswitch Failover uses DNS Update task to update Microsoft Windows 2003, 2003 R2, 2008, 2008 R2, 2012, and 2012 R2 DNS servers with the new Public IP address. DNS Update runs the `DNSUpdate.exe` to perform the following actions:

- First, *DNSUpdate* must unregister the current address with all DNS servers that have an entry for the server (this may not be all DNS servers in the enterprise). Unregistering the address involves removing the 'A host record' from the Forward lookup zone and removing the 'PTR record' from any relevant reverse lookup zones.
- Next, *DNSUpdate* must register the new address with all DNS servers that need an entry (again this may not be all DNS servers in the enterprise). Registering the address involves adding the 'A host record' to the Forward lookup zone and adding the 'PTR record' to the pertinent reverse lookup zone.
- Finally, where secondary DNS servers are present, *DNSUpdate* must instruct them to force a replication with the already updated Primary servers.

The NICs on the Primary and Secondary servers intended for use by the Ipswitch Channel must be configured so that they use IP addresses outside of the Public Network subnet range. These addresses are termed the Ipswitch Channel addresses.

Important: *NetBIOS must be disabled for the Ipswitch Channel(s) on the active and passive servers because the Primary and Secondary servers use the same NetBIOS name. When Ipswitch Failover installation is complete (runtime), NetBIOS will automatically be disabled across the channel(s) preventing NetBIOS name conflicts.*

The NICs that allow the connectivity across the Ipswitch Channel can be standard 100BaseT or Gigabit Ethernet cards providing a throughput of 100Mbits per second or more across standard Cat-5 cabling.

Note: *A dedicated channel requires no hubs or routers, but any direct connection requires crossover cabling.*

When configured for a WAN deployment, the Ipswitch Channel is configured using static routes over switches and routers to maintain continuous communications independent from traffic on the Public Network.

Ipswitch Failover Communications

The Ipswitch Channel is a crucial component of the setup and is configured to provide dedicated communications between the servers. When deploying in a pair configuration, each server in the pair requires at least one network card (see Single NIC configuration in the Installation Guide) although two network cards are recommended (one NIC for the Public Network connection and at least one NIC for the Ipswitch Channel connection). An additional pair of NICs may be used for the Ipswitch Channel to provide a degree of redundancy. In this case, the Ipswitch Channel is said to be *Dualed* if more than one dedicated NIC is provided for the Ipswitch Channel on each server.

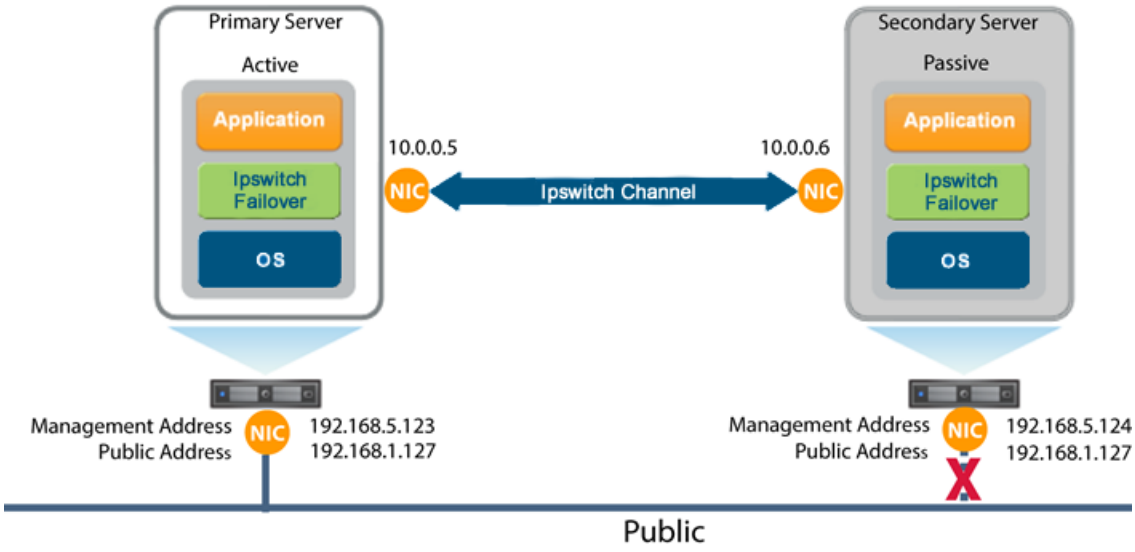

Figure 3: Ipswitch Failover Pair Communications

Note: *To provide added resilience, the communications for the second channel must be completely independent from the first channel, for example, they must not share any switches, routers, or WAN connection.*

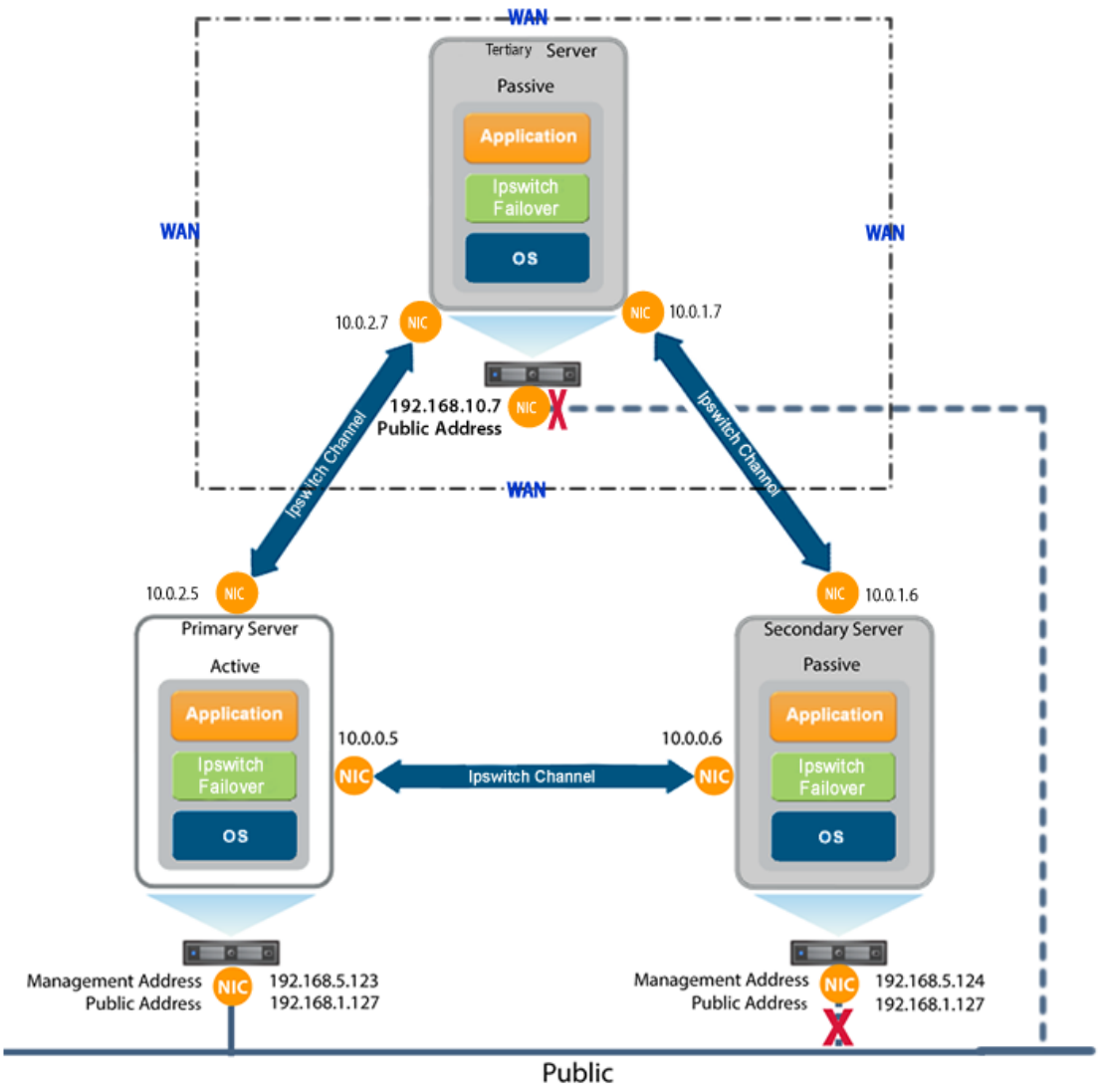

Figure 4: Trio Configuration

Ipswitch Failover Switchover and Failover Processes

Ipswitch Failover uses four different procedures to change the role of active and passive servers depending on the status of the active server.

> ***Note:*** *This section illustrates the simpler cases of switchover and failover in an Ipswitch Failover Pair.*

The Managed Switchover Process

A managed switchover can be initiated manually from the Failover Management Service or the Advanced Management Client **Server Summary** page by selecting the server to make active and clicking the **Make Active** button. When a managed switchover is initiated, the running of protected applications is transferred from the active machine to a passive machine in the Cluster - the server roles are reversed.

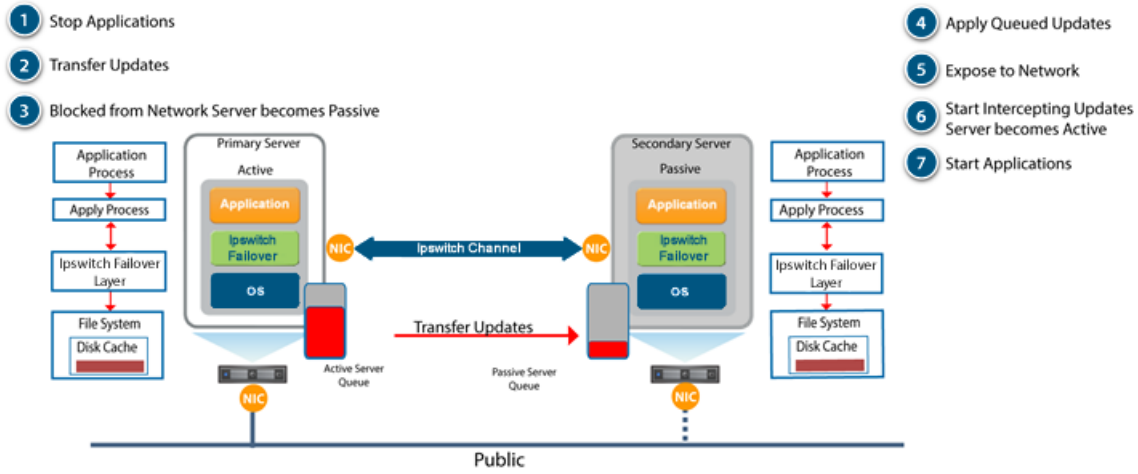

Figure 5: Ipswitch Failover Switchover Process

The automatic procedure executed during a managed switchover operation includes the following steps:

1. Stop the protected applications on the active server. Once the protected applications are stopped, no more disk updates are generated.
2. Send all updates that remain queued on the active server to the passive server. After this step, all updates are available on the passive server.
3. Change the status of the active server to '*switching to passive*'. The server is no longer visible from the network.
4. Apply all queued updates on the passive server.
5. Change the status of the passive server to '*active*'. After this step, the new active server starts intercepting disk I/Os and queues them for the new passive server. The new active server becomes visible on the network with the same identity as the old active server.
6. Change the status of the old active server from '*switching to passive*' to '*passive*'. The new passive server begins accepting updates from the active server.
7. Start the same protected applications on the new active server. The protected applications become accessible to users.

The managed switchover is complete.

The Automatic Switchover Process

An automatic-switchover (auto-switchover) is triggered automatically if a protected application, which the system is monitoring, fails.

An auto-switchover is different from a managed switchover in that although the server roles are changed, Ipswitch Failover is stopped on the previously active server to allow the administrator to verify the integrity of the data on the newly passive server and to investigate the cause of the auto-switchover.

Auto-switchovers are similar to failover (discussed next) but initiated upon the failure of a monitored application. Once the cause for the auto-switchover is determined and corrected, the administrator can use the **Configure Server Wizard** to change the server roles to their original state.

The Automatic Failover Process

When a passive server detects that the active server is no longer running properly, it assumes the role of the active server.

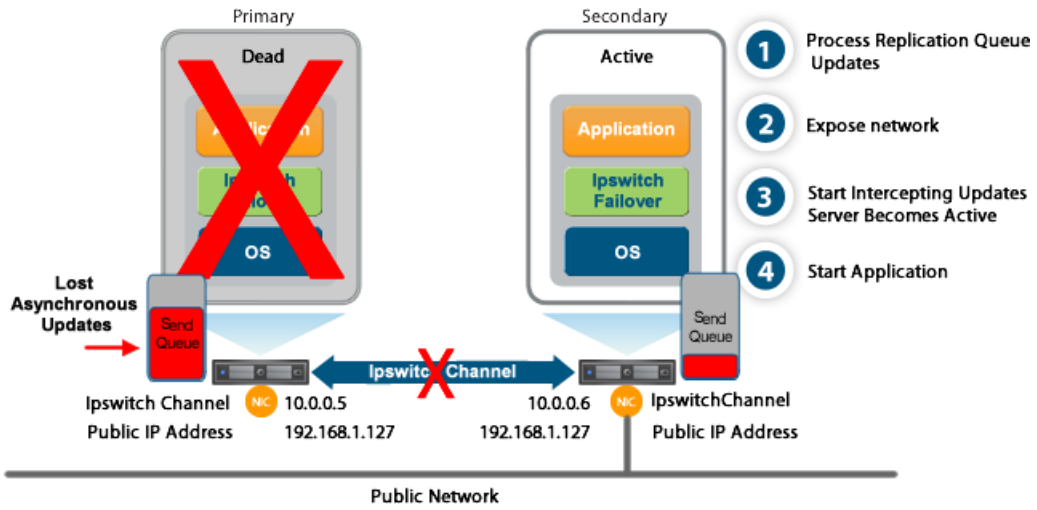

Figure 6: Ipswitch Failover Failover Process

During automatic failover, the passive server performs the following steps:

1. It applies any intercepted updates that are currently saved in the passive server receive queue as defined by the log of update records that are saved on the passive but not yet applied to the replicated files.

   The length of the passive server receive queue affects the time the failover process takes to complete. If the passive server receive queue is long, the system must wait for all updates to the passive server to complete before the rest of the process can take place. When there are no more update records that can be applied, it discards any update records that it is unable to apply (an update record can only be applied if all earlier update records are applied, and the completion status for the update is in the passive server receive queue).

2. It switches its mode of operation from passive to active.

   It enables the public identity of the server. The active and passive servers both use the same system name and same Public IP address. This Public IP address can only be enabled on one of the systems at any time. When the public identity is enabled, any clients previously connected to the server before the automatic failover are able to reconnect.

3. It starts intercepting updates to the protected data. Updates to the protected data are saved in the send queue on the local server.

4. It starts all the protected applications. The applications use the replicated application data to recover, and then accept re-connections from any clients. Any updates that the applications make to the protected data are intercepted and logged.

   At this stage, the originally active server is “off the air,” and the originally passive server assumes the role of the active server and runs the protected applications. Because the originally active server stopped abruptly, the protected applications may lose some data, but the updates that completed before the failover are retained. The application clients can reconnect to the application and continue running as before.

The Managed Failover Process

A managed failover is similar to an automatic-failover in that the passive server automatically determines that the active server has failed, and can warn the system administrator about the failure; but no failover occurs until the system administrator chooses to trigger this operation manually.

Recovery from a Failover

Assuming the Primary server was active and the Secondary server was passive before the failover, the Secondary server becomes active and the Primary server becomes passive after the failover.

Once the problem that initiated the failover is rectified it is a simple process to reinstate the Primary server as the active server and the Secondary server as the passive server.

The following steps are used to restore the previously failed server to the active role.

1. Correct the incident that caused the failover.
2. Verify the integrity of the disk data on the failed server.
3. Restart the failed server.
4. Ipswitch Failover will detect that it has not shut down correctly, and enter a *Pending Active* mode. In this mode, applications are not started, and the server is not visible on public network.
5. The server will attempt to connect to its peers, to determine if there is an active server. If it connects to its peers, and another server is active, it will become passive and begin replication. If it connects to its peers and no other server is active, it will become active, and begin replication. If it doesn't connect with its peers within 2 minutes, it becomes passive.
6. At this stage, the instances of Ipswitch Failover running on the servers connect and start to resynchronize the data on the Primary server.
7. Allow Ipswitch Failover to fully synchronize.

   When synchronization is complete, you can continue running with this configuration (for example, the Secondary is the active server and the Primary is the passive server), or initiate a managed switchover to reverse the server roles in the Ipswitch Failover Pair (for example, giving the Primary and Secondary the same roles that they had before the failover.
8. Perform a managed switchover.

Configuration

Chapter 2

Status and Control

Using the Failover Management Service User Interface

The Failover Management Service is the primary tool used for deployment and normal daily control of Ipswitch Failover. Most routine operations can be performed from the Failover Management Service User Interface thereby providing a lightweight, easily accessible, method of conducting Ipswitch Failover operations.

Configure Connection to VMware vCenter Server

The Configure Connection to VMware vCenter Server feature provides the ability to select and deploy Ipswitch Failover on a powered-on VM, with VMtools running, from the vCenter inventory. Also, a VMware vCenter Server connection is required to automatically create a stand-by Secondary and/or Tertiary VM server from the cluster and place them on a specific Host/Datastore.

Procedure

To configure a connection to VMware vCenter Server:

1. Click the **vCenter** button to display the *Configure Connection to VMware vCenter Server* page.
2. Enter the URL for the VMware vCenter Server, the username, and the password for a user account with the minimum privileges required by EMS to operate (see KB 2901), and then click **Next**.

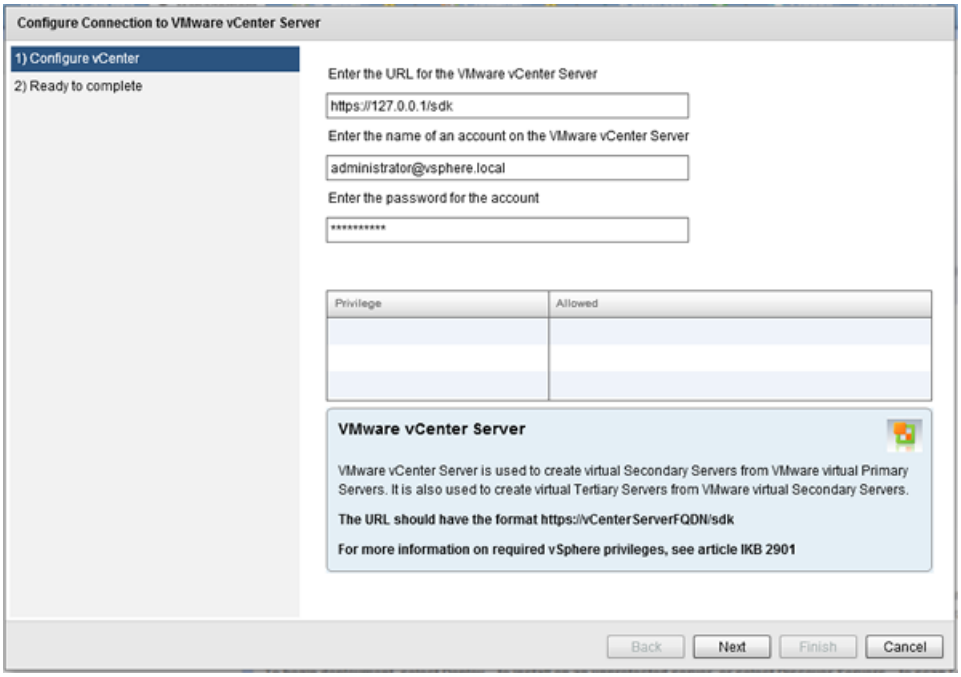

Figure 7: Configure vCenter

3. Review the information in the *Ready to Complete* dialog and then click **Finish**.

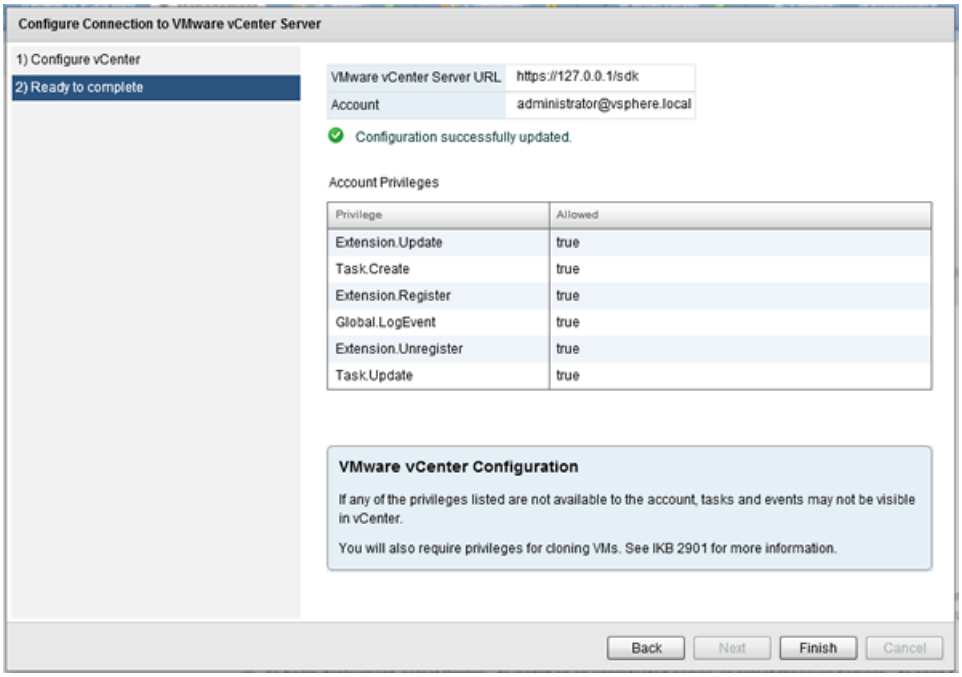

Figure 8: Ready to Complete

Configure VMware vCenter Converter

Use the *Configure VMware vCenter Converter* feature to convert physical Primary or VMs with a different hypervisor than ESXi to virtual Secondary and/or Tertiary servers during the automated cloning process used by Ipswitch Failover Management Service to create the Secondary and/or Tertiary servers.

Prerequisites

VMware vCenter Converter 5.5 or later must be installed manually.

Procedure

To configure the VMware vCenter Converter:

1. Click the **Converter** button to display the *Configure Connection to VMware vCenter Converter* page.

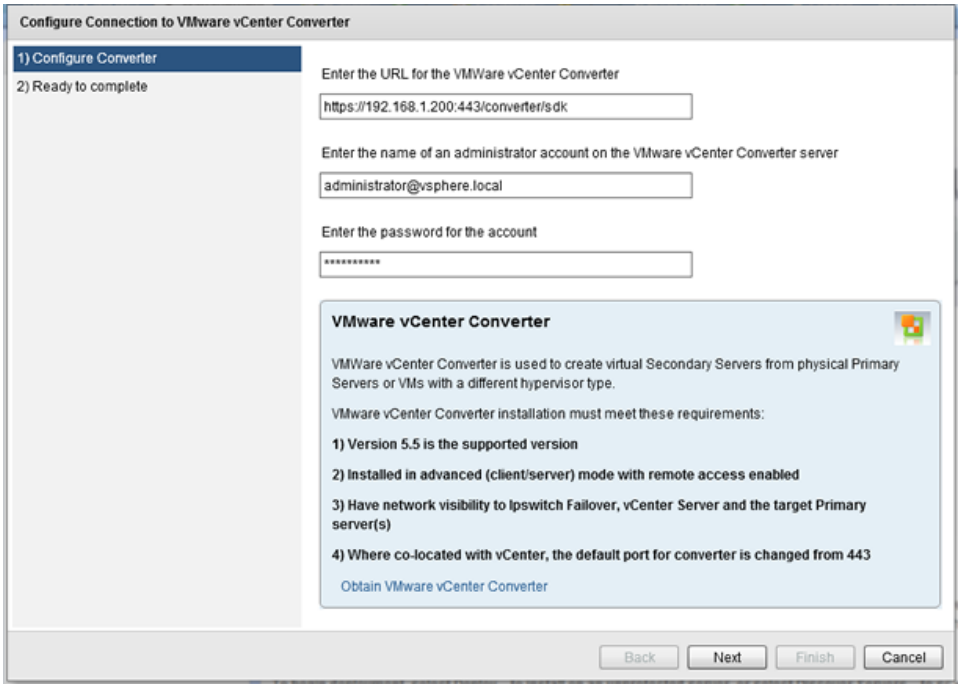

Figure 9: Configure VMware vCenter Converter

2. Enter the URL to where VMware vCenter Converter resides.
3. Enter the Username and Password for an account with Administrator permissions on the VMware vCenter Converter server. Click **Next**.

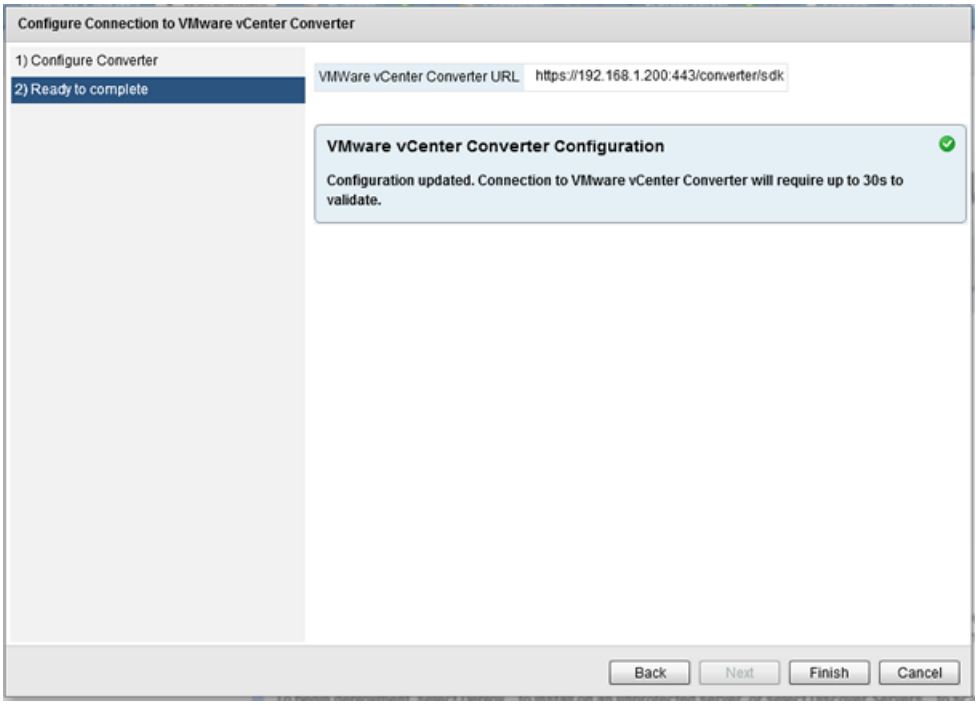

Figure 10: Ready to Complete

4. Click **Finish** to accept the configuration parameters.

Protected Servers

The *Protected Servers* pane provides a view of all servers that are currently protected by Ipswitch Failover and managed by Ipswitch Failover Management Service.

To view the status of a protected server, simply select the intended protected server.

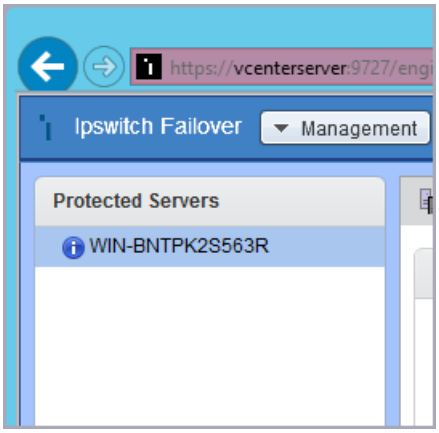

Figure 11: Protected Servers

Management

The *Management* drop-down menu provides access to all of the key functions to deploy Ipswitch Failover and get Ipswitch Failover up and running. It provides the ability to Deploy, Manage, Integrate, and License Ipswitch Failover.

Deploy

The Deploy group is focused on deployment actions and provides the functions to deploy Ipswitch Failover as a Primary, Secondary, or Tertiary server.

Configure Windows Firewall for Deployment

Ipswitch Failover Management Service, by default, automatically configures Windows Firewall rules for RPC Dynamic (recommended). In the event that a non-Windows firewall is being used, you must manually configure firewall rules to allow for deployment and operations.

- Configure the following firewall rules:
  - RPC Dynamic is required to allow remote deployment.
  - Ports 9727, 9728 for management from Ipswitch Failover Management Service.
  - Port 57348 for replicating data via the Ipswitch Channel between the Primary and Secondary servers.

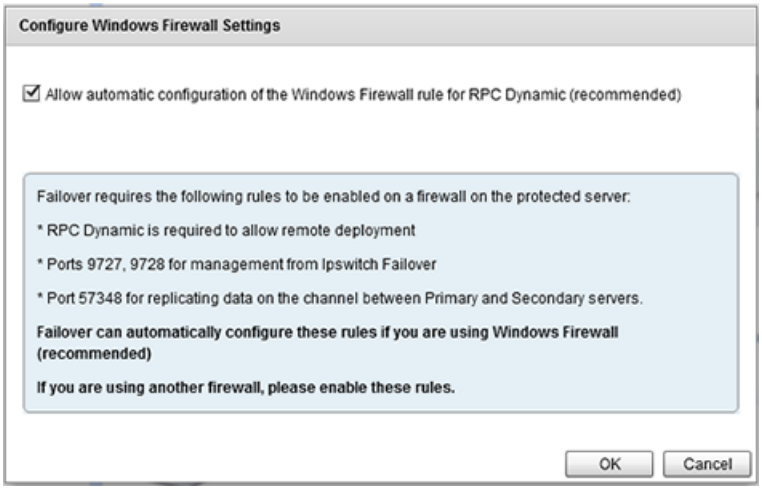

Figure 12: Configure Windows Firewall Settings

Deploy to a Primary Server

When this option is selected, Ipswitch Failover is installed onto the Primary server.

Prerequisites

Prior to attempting installation of Ipswitch Failover on the Primary server, ensure that the server meets all of the pre-requisites stated in the *Pre-install Requirements* section of the *Ipswitch Failover Installation Guide.*

Important: *Ipswitch Failover requires that Microsoft™ .Net Framework 4 be installed prior to Ipswitch Failover installation. If .Net Framework 4 is not installed, Ipswitch Failover will prevent installation until .Net Framework 4 is installed.*

Procedure

To Deploy Ipswitch Failover:

1. Having verified all of the environmental prerequisites are met, click on **Management** and navigate to **Deploy** > **Deploy to a Primary Server**.
   The *Deploy Failover* page is displayed.

   Note: *When deploying a Primary server, use a local administrator account to successfully deploy the Primary server.*

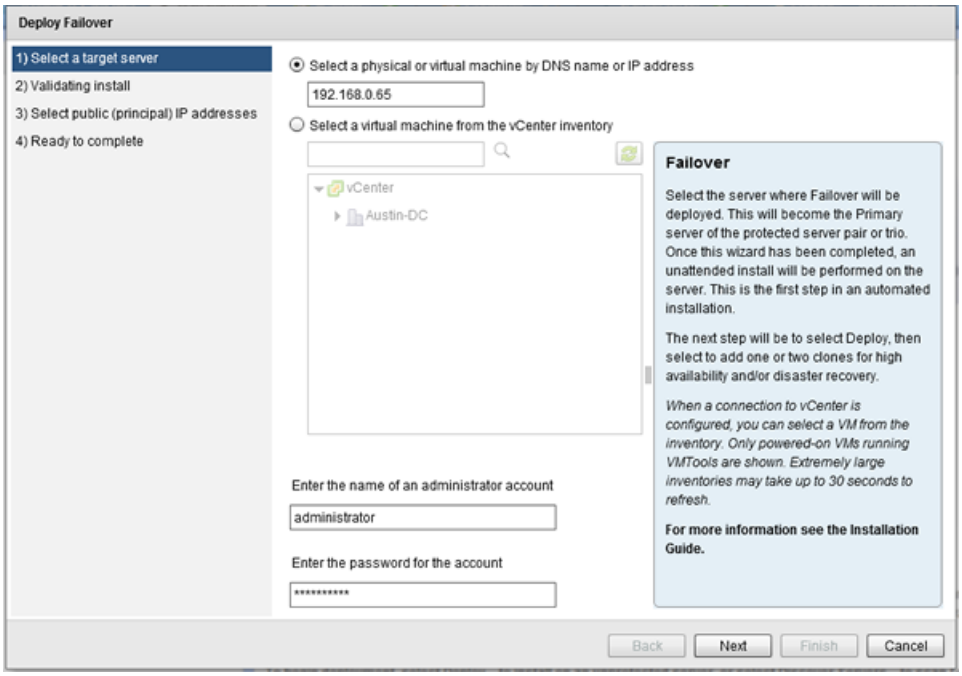

Figure 13: Deploy Ipswitch Failover page

2. Enter the DNS name or IP address of the server that will be the Primary server, or select a virtual server from the inventory. Enter credentials for a user that is a member of the local Administrator group on the target server and click **Next**.
   The *Validating Install* step is displayed. Ipswitch Failover automatically configures Windows firewalls to allow installation to continue and communications via the Ipswitch Channel and the Ipswitch Failover Management Service.

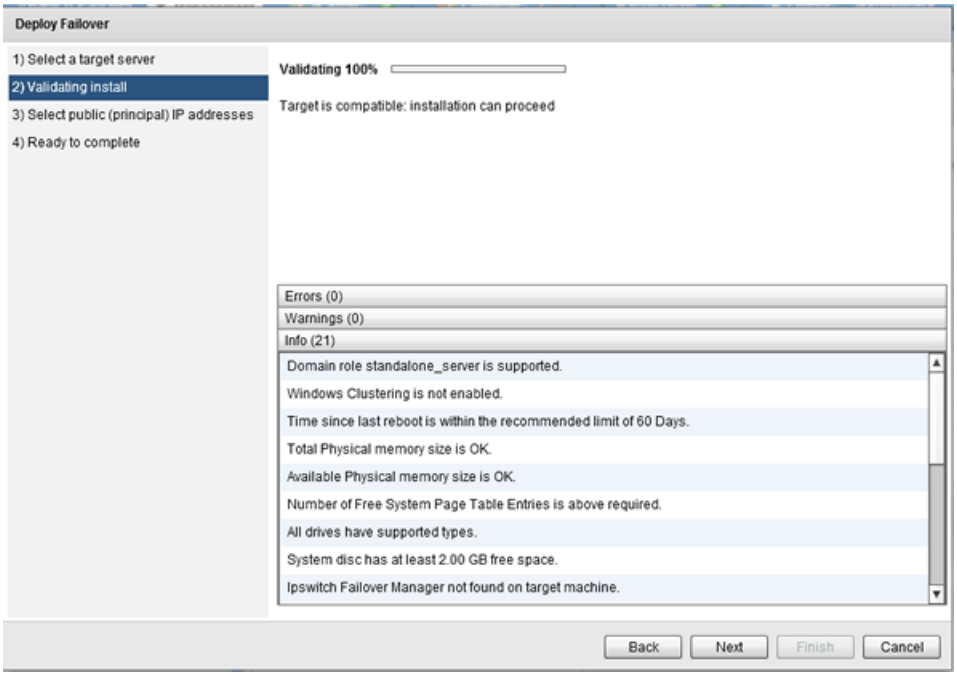

Figure 14: Validating Install step

3. Once the *Validating Install* dialog completes and displays that the server is a valid target, click **Next**. The *Select public (principal) IP addresses* step is displayed.

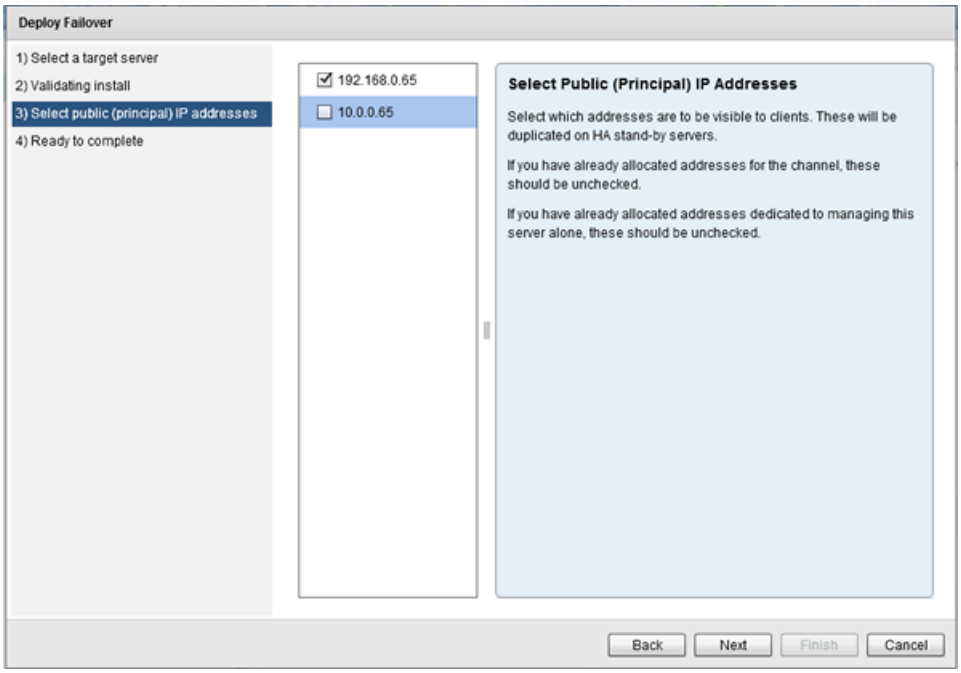

Figure 15: Select public (principal) IP addresses step

4. Verify that the proper IP address for the Public IP address is configured/selected and that the check box is selected. Click **Next**.
The *Ready to complete* step is displayed.

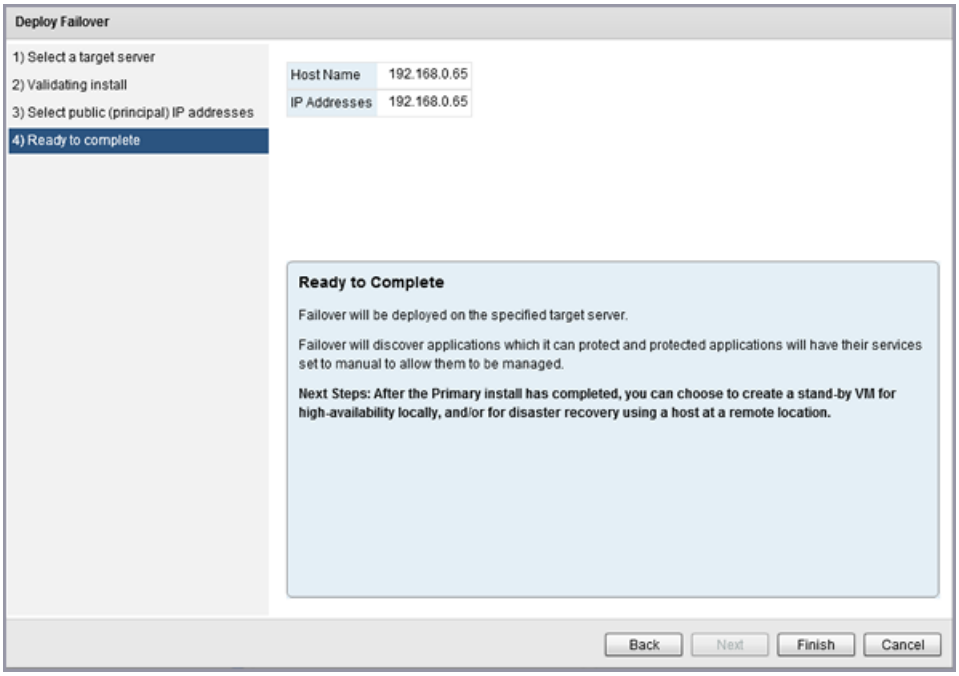

Figure 16: Ready to complete step

5. Review the information and click **Finish**.
   The installation of the Primary server proceeds.
6. Once installation of the Primary server is complete, in the *Protected Servers* pane, select the Primary server to display the *Server Summary* page .

Upgrade the Selected Server

Ipswitch Failover Management Service provides a simple process incorporating a wizard to upgrade from previous versions of the product.

1. From the **Management** drop-down menu, navigate to **Deploy** > **Upgrade the selected server**.
   The *Upgrade Failover* page is displayed.

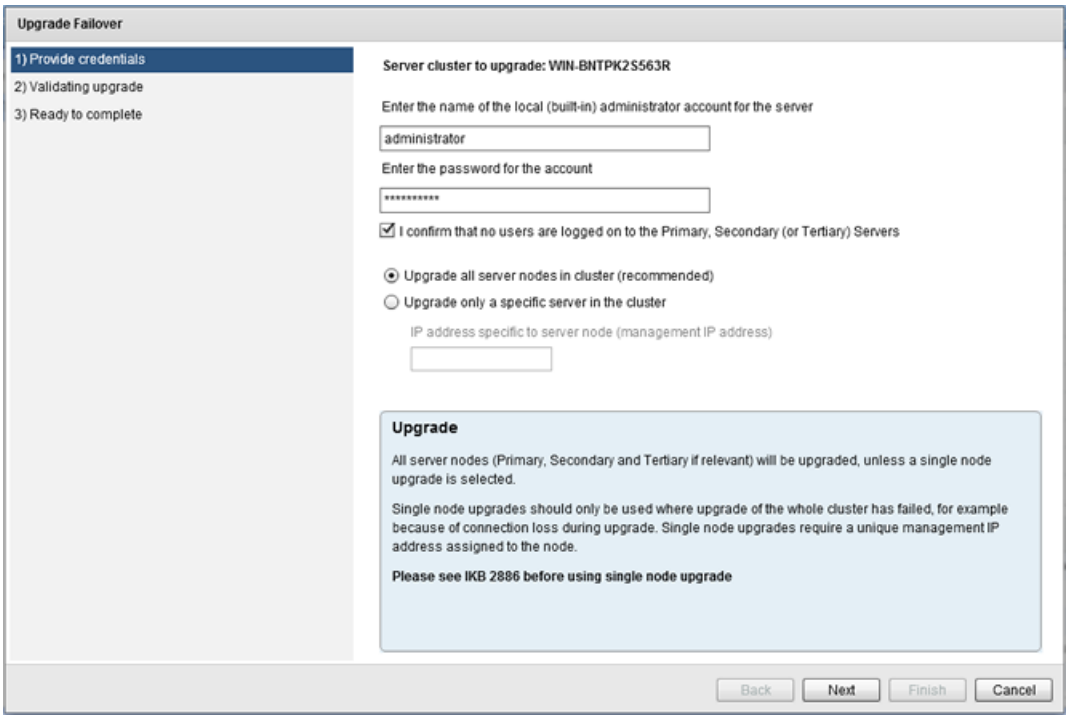

Figure 17: Upgrade Failover

2. Enter the name of the local built-in Administrator account and password. After confirming that no users are logged into the Primary, Secondary (or Tertiary) servers, select the check box.
3. Select to either upgrade all server nodes or only a specific server in the cluster. Click **Next**.

> ***Note:*** *Single node upgrades should only be used in the event the upgrade of the whole cluster has failed. If you select to upgrade only a specific server in the cluster, you must configure a Management IP address on the target server prior to attempting the upgrade. A new instance will then be added in the Protected Servers list represented by the management IP.*

The *Validating upgrade* step is displayed.

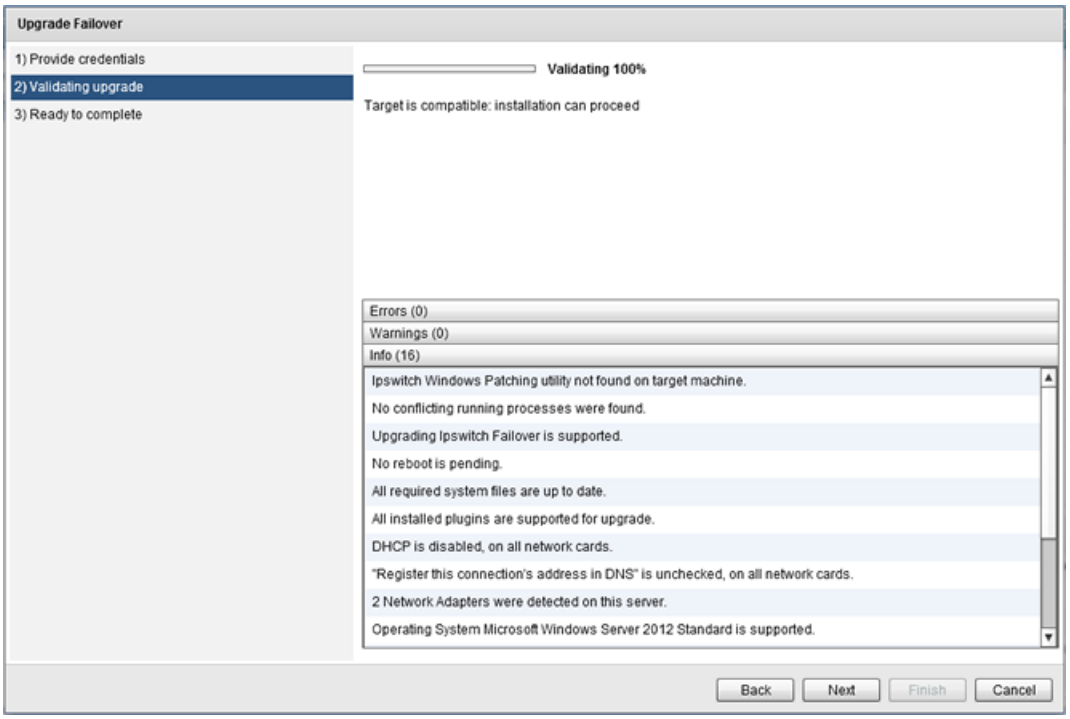

Figure 18: Validating upgrade step

4. Once validation is complete, click **Next**.
   The *Ready to complete* step is displayed.

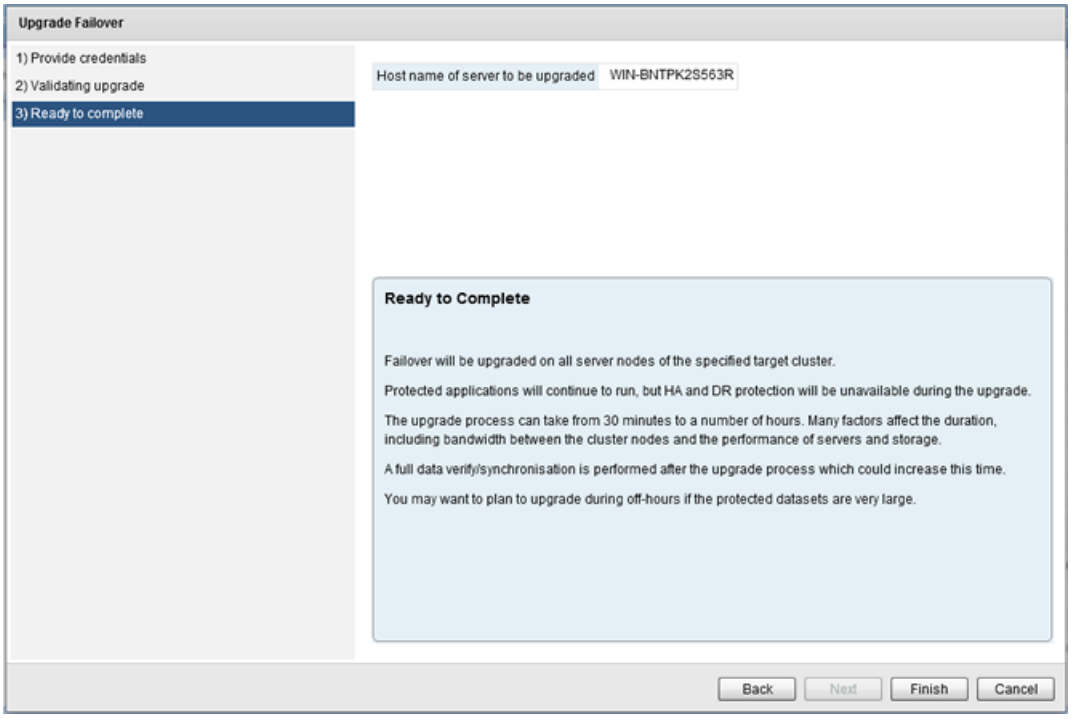

Figure 19: Ready to complete step

5. Review the information and click **Finish** to initiate the upgrade of the selected cluster or single server.

Uninstall from the Selected Server

The Ipswitch Failover Management Service allows you to uninstall Ipswitch Failover from a selected cluster.

Procedure

To uninstall from the selected server:

1. Select the intended server and from the **Management** drop-down menu, navigate to **Deploy** > **Uninstall from the Selected Server**.
   The *Uninstall Failover* step is displayed.

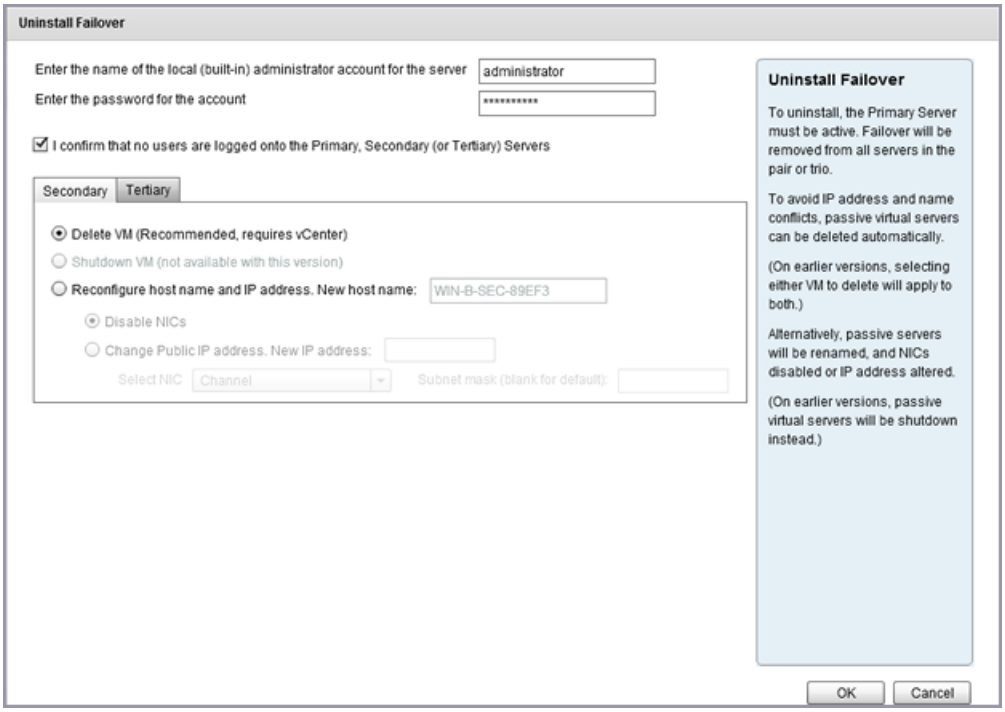

Figure 20: Uninstall Failover

2. Select one of the available (and applicable) uninstall options for Secondary (and Tertiary - if present).
   - Delete VM (Recommended, requires vCenter) - this option will delete the VM.
   - Shutdown VM - this option will uninstall Ipswitch Failover then shutdown the formerly passive server. This feature is only available when you have an Ipswitch Failover Management Service v9.5 managing a v9.0.x cluster.
   - Reconfigure host name and IP address - specify the new host name for the formerly passive server.

   Note: *This option is only available if you attempt to uninstall a v9.5 cluster from Ipswitch Failover Management Service v9.5*

3. Choose one of the available options:
   - Disable NICs - this option will uninstall Failover and disable all the existing NICs on the formerly passive server. The server will be shutdown and removed from the domain if it was previously a domain member.
   - Change Public IP address - this option will uninstall Failover then configure the newly specified IP address on the formerly passive server. The server will be left running.

Note: *In both cases, the passive server(s) will be removed from the domain.*

4. After verifying that no users are logged onto the Primary, Secondary, or Tertiary (if installed) servers, select the confirmation check box and provide the local (built-in) Administrator account valid on all servers. Click **OK**.
   The Uninstall Validation process will start. If no issues are found, Ipswitch Failover is uninstalled from the Primary, Secondary and Tertiary (if installed) servers.

Add a Stand-by Server for High Availability

The *Add a stand-by server for high availability* feature is used to create a Secondary server when deployed for high availability. Deploying for high availability means that failover will occur automatically when the active server fails. This feature can also be used to add a stand-by server for high availability to an existing disaster recovery pair. In this case, the new server will become the Secondary server and the existing Secondary/DR server will be re-labeled as the Tertiary.

Procedure

To add a stand-by VM for high availability:

1. On the Ipswitch Failover Management Service user interface, click the **Management** drop-down menu and navigate to **Deploy** > **Add a stand-by Server for high availability**.
   The *Add a Stand-by Server for High Availability* page is displayed.
2. Select clone type – select to use either automated cloning (recommended) or manual (using a third-party cloning tool) to clone a specific server. Click **Next**.

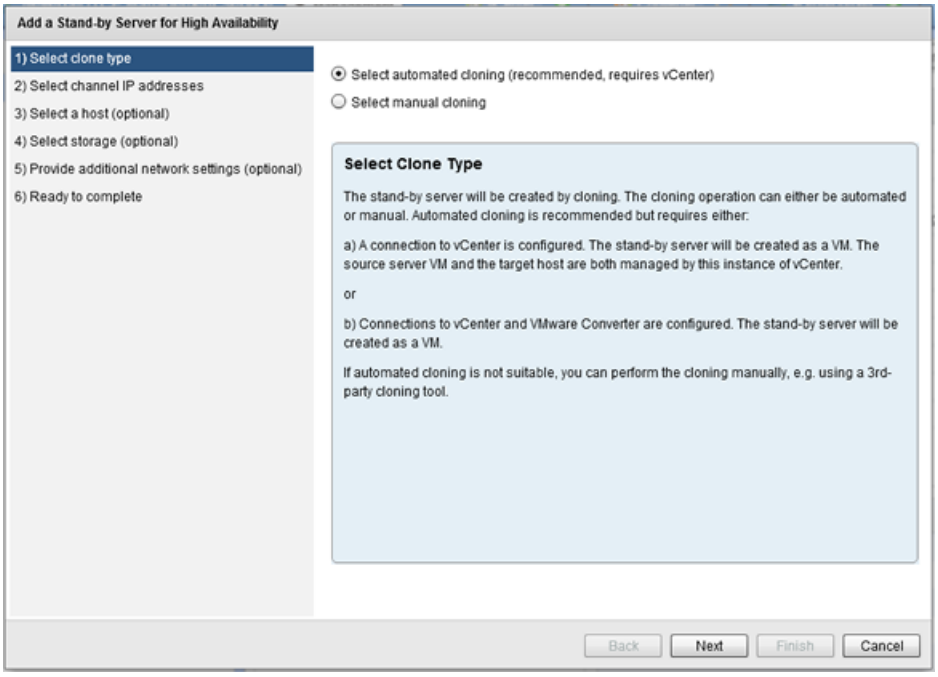

Figure 21: Select Clone Type step

   The *Select channel IP addresses* step is displayed.
3. Select the NIC which is to host the Channel IP addresses. Enter the Channel IP addresses for the Primary and Secondary servers. Manually enter the subnet mask or leave blank to set to the default subnet mask. If you are adding high-availability to an existing DR pair, enter the IP addresses and associated information for the Secondary-Tertiary and Tertiary-Primary (when deployed) Channel. Click **Next**.

Note: *If the IP addresses chosen are not already present on the server's NICs, they will be added automatically.*

The *Select a host (optional)* step is displayed.

4. Select the Datacenter and Host where the Secondary server will be created and click **Next**.
The *Select Storage* step is displayed.

Note: *If the Primary server is a virtual machine, then the Secondary server should be on a separate host to protect against host failure.*

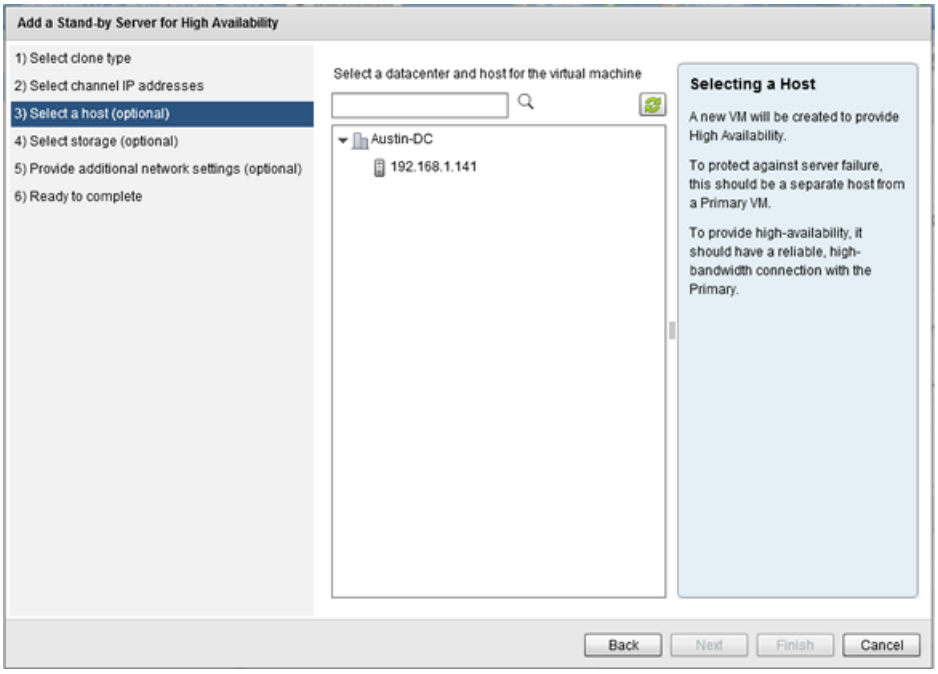

Figure 22: Select Host step

The *Select storage (optional)* step is displayed.

5. Select a storage location for the virtual machine. Click **Next**.

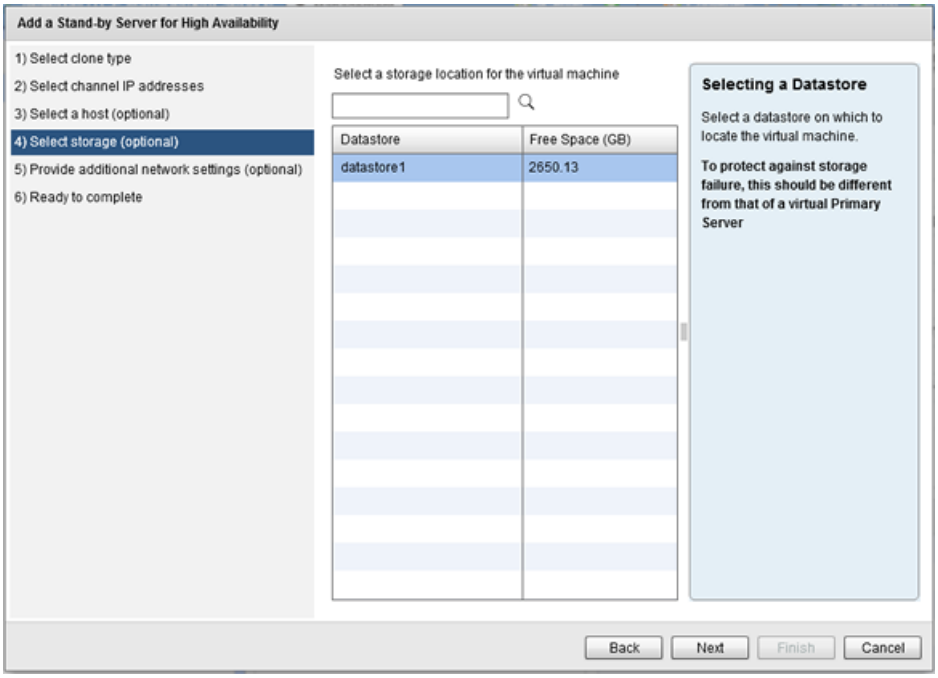

Figure 23: Select Storage step

Note: *The option to provide additional network settings is not available if Failover is deployed on a Windows based server.*

The *Ready to complete* step is displayed.

6. Click **Finish** to initiate installation of the Secondary server.

Note: *Once installation of the Secondary server is complete, automatic reconfiguration of the Secondary server will take place requiring only a few minutes to complete.*

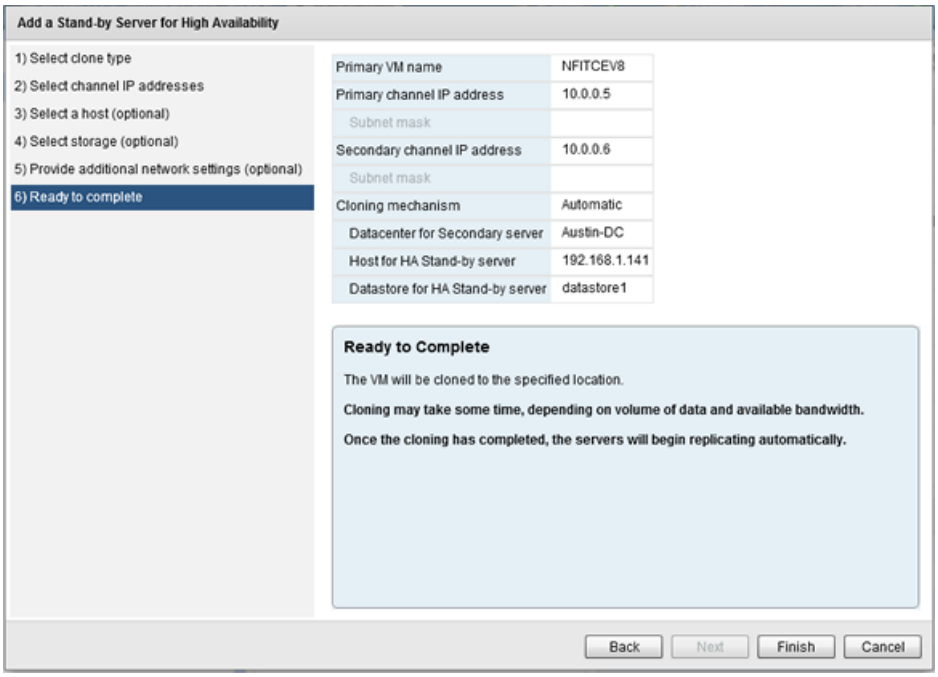

Figure 24: Ready to Complete step

7. Once complete, perform *Post Installation Configuration* tasks listed in this guide.

Add a Stand-by Server for Disaster Recovery

The *Add a stand-by server for disaster recovery* feature is used to create a Secondary server when deployed for disaster recovery. A Secondary server created for disaster recovery will typically be located at a different site from that of the Primary server. By default, automatic failover is disabled between the active and passive servers. This feature can also be used to add a stand-by server for disaster recovery to an existing high availability pair.

Procedure

To add a stand-by server for disaster recovery:

1. On the Ipswitch Failover Management Service user interface, click the **Management** drop-down menu and navigate to **Deploy** > **Add a stand-by server for Disaster Recovery**.
   The *Add a stand-by server for disaster recovery* page is displayed.
2. Select either of the following:

   - The public (principal) IP address will be identical to the Primary server.
   - The public (principal) IP address will be different than the Primary server - you must add credentials to be used for updating DNS.

   Click **Next**.

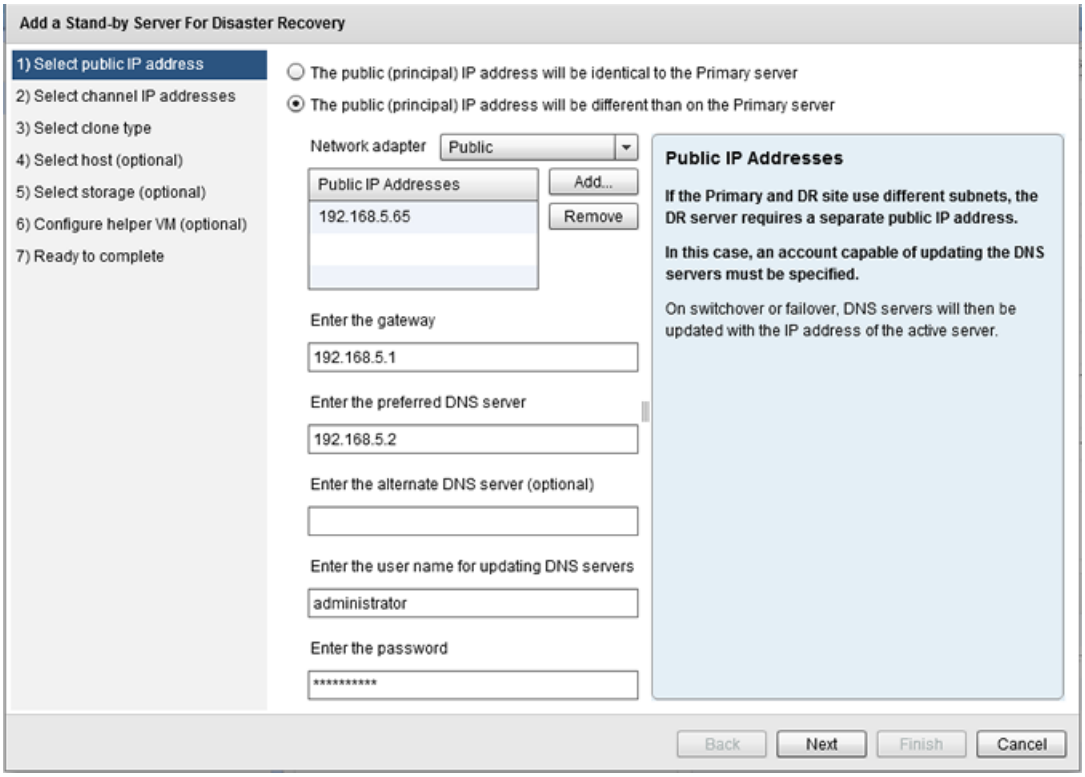

Figure 25: Select Public IP Address step

The *Select Channel IP Addresses* step is displayed.

3. Enter the Ipswitch Channel IP addresses for the Primary and Secondary servers. Manually enter the subnet mask or leave blank to set to the default subnet mask. If you are adding Disaster Recovery to an existing pair, then enter the IP Addresses and associated information for the Primary-Tertiary and Secondary-Tertiary channels. Click **Next**.

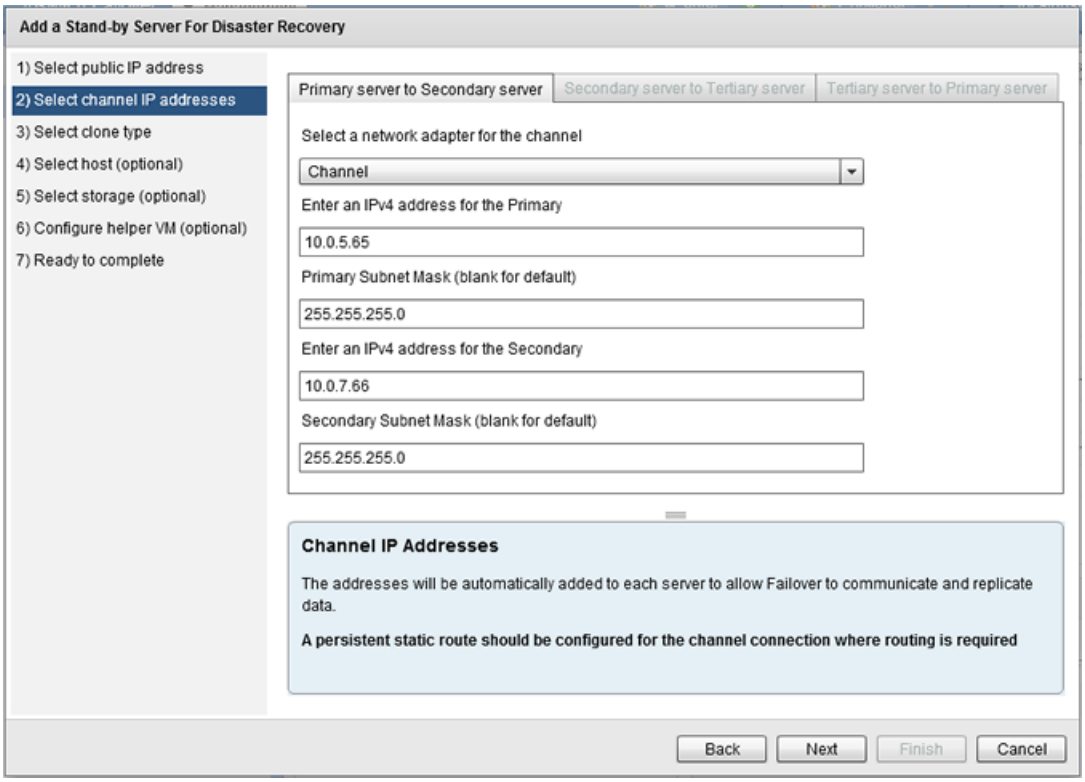

Figure 26: Select Channel IP Addresses step

The *Select Clone Type* step is displayed.

4. Select whether to clone the Primary server to create a Secondary server and power-on the Secondary server or to clone the Primary server to create the `.vmdk` files to be ported manually to the DR site. Additionally, you can select to perform a manual clone using a third-party cloning tool to clone a specific server. Click **Next**.

> ***Note:*** *If you have selected to move the `.vmdk` files, this refers to where the files will be created, not the final destination.*

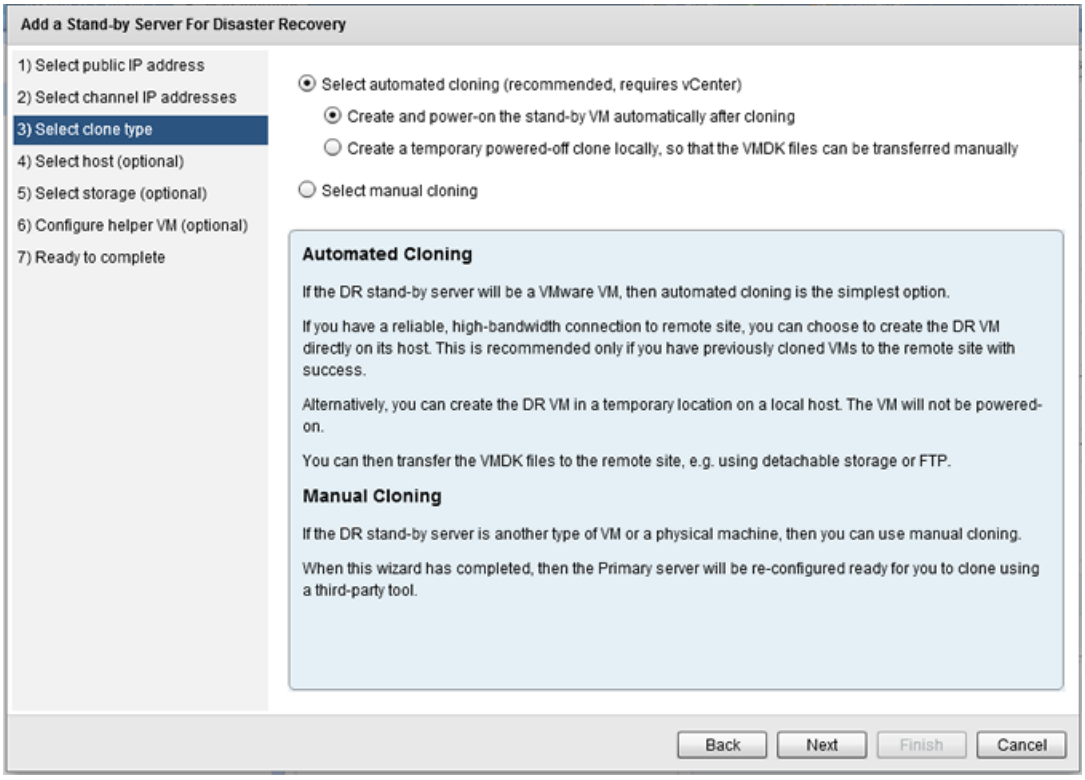

Figure 27: Select Clone Type step

The *Select Host* step is displayed.

5. Select a Datacenter and Host for the virtual machine. Click **Next**.

> ***Note:*** *If you have selected to move the* `.vmdk` *files, this refers to where the files will be created, not the final destination.*

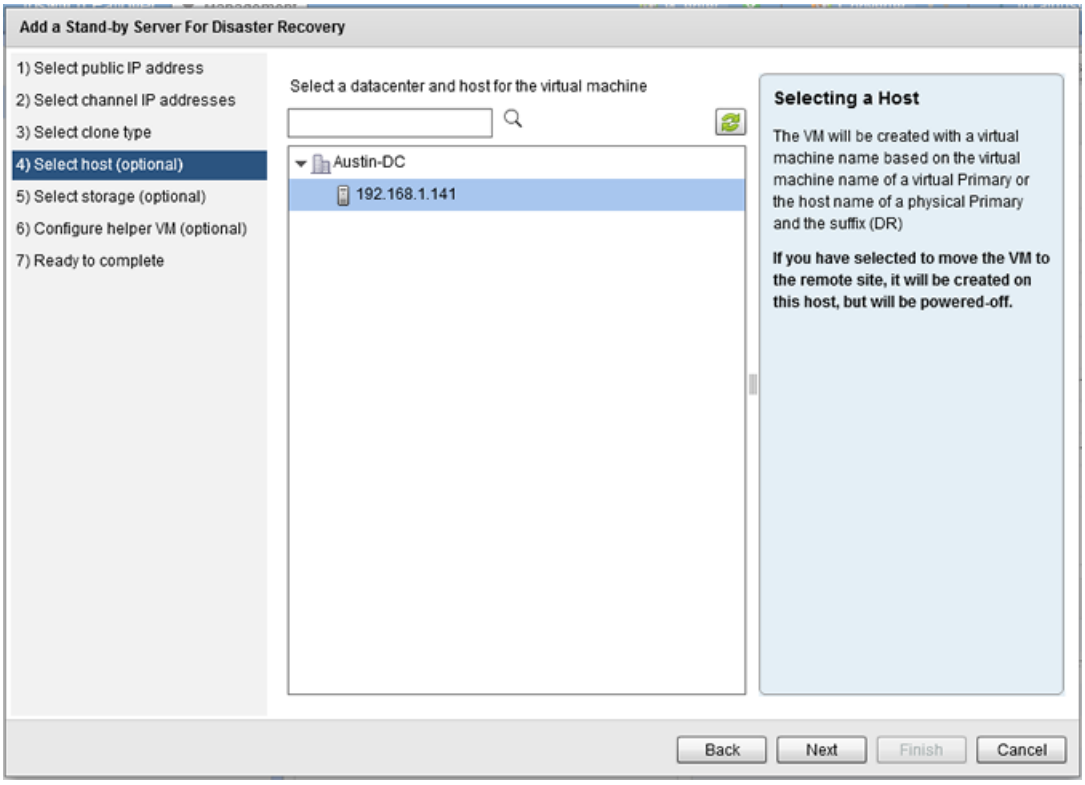

Figure 28: Select Host step

The *Select Storage* step is displayed.

6. Select the storage location for the virtual machine. Click **Next**.

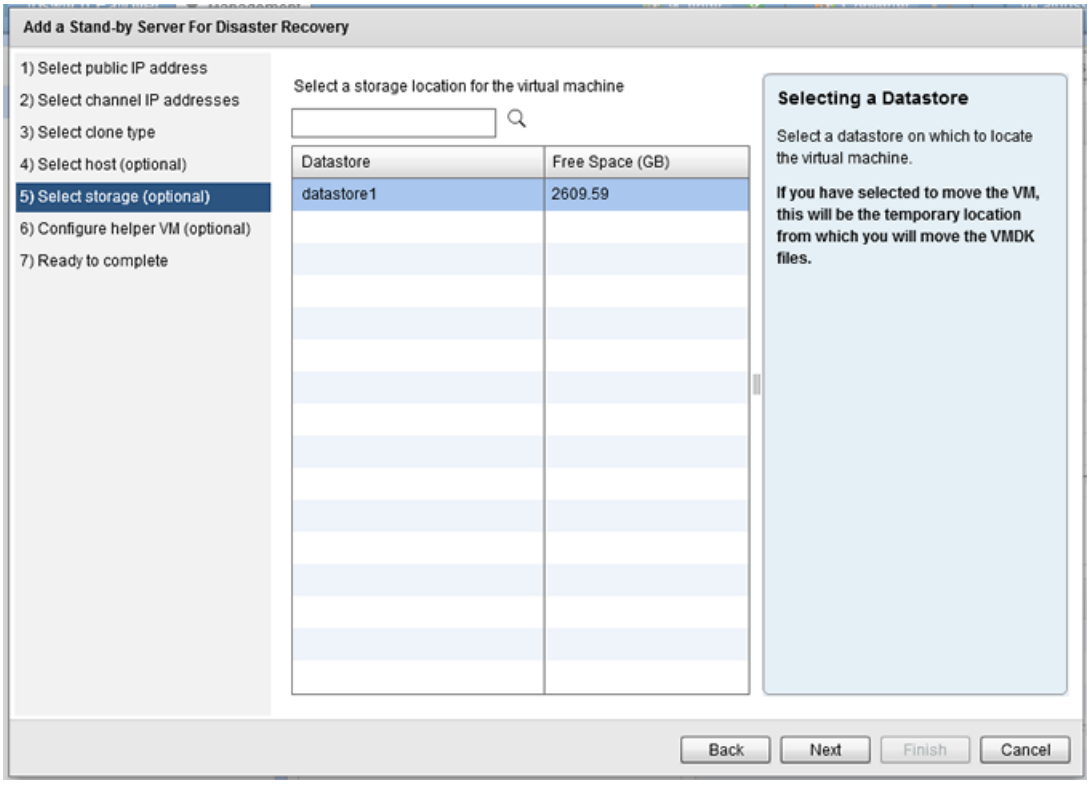

Figure 29: Select Storage step

Note: *The option to Configure helper VM (optional) is not available if Failover is deployed on a Windows based server.*

7. Review the information on the *Ready to Complete* step and if accurate, click **Finish** to create the Secondary server.

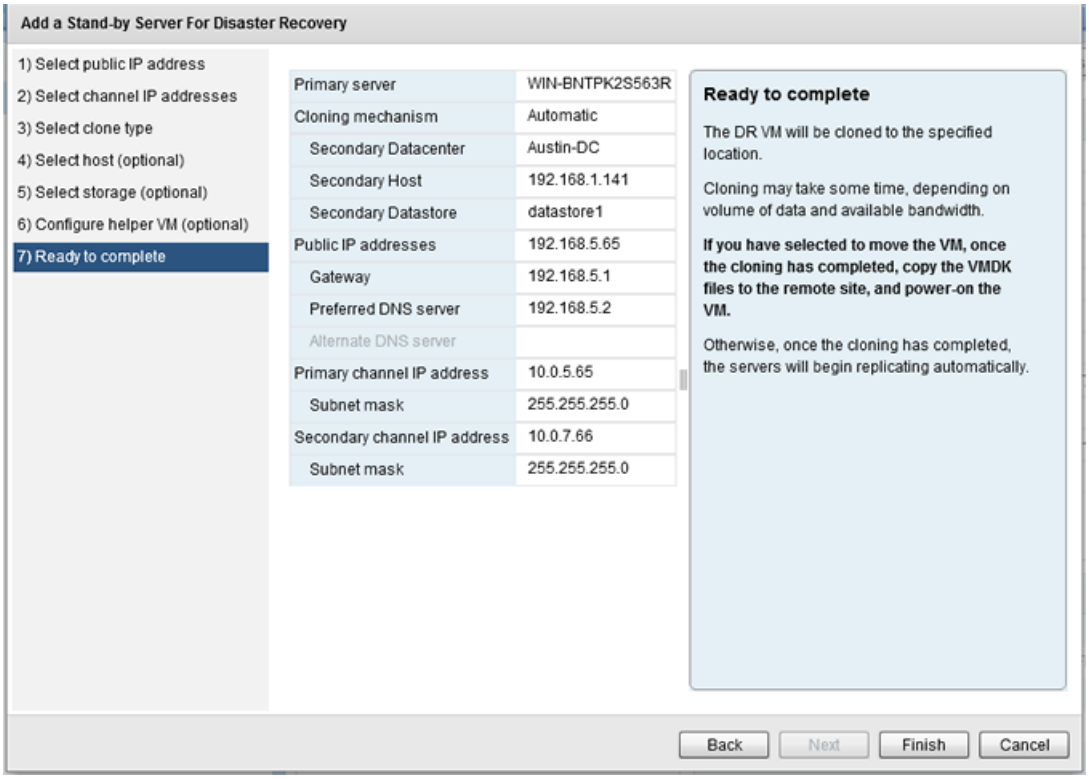

Figure 30: Ready to Complete step

Create Secondary and Tertiary stand-by VMs for HA and DR

This feature works to extend capabilities of Ipswitch Failover to incorporate both High Availability and Disaster Recovery by deploying both a Secondary server (for HA) and a Tertiary server (for DR).

Procedure

To deploy Secondary and Tertiary VMs for High Availability and Disaster Recovery:

1. On the Ipswitch Failover Management Service, navigate to the **Management > Deploy** drop-down menu and select *Create Secondary and Tertiary stand-byVMs for HA and DR*.
   The *Create Secondary and Tertiary VMs for High Availability and Disaster Recovery* page is displayed.

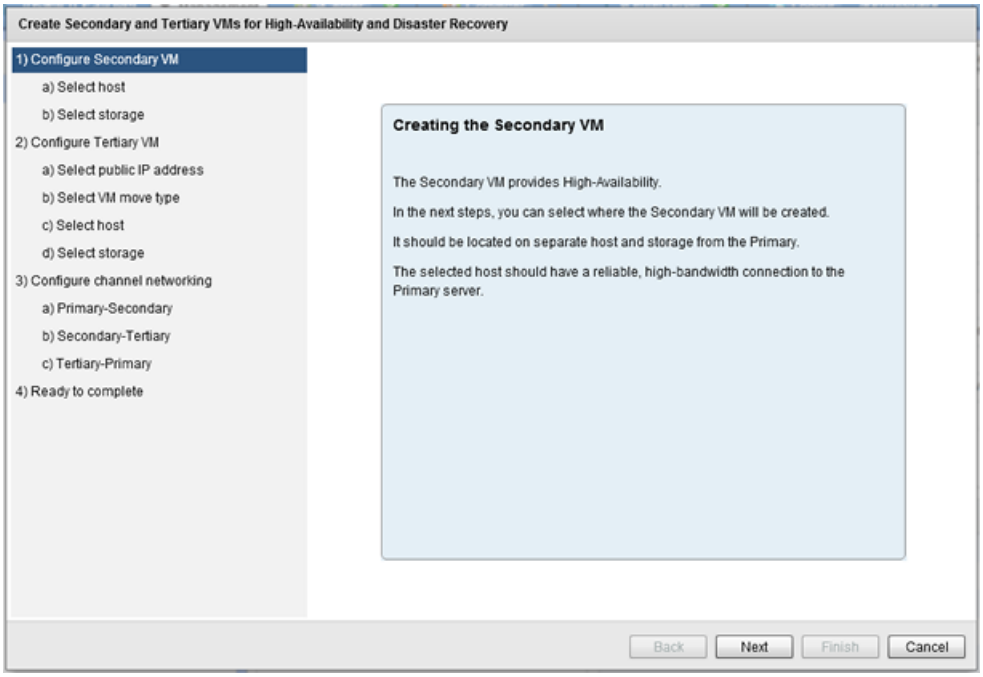

Figure 31: Configure Secondary VM step

2. Review the information in the step and then click **Next**.
   The *Select host* step is displayed.

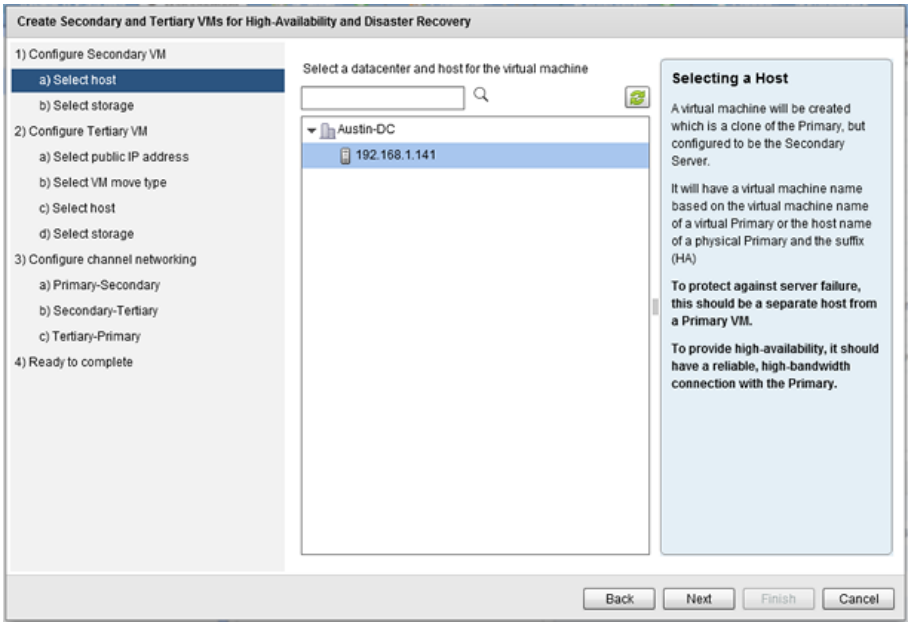

Figure 32: Select host step

3. Click on the appropriate Datacenter to display all available hosts. Select the intended host for the Secondary server and then click **Next**.
   The *Select storage* step is displayed.

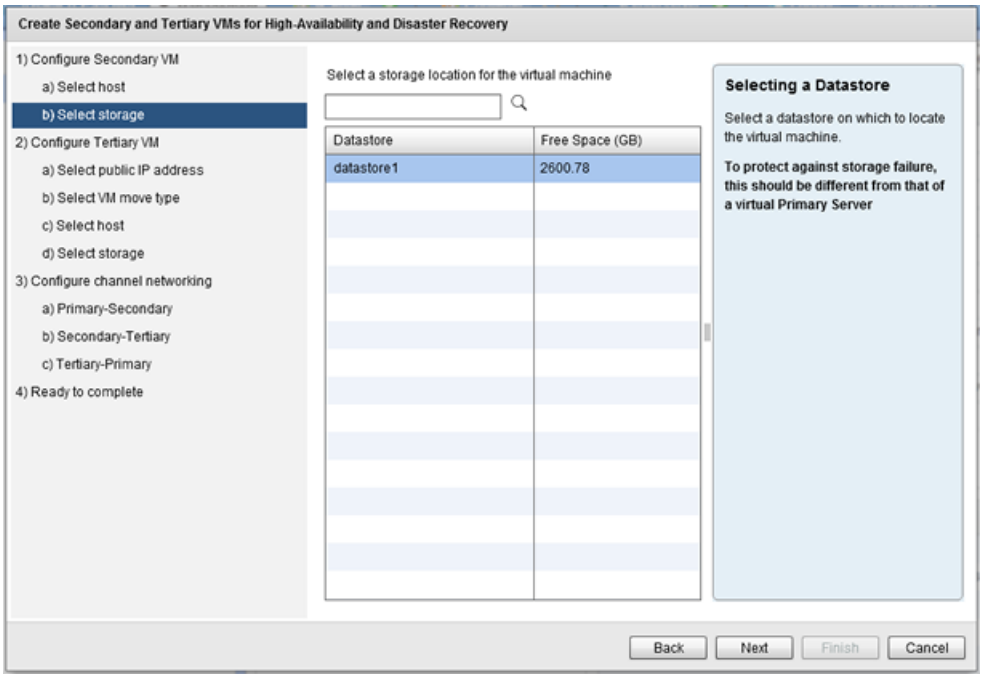

Figure 33: Select storage step

4. Select the intended datastore for the Secondary VM, and then click **Next**.
   The *Configure Tertiary VM* step is displayed.

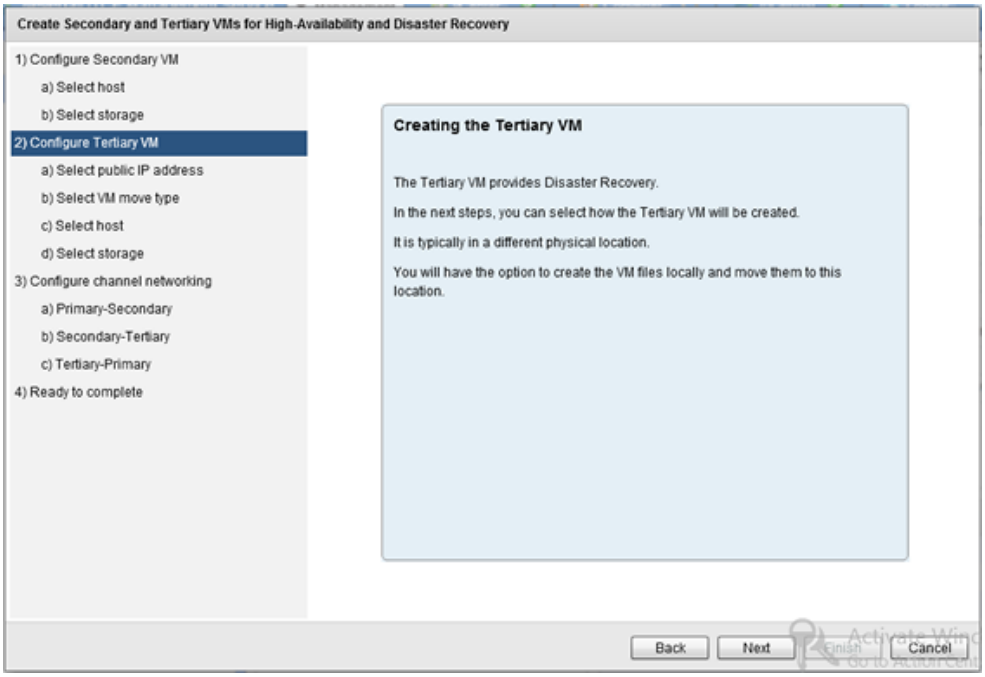

Figure 34: Configure Tertiary VM step

5. Review the contents of the step and then click **Next**.
   The *Select public IP address* step is displayed.

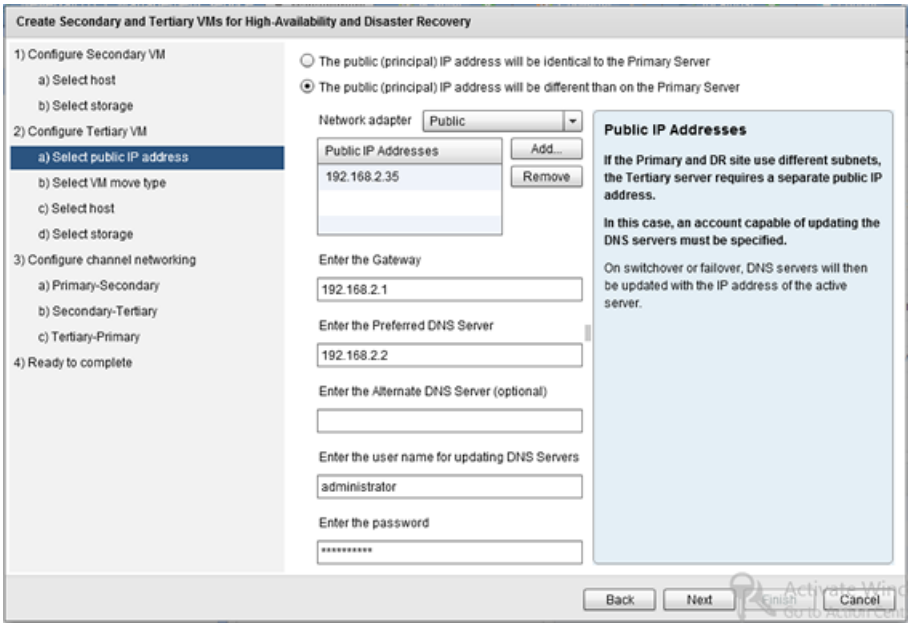

Figure 35: Select public IP address step

6. If the public IP address will be different than the Primary server, select which NIC this should be assigned to and add a static IP address in a separate subnet in the *Public IP Addresses* field. Additionally, add the Gateway IP, Preferred DNS server IP, and the user name and password of an account used for updating DNS servers. Click **Next**.
   The *Select VM move type* step is displayed.

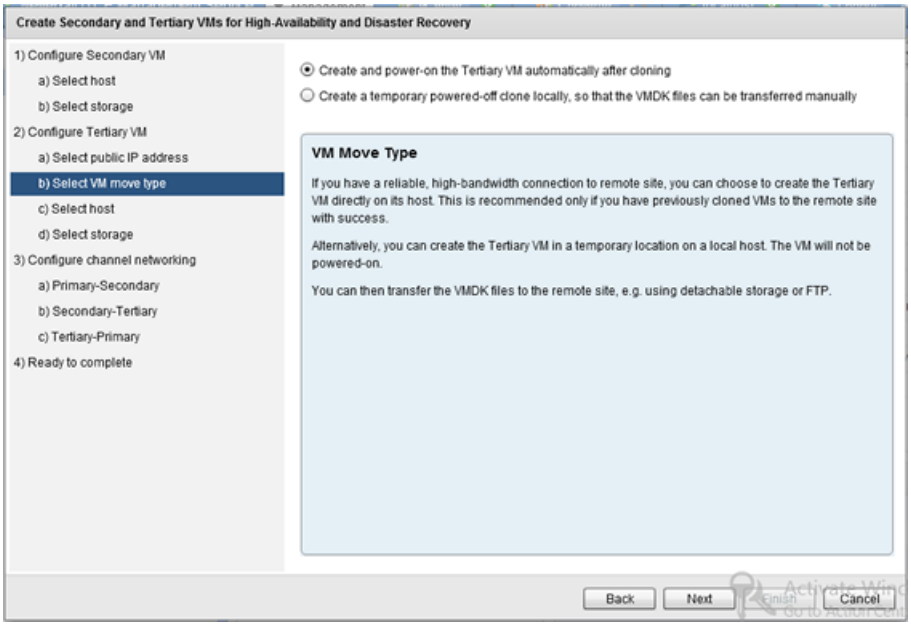

Figure 36: Select VM move type step

7. Review the definitions of the options and then select whether the VM will be transferred manually or not. Click **Next**.
   The *Select host* step is displayed.

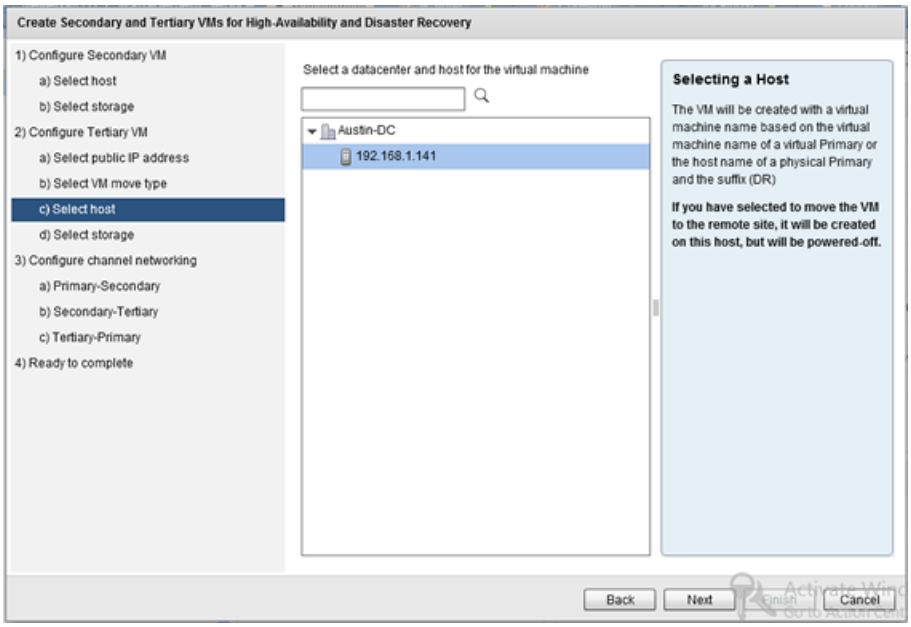

Figure 37: Select host step

8. Click on the appropriate Datacenter to display all available hosts. Select the intended host for the Tertiary server and then click **Next**.
   The *Select storage* step is displayed.

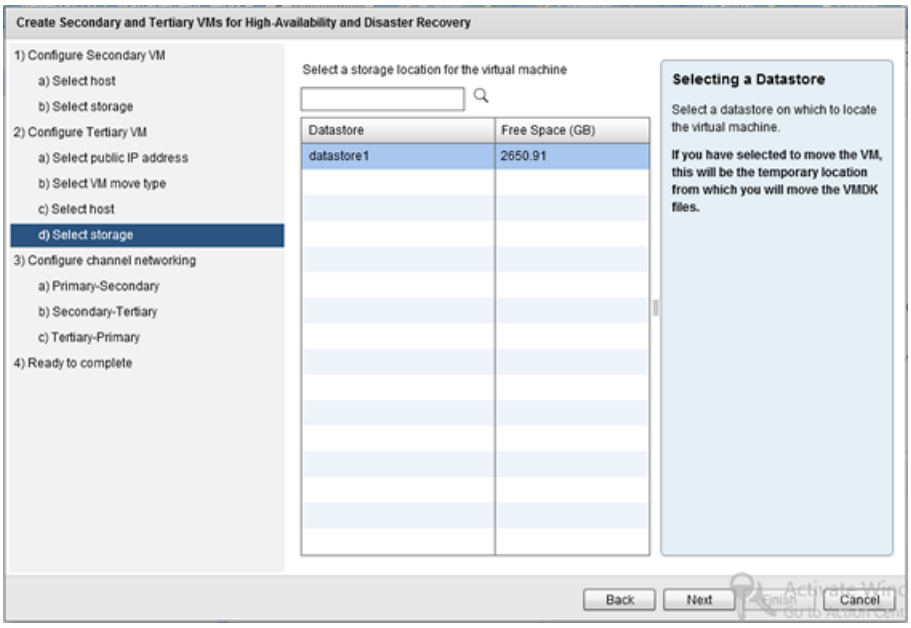

Figure 38: Select storage step

9. Select the intended datastore for the Tertiary VM, and then click **Next**.
   The *Configuring Channel Communications* step is displayed.

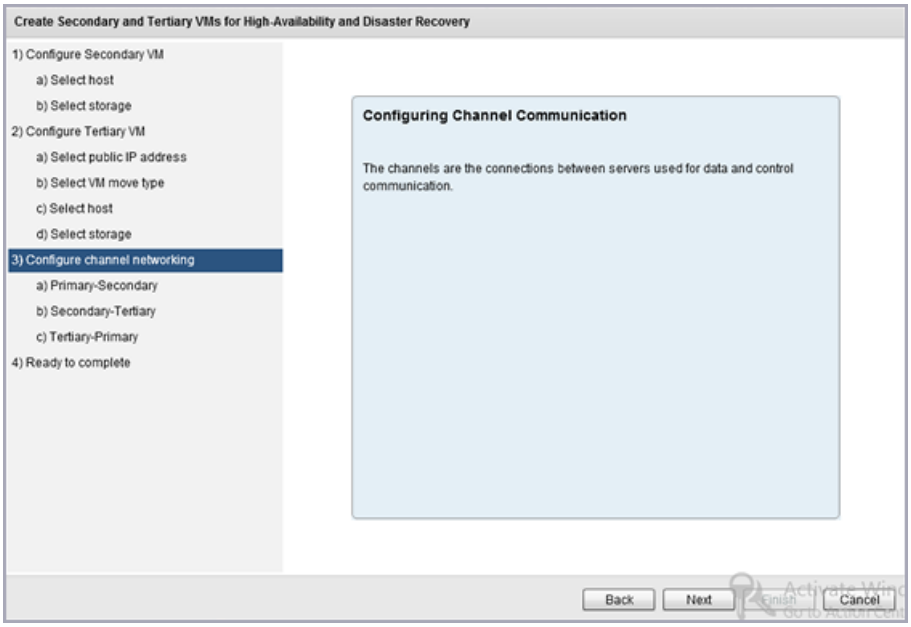

Figure 39: Configure channel networking step

10. Review the contents of the step and then click **Next**.
The *Primary-Secondary* step is displayed.

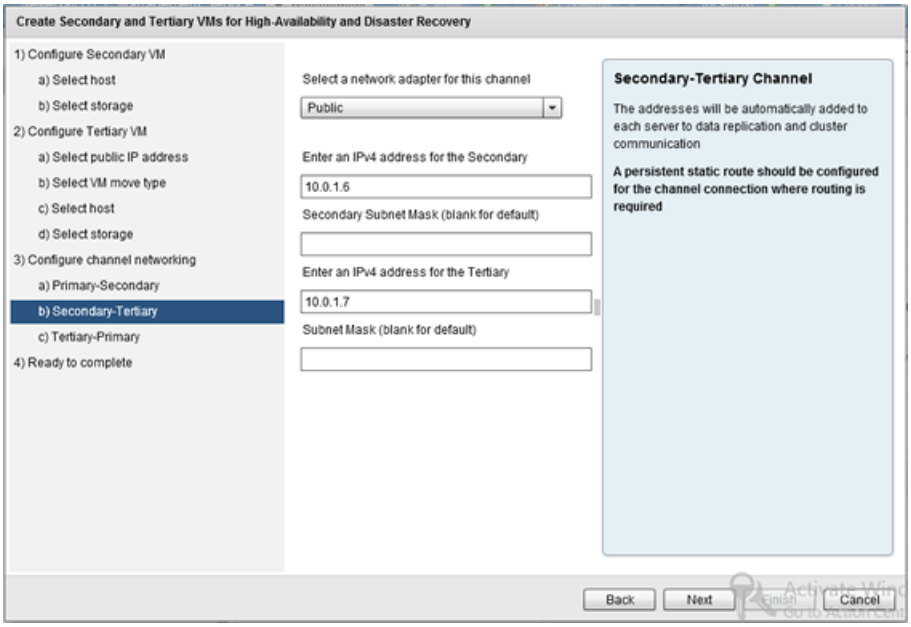

Figure 40: Primary-Secondary step

11. Select the appropriate network adapter and then enter the channel IP addresses for Primary-Secondary communications. Click **Next**.
The *Secondary-Tertiary* step is displayed.

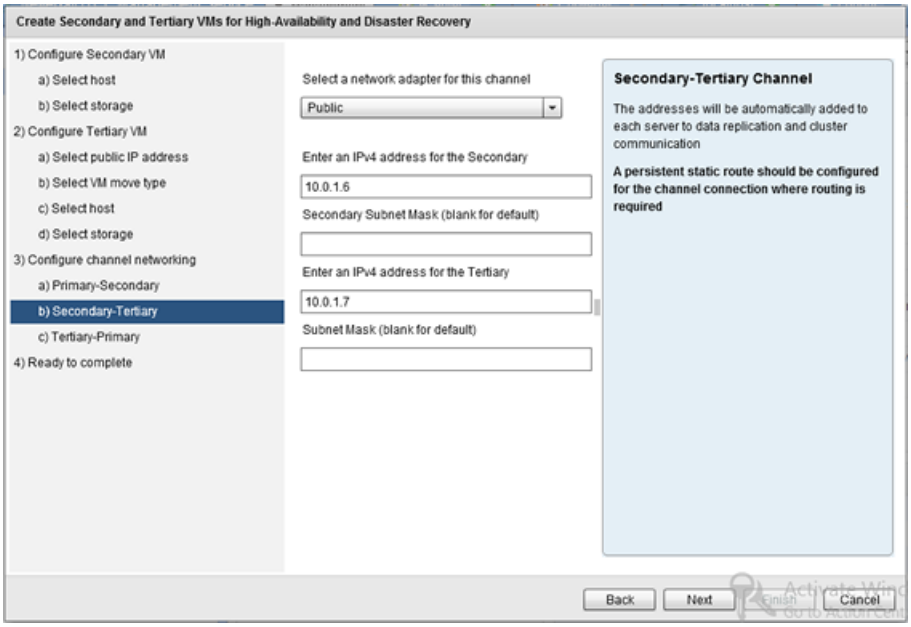

Figure 41: Secondary-Tertiary step

12. Select the appropriate network adapter and then enter the channel IP addresses for Secondary-Tertiary communications. Click **Next**.
The *Tertiary-Primary* step is displayed.

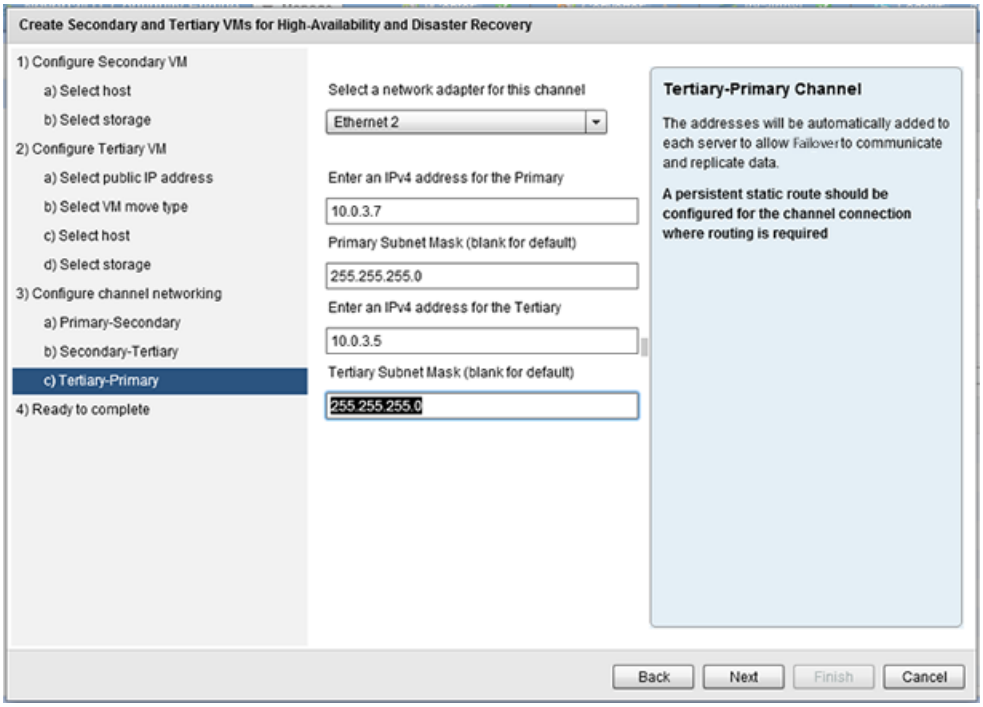

Figure 42: Tertiary-Primary step

13. Select the appropriate network adapter and then enter the channel IP addresses for Tertiary-Primary communications. Click **Next**.
The *Ready to complete* step is displayed.

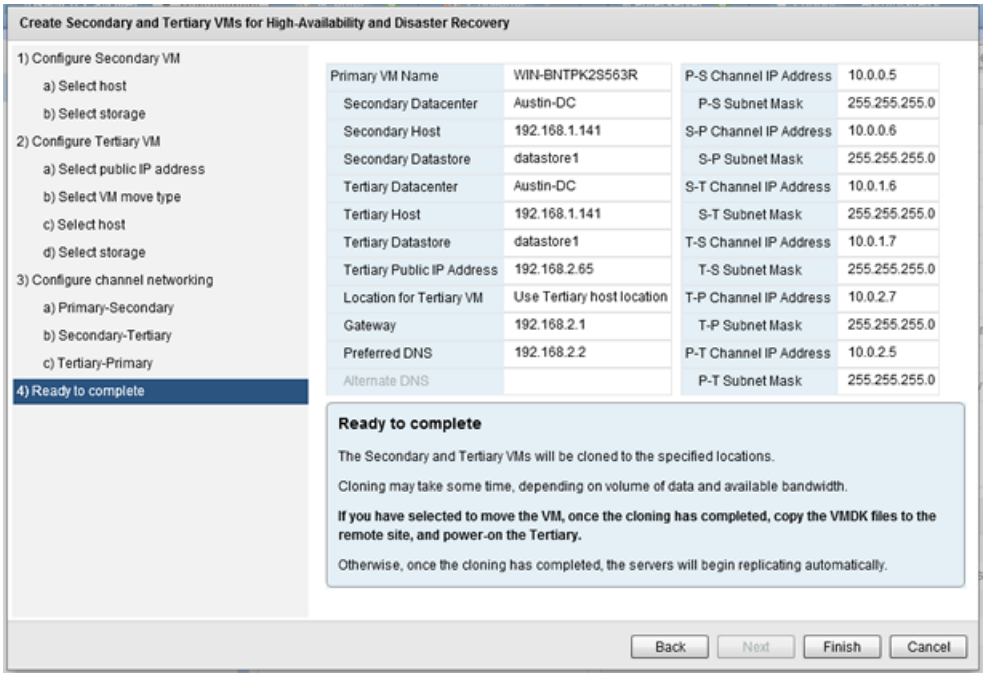

Figure 43: Ready to complete step

14. Review all of the summary information on the step. If any errors are found, use the **Back** button to navigate to the step with the error and correct it. If no errors are found, click **Finish** to deploy the Secondary and Tertiary servers.

Manage

The **Manage** drop-down menu provides key management abilities such as to Discover Protected Servers, Add a Protected Server, Remove the Selected Server, and Download the Advanced Management Client.

Discover Protected Servers

Ipswitch Failover Management Service provides the ability to perform discovery to identify all Ipswitch Failover Clusters.

Procedure

To discover protected servers:

1. From the **Management** > **Manage** drop-down menu, click **Discover Protected Servers**.
   The *Discover Protected Server* dialog is displayed.

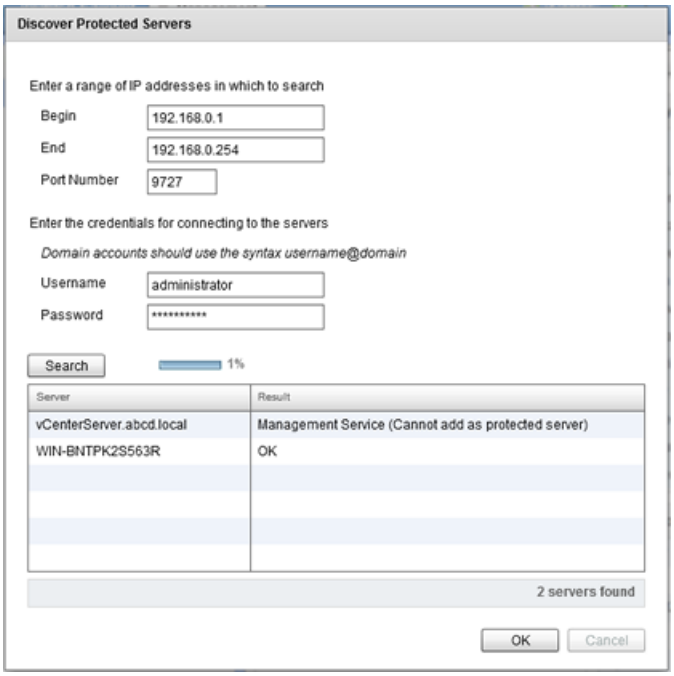

Figure 44: Discover Protected Servers dialog

2. Identify the IP address range to search by adding a beginning and ending IP address in the *Begin* and *End* fields.
   Ipswitch recommends leaving the *Port Number* field with the default port unless the default port is in use by another application and a custom port has been configured.
3. Add a username and password used to connect to Ipswitch Failover in the *Username* and *Password* fields.

   Note: *If the username is a domain account, use the following format: username@domain.xxx*

4. Click **Search** to run Ipswitch Failover server discovery.
   The Ipswitch Failover Management Service displays all Ipswitch Failover clusters discovered. Discovered items will be added automatically to the Protected Servers pane in the background.
5. Click **OK** or **Cancel** to dismiss the Discover Protected Servers dialog.

Add a Protected Server

Procedure

To add a protected server:

1. Ipswitch Failover Management Service allows you to add individual protected servers which may be part of a cluster. Click **Add a Protected Server** in the **Management** >**Manage** drop-down menu to add a server. The **Add Server** dialog is displayed.

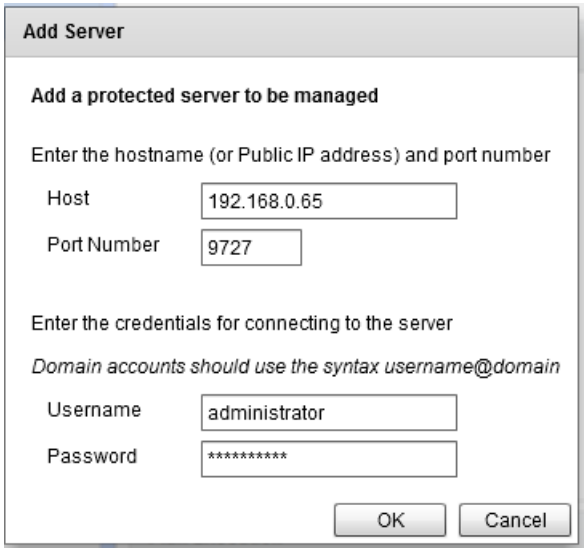

Figure 45: Add Server dialog

2. Enter the hostname or IP address of server to be added in the *Host* field.
   Ipswitch Failover Management Service recommends leaving the *Port Number* field with the default port unless the default port is in use by another application and a custom port has been configured.
3. Add a username and password used to connect to Ipswitch Failover in the *Username* and *Password* fields.

> ***Note:*** *If the username is a domain account, use the following format: username@domain.xxx.*

4. Click **OK** to add the Ipswitch cluster.
   The Ipswitch Failover Management Service adds the Ipswitch Failover cluster to the Protected Servers pane of the *Ipswitch Failover Management Service Summary* page.

Remove the Selected Server

The Ipswitch Failover Management Service provides the ability to remove specific Ipswitch servers from the Ipswitch Failover Management Service *Protected Servers* pane.

Procedure

To remove the selected server:

1. Select the server to be removed from *Protected Servers* pane of the Ipswitch Failover Management Service.
2. Select **Remove the Selected Server** in the **Management** >**Manage** drop-down menu.
   The *Remove Server* dialog is displayed.

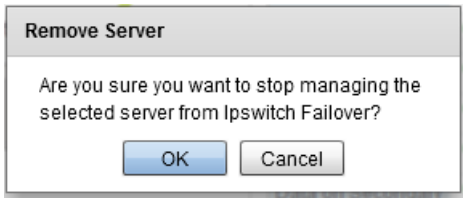

Figure 46: Remove Server dialog

You are prompted to verify that you want to remove the selected server from management by the Ipswitch Failover Management Service.

3. Click **OK**.
   The intended Ipswitch Failover server is removed from the Ipswitch Failover Management Service *Protected Servers* pane.

Download the Advanced Management Client

The *Download the Advanced Management Client* feature is used to download the Advanced Management Client (Client Tools) to a workstation or server for remote management of Ipswitch Failover.

Procedure

To download the Advanced Management Client:

1. Select the *Download Advanced Management Client* feature.

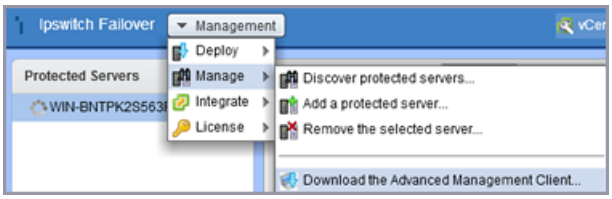

Figure 47: Download Advanced Management Client

2. Select a target location for the downloaded file using the dialog navigation features.
3. Click **Save**.

Integrate

Ipswitch Failover Management Service allows you to easily integrate some VMware vCenter functionality directly from the Ipswitch Failover Management Service user interface.

Log in to VMware vSphere Client

Ipswitch Failover Management Service provides the ability to log in to the VMware vSphere Client directly from Ipswitch Failover Management Service to manage VMware resources.

Procedure

To log in to VMware vSphere Client:

- Using the Ipswitch Failover Management Service user interface, navigate to **Management** > **Integrate** > **Log in to VMware vSphere Client**.
  A browser is launched providing access to the VMware vSphere Client.

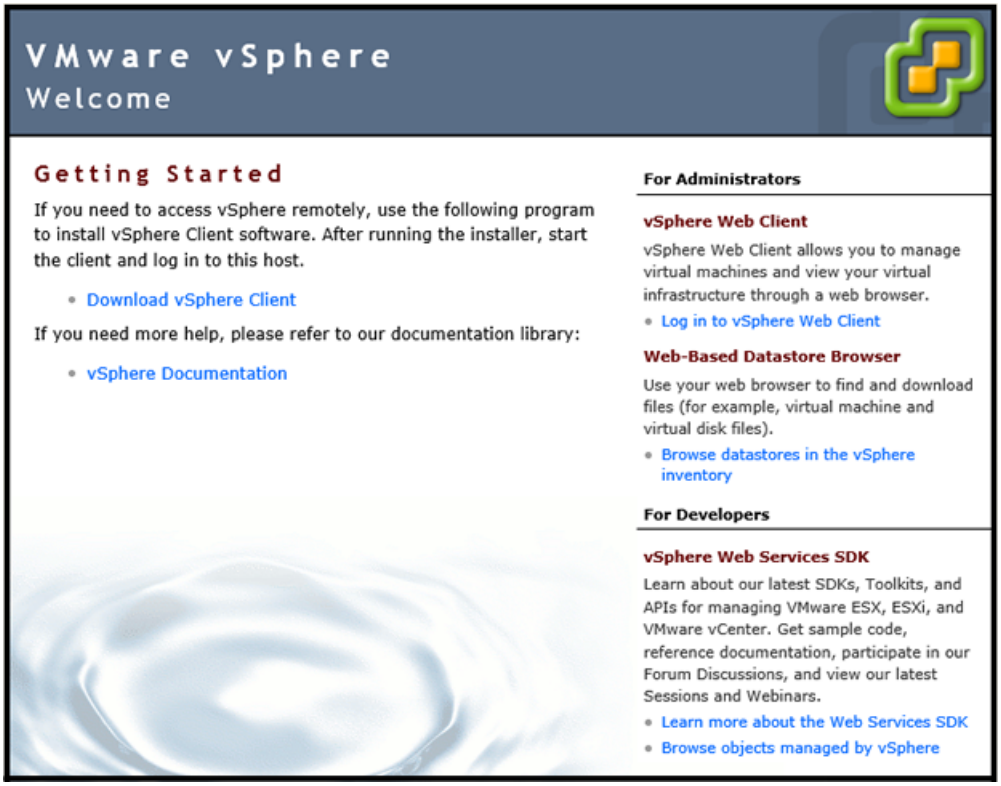

Figure 48: VMware vSphere

Create VMware SRM Plan Step for Selected Server

This feature works to extend capabilities of VMware's Site Recovery Manager (SRM). While SRM provides the ability to failover virtual servers to a secondary site, this feature integrates Ipswitch Failover physical or virtual servers into the failover process as a natural step in the SRM Site Recovery Plan executed by SRM. It works by allowing the administrator to create an SRM Step that can be added to the SRM Site Recovery Plan thereby allowing servers protected by Ipswitch Failover to participate in failover of servers protected by Site Recovery Manager.

Prerequisites

- The Ipswitch Ipswitch Failover Management Service installed on vCenter Server in the Recovery and Protected Sites
- Microsoft PowerShell 2.0 installed on all SRM servers that will run command files, for example the SRM Servers in the Recovery and Protected sites
- The PowerShell Execution Policy must be set to *RemoteSigned* on all SRM Servers, use the following PowerShell command:

  ```
  PS C:\> Set-ExecutionPolicy RemoteSigned
  ```

1. Launch the Ipswitch Failover Management Service user interface.
2. Select an Ipswitch Failover server in the left pane to be added to the SRM Site Recovery Plan.

   Important: *If the server is a member of a cluster, then select the server from the cluster which is to switchover first. All members of a cluster will switchover when a single member server receives the switchover command.*

3. Click the **Management** > **Integrate** > **Create VMware SRM Plan Step for Selected Server** button.

The *Create a Plan Step for VMware vCenter Site Recovery Manager* dialog is displayed.

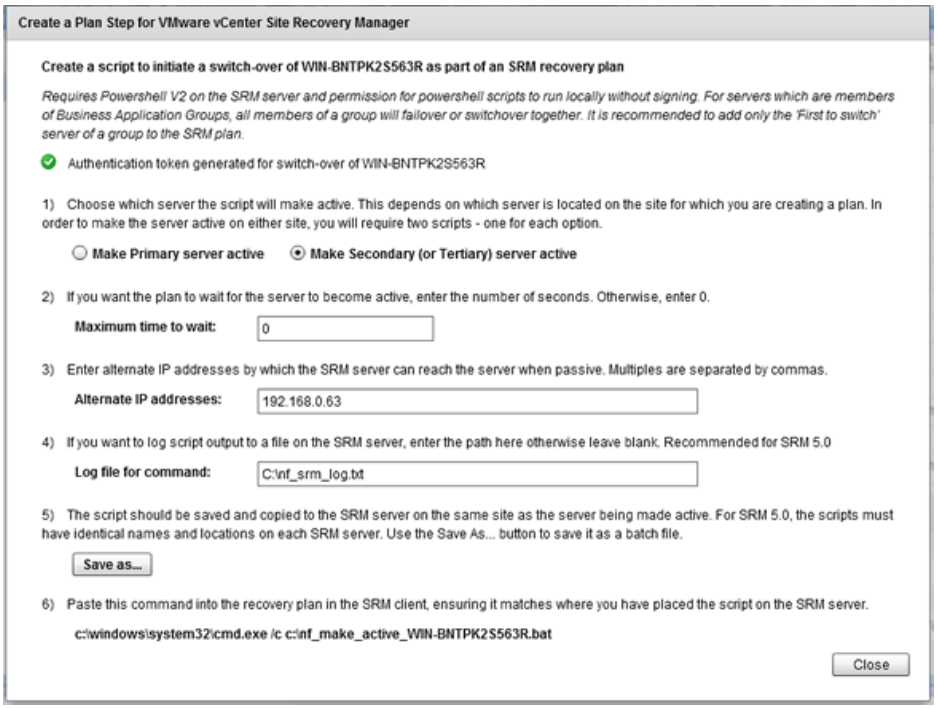

Figure 49: Create SRM Plan Step

4. Select the server to be controlled by the SRM Plan. This depends on which server is located at the site for which you are creating a plan. To make the server active on either site, you will require two scripts - one for each option.

   Note: *If the SRM Plan Step is being created on the site where the Primary server is located, select Make Primary Server Active. If the SRM Plan Step is being created on the site where the Secondary server is located, select Make Secondary server active.*

5. If you want the SRM plan to wait for the Ipswitch Failover server to switchover and become active before the plan continues with the next step, enter the number of seconds to wait in the *Maximum time to wait* field.

   Note: *If the Maximum time to wait is set to zero, execution of the SRM Plan will continue without waiting for the Ipswitch Failover server to become active.*

6. Alternate IP addresses are configured on each server in the Ipswitch pair so that SRM can switch the servers even when the Protected Site cannot be contacted, for example in times of disaster. Enter the Alternate IP address that will be used by SRM to contact the Ipswitch Failover server in the *Alternate IP addresses* field, separate multiple IP addresses with a comma.

   These IP addresses are typically added to the servers as *Management IP Addresses*.

7. If you want to log the script output to a file on the SRM server, enter a path in the *Log file for command:* field (recommended for SRM 5.0), otherwise, leave the field blank.
8. Generate two scripts using the SRMXtender Plug-in.
   a) Generate one script with *Make Primary Server Active* selected.
   b) Generate one script with *Make Secondary Server Active* selected.

9. The scripts should be saved as `.bat` files with each being saved to a file share on the SRM server in the same site as the server being made active. Click the **Save As** button to save the script as a `.bat` file.

> ***Note:*** *For SRM 5.0, the scripts must have identical names and locations on each SRM server.*

10. Launch the VMware vSphere Web Client and connect to the Recovery vCenter Server.
11. Navigate to **Home** > **Solutions and Applications** > **Site Recovery Manager** and select the intended **Recovery Plan**.
12. Select the *Recovery Steps* tab.

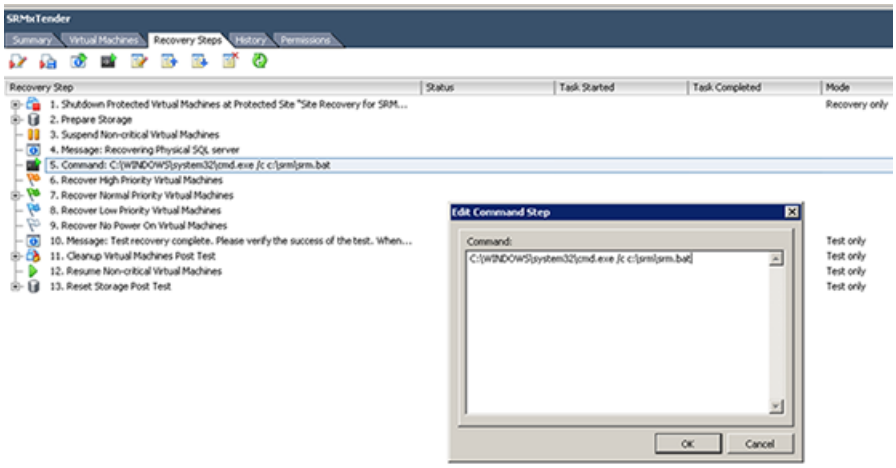

Figure 50: SRM Edit Command Step

13. Add a *Command Step* at the desired point in the Recovery Plan, for example before the *Recover High Priority Machines* Step if the applications running on these servers depend upon the physical server.
14. In the **Add Command Step** dialog enter:

```
C:\WINDOWS\system32\cmd.exe /c <path_to_saved_file>\<file_name>.bat
```

> ***Note:*** *`<path_ to_saved_file>` is the path where you have copied the `\<file_name>.bat` file at step 10.*

15. Click **OK**.

> ***Note:*** *Repeat the step creation process for each Ipswitch pair that is to participate in the Site Recovery Plan.*

License

The Ipswitch Failover Management Service user interface provides the ability to license your Ipswitch Failover cluster using a simple wizard.

Configure an Internet Proxy Server for Licensing

For organizations that use an Internet Proxy, the *Configure Internet Proxy Settings* dialog provides the ability to configure settings for the proxy to allow Ipswitch Failover licensing to successfully complete.

Procedure

To configure for use with an internet proxy:

1. Select **Configure an Internet Proxy Server for Licensing** from the **Management** > **License** drop-down menu.
2. Provide the hostname or IP address of the proxy, the port number, and if required account credentials.

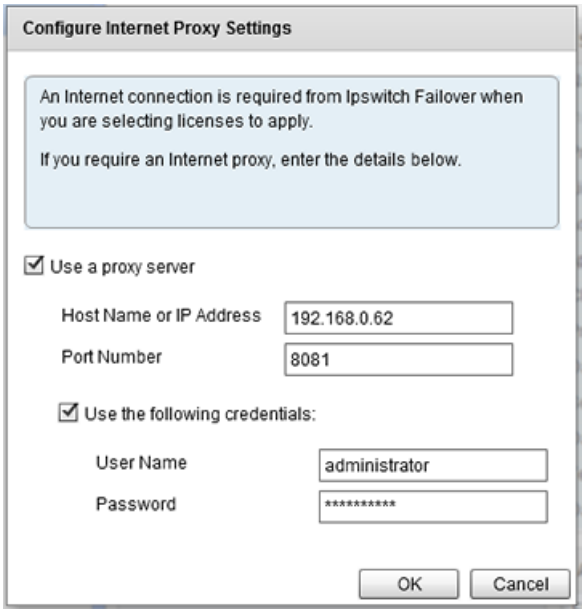

Figure 51: Configure Internet Proxy Settings

License the Selected Server

Licensing is performed via the Ipswitch Failover Management Service.

To license Ipswitch Failover:

Note: *Automated licensing of Ipswitch Failover requires use of the internet. If your organization uses an internet proxy, configure proxy information in the* ***Management*** *>* ***License*** *>* ***Configure an Internet proxy server for licensing*** *dialog.*

1. To add a license for Ipswitch Failover, navigate to the **Management** drop-down menu and click on **License** > **License the Selected Server**.

   The *ActivateLicense* wizard is displayed. Click **Next**.

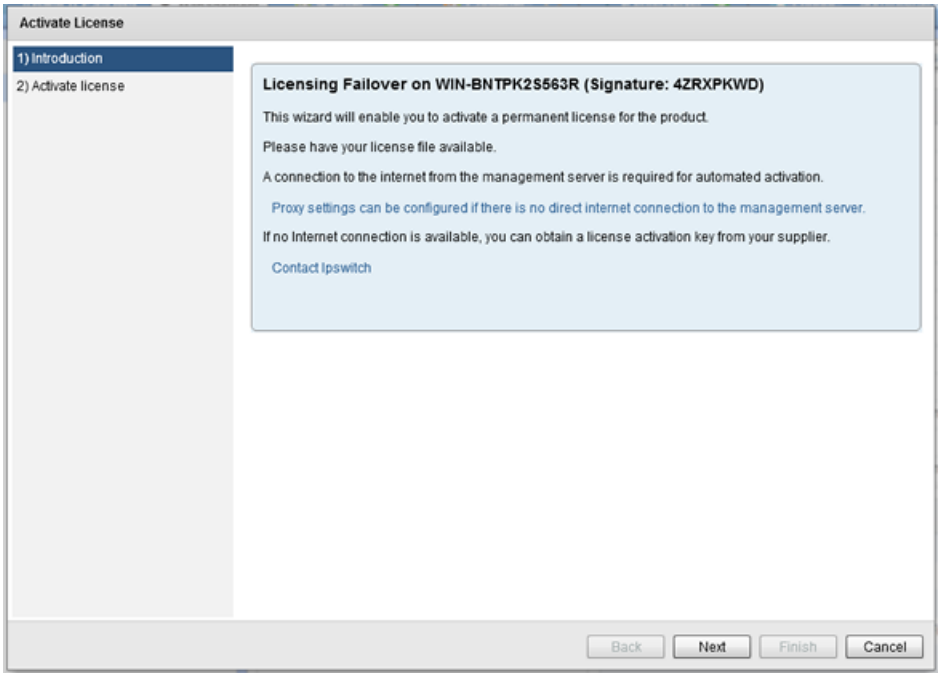

Figure 52: Activate License page

2. The *Activate License* step is displayed. If there is an Internet connection from the Ipswitch Failover Management Service, select the *"Upload a license...."* radio button and browse to the license file. I an Internet connection is not available, select the *"Enter an activation key..."*. and enter the activation key that was supplied. Click **Finish**.

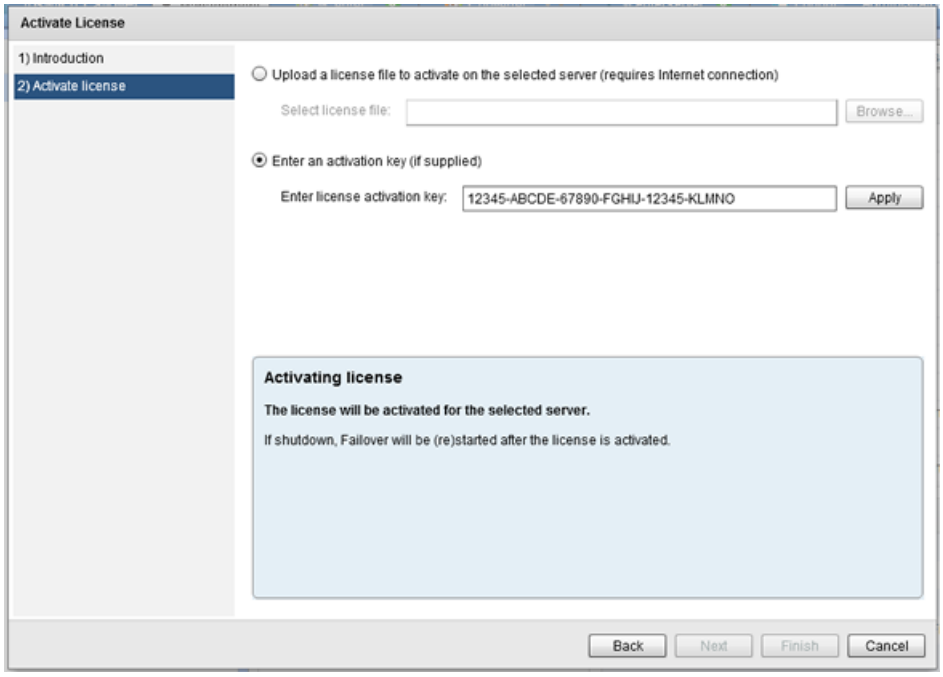

Figure 53: Activate License step

Summary

The *Summary Page* contains multiple panes that provide the current status of the server, the version of the cluster, and details about licensing of the cluster.

The Ipswitch Failover Management Service identifies the current active server and provides the status of Replication, the Application State, the File System State, and the Client Network State of servers in the cluster.

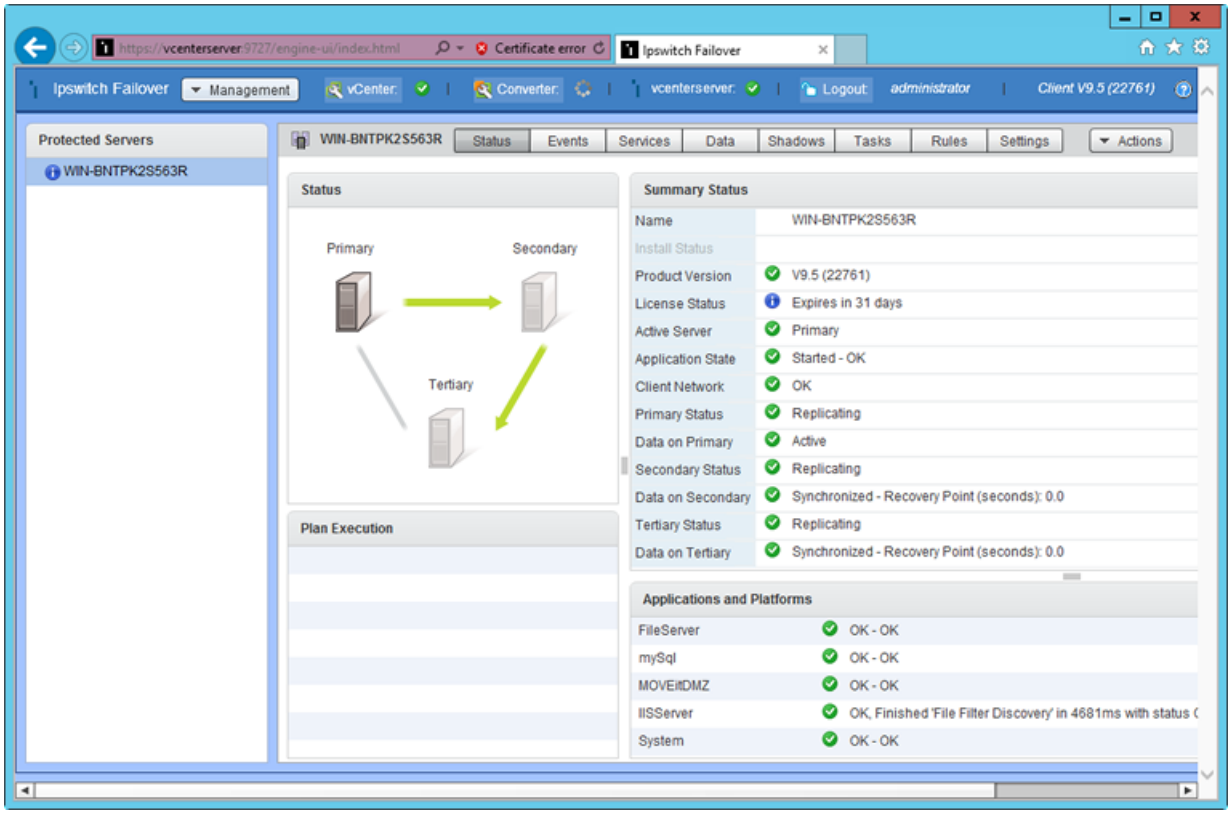

Figure 54: Summary Page

Status

The *Status* pane provides a view of the currently selected server pair or trio.

The *Status* pane displays a graphic representation of the currently selected cluster and what the cluster is doing. Additionally, it displays which of the servers are active, the status of replication, and the direction of replication (for example in a pair, Primary to Secondary or Secondary to Primary).

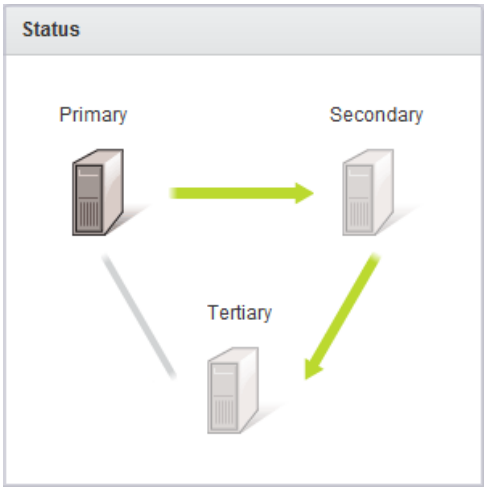

Figure 55: Status Pane

Summary Status

The *Summary Status* pane provides a status of all operations currently being performed on the server cluster.

The *Summary Status* pane displays the status of replication, synchronization, the application and network state, license status, and the installed version of Ipswitch Failover.

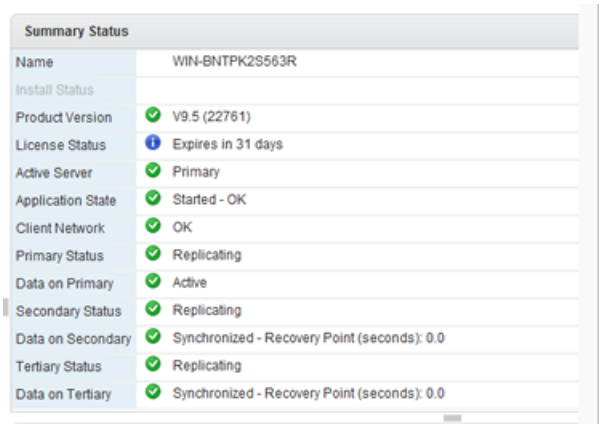

Figure 56: Summary Status pane

Plan Execution

The *Plan Execution* pane displays plans being executed by Ipswitch Failover.

Plans are sequences of actions required to perform functions such as switch-over or installing a new plug-in. Plans can be executed in response to user action (such as Make Active) or automatically (such as failover). The *Plan Execution* pane will display the progress of the plan as it is executed. Once the plan is complete, it is removed from the *Plan Execution* pane.

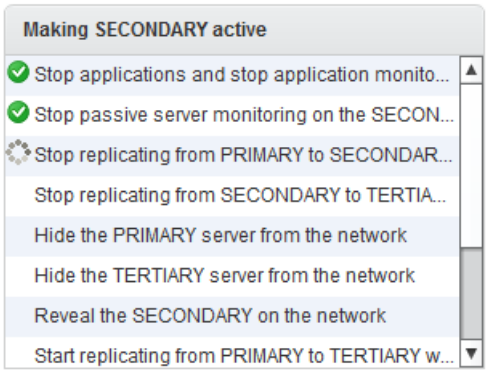

Figure 57: Plan Execution pane

Applications and Platforms

The *Applications and Platforms* pane displays the currently installed protected applications and their status. It also shows the health status of platforms such as the OS and hardware.

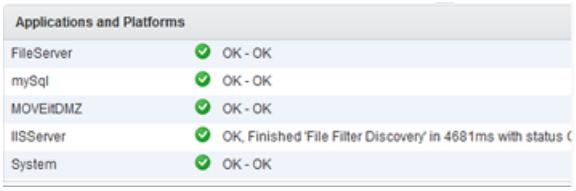

Figure 58: Applications and Platforms

Events

The events that Ipswitch Failover logs are listed chronologically (by default) on the *Events* page, the most recent event appears at the top of the list with older events sequentially below it.

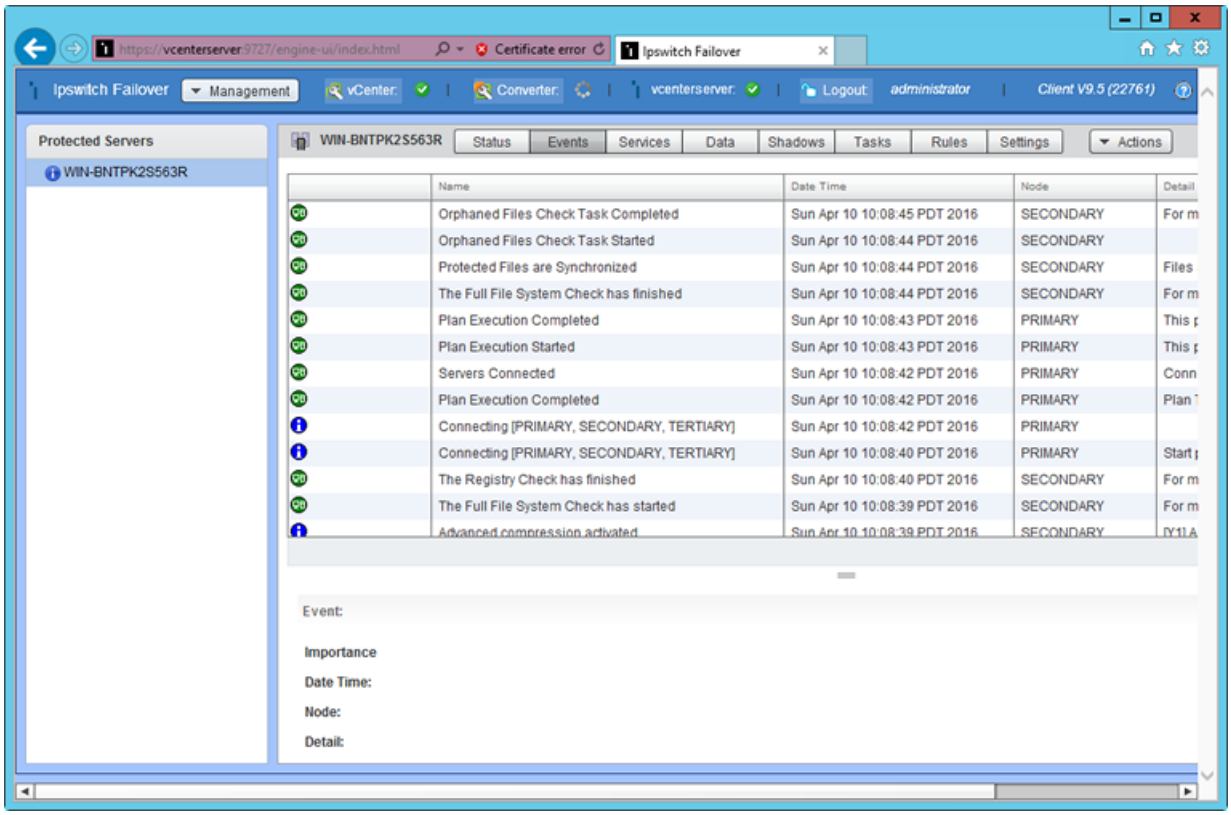

Figure 59: Events page

The events listed in the Event page show the time the event happened, its importance, the type of event that triggered the log, and its detail. Since the detail in the data grid is truncated, the full detail of the entry can be found in the lower portion of the pane when an event is selected.

There are four categories of importance of events that Ipswitch Failover is configured to log:

Icon	*Definition*
	These are critical errors within the underlying operation of Ipswitch Failover and can be considered critical to the operation of the system.
	Warnings are generated where the system finds discrepancies within the Ipswitch Failover operational environment that are not deemed critical to the operation of the system.
	System logs are generated following normal Ipswitch Failover operations. Review these to verify the success of Ipswitch Failover processes such as file synchronization.
	Information events are similar to system logs but reflect operations carried out within the graphical user interface rather than operations carried out on the Ipswitch Failover Server service itself such as logging on etc.

Services

The status of all protected services is displayed on the **Services** page. The status shows both the target and actual state for all servers in the cluster and the Failure Counts for each of the server.

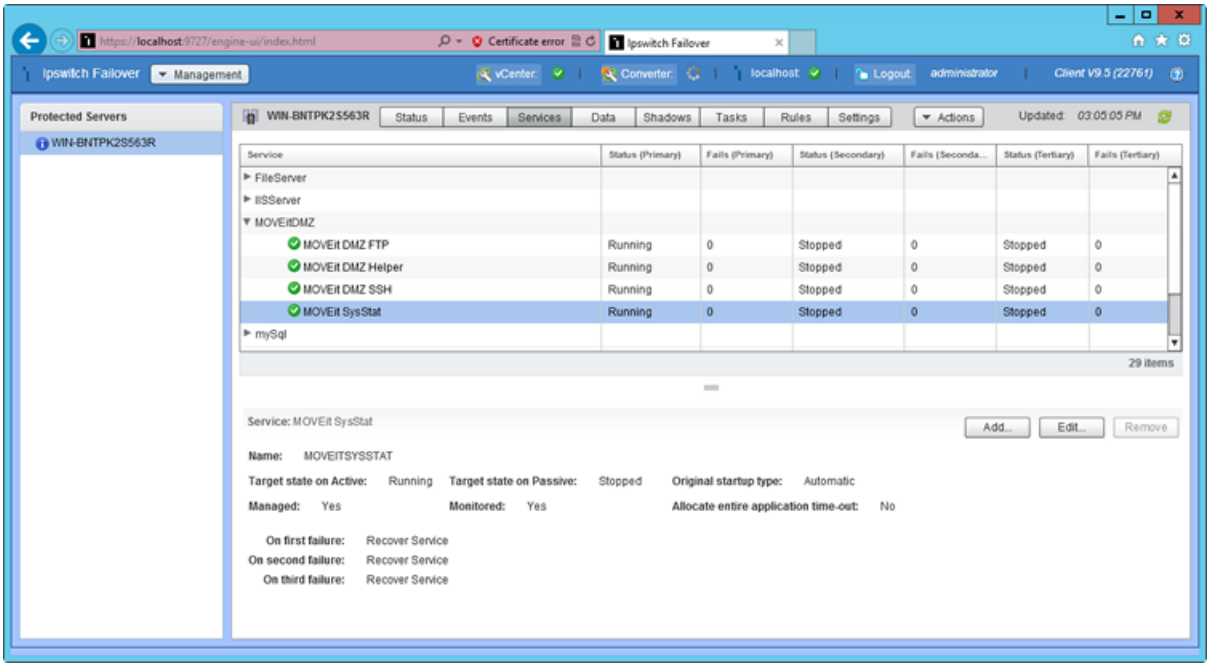

Figure 60: Applications: Services page

The target state of protected services can be specified for the active and passive server(s), and is typically *Running* on the active and *Stopped* on the passive(s). Services are protected when they are in a Running state in Failover Management Service or set to Automatic in Windows Services, and otherwise are logged as unprotected. Services depending on protected services are managed (for example, started and stopped) by Ipswitch Failover but not monitored (for example, not restarted if stopped by some external agency). Services upon which protected services depend are monitored (for example, restarted if stopped) but not managed (for example, not stopped if protected applications are stopped).

Add a Service

To protect a service that was not automatically added by Ipswitch Failover during installation, the service must be added through the Ipswitch Failover Management Service and be in a *Running* state.

Procedure

To add a service:

1. Select the Service tab and then click **Add** at the lower right of the pane.

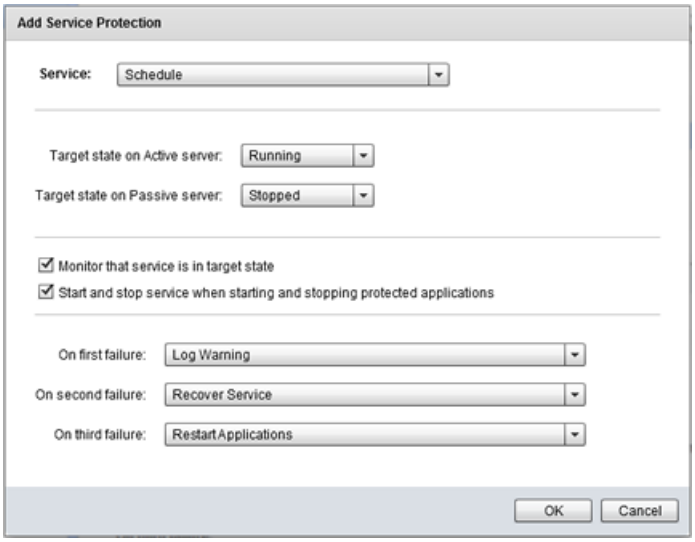

Figure 61: Add Service

2. Select the service and set the *Target State on Active server* and *Target State on Passive server* values. Normally, the *Target State on Active server* is set to *Running* and the *Target State on Passive server* is set to *Stopped*. User defined services configured with a target state of *Running* on both active and passive servers do not stop when **Stop Applications** is clicked.
3. To make Ipswitch Failover monitor the state of the service, select the *Monitor State* check box. To let Ipswitch Failover manage the starting and stopping of the service, select the check box.
   Ipswitch Failover also lets you assign three sequential tasks to perform in the event of failure. Task options include the following:

   - *Restart Applications* – Restarts the protected application.
   - *Switchover* – Initiates an automatic failover to the currently passive server.
   - *Recover Service* – Restarts the service.
   - *Log Warning* – Adds an entry to the logs.
   - A User Defined task, created in the *Tasks* page, as a *Rule Action* task type.
   - vSphere Integration\RestartVM – Cleanly shuts down and restarts the Windows OS on the target VM.
   - vSphere Integration\ TriggerMigrateVM – Depending on the parameters specified it can be vMotion, enhanced vMotion or storage vMotion.
   - vSphere Integration\ TriggerMigrateVMandRestartApplications – Same as TriggerMigrateVM + application restart.
   - vSphere Integration\ TriggervSphereHaVmReset – Communicates with vCenter Server to reset the virtual machine, but does so using the vSphere HA App Monitoring mechanism. This is potentially more robust, but requires the VM to be on an vSphere HA cluster with *Integrate with vSphere HA Application Monitoring* enabled in the VmAdaptor plug-in settings.

   Note: *Rule Action tasks are additional user defined tasks previously created by the user and must be created on the active Ipswitch Failover server*

4. Assign a task to each of the three failure options and after all selections are made, click **OK** to dismiss the dialog.

   Note: *When dependent services are involved, actions to take on failure should match the protected service.*

   If a service fails and the failure option is set to Restart Applications, all applications are restarted.

Edit a Service

To change the options of a protected service, select the service listed in the pane and perform the following steps:

Procedure

Note: *Only user defined services can be configured regarding the target state, Monitor State, and Manage Starting and Stopping. The plug-in defined services cannot be edited in this sense. Only their recovery actions can be edited.*

1. Click the **Edit** button at the lower portion of the pane.

   The **Edit Service Protection** dialog appears, which provides a subset of same options available when a new service is added.

2. After making modifications, click **OK** to accept the changes.

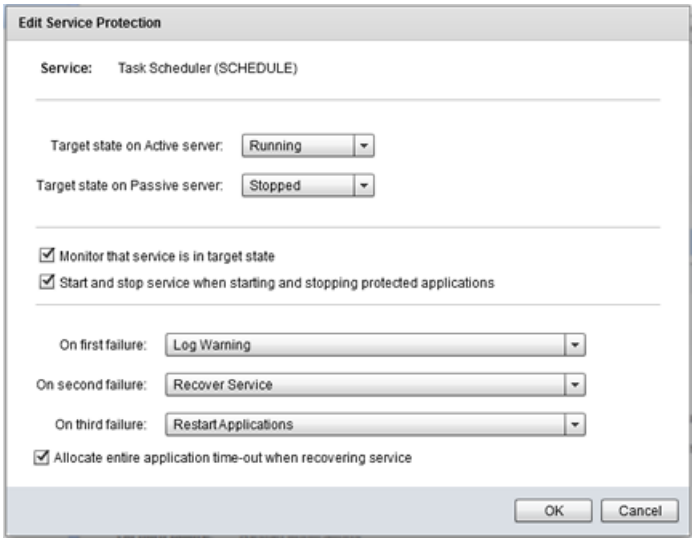

Figure 62: Edit Service Protection

3. To unprotect a User Defined service and stop monitoring the service, click on the *Services* tab. Select the service and click **Edit**.
4. Clear the *Start and stop service when starting and stopping protected applications* check box, and then click **OK**.

Configure Service Recovery Options for Protected Services

Ipswitch Failover Management Service provides the ability to configure the Service Recovery Options for services that are protected.

Procedure

1. Navigate to the Services page.
2. Click the **Edit** button.
   Select the action to take for the 1st, 2nd, and 3rd instance of failure. Click **OK**.

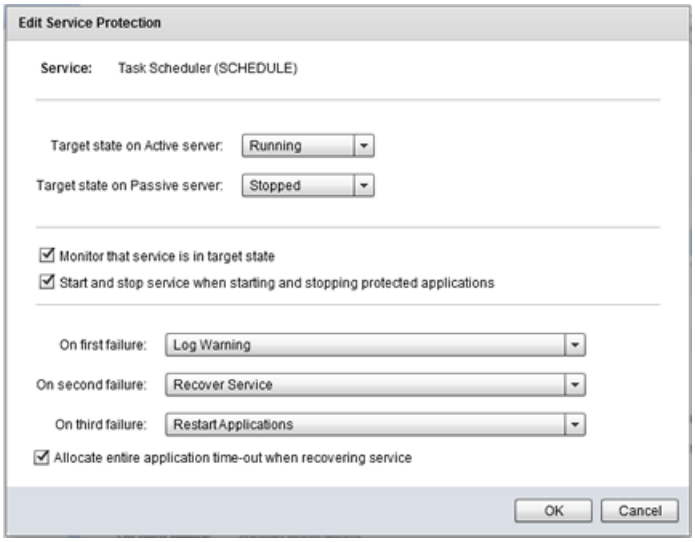

Figure 63: Edit Service Protection

Remove a Service

To remove a service, select the service in the pane and perform the following steps:

Procedure

Note: *Only user defined services can be removed. Plug-in defined services can not be removed.*

- Select the user defined service to be removed and click **Remove** at the lower portion of the pane. The user defined service is removed from the list of protected services.

Data

Ipswitch Failover can protect many permutations or combinations of file structures on the active server by the use of custom inclusion and exclusion filters configured by the administrator.

Note: *The Ipswitch Failover program folder holds the send and receive queues on the active and passive servers, and therefore should be explicitly excluded from the set of protected files.*

You can view replication status and manage data replication through the **Data: Replication Queues.**

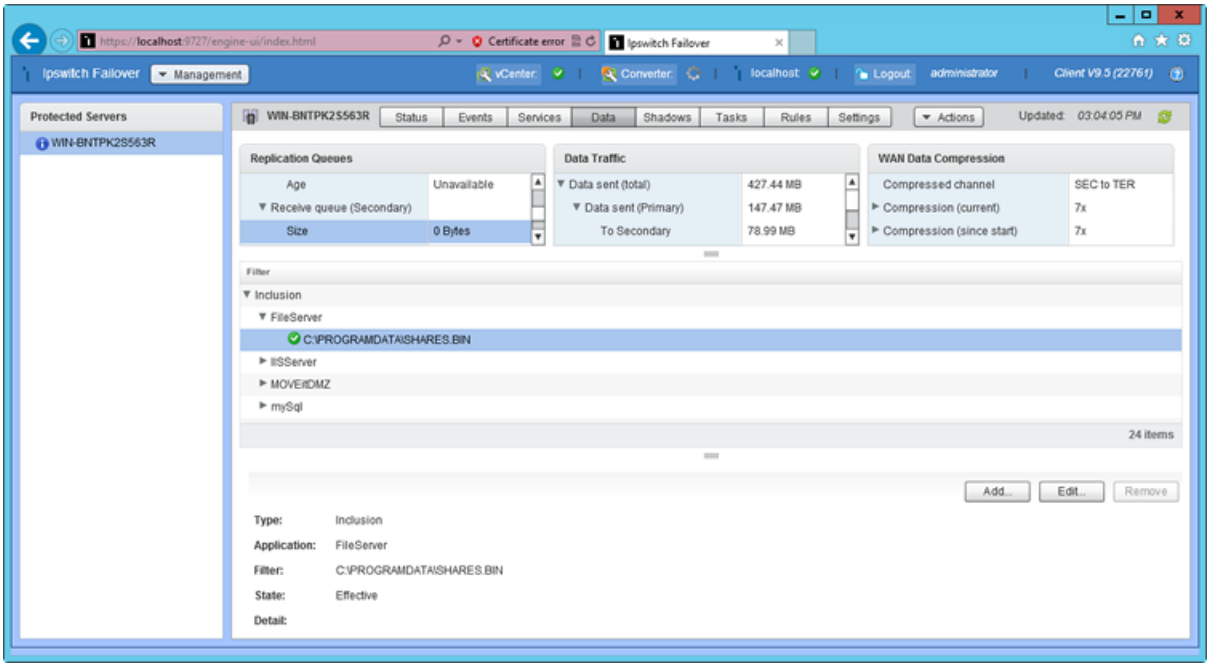

Figure 64: Data page

The *Replication Queues* pane – The statistics of the connection with regards to the data sent by either server and the size of the active server's send queue and passive server's receive queue are displayed.

The *Data Traffic* pane – The Data Traffic displays the volume of data that has been transmitted across the wire from the active server to the passive server.

The *WAN Data Compression* pane – Ipswitch Failover offers WAN Compression as an optional feature to assist in transferring data fast over a WAN. When included in your Ipswitch Failover license, WAN Compression can be configured through the **Settings** page. The **Data** page provides a quickly accessible status on the current state of WAN operations, identifies the compressed channel, and displays the amount of compression that is being applied currently and since the start.

Add Filters

Administrators can add filters to include additional files or folders in the protected set or to exclude a subset of files or folders within the protected set.

Procedure

To add a user defined Inclusion Filter to add to the protected set, perform the following steps:

1. Click the **Add** button to open the **Add Filter** dialog.

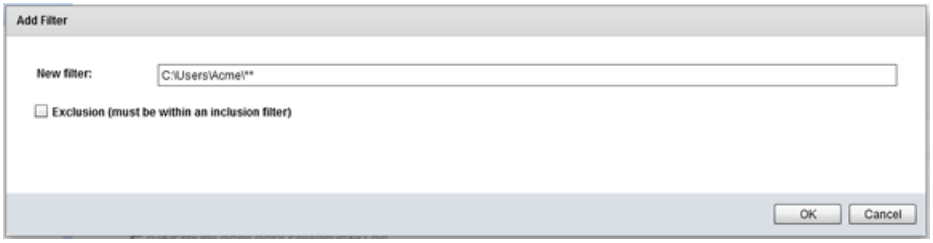

Figure 65: Add Filter

2. Filters to protect user defined files and folders are defined by typing the complete path and pattern or by specifying a pattern containing wildcards.
3. Click **OK** to accept the changes, or **Cancel** to dismiss the dialog without making any changes.

   The two forms of wildcard available are `*`, which matches all files in the current folder or `**`, which matches all files, subfolders and the files in the subfolders of the current folder. After the filter is defined, subsequent inclusion filters may be added.

> ***Note:*** *Ipswitch Failover "vetoes" replication of a few specific files and folders such as the Ipswitch Failover installation directory or the `System32` folder. If you create an inclusion filter that includes any of these off-limits files or folders, the entire filter is vetoed, even if you have created an exclusion filter to prevent replication of those files or folders.*

Add an Exclusion Filter

Exclusion Filters are configured to create a subset of an Inclusion Filter to exclude data from protection. The Exclusion Filter is created in the same way as the Inclusion Filter.

Procedure

1. Filters to exclude files and folders from protection and replication are defined by clicking **Add** button on the **Data** page of the Ipswitch Failover Management Service.

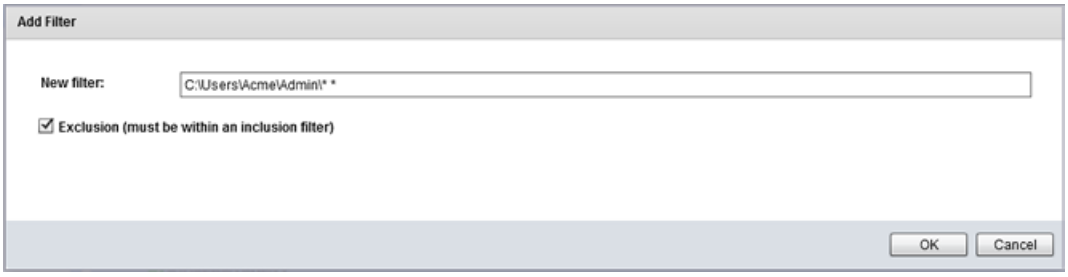

Figure 66: Add Exclusion Filter

2. Type the complete path and pattern or specify a pattern containing wildcards.
3. Click **OK** to accept the changes.
   The two forms of wildcard available are `*`, which matches all files in the current folder, and `**`, which matches all files, subfolders and the files in the subfolders of the current folder.

Edit Filters

User defined Inclusion/Exclusion filters can be edited to enable/disable the filter using the Ipswitch Failover Management Service.

Procedure

To Edit a user defined Inclusion/Exclusion Filter:

1. Select the filter and click the **Edit** button located under the filters pane on the **Data** page.

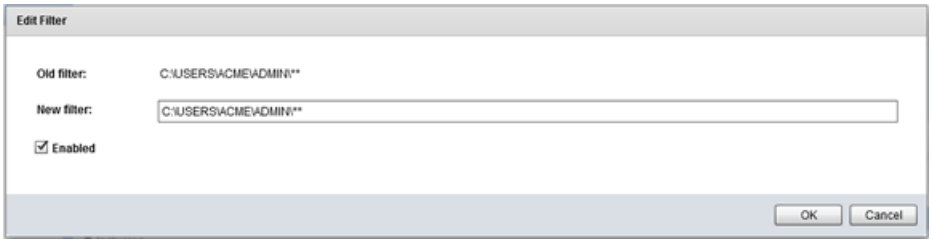

Figure 67: Edit Inclusion Filter

2. Edit the value in the *New Filter* text box by typing over the current file filter definition or select to enable/disable the filter.
3. Click **OK**.
   The file filter is changed and becomes active.

Note: *Plug-in defined filters can only be edited to enable/disable the filter.*

Remove Filters

Procedure

To Remove a user defined filter:

Note: *Plug-in filters can not be removed.*

- To remove an Inclusion filter or Exclusion filter, select the filter in the *Filter* pane and click **Remove**.

Shadows

The Ipswitch Failover Data Rollback Module (DRM) provides a way to rollback data to an earlier point in time. This helps mitigate problems associated with corrupt data such as can result from virus attacks. Before configuring or using any of the DRM features accessed through this page, Ipswitch recommends that you read and follow the steps described in the section immediately below, *Best Practices for Using Volume Shadow Copy Service & DRM*.

Best Practices for Using Volume Shadow Copy Service & DRM

The Volume Shadow Copy Service (VSS) component of Windows 2008 and Windows 2012 takes shadow copies and allows you to configure the location and upper limit of shadow copy storage.

1. To configure VSS, right-click on a volume in Windows Explorer, select *Properties*, and then select the *Shadow Copies* tab.

   Note: *VSS is also used by the Shadow Copies of Shared Folders (SCSF) feature of Windows 2008, and consequently, some of the following recommendations are based on Microsoft™ Best Practices for SCSF.*

2. Decide which volume to use for storing Shadow Copies before using DRM because you must delete any existing shadow copies before you can change the storage volume.
   Ipswitch recommends that a separate volume be allocated for storing shadow copies. Do not use a volume to store both Ipswitch Failover protected data and unprotected, regularly updated data. For example: do not write backups of data (even temporarily) to a volume that contains Ipswitch Failover protected files, as that increases the space required for snapshots.

   In accordance with the following guidelines from Microsoft:

Select a separate volume on another disk as the storage area for shadow copies. Select a storage area on a volume that is not shadow copied. Using a separate volume on another disk provides two advantages. First, it eliminates the possibility that high I/O load causes deletion of shadow copies. Second, this configuration provides better performance.

3. Be sure to allocate enough space for the retained shadow copies.
   This is dependent on the typical load for your application, such as the number and size of emails received per day, or the number and size of transactions per day. The default is only 10% of the shadowed volume size and should be increased. Ideally, you should dedicate an entire volume on a separate disk to shadow storage.

   Note: *The schedule referred to in the* ***Volume Properties*** > ***Shadow Copies*** > ***Settings*** *dialog is for Shadow Copies for Shared Folders. This is not used for DRM - the DRM schedule is configured in the Rollback Configuration pane of the Ipswitch Advanced Managment Client.*

4. Configure the schedule to match your clients' working patterns. Considering both the required granularity of data restoration, and the available storage.

   DRM provides a means of flexibly scheduling the creation of new Shadow Copies, and the deletion of older Shadow Copies. Adjust this to suit the working-patterns of your clients and applications. For example, do clients tend to work 9am-5pm, Monday-Friday in a single time zone, or throughout the day across multiple time zones? Avoid taking Shadow Copies during an application's maintenance period, such as Exchange defragmentation, or a nightly backup.

   In selecting how frequently to create new shadow copies, and how to prune older ones, you must balance the advantages of fine-granularity of restorable points-in-time versus the available disk space and the upper limit of 512 Shadow Copies across all shadowed volumes on the server.

5. Perform a trial-rollback.

   After DRM is configured, Ipswitch recommends that you perform a trial-rollback, to ensure that you understand how the process works, and that it works correctly.

   If you do not select the option *Restart applications and replication*, then you can rollback to Shadow Copies on the passive server without losing the most recent data on the active server.

6. Start the application manually to verify that it can start successfully using the restored data.
   Note the following:

   - The application is stopped on the active during the period of the test.
   - Following the restoration of data on the passive, it becomes active and visible to clients on the network.

   After the test is complete, shut down Ipswitch Failover on both servers. Use the **Server Configuration Wizard** to swap the active and passive roles, and then restart. This re-synchronizes the application data from the active to the passive, and allows you to restart using the application data as it was immediately before the rollback.

7. Monitor Ipswitch Failover to identify any Shadow Copies that are discarded by VSS.

   If DRM detects the deletion of any expected Shadow Copies, this is noted in the Ipswitch Failover *Event Log*.

   This is an indication that VSS reached its limit of available space or number of Shadow Copies. If many Shadow Copies are automatically discarded, consider adding more storage, or reconfiguring your schedule to create and maintain fewer shadow copies.

Configure Shadow Creation Options

These options set the frequency for shadow creation on the passive and active servers respectively.

Procedure

Note: *No shadows are created when the system status is Out-of-sync or Not Replicating.*

- **Create a shadow every:**
  This drop-down list controls how frequently a shadow copy is taken on the passive servers, the default setting is every 30 minutes. When the shadow is actually taken is also controlled by *Only between the hours:* and *Only on the days:*, if either of these are set then shadows are taken at the frequency defined by this drop down list but only within the days/hours defined by them.
- **Create a shadow on the Active once per day at:**
  If the check box is cleared, then no shadows are automatically created on the active. If it is selected, then a Shadow is taken each day at the time selected from the drop down list. The Shadow is taken with "application co-operation", which means that if the application protected by Ipswitch Failover is integrated with VSS, it is informed before the shadow is taken and given the opportunity to perform whatever tidying up it is designed to do when a VSS Shadow is taken.

  Note: *It is possible to select a time outside of the Only between the hours: range. This prevents creation of the shadow.*

  Whether a shadow is actually taken is also controlled by *Only between the hours:* and *Only on the days:*, if either of these are configured, then a shadow is taken only within the days/hours defined by them. The following two options limit the number of shadows taken during periods when the data is not changing.

- **Only between the hours:**

  If this check box is selected, then the range defined by the two drop down lists are applied to the automatic creation of shadows on either on the passive server(s) (as controlled by *Create a shadow every:*), or on the active server (as controlled by *Create a shadow on the Active once per day at:*).

  For example, to limit shadow captures to night time hours, you can define a range of 20:00 to 06:00.

- **Only on the days:**

  When the check box is selected, the range defined by the two drop down lists is applied to the automatic creation of shadows either on the passive server(s) (as controlled by *Create a shadow every:*) or active server (as controlled by *Create a shadow on the Active once per day at:*).

  For example, to limit shadow captures to weekend days, you can define a range of Saturday to Sunday.

  Note: *The shadow copy information location is configurable. The default location ensures that the information location includes a copy of the necessary file filters to be used in a rollback. Ipswitch recommends that the default setting be used for shadow copy information location.*

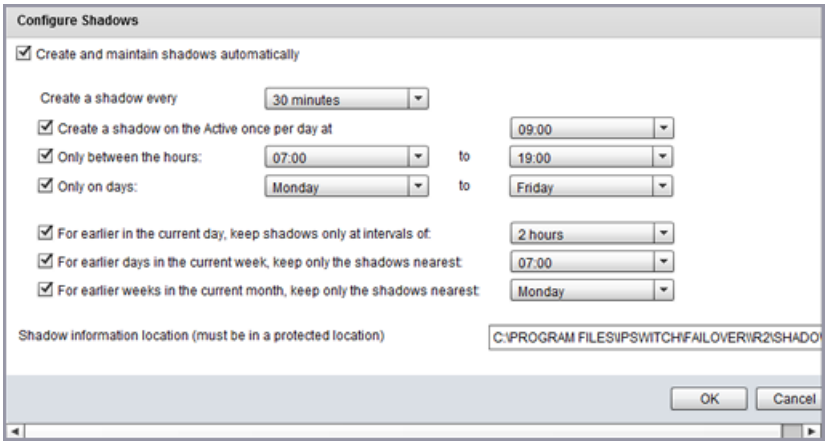

Figure 68: Shadow Creation Options

Configure the Shadow Copy Schedule

DRM can create and delete shadow copies automatically according to a configurable schedule. The aim of the schedule is to provide a balance between providing a fine-granularity of rollback points-in-time on the one hand, and conserving disk space and number of shadow copies on the other. To achieve this balance, the available configuration options reflect the observation that recent events generally are of more interest and value than older ones. For example, the default schedule maintains one shadow from every day of the last week, and one shadow from every week of the last month.

Procedure

Ipswitch Failover can be configured to automatically create shadow copies by performing the following steps:

1. Navigate to the **Shadows** page and click **Configure**. The *Configure Shadow Schedule* dialog appears.

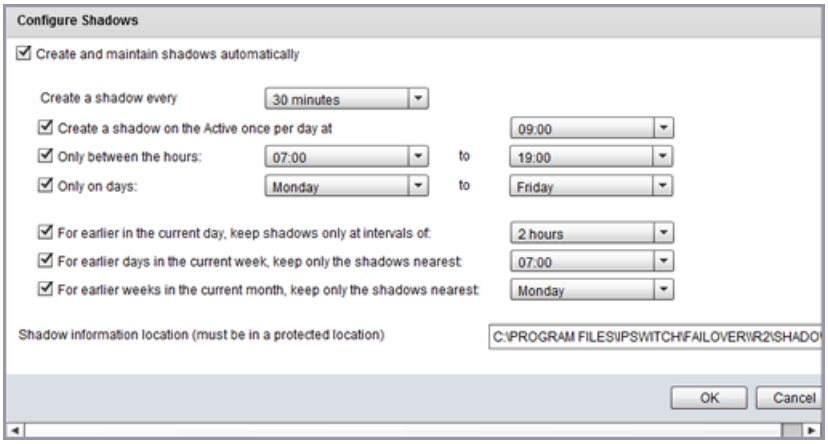

Figure 69: Configure Shadow Schedule

2. Select the *Create and maintain shadows automatically* check box.
   The *Create and maintain shadows automatically* check box controls the automatic creation and deletion of Shadow copies. When selected, automatic Shadow copies are created and deleted in accordance with other user configuration settings. When cleared, you can still manually create, delete, and rollback shadow copies from the *Shadow* pane.

> ***Note:*** *Configure the schedule to suit your clients' working patterns; the required granularity of data restoration, and the available storage.*

3. Select the frequency and time periods for creating shadows. (See *Configure Shadow Creation Options*, above.)
4. Select the shadows to keep or remove from earlier time periods. (See *Configure Shadow Keep Options*.)

> ***Note:*** *The Volume Shadow Copy Service (VSS) component of Windows 2008/2012, may automatically delete old shadows because of lack of disk space even when the Create and maintain shadows automatically check box is not selected.*

Configure Shadow Keep Options

The purpose of the following three options is to reduce the number of older shadows while preserving a series, which spans the previous 35 days.

Procedure

Manually created shadows are not deleted automatically, but VSS deletes old shadows (whether manually created or not) whenever it requires additional disk space for the creation of a new shadow. When manually created shadows match the criteria for keeping a shadow from a particular time period, automatic shadows in close proximity are deleted. For example, a manually created shadow is not deleted, but can be used for the "keep algorithm".

- **For earlier in the current day, keep shadows only at an interval of:**

  If the check box is selected, then only the first shadow is kept for each interval as defined by the value (hours) selected from the drop-down list. Earlier in the current day means since Midnight and older than an hour. The intervals are calculated from either at Midnight or if *Only between the hours:* is selected, then from the start hour. For shadows taken before the start time (as the start time may change), the interval is calculated backwards again starting at the start time.

- **For earlier days in the current week, keep only the shadow nearest:**

  If the check box is selected, then only the shadow nearest to the time (24 hour clock) selected from the drop-down list is kept for each day. Earlier days in the current week means the previous seven days not including today (as today is covered by the above option). A day is defined as Midnight to Midnight.

  If a shadow was taken at 5 minutes to midnight on the previous day it is not considered when calculating the nearest.

- **For earlier weeks in the current month, keep only the shadows nearest:**

  If the check box is selected, then only the shadow nearest to the selected day is kept for each week. Earlier weeks in the current month means the previous four weeks not including either today or the previous 7 days (as they are covered by the above two options).

  To calculate the "nearest", an hour is required. The calculation attempts to use the selected time from *For earlier days in the current week, keep only the shadow nearest:* if it is selected, otherwise the *Only between the hours* start time is used if it is selected, finally, when neither of these options are configured, Midnight is used.

  All automatic shadows taken more than 35 days ago are deleted. The intervening 35 days are covered by the above three options.

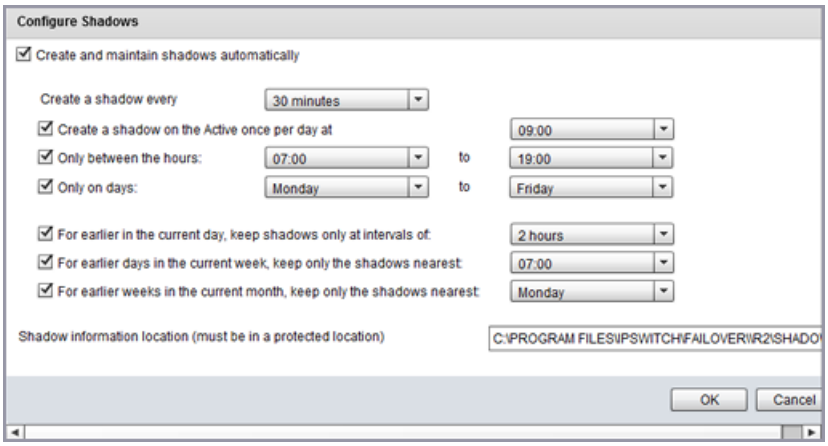

Figure 70: Shadow Keep Options

Manually Create Shadow Copies

Shadow Copies can be created manually using the steps below:

Procedure

- In the *Shadow* pane of the **Shadows** page, click **Create (Primary)**, **Create (Secondary)** or if present, **Create (Tertiary)**.
  A Shadow Copy is created on the selected node.

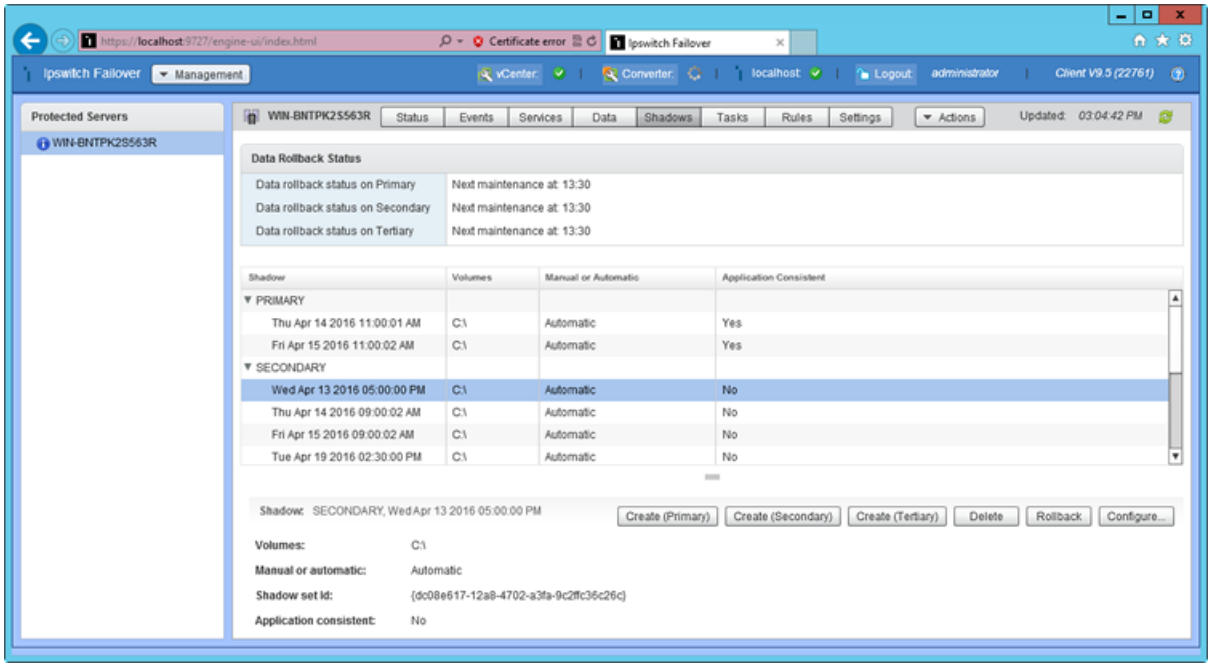

Figure 71: Create Shadow Dialog

Delete a Shadow Copy

Procedure

Should the need arise to delete shadow copies, follow the procedure below:

- To delete a shadow copy, select it in the *Shadow* pane of the **Shadows** page. Click **Delete**.
  The selected shadow copy is deleted.

Roll Back Protected Data to a Previous Shadow Copy

Should the need arise to roll data back to a previous point in time, perform the following:

Procedure

1. Go to the *Shadow* pane of the **Shadows** page and select an existing Shadow from the Primary, Secondary, or Tertiary server list and click **Rollback**.
2. A dialog is presented allowing you to create a shadow immediately before the rollback, and select whether to restart applications and replication after the rollback.

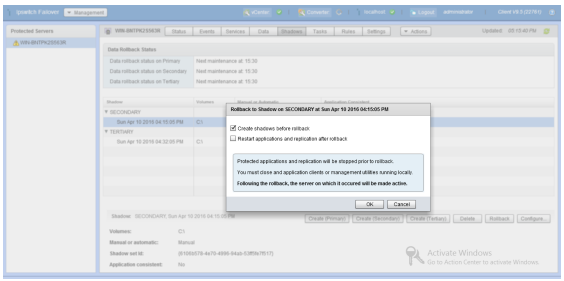

Figure 72: Rollback to Shadow dialog

> ***Note:*** *Electing to create a shadow before the rollback means that if you change your mind, you can restore to the most recent data.*
>
> *Choosing to restart applications and replication simplifies the restore procedure, but eliminates the chance to examine the data before it is replicated to the other server.*

3. Click **OK**.
   A confirmation dialog is presented.
4. Click **Yes**.

   Ipswitch Failover stops the applications and replication, and then restores protected files and the registry from the Shadow Copy. Ipswitch Failover then sets the file and registry filters to those persisted in the Shadow Copy. If the Shadow Copy is on a currently passive server, then this server will become active after the rollback.

   If the rollback fails, the reason for the failure is shown in the status display. This may be because a particular file set of files or registry key cannot be accessed. For example, a file may be locked because the application is inadvertently running on the server performing the rollback, or permissions may prevent the SYSTEM account from updating. Rectify the problem and try performing the rollback again.

5. If selected, applications and replication are restarted and the Cluster re-synchronizes with the restored data.

   - If you selected not to restart applications and replication automatically, you can now start the application manually. This allows you to check the restored data.
   - If you decide to continue using the restored data, click **Start** on the Ipswitch Failover *System Overview* pane to re-synchronize using this data.
   - If you decide you want to revert to the pre-rollback data, which is still on the other (now passive) server, you can shut down Ipswitch Failover, use the **Configure Server Wizard** to swap the active and passive roles, and then restart. This re-synchronizes the servers with the pre-rollback data.

As a result of the rollback, the file and registry filters are set to the configuration, which was in use when the shadow copy was taken.

Tasks

Tasks are actions which are required for automated application management.

Task types are determined by when the tasks are run, and include the following:

- **Network Configuration** — This is the first type of task run when applications are started, and is intended to launch Dnscmd, DNSUpdate or other network tasks. Where multiple DNScmds are required, these can be contained in a batch script, which is then launched by the task. Network Configuration tasks are the only types of task that can vary between Primary, Secondary, and/or Tertiary servers.
- **Periodic** — These tasks are run at specific configurable intervals.
- **Pre/Post Start** — These tasks are run before and after services are started on the active server.
- **Pre/Post Stop** — These tasks are run before and after services are stopped on the active server.
- **Pre/Post Shadow** — These tasks are run before and after a shadow copy is created on the active server by the Data Rollback Module.
- **Rule Action** — These tasks can be configured to run in response to a triggered rule, or when a service fails its check.

Tasks can be defined and implemented by plug-ins or by the user, or they can be built-in tasks defined by Ipswitch Failover. User defined tasks are implemented as command lines, which can include launching a batch script. Examples of built-in tasks include monitoring a protected service state on the active and passive servers. An example of a plug-in-defined task is the discovery of protected data and services for a particular application.

The Ipswitch Failover Management Service Tasks page provides a list of tasks and associated status information, as well as features to quickly manage tasks.

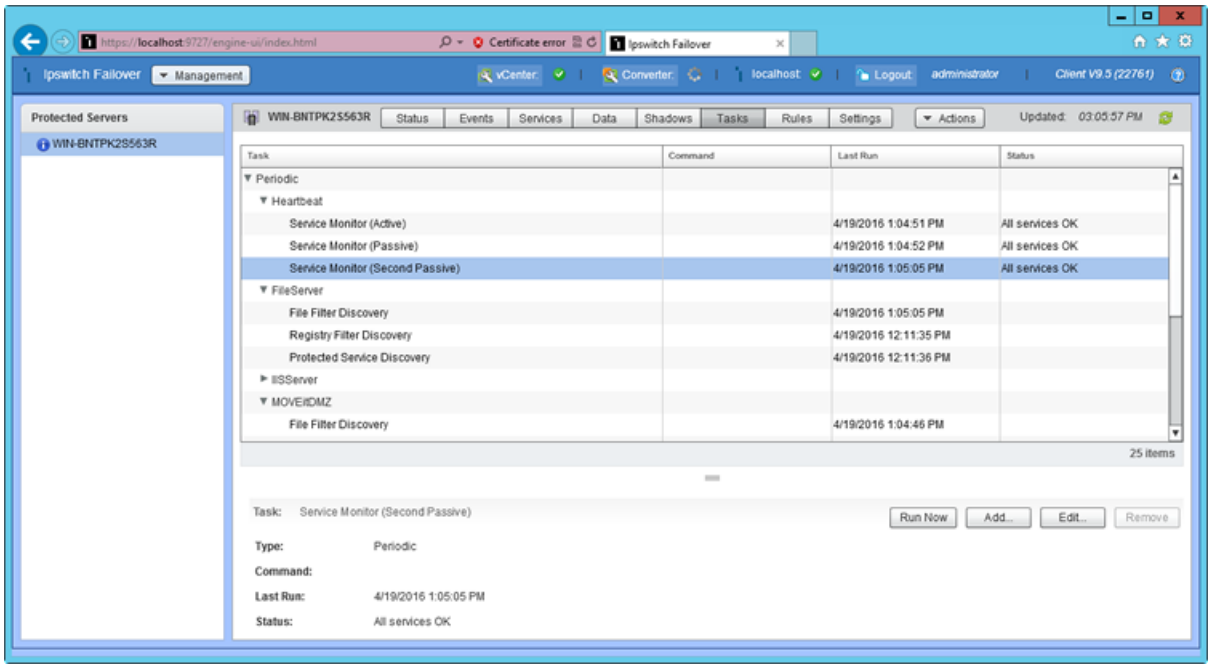

Figure 73: Tasks page

Run Now

When manually starting a task, you have the option to wait for a designated period or event to occur before launching the task, or to launch the task immediately. To launch a task immediately, select the task from the list and perform the following step:

Select an existing task and click **Run Now** at the lower right of the pane.

The task runs. You can watch the *Status* column of the *Task* list for messages as the task runs to completion.

Add Task

Tasks can be added from the Tasks page of the Ipswitch Failover Management Service.

To add a User Defined task:

1. Click **Add** at the lower right of the pane. The *Add Task* dialog appears.
2. Type a *Name* for the task into the text box.
3. Select the *Task Type* from the drop-down list. Task types include: *Network Configuration*, *Periodic*, *Pre/Post Start*, *Pre/Post Stop*, *Pre/Post Shadow*, and *Rule Action*.
4. Select the identity of the server the task *Runs On* (Primary, Secondary, or Tertiary).

   Note: *This is required only for Network Configuration tasks.*

5. In the *Command* text box, type in the path or browse to the script, `.bat` file, or command for the task to perform.

   Note: *When the Command entry requires specific user credentials, you must select that user from the Run As drop-down list.*

6. Select from the options presented in the *Run As* drop-down list (typically includes local and administrator accounts).
7. Click **OK** to add the task, or **Cancel** to exit the dialog without adding the task.

Edit Task

You can edit the interval, a command, or disable an existing task. To edit a task:

1. Click **Edit** at the lower right of the pane. The *Edit Task* dialog appears. The parameters available to edit vary according to the task type.
2. After completing edits of the task, click **OK** to accept the settings and dismiss the dialog.

Remove Task

Note: *Only user defined tasks can be removed. Plug-in task removal will be vetoed.*

To remove a task, select the task from the list and perform the following steps:

1. Select an existing task click **Remove** at the lower right of the pane. A confirmation message appears.
2. Click **Yes** to remove the task, or click **No** to close the message without removing the task.

Rules

Rules are implemented by plug-ins (there are no user-defined rules). Rules can be either timed (they must evaluate as true continuously for the specified duration to trigger) or latched (they trigger as soon as they evaluate to true). Rules can be configured with rule actions, which are the tasks to perform when the rule triggers.

Rules use the following control and decision criteria for evaluation:

- Name: (the name of the rule).
- Enabled: (whether the rule is enabled or not).
- Condition: (the condition being evaluated).
- Status: (the current status of the rule being evaluation)
- Triggered: (the condition fails to meet configured parameters resulting in initiation of a duration count)
- Triggered Count: (a count of the number of times the rule has failed)
- Duration: (the length of time the condition exists before triggering the failure action).
- Interval: (the length of time between failure actions).
- First Failure: (action to take upon first failure) The default is set to Log Warning.
- Second Failure: (action to take upon second failure) The default is set to Log Warning.
- Third Failure: (action to take upon third failure) The default is set to Log Warning.

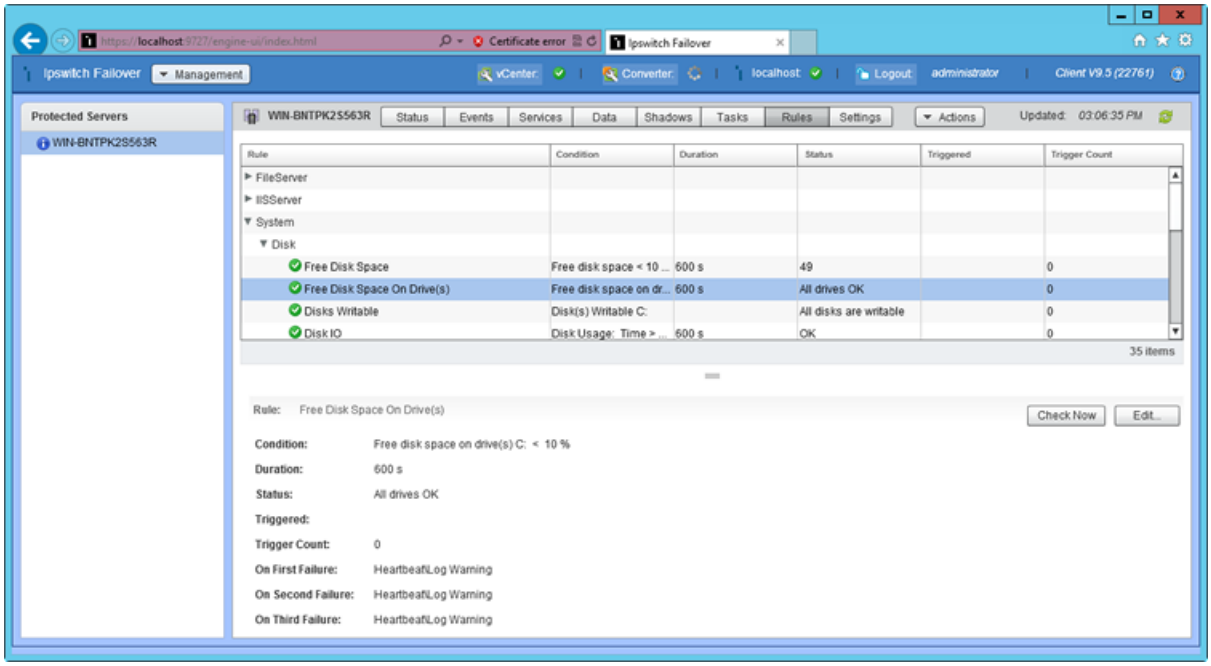

Figure 74: Rules page

Check a Rule Condition

To check a rule condition, select the rule in the *Rules* page and click **Check Now** on the lower right portion of the page.

Ipswitch Failover immediately checks the rule conditions of the current configuration against the attributes of the system and application.

Edit a Rule

Rules are implemented by plug-ins and cannot be created by users. Each plug-in contains a default set of rules with options that may be modified by the user.

To Edit a rule:

1. To edit a rule, select the rule in the *Rules* list.
2. Click **Edit** at the lower right of the page.

   The *Edit Rule* dialog appears.

   Use this dialog to *Enable* or *Disable* a Rule, set the specific options for the Rule, and to assign tasks to perform *On First Failure*, *On Second Failure*, and *On Third Failure*. The following tasks can be assigned in the event of a failure:

   - **Recover Service** – Restarts the service.
   - **Restart Applications** – Restarts the protected application.
   - **Log Warning** – Adds an entry to the logs.
   - **Switchover** – Initiates a switchover to the currently passive server.
   - **Rule Action** – Executes the command or script previously defined as a *Rule Action* task.

   If the installed servers are in a virtual to virtual configuration, the following additional tasks are available as a result of the vSphere Integration Plug-in.

   - **vSphere Integration\RestartVM** — Cleanly shuts down and restarts the Windows OS on the target VM
   - **vSphere Integration\ TriggerMigrateVM** — Depending on the parameters specified it can be vMotion, enhanced vMotion or storage vMotion
   - **vSphere Integration\ TriggerMigrateVMandRestartApplicatio**n — Same as TriggerMigrateVM + application restart
   - **vSphere Integration\ TriggervSphereHaVmReset** — Hard Reset of the VM implemented by integration with VMware HA

   > ***Note:*** *This option requires vSphere HA Application monitoring for the cluster and VM.*

3. When all options are selected, click **OK** to accept changes and dismiss the dialog.

Settings

The *Settings* page contains features to configure Plug-ins, Alerts, Email, WAN Compression and Replication Queue settings.

Configure Plug-ins

The Ipswitch Failover Management Service allows you to edit the configuration of user installed plug-ins.

To edit an existing plug-in, select *Plug-ins* in the left pane and then select the intended Plug-in from the *Plug-ins* list and perform the following steps:

1. Click the **Edit** button on the right side of the *Plug-in Detail* pane. The *Edit Plug-in* dialog appears.

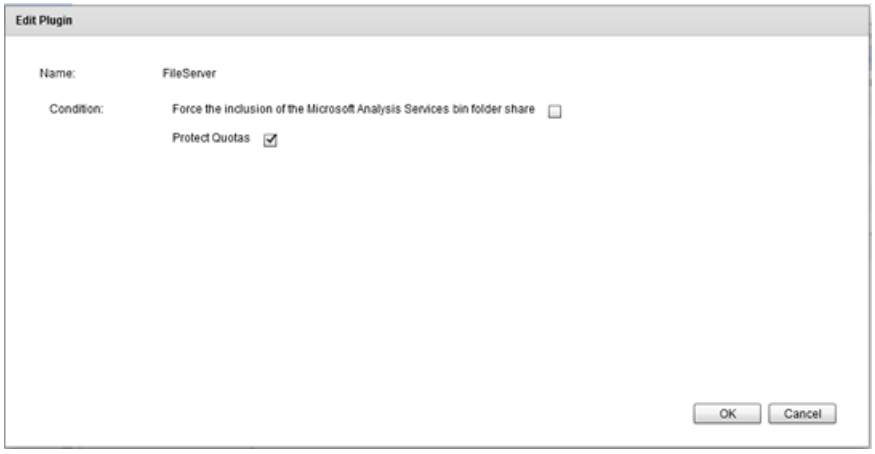

Figure 75: Edit Plug-in dialog

Note: *Configuration options are specific to each plug-in and must be reviewed before making modifications.*

2. Click **OK** to save the changes to the plug-in configuration, or click **Cancel** to close the dialog without making any changes.

Alert Settings

The *Settings* page lets you configure the Ipswitch Failover server to send predefined alerts to remote Ipswitch Failover administrators via email. The process for adding recipients is the same for all three trigger levels.

1. Select the type of alert (Red, Yellow, and Green) in the left pane resulting in the *Alert Settings* pane displaying for the selected alert.
2. Click the **Edit** button in the upper right portion of the *Alert Settings* pane.

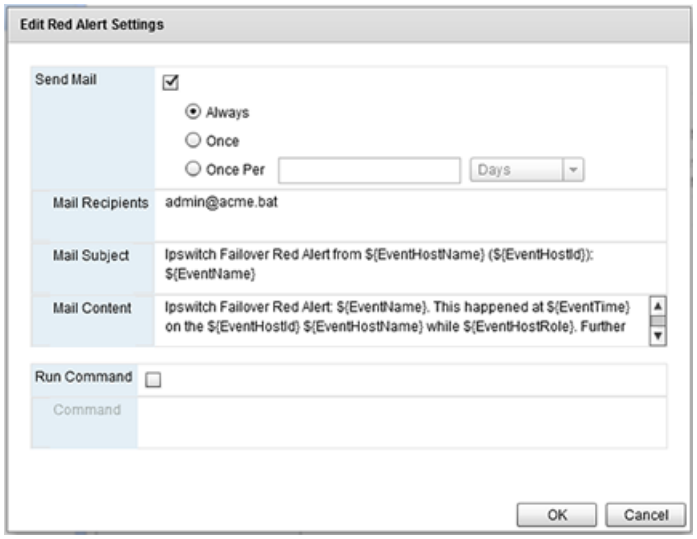

Figure 76: Alert Settings

3. Select the *Send mail* check box.
4. Select how many times to send the email (*Always*, *Once*, or *Once per* [user configurable time period]).
5. Enter a recipient's fully qualified email address into the *Mail Recipients* text box. Add additional recipients separated by a semi-colon.

6. Repeat step 4 to until all recipients have been added.
7. The Subject and Content of the alert emails for all three alerts can be adjusted to suit the environment. Ipswitch recommends using the pre-configured content and adding customized content as needed.

Note: *When Send mail is selected, there are three alternatives:*

- ***Always*** *– this will always send an email if this alert type is triggered.*
- ***Once*** *– this will send an email once for each triggered alert. An email will not be sent again for the same triggered alert, until Ipswitch Failover is re-started.*
- ***Once per*** *– within the time period selected, an email will only be sent once for the same triggered alert, subsequent emails for that trigger will be suppressed. Once the time period has expired, an email will be sent if the same alert is triggered.*

Using WScript to Issue Alert Notifications

An alternative way of issuing notifications for alerts is to run a command by selecting the *Run Command* check box under the relevant alert tab and typing a command into the associated text box. This command can be a script or a command line argument to run on the alert trigger and requires manual entry of the path to the script or command.

The pre-configured WScript command creates an event in the *Application Event Log* and can be customized to include the Ipswitch Failover specific informational variables listed in the following table.

Table 2: Ipswitch Failover Variables

Variables	*Values*
$EventHostID	Host ID
$EventHostName	Host name
$EventHostRole	Role of the host at the time of the event
$EventId	ID of event as listed above
$EventName	Human-readable name of event
$EventDetail	Detail message for event
$EventTime	Time at which event occurred

For example, the following command line argument creates an event in the *Application Event Log* that includes the machine that caused the alert, the time the alert happened, the name and details of the alert:

```
Wscript //T:10 $(installdir)\bin\alert.vbs "Ipswitch Failover alert on
$EventHost at $EventTime because $EventName ($EventDetail). Event Id is
$EventId"
```

After the alert recipients and/or actions to run are defined, click **OK** to save the changes and enforce the defined notification rules or click **Cancel** to close the dialog without making any changes.

Alert Triggers

Select *Alert Triggers* under *Alerts* in the left pane of the *Settings* page to view the currently configured alert triggers.

There are three alert states that can be configured: Red alerts, which are critical alerts, Yellow alerts, which are less serious, and Green alerts which are informational in nature and can be used for notification of status changes

(for example, a service that was previously stopped now is started). The alerts are preconfigured with the recommended alerting levels.

To modify the current configuration, click the **Edit** button in the upper left portion of the *Alert Triggers* pane. Each alert can be re-configured to trigger as a red, yellow, or green alert or no alert by selecting or clearing the appropriate check boxes. After the alert trigger levels are defined, click **OK** to save the configuration.

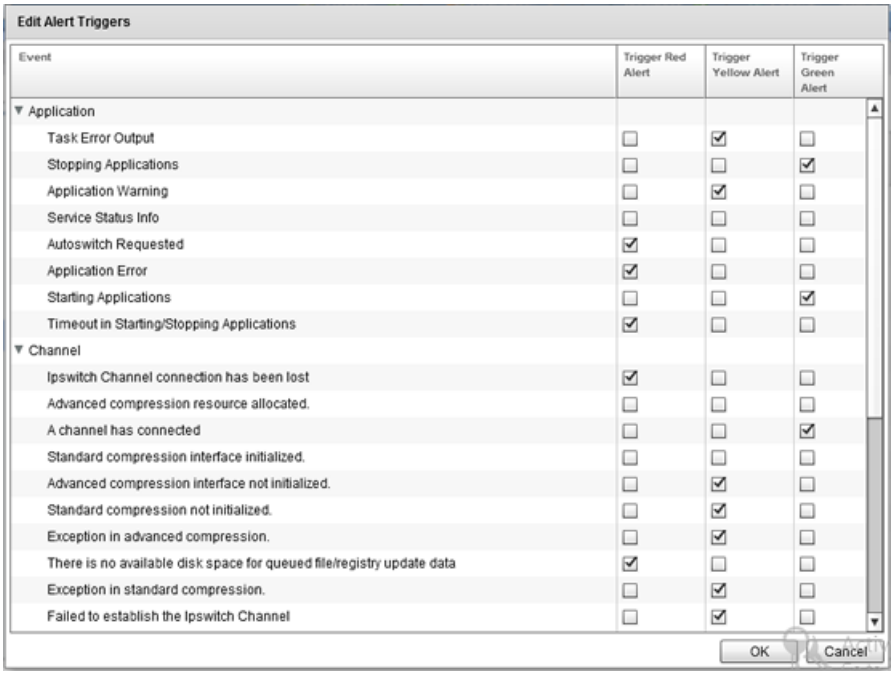

Figure 77: Edit Alert Triggers

Email Settings

Ipswitch Failover can alert the administrator or other personnel and route logs via email when an Alert condition exists. To configure this capability, in the *Settings* page, select *Email* in the left pane and click the **Edit** button in the upper right of the *Email Settings* pane.

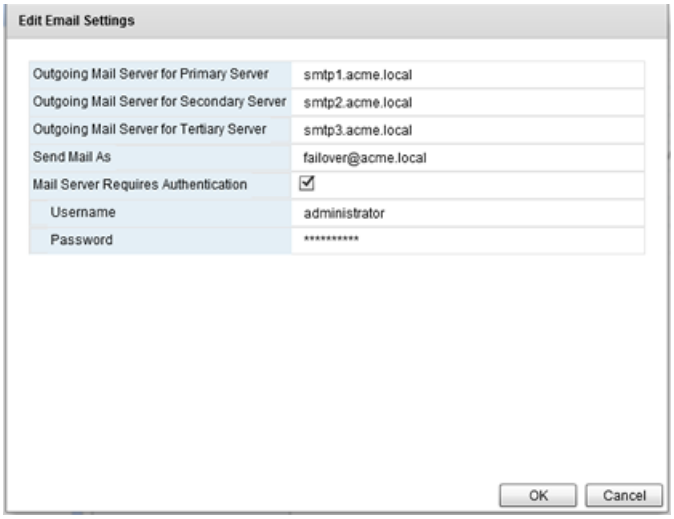

Figure 78: Email Settings

In the *Edit Email Settings* dialog, enter the Outgoing mail server (SMTP) of each server in the Cluster. Enter the mail server name using its fully qualified domain name. Next, configure the default *Send Mail as* email address. This can be customized but the email address used must be an email account authorized to send mail through the SMTP server.

Note: *Where Ipswitch Failover is protecting an Exchange Server, it is not recommended to configure the alerts to use the protected Exchange server and is advisable if at all possible to use a different Exchange server somewhere else within the organization.*

Where SMTP servers require authentication to accept and forward SMTP messages, select the *Mail Server requires authentication* check box and specify the credentials for an appropriate authenticated user account. Click **OK** to save the changes or click **Cancel** to close the dialog without making any changes.

After the trigger levels are configured and the email server defined in the *Settings* page *Edit Email Settings* dialog, configure the recipients of email alerts in the *Alert Settings* dialog. Email alerts for Red, Yellow, and Green alert triggers can be sent to the same recipient, or configured separately to be sent to different recipients depending on the level of alert.

Wan Compression

The WAN Compression feature allows the administrator to select from the following drop-down options:

Note: *Enabled compression type – Auto – is the recommended setting.*

- *Enabled compression type – Auto* . Ipswitch Failover selects the level of WAN compression based upon current configuration without user intervention.
- *Advanced* — Ipswitch Failover uses the WAN Deduplication feature in addition to compression to remove redundant data before transmitting across the WAN thereby increasing critical data throughput.
- *Standard* — Ipswitch Failover uses compression on data before it is sent across the WAN to improve WAN data throughput speed.
- *None* — Selected when deployed in a LAN or where WAN Compression is not required.

When Ipswitch Failover is deployed for Disaster Recovery (in a WAN), WAN Compression is by default configured to *Auto*. Ipswitch recommends that this setting not be changed unless specifically instructed to do so by Ipswitch Support.

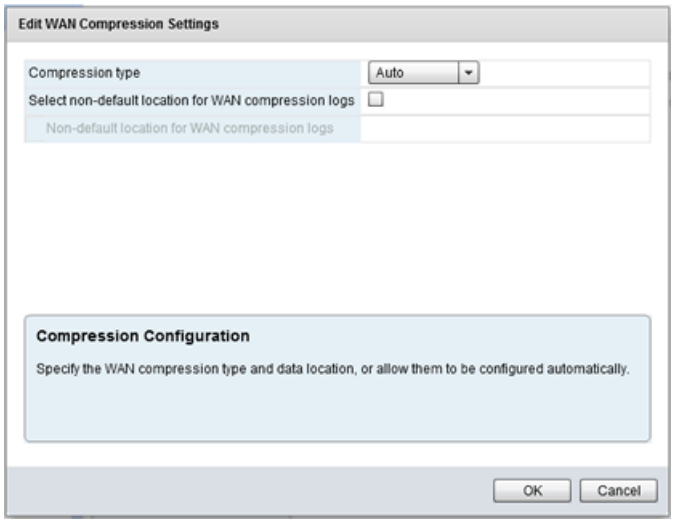

Figure 79: Edit WAN Compression dialog

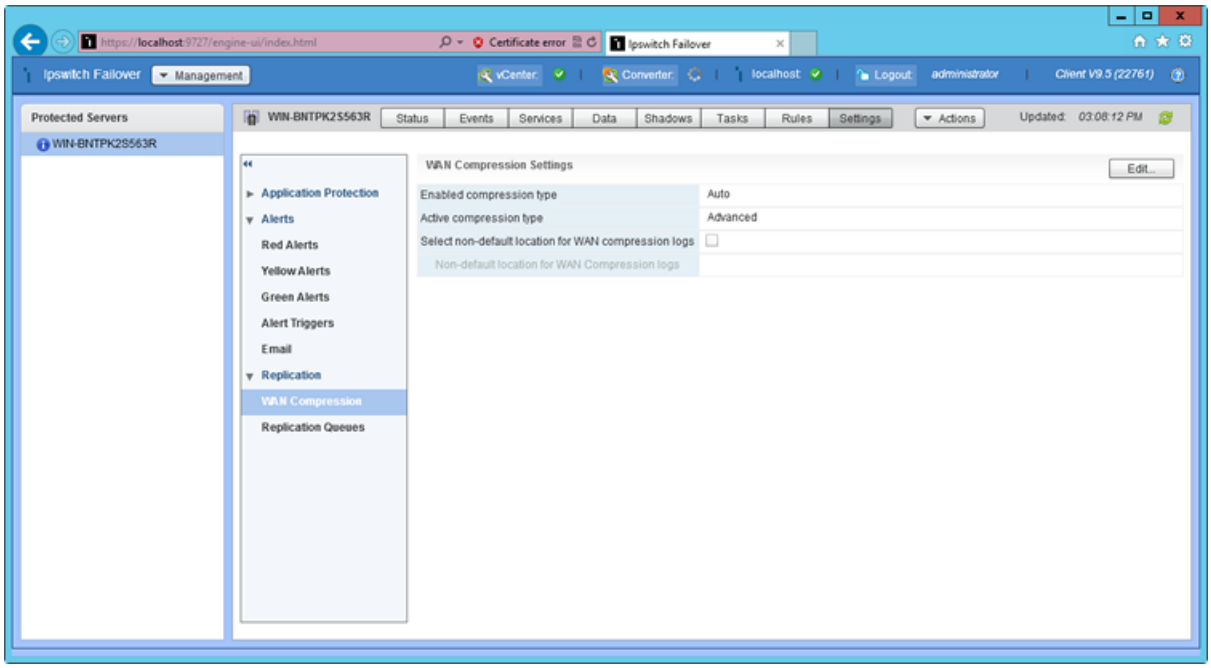

Figure 80: WAN Compression page

Replication Queue Settings

The **Settings** page displays the size of the replication queues configured on each server in the cluster.

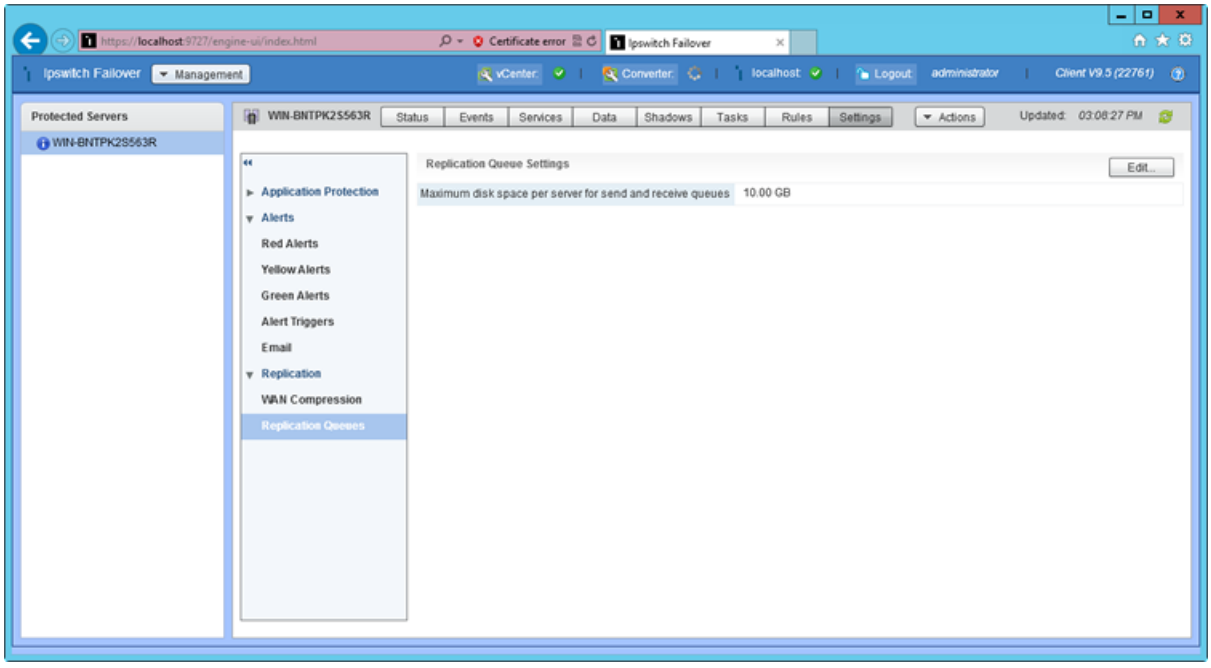

Figure 81: Configured Queue Size

The Edit Replication Queue Settings dialog allows you to configure the maximum disk space per server for the Send and Receive queues on each server.

To configure the maximum disk space to be used for the Send and Receive queues:

1. Click the **Edit** button.

2. Enter the maximum disk space to reserve for the *Send* and *Receive* queue.
3. Click **OK**.

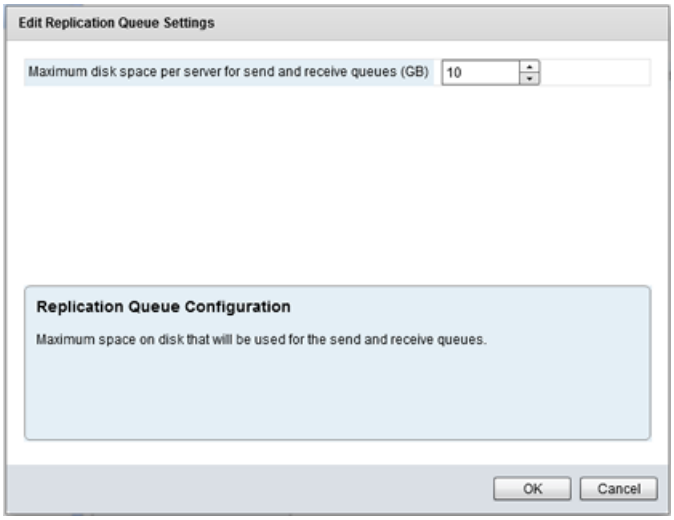

Figure 82: Edit Replication Queue Settings dialog

Actions

The *Actions* drop-down menu provides the ability to *Control* Ipswitch Failover using the Ipswitch Failover Management Service.

The Ipswitch Failover Management Service allows administrators to manage Ipswitch Failover clusters similar to the Ipswitch Advanced Management Client. The Ipswitch Failover Management Service provides the ability to perform the main operations, comprising a Switchover, Start/Stop Replication, Start/Stop Applications, Create Shadows, Check file and registry system, and Startup/Shutdown of Ipswitch Failover.

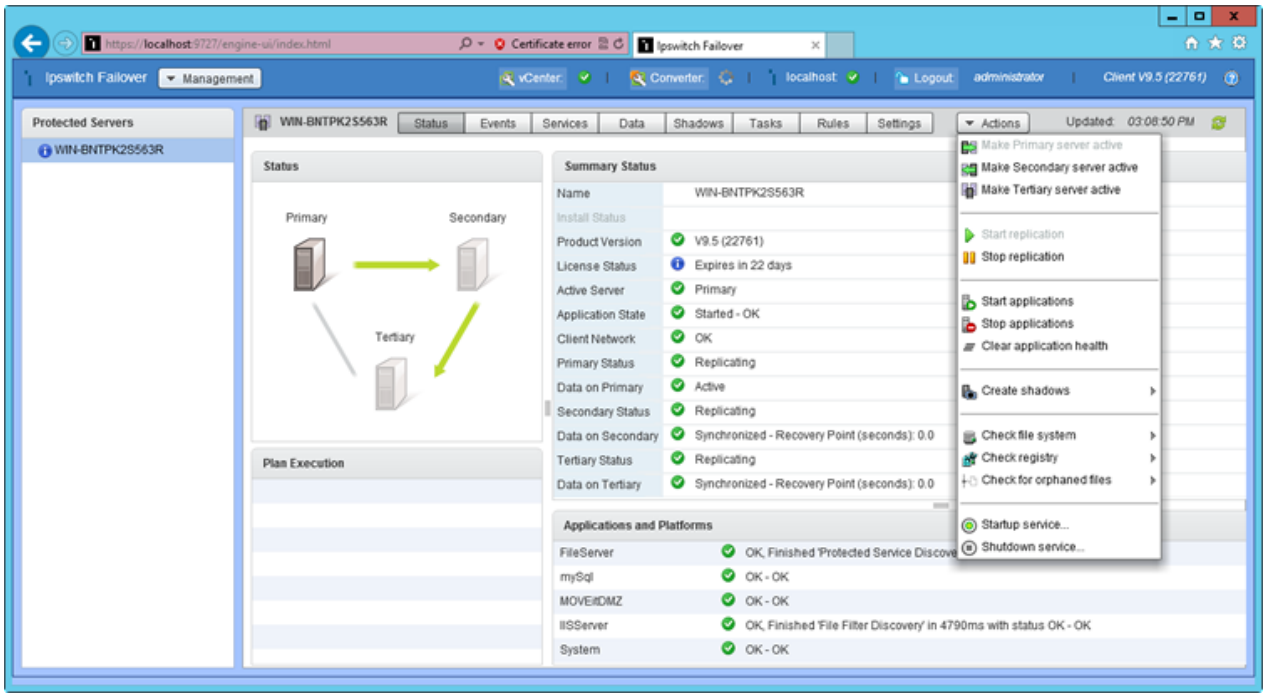

Figure 83: Actions drop-down pane

Perform a Switchover

- To make the Primary server of the Ipswitch cluster active, click the **Make Primary Server Active** button. The **Make Primary Server Active** dialog asks you to verify that you want to make the Primary server active. Click **OK** to make the Primary Server Active.
- To make the Secondary server of the Ipswitch cluster active, click the **Make Secondary Server Active** button. The **Make Secondary Server Active** dialog asks you to verify that you want to make the Secondary server active. Click **OK** to make the Secondary Server Active.
- To make the Tertiary server of the Ipswitch cluster active, click the **Make Tertiary Server Active** button. The **Make Tertiary Server Active** dialog asks you to verify that you want to make the Tertiary server active. Click **OK** to make the Tertiary Server Active.

Start Replication

When replication is stopped, click the **Start Replication** to initiate replication between the servers. Ipswitch Failover responds by starting replication between the configured servers.

Stop Replication

To stop replication, click the **Stop Replication** button. The **Stop Replication** dialog asks you to verify that you want to stop replication. Click **OK** to stop replication.

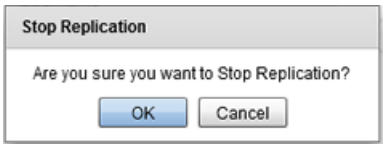

Figure 84: Stop Replication

Start Applications

When protected applications are stopped, click the **Start Applications** to start the protected applications once again.

Stop Applications

To stop protected applications, click the **Stop Applications** button. The **Stop Applications** dialog asks you to verify that you want to stop protected applications. Click **OK** to stop replication.

Clear Application Health

To reset the health status displayed in the *Summary* pane, click the **Clear Application Health** button.

The health status is reset to green.

Create Shadows

To manually create a shadow copy on a designated node, navigate to **Actions** > **Create Shadows** and then select the designated node, **Create (Primary)**, **Create (Secondary)** or if present, **Create (Tertiary)**.

Check File System, Registry System, or Check for Orphaned Files

To manually check the files system, registry, or for orphaned files, navigate to **Actions** drop-down menu and select the system to check and then select the designated node, for example **Check Primary file system**, **Check Secondary file system** or if present, **Check Tertiary file system**.

Startup Service

Ipswitch Failover can be started by logging on to the Ipswitch Failover Management Service and selecting **Startup Service** from the **Actions** drop-down menu. The **Startup Options** dialog is displayed. Select one or more servers in the Ipswitch cluster to start. Click **OK** to start Ipswitch Failover on the selected servers in the cluster.

Figure 85: Startup Services

Shutdown Service

To shutdown Ipswitch Failover, click **Shutdown Service** from the **Actions** button. The **Shutdown Options** dialog is displayed. Select one or more servers in the Ipswitch cluster to shutdown. Click **OK** to stop Ipswitch Failover on the selected servers in the cluster.

Figure 86: Shutdown

Managing Ipswitch Failover Clusters

Ipswitch Failover operates in Clusters of two or three servers with each Cluster administered as a single entity using the Failover Management Service or Ipswitch Advanced Management Client. The Ipswitch Advanced Management Client, which can be run from any server in the Cluster or remotely from another machine in the same subnet, simplifies routine administration tasks for one or more Clusters.

Note: *The controlling workstation must have Failover Management Service or Ipswitch Advanced Management Client. The Advanced Client can be downloaded from Failover Management Service UI.*

Review the Status of Ipswitch Failover Clusters and Groups

Procedure

- Click on the top level of the Ipswitch Advanced Management Client *Groups*, to view a list of all managed Clusters and a quick status of the protected applications, network, file system, and registry settings for each Cluster. In the example below, two Clusters are identified and both are operating as expected.

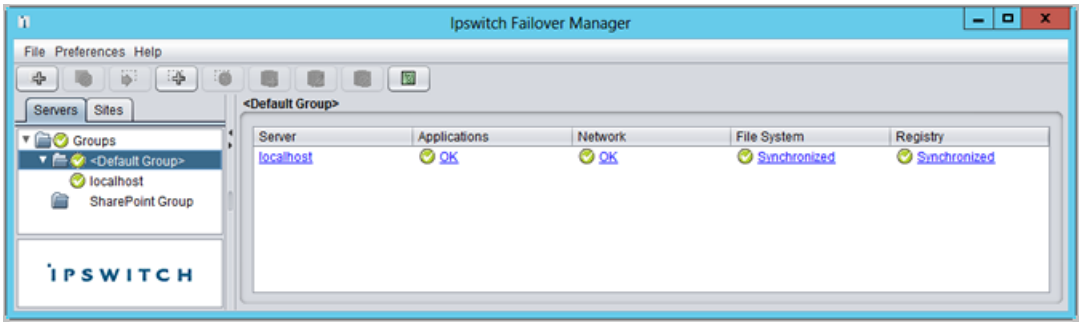

Figure 87: Ipswitch Failover Servers Overview page

The status hyperlinks in the overview page link to pages that provide more specific, related information and management controls.

- Click:

Option	*Description*
Server	To view the **Server: Summary** page
Applications	To view the applications status on the **Applications: Summary** page
Network	To view the network status on the **Network Monitoring** page
File System	To view the File System status on the **Data: Replication** page
Registry	To view the Registry status on the **Data: Replication** page

Exit Ipswitch Advanced Management Client

Procedure

1. Click **Exit** on the **File** menu.
   The **Confirm Exit** message appears.
2. Click **Yes** to close the Ipswitch Advanced Management Client window or **No** to dismiss the message without exiting the Ipswitch Advanced Management Client.

Shutdown Windows with Ipswitch Failover Installed

Procedure

- Always stop Ipswitch Failover before attempting to shut down Microsoft Windows. If an attempt is made to shut down Windows without stopping Ipswitch Failover, Ipswitch Failover will not stop in a graceful manner.

Controlled Shutdown

A Controlled Shutdown is a process where the Ipswitch Failover service is able to delay a system shutdown for a sufficient period to perform all of the necessary steps required to stop the applications and replication in a synchronized state. The Controlled Shutdown is intended for situations where an unattended planned shutdown of the server is necessary. When configured in the Ipswitch Advanced Management Client **Data: Replication** page, this feature allows Ipswitch Failover to gracefully shutdown in the absence of the administrator.

Procedure

1. Navigate to the **Data: Replication** page of the Ipswitch Advanced Management Client.
2. Click the **Configure** button.
3. Select the *Controlled Shutdown* tab of the **Replication Configuration** dialog.
4. Select the servers on which to enable Controlled Shutdown.
5. Select the days and hours parameters under which the server(s) will perform Controlled Shutdown.
6. Configure the length of time for the server(s) to wait for the Controlled Shutdown.

> ***Note:*** *The ability to configure the length of time for the server(s) to wait for the Controlled Shutdown is configurable on Windows Server 2008 and 2012 but is not configurable on Windows Server 2003.*

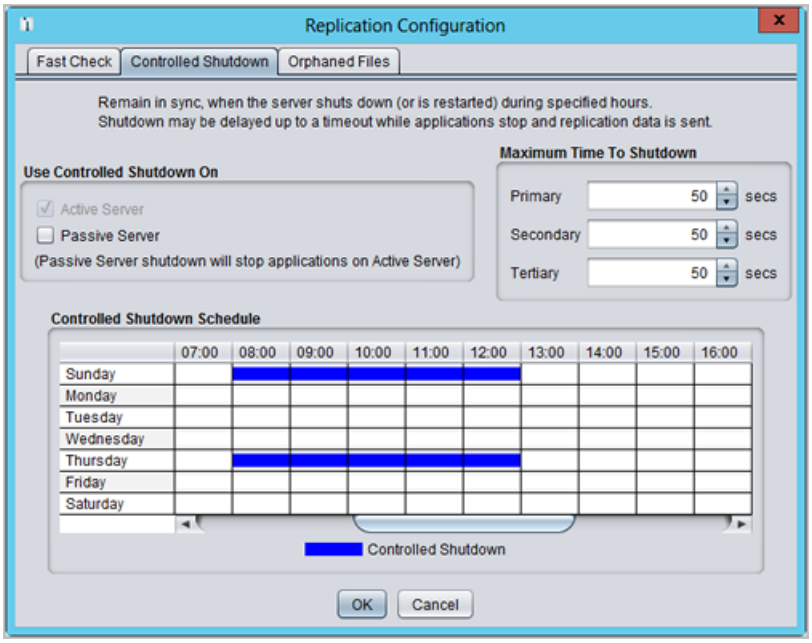

Figure 88: Controlled Shutdown

7. click **OK**.

> ***Note:*** *When the Fast Check process is enabled in addition to the Controlled Shutdown process, Ipswitch Failover can be scheduled to perform unattended restarts of the system while maintaining synchronization of data. For more information about Fast Check, see Configure Fast Check.*

Chapter 3

Configuring Ipswitch Failover

Configure Server Wizard

The Ipswitch Failover - **Server Configuration Wizard** (**Configure Server Wizard**) helps you set up and maintain communications between Ipswitch Failover servers. Configuration information includes the IP address for the Ipswitch Channel(s) and Public addresses on all servers in the Pair. The identity of a server (Primary and Secondary) describes the physical hardware of the machine and should not be confused with what the server is doing (the role).

Prerequisites

Prior to making changes using the Ipswitch Failover **Configure Server Wizard**, you must stop Ipswitch Failover.

Procedure

- Once Ipswitch Failover is stopped, navigate to **Start** > **All Programs** > **Ipswitch Failover** > **Configure Server Wizard** to launch the *Configure Server Wizard*.

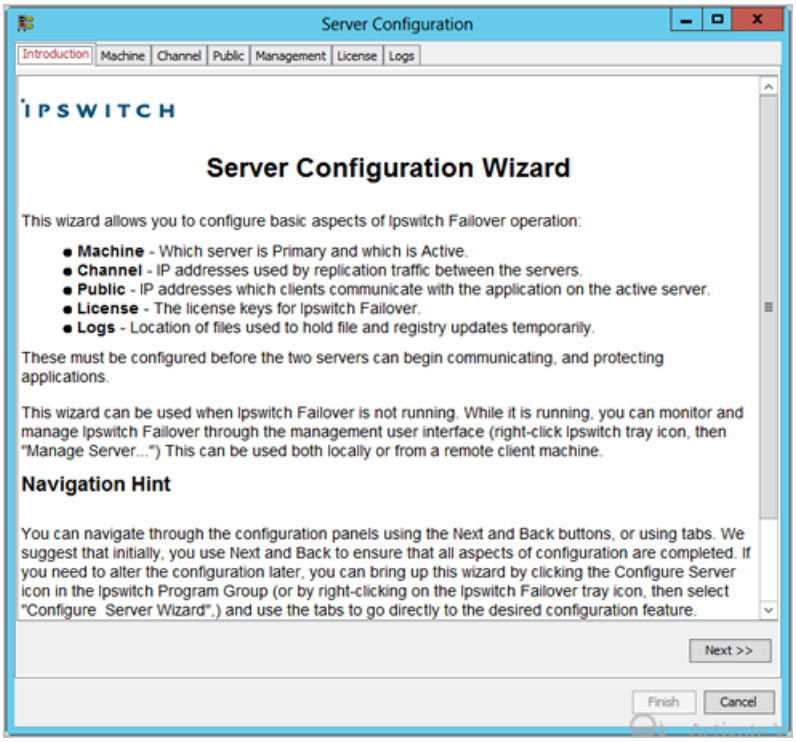

Figure 89: Configure Server Wizard - Introduction Tab

Configure Machine Identity

The identity of a server (Primary and Secondary) describes the physical hardware of the machine and should not be confused with what the server is doing (the role).

Prerequisites

Prior to making changes using the **Configure Server Wizard**, you must stop Ipswitch Failover.

Procedure

- To change the machine *Identity*, select the **Machine** tab of the **Configure Server Wizard** and select the *Physical Hardware Identity* of the local machine and click **Next** or **Finish.**

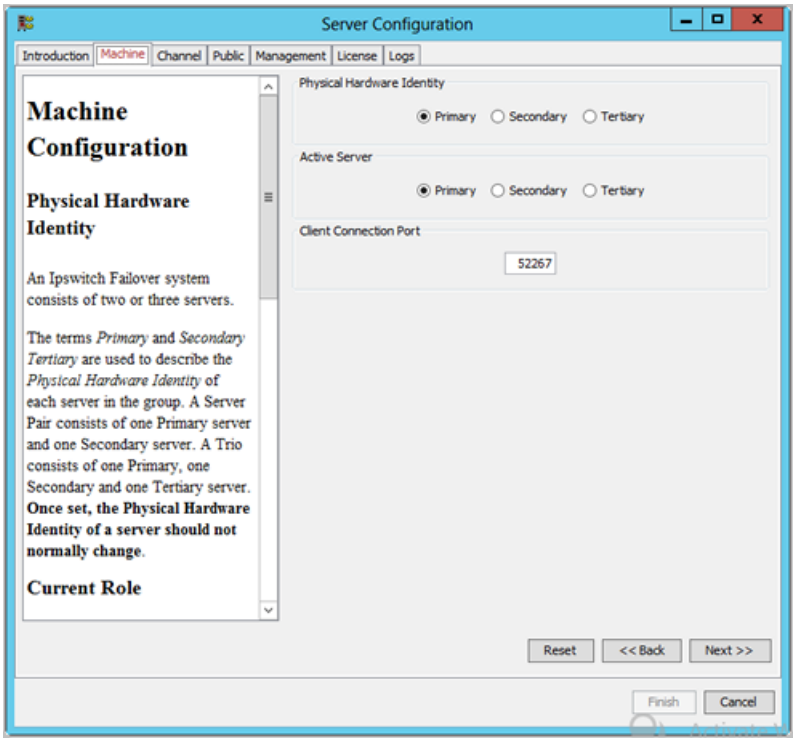

Figure 90: Configure Server Wizard - Machine Tab

Configure Server Role

The server's role describes what the server is currently doing.

Prerequisites

Before changing the *Role* of the local server to active, verify that no other server (including remote servers) in the Cluster is active.

Procedure

- To change the *Role* of the server, select the **Machine** tab of the **Configure Server Wizard** and specify which server in the Cluster is active. Click **Next** or **Finish**.

Change the Client Connection Port

The *Client Connection Port* specifies the port through which clients (such as the Failover Management Service) connect to Ipswitch Failover.

Procedure

- To change the *Client Connection Port*, select the **Machine** tab of the **Configure Server Wizard** and type a new value in the text box. Click **Next** or **Finish** to accept changes.

> ***Note:*** *Do not change this port unless the default port (52267) is required by another application.*

Configure Channel IP Routing

Channel IP routing defines the IP addresses used to communicate between the local server (such as the Primary) and the adjacent servers (such as the Secondary). Each link uses two addresses, one for the local server and one for the remote server.

Procedure

- To add a channel after installing and configuring the NICs, select the **Channel** tab of the **Configure Server Wizard**. Add the new IP addresses for the local server and the remote server to the *Ipswitch Channel IP Routing* table by clicking the **Add Row** icon. The drop-down list shows the IP addresses available on the local server. Manual entry of the IP addresses for remote servers is required

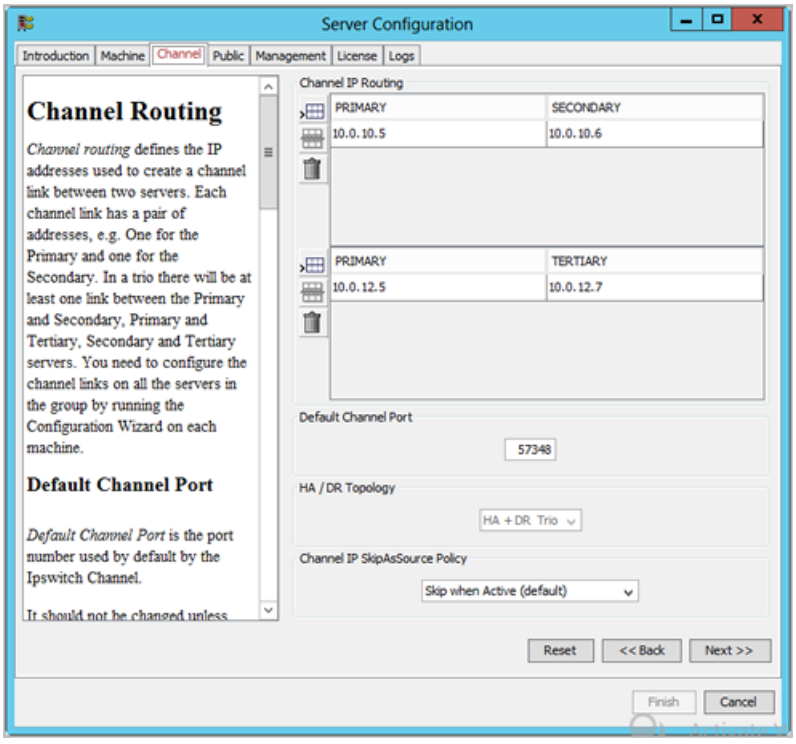

Figure 91: Configure Server Wizard - Channel IP Routing

- Additionally, you can specify a SkipAsSource policy for channel addresses to ensure that they are not used for public traffic. SkipAsSource prevents an IP address from being selected by the operating system as a source IP address for out-going network connections.

- Never Skip – channel IP addresses will never have SkipAsSource set.
- Always Skip – channel IP addresses will always have SkipAsSource set.
- Skip when Active – channel IP addresses will have SkipAsSource set when the server is active but not when passive.
- Skip when Active and Public Subnet – channel IP addresses will have SkipAsSource set if the server is active and the channel IP address is in the same subnet as a public IP address. When the server is passive the SkipAsSource setting is removed from the channel IP addresses.

- To change the channel IP addresses, select and edit the entry in the table. Click **Next** or **Finish** to accept changes.

Configure the Default Channel Port

The Ipswitch Channel uses the *Default Channel Port* to communicate between the Primary and Secondary servers. Do not change this port unless required by another application.

Procedure

- To change the *Default Channel Port*, select the **Channel** tab of the **Configure Server Wizard** and edit the default entry (57348). Click **Next** or **Finish** to accept changes.

Configure Low Bandwidth Optimization

Low Bandwidth Optimization is configured automatically during installation based upon the configuration options selected during Installation. Low Bandwidth Optimization can be configured for: High Availability (HA) when deployed as a pair in a LAN or DR when deployed in a WAN.

In a High Availability (HA) server pair, the queues and buffers are optimized for a high-speed local area network (LAN) connection, compression is disabled, and automatic failover between servers is enabled. In a Disaster Recovery(DR) pair, the queues and buffers are optimized for a low-bandwidth wide area network (WAN) connection, compression may be used, and automatic failover between servers is disabled. In a server pair you can choose HA or DR topology. However, if you have manually configured a non-standard topology, for example, by changing the Auto-Failover setting, then "Non-Standard" will appear in the menu and you can choose to leave the non-standard topology option as it is, or reset it to one of the standard topologies.

Note: *The same HA/DR configuration must be set on all servers in the pair.*

- To change Low Bandwidth Optimization after installation, select the **Channel** tab of the **Configure Server Wizard** and use the *HA/DR Topology* drop-down menu to select the appropriate topology. Click **Next** or **Finish** to accept changes.

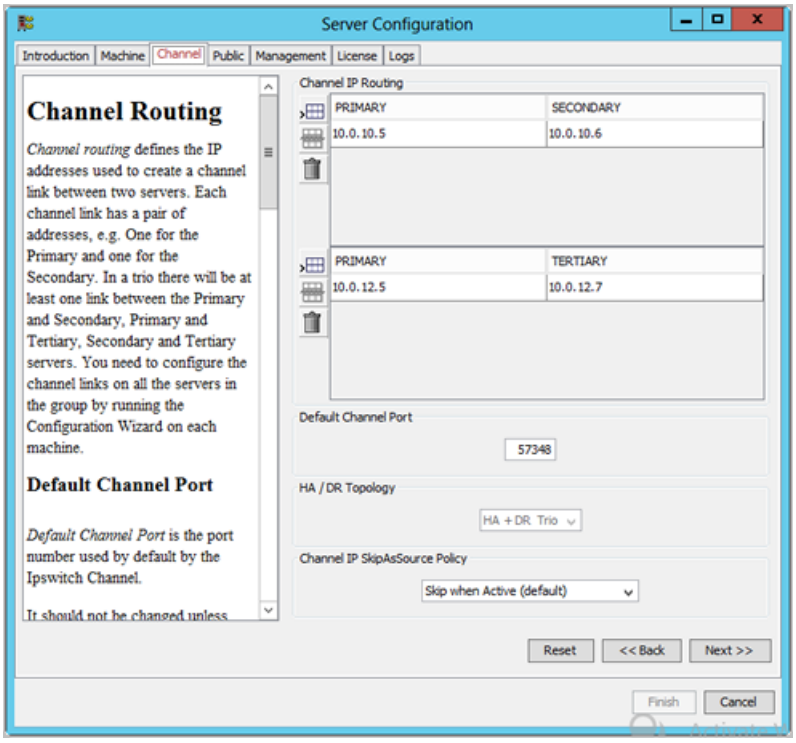

Figure 92: Configure Server Wizard - Channel tab

Configure Public IP Addressing

A typically configured Ipswitch Failover Cluster uses only one Public IP address when deployed as a pair or on a LAN, but can be configured with more than one Public IP address. These are the addresses by which clients of the protected application connect to the application. Typical installations configure the same Public IP address on the Primary and Secondary servers. All traffic to and from these Public IP addresses is passed through to the active server but blocked on the passive server(s). When the server roles are switched, the IP filtering mode also switches, so client systems always connect to the Public IP addresses on whichever server is currently active. When the Ipswitch Failover service is shut down, the filtering remains in place to prevent IP address conflicts between servers.

Procedure

1. To configure Public IP addressing, select the **Public** tab of the **Configure Server Wizard** and list all of the addresses intended for use as Public IP addresses.

   Note: *An address must not appear more than once, and no Public IP address may appear in the list of IP addresses on the Channel tab.*

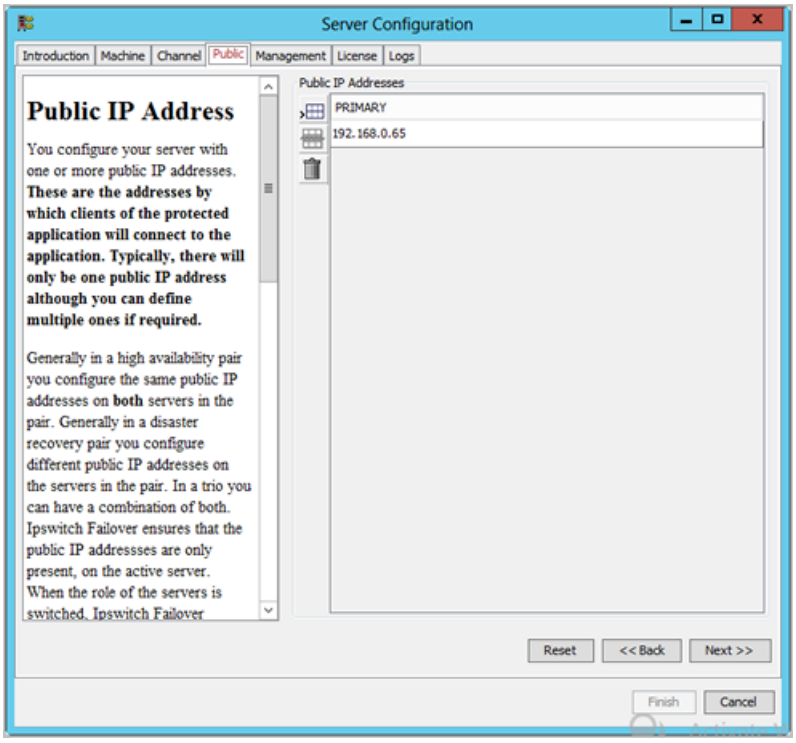

Figure 93: Configure Server Wizard - Public Tab

2. To add an address, double-click a row and manually type in the address or select one from a list of currently defined addresses. Click **Next** or **Finish** to accept changes.

Management IP Addressing

Management IP addresses are additional IP addresses that you manually configure on a server; they are IP addresses that are neither public or channel IP addresses. Management IP addresses are typically used to access a server for management purposes and can be used to access a server when it is passive. Management IP addresses are displayed here so that you can see the management IP addresses on your local server.

Additionally, you can specify a SkipAsSource policy for Management IP addresses to ensure that they are not used for public traffic. SkipAsSource prevents an IP address from being selected by the operating system as a source IP address for out-going network connections.

The following options are available:

- Never Skip – channel IP addresses will never have SkipAsSource set.
- Always Skip – channel IP addresses will always have SkipAsSource set.
- Skip when Active – channel IP addresses will have SkipAsSource set when the server is active but not when passive.
- Skip when Active and Public Subnet – channel IP addresses will have SkipAsSource set if the server is active and the channel IP address is in the same subnet as a public IP address. When the server is passive the SkipAsSource setting is removed from the channel IP addresses.

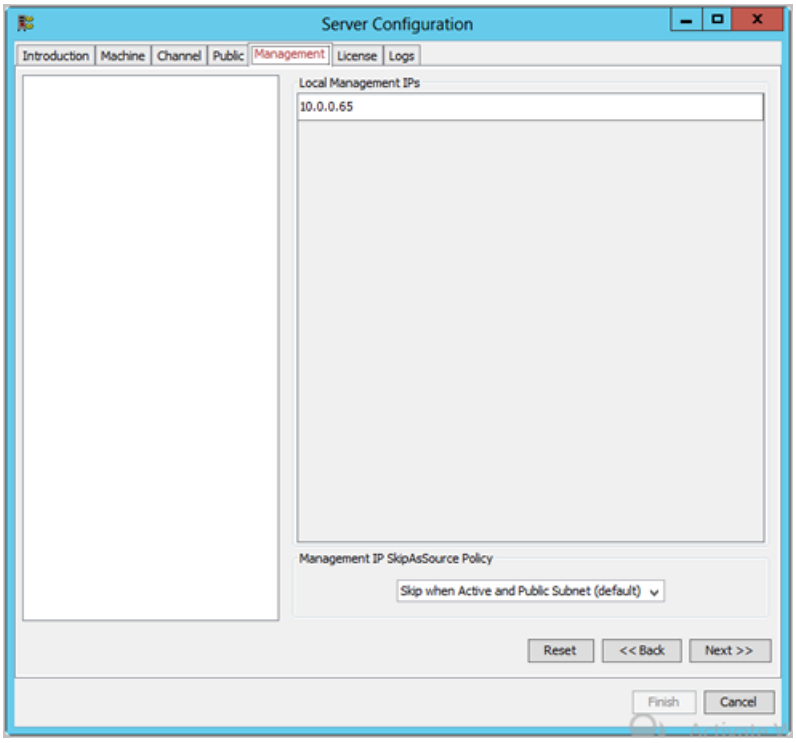

Figure 94: Configure Server Wizard Management IP Addresses

Add/Remove an Ipswitch Failover License Key

Ipswitch recommends using the Failover Management Service user interface for licensing Ipswitch Failover (see the Installation Guide).

Procedure

If requested by Ipswitch Support, you can also use the Configure Server Wizard as follows:

1. To manage Ipswitch Failover License Keys, select the **License** tab of the **Configure Server Wizard**.
2. To add an entry to the *License Keys* table, manually type or paste (using **Ctrl+V**) your license key into the table. Alternatively, click **Import** on the tool bar to import a license file (`.txt`). License keys are available from Ipswitch or your distributor.

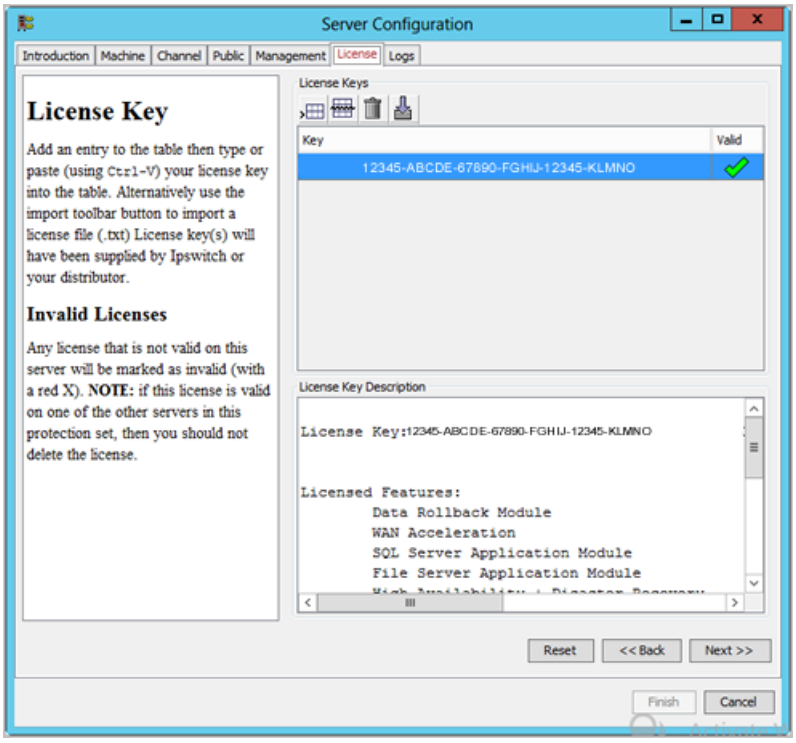

Figure 95: Configure Server Wizard - License Tab

3. After entering your license keys click **Next** or **Finish**.

Configure the Message Queue Logs

The configured message queue logs location determines where the local server temporarily stores replication data received (the receive queue) and the replication data waiting to send (the send queue). This configuration affects only the local server; logs can be in different locations on the Primary and Secondary servers.

Procedure

- To configure the location of the message queue logs, select the **Logs** tab of the **Configure Server Wizard**. Click **Browse** to open an Explorer-like window. Navigate to and select the folder for storing the message queue logs, and click **Finish** to accept the location.

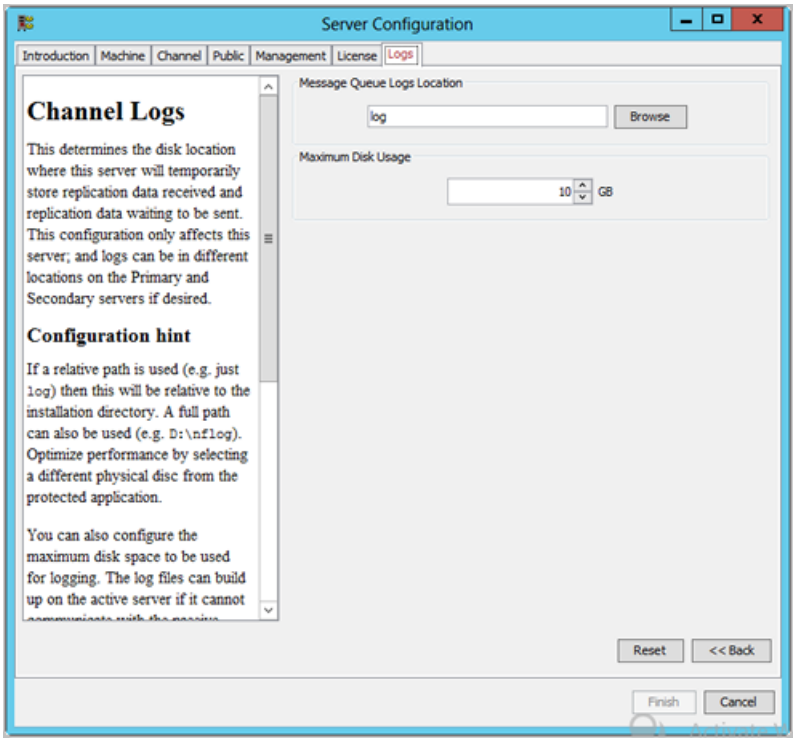

Figure 96: Configure Server Wizard - Logs Tab

Configure Maximum Disk Usage

You can configure the maximum disk space allocated for logging. Log files accumulate when the active server cannot communicate with the passive server, when a passive server is performing certain operations, or when a server is under heavy load. Configuring this value is important because when the value set for maximum disk usage is reached, replication stops, and your system is no longer protected. If your system uses a dedicated disk for log files, consider disabling the maximum disk usage setting.

Procedure

- If your system uses a dedicated disk for log files, consider disabling the maximum disk usage setting. To do this, set *Maximum Disk Usage* to zero (0).

  Note: *When Maximum Disk Usage is disabled, there is a risk that Ipswitch Failover may run out of physical disk space, and when this happens, a shutdown and restart may be required before replication can resume.*

- Ipswitch recommends a *Maximum Disk Usage* setting that leaves a little overflow space to enable Ipswitch Failover to stop replicating gracefully. To configure *Maximum Disk Usage*, select the **Logs** tab of the **Configure Server Wizard** and enter the maximum dedicated disk space allocated for message queue log files and click **Finish** to accept the changes.

Management

Chapter 4

Server Protection

Overview

Protection against operating system or hardware failure affecting the active server is facilitated by multiple instances of Ipswitch Failover that monitor one another by sending “I am alive” messages and reciprocating with acknowledgments over the Ipswitch Channel. If a passive server detects that this process (heartbeat) has failed, an automatic-failover is initiated.

Monitoring the Status of Servers

The Ipswitch Advanced Management Client **Server: Monitoring** page provides information about the status of communications between the servers within the Cluster. The graphical representation provides an overview of the status of communications between the servers. A green channel icon indicates that the channel is connected and healthy, a red-dashed channel icon indicates that communications are not operational between the indicated servers, and an orange icon with an exclamation mark on it indicates that the channel has just disconnected and Ipswitch Failover will wait for the configured amount of time before determining that the channel is disconnected. In addition to the heartbeat sent between the servers, Ipswitch Failover also sends a ping to ensure that the servers remain visible to one another.

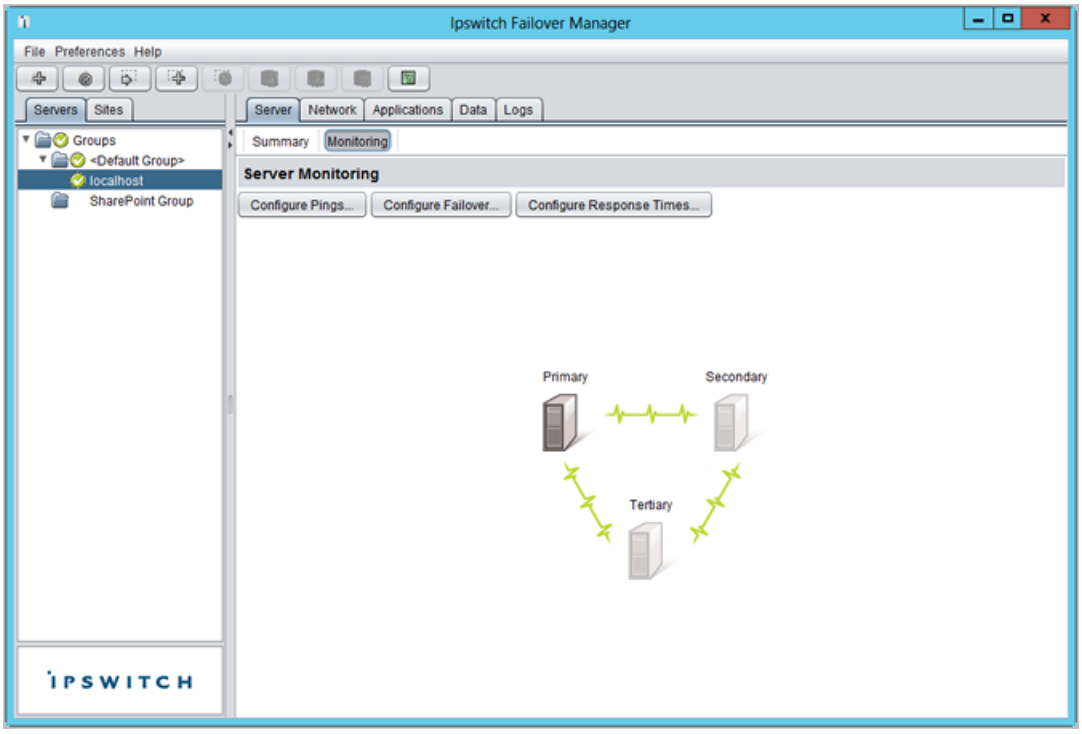

Figure 97: Server Monitoring page

Configure Ipswitch Failover Settings

The **Server Monitoring** page provides three configuration features: *Configure Pings*, *Configure Failover*, and *Configure Response Times*.

Configure Pings

The **Server Monitoring Ping Configuration** dialog allows you to configure the *Ping Interval* and the *Ping Echo Timeout* used to conduct ping operations between servers. Additionally, ping routing can be configured to add additional ping targets by selecting the *Ping Routing* tab of the dialog. The IP addresses of all NICs used for the Ipswitch Channel were identified during installation and do not need to be added. You can add additional targets to the list for each server's channel connection in the event of redundant NICs. The settings in the **Server Monitoring Ping Configuration** dialog allow Ipswitch Failover to send pings across the Ipswitch Channel and the Public Network in addition to the heartbeat ("I am alive" messages) to confirm that the server is still operational and providing service.

Procedure

- Click **Configure Pings** to open the **Server Monitoring Ping Configuration** dialog.

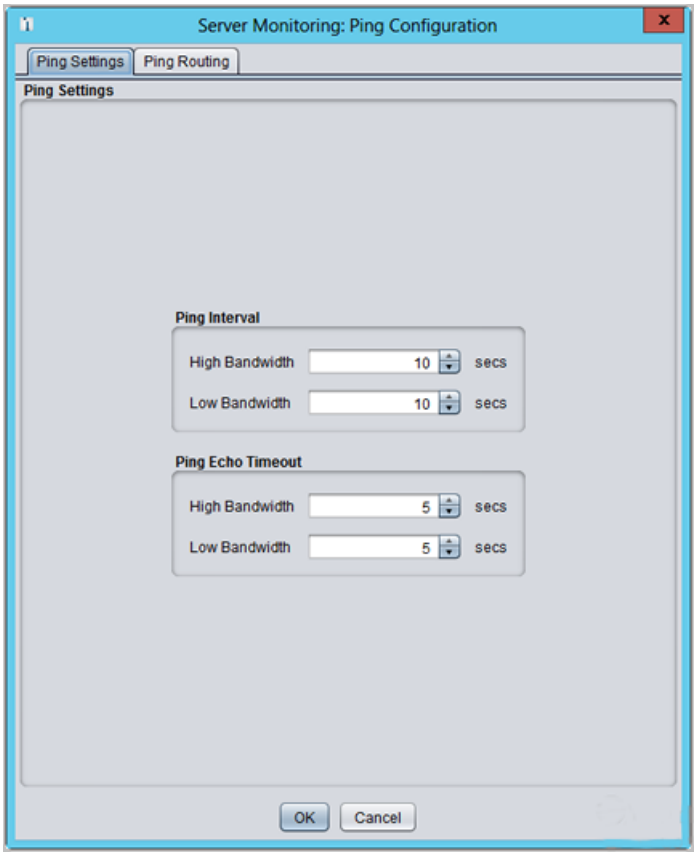

Figure 98: Server Monitoring: Ping Configuration: Ping Settings Tab

- Select the *Ping Routing* tab and enter the auxiliary IP addresses of the appropriate servers.

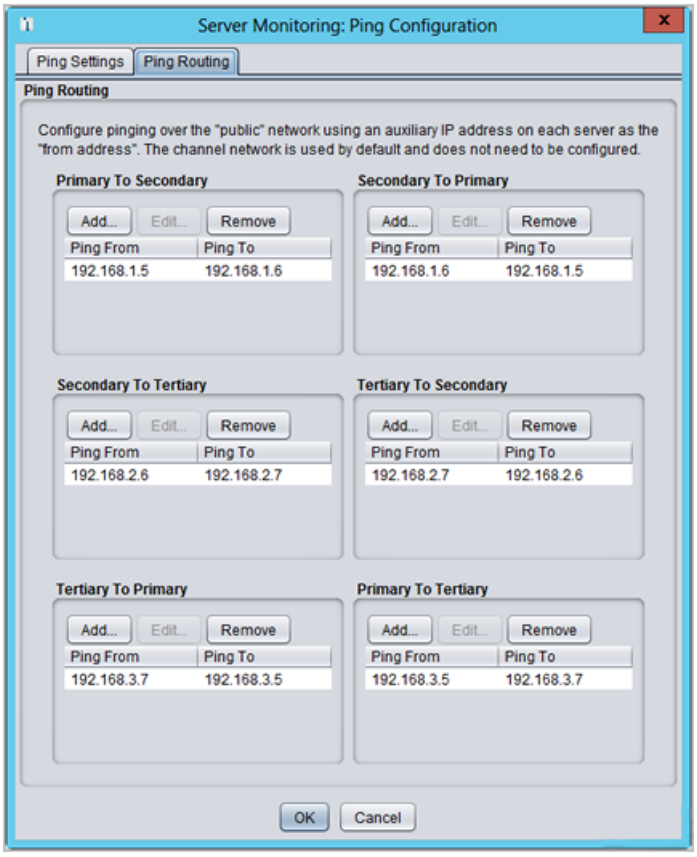

Figure 99: Server Monitoring: Ping Configuration: Ping Routing Tab

Configure Failover

The Failover timeout dictates how long Ipswitch Failover waits for a missed heartbeat before it takes a pre-configured action. This value is set to 60 seconds by default.

Procedure

1. To configure the *Failover timeout*, click **Configure Failover** to open the **Server Monitoring: Failover Configuration** dialog.

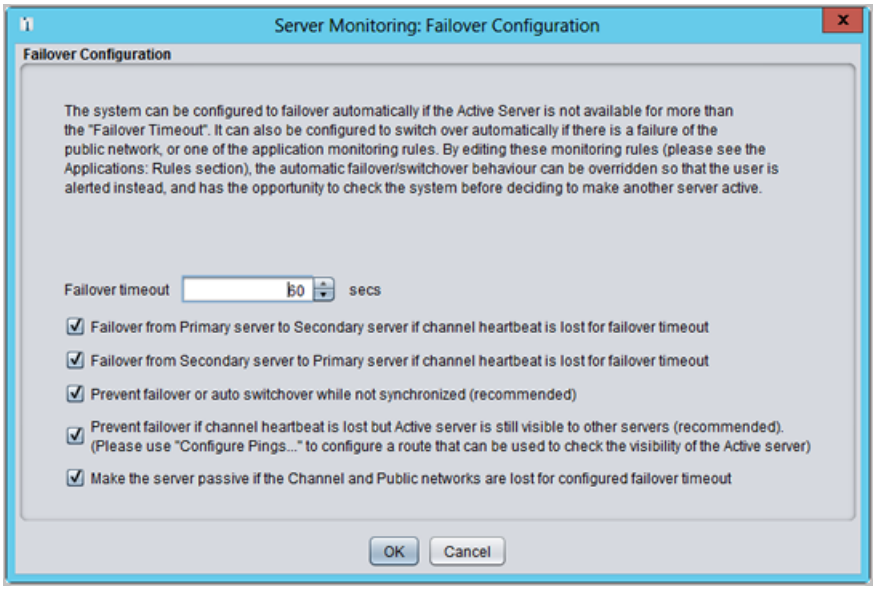

Figure 100: Server Monitoring: Failover Configuration

2. Type a new numeric value (seconds) in the *Failover timeout* text box or use the arrow buttons to set a new value.
3. Select or clear the check boxes to select the actions to take if the specified *Failover timeout* is exceeded.

> ***Note:*** *For more information about configuring options for failover, see Split-brain Avoidance.*

4. Click **OK** to accept the changes or **Cancel** to dismiss the dialog without making any changes.

> ***Note:*** *The default configuration for a WAN installation is with the automatic switchover (spontaneous failover) DISABLED. To enable Auto-switchover in a WAN pair, select* ***Network*** *>* ***Configure Auto-Switchover****, select the check box and set the missed ping failover count.*

Configure Response Times

Ipswitch Failover also allows you to configure channel connection timeouts.

Procedure

1. Click **Configure Response Times** to open the **Server Monitoring: Response Times** dialog. The following options are available:
   - Time to wait following channel connection before starting replication
   - Time to wait following channel disconnection before stopping replication

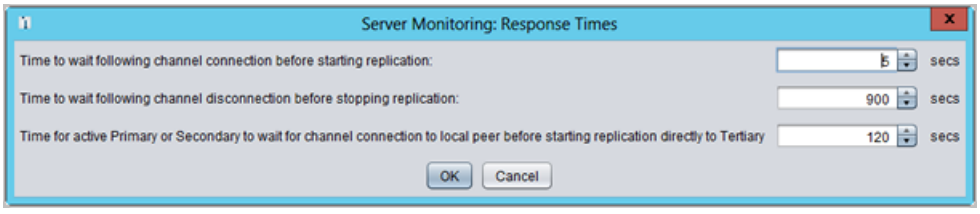

Figure 101: Server Monitoring: Response Times

2. Type new numeric values (second) into the text boxes or use the arrow buttons to select new values.
3. Click **OK** to accept the changes or **Cancel** to dismiss the dialog without making any changes.

Common Administrative Tasks in Ipswitch Failover

The **Server Summary** page provides the following buttons that allow you to quickly perform common administrative tasks:

- **Configure** — Click to open the **Configure** dialog.

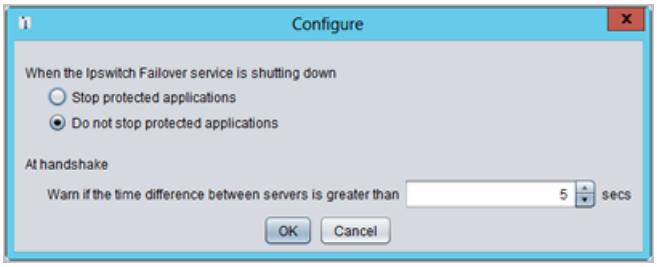

Figure 102: Configure (Shutdown)

Select the radio button corresponding to whether you want to stop or leave running the protected applications when Ipswitch Failover is shut down. You can select whether to leave protected applications running upon shutdown when a net stop command is issued, and to start protected applications upon startup when a net start command is issued. Type a number (seconds) or use the arrow buttons to select an alert threshold value for time difference between servers, which is checked at handshake following startup. Click **OK** to accept the changes or **Cancel** to dismiss the dialog without making any changes.

Forcing a Switchover

After Ipswitch Failover is configured to protect all required applications and data, it allows the Secondary to take over from the Primary server in a managed and seamless way called a managed switchover.

This is particularly useful when maintenance work performed on the Primary server requires rebooting the server.

Prior to performing work on the Primary server, a managed switchover can be triggered by selecting the server to make active and then clicking **Make Active** in the **Server: Summary** page. This changes the server roles such that the active server becomes passive and the selected server becomes active. This action also changes the replication chain depending on which server becomes active. This means users are able to work continuously while the Primary server is off line.

When the Primary server is back up and running, the managed switchover can be triggered again so that the Primary server becomes active and the previously active server becomes passive.

Important: *The managed switchover process may be performed at any time as long as the systems are fully synchronized with respect to data files and registry replication. Switchovers cannot be performed if either server is in an unsynchronized or unknown state.*

Since a managed switchover cannot be performed during synchronization, it is important to review the queue information prior to attempting a managed switchover. If the queues are large, file operations on the active server are high and for this reason it may be prudent to delay a managed switchover due to the length of time required to completely clear the queue. Queue lengths can be viewed in the **Data: Traffic/Queues** page of the Ipswitch Advanced Management Client.

Failover versus Switchover

Do not confuse a failover with a switchover.

A switchover is a controlled switch (initiated from the Failover Management Service, Ipswitch Advanced Management Client, or automatically by Ipswitch Failover when pre-configured) between the active and passive servers. A failover may happen when any of the following fail on the active server: power, hardware, or Channel communications. The passive server waits a pre-configured period of time after the first missed heartbeat before initiating a failover. When this period expires, the passive server automatically assumes the active role and starts the protected applications.

Configuring Failover and Active Server Isolation

Ipswitch Failover continuously monitors the servers in the Cluster and the network to ensure availability and uses native logic and a combination of elapsed time, administrator configured rules, current server network status, and configured ping routing to determine if failover or isolation of the active server is warranted should the servers experience missed heartbeats.

Procedure

To configure failover:

Note: *For information on configuring ping routing, see Configure Pings and Configure Public Network Monitoring.*

1. Navigate to **Server: Monitoring** > **Configure Failover** to open the **Server Monitoring: Failover Configuration** dialog.
2. The *Failover timeout* can be customized by changing the default value (60 seconds) to a custom value. Type a new numeric value (seconds) in the *Failover timeout* text box or use the arrow buttons to configure how long Ipswitch Failover waits for a missed heartbeat before it takes a pre-configured action to failover or isolate the active server from the network.
3. Select or clear check boxes for the items listed below to select the actions to take if the specified *Failover timeout* is exceeded.
   When the configured *Failover timeout* value has elapsed, Ipswitch Failover will evaluate, in order, the following pre-configured rules before taking action:

   Note: *If a rule is not selected, Ipswitch Failover will skip the rule and move to the next rule in the list. After all selected rules have been evaluated Ipswitch Failover will take action.*

   - Failover from Primary server to Secondary server if channel heartbeat is lost for failover timeout
   - Failover from Secondary server to Primary server if channel heartbeat is lost for failover timeout
   - Prevent failover or auto switchover while not synchronized
   - Prevent Failover if channel heartbeat is lost but Active server is still visible to other servers
   - Make the server passive if the Channel and Public networks are lost for the configured failover timeout

   Note: *You must configure Management IP addresses on the Public network cards of each server to allow the passive server to send a ping via the Public network. Management IP addresses are additional IP addresses assigned to the network card connected to the Public network. They are used to allow the passive server to communicate, because unlike the Public IP address, they are not filtered. For information about how to configure Management IP addresses, see Configuring Management IP Addressing.*

4. Click **OK**.

Important: *If either Server: Monitoring Ping Routing or Network Monitoring Ping Routing is misconfigured, unpredictable behavior can occur.*

Typical Failover and Active Server Isolation Scenarios

The following scenarios assume that Ipswitch Failover is deployed in a LAN with all rules selected in the **Server: Monitoring** > **Configure Failover** > **Failover Configuration dialog**.

Failover

The following scenario assumes the active server has failed and is no longer available.

Upon detection of missed heartbeats, Ipswitch Failover on the passive server performs the following steps:

1. As soon as the passive server detects that the Ipswitch Channel is experiencing missed heartbeats, it will determine it itself is a valid failover target to the currently active server.
2. As soon as the passive server detects that the Ipswitch Channel is experiencing missed heartbeats. It will attempt to ping the active server's Management IP address via the Public network using the passive server's NIC configured with the Management IP address. If the ping is successful, the passive server will veto the failover. If the ping is unsuccessful, it will continue to the next step.

Note: *Since the passive server assumes that active server has failed, the passive server will not attempt to verify synchronization with the active server.*

3. At this point, the passive server checks the configured value of the *Failover timeout* and starts a "Heartbeat lost" countdown The passive server continues with the next step.
4. At this point, failover to the passive server is postponed until the value of the *Failover timeout* has elapsed.
5. The passive server changes its role to active, removes the packet filter, and starts all services.
6. As the new active server, it will begin accepting traffic from clients.

Active Server Isolation

The figure below illustrates a scenario where the active server has lost connection with the passive server via the Ipswitch Channel.

Figure 103: Network Isolation Workflow Diagram

Upon detection of missed heartbeats Ipswitch Failover performs the following steps:

1. As soon as the active server detects that the Ipswitch Channel is experiencing missed heartbeats, it will determine *if a valid failover target (the passive server) is present*.

   Simultaneously, once the passive server detects missed heartbeats, it will determine *if it is a valid failover target*.

2. Next, the active server will determine if it is synchronized with the failover target (the passive server). If synchronized, it will continue to the next step. If it is not synchronized, it will veto a failover.

   Simultaneously, the passive server checks to see if it is synchronized with the active server. If synchronized, it will continue to the next step. If it is not synchronized, it will veto a failover.

3. At this point, both the active and passive servers check the configured value of the *Failover timeout* and start a "Heartbeat lost" countdown. Both servers should start the countdown at approximately the same time.
4. Failover or isolation of the active server is postponed until the configured *Failover timeout* value (in seconds) has elapsed and it is during this period that both servers accomplish steps 1 & 2.
5. Once the configured *Failover timeout* period has elapsed, the active server assumes the Ipswitch Channel is lost and will attempt to ping the failover target (passive server) via the Public network. If the ping is successful,

active server isolation is vetoed. If the attempt to ping the failover target is unsuccessful, the active server will proceed to the next step.

Simultaneously, the passive server assumes the Ipswitch Channel is lost and attempts to ping the active server via the Public network. If the ping is successful, failover is vetoed. If the ping attempt is unsuccessful, the passive server proceeds to the next step.

Note: *If the servers have reached this point, then neither server can see the other server.*

6. The active server checks only its own network connectivity to the Public network. If the active server has lost connectivity to the Public network, it will isolate itself by making itself passive (potential active).
7. Both the active and passive servers will check their connectivity to the Public network. If the active server has lost connectivity to the Public network, it will isolate itself by making itself passive (potential active). Should the active server reconnect with the passive, it will become active again. Otherwise, it will remain passive. If the passive server has lost connectivity to the Public network, it will veto a failover.

Recover From a Failover

This recovery scenario is based on Ipswitch Failover in a configuration with the Primary server as active and the Secondary server as passive.

Procedure

Note: *When failover conditions, such as a power failure, cause failures in both active and passive servers, a condition may result that causes all servers to restart in Passive mode. In this situation, manual intervention is required. See Two Passive Servers for more information.*

In the following case, a failover occurred and the Secondary server is now running as the active server.

1. Review event logs on all servers to determine the cause of the failover. If you are unsure how to do this, use the *Ipswitch Failover Log Collector* tool to collect information and send the output to Ipswitch Support.
2. If any of the following issues exist on the Primary server, performing a switchover back to the Primary server may not be possible until other important actions are carried out. Do not restart Ipswitch Failover until the following issues are resolved:
   - **Hard Disk Failure** – Replace the disk.
   - **Power Failure** – Restore power to the Primary server.
   - **Virus** – Clean the server of all viruses before starting Ipswitch Failover.
   - **Communications** – Replace or repair the physical network hardware.
   - **Blue Screen** – Determine and resolve the cause of the blue screen. This may require you to submit the Blue Screen dump file to Ipswitch Support for analysis.
3. Run the **Configure Server Wizard** and verify that the server *Identity* is set to *Primary* and its *Role* is *passive*. Click **Finish** to accept the changes.
4. Disconnect the channel network cables or disable the network card.
5. Resolve the problem – list of possible failures, etc.
6. Reboot the server and reconnect or re-enable the network card.
7. After the reboot, verify that the taskbar icon now reflects the changes by showing **P** / **-** (*Primary* and *passive*).
8. On the Secondary active server or from a remote client, launch the Ipswitch Advanced Management Client and confirm that the Secondary server is reporting as *active*. If the Secondary server is not displaying as *active*, follow the steps below:

a) If the Ipswitch Advanced Management Client is unable to connect remotely, try running it locally. If you remain unable to connect locally then verify that the Ipswitch service is running via the Service Control Manager. If it is not, review the event logs to determine a cause.

b) Run the **Configure Server Wizard** and confirm that the server is set to Secondary and is *active*. Click **Finish** to accept the changes.

> ***Note:*** *If Ipswitch Failover is running, you can run the* ***Configure Server Wizard****, but you will not be able to make any changes. You must stop the Ipswitch Failover service before attempting to make changes via the* ***Configure Server Wizard****.*

c) Determine whether the protected application is accessible from clients. If it is, then start Ipswitch Failover on the Secondary server. If the application is not accessible, review the application logs to determine why the application is not running.

> ***Note:*** *At this point, the data on the Secondary (active) server should be the most up to date and this server should also be the live server on your network. After Ipswitch Failover starts, it overwrites all protected data (configured in the File Filter list) on the Primary passive server. Contact Ipswitch Support if you are not sure whether the data on the active server is 100% up to date. Go on to the next step only if you are sure that you want to overwrite the protected data on the passive server.*

9. Start Ipswitch Failover on the Secondary active server and verify that the taskbar icon now reflects the correct status by showing **S**/**A** (Secondary and active).
10. Start Ipswitch Failover on the failed Primary server and allow the system to synchronize. When the re-synchronization is complete, you can continue running with this configuration (for example, the Secondary is the active server and the Primary is the passive server), or initiate a managed switchover.
11. Optionally, perform a managed switchover to return the Primary and Secondary servers to the same roles they had before the failover.

Split-brain Avoidance

Split-brain Avoidance ensures that only one server becomes active if the channel connection is lost, but all servers remain connected to the Public network. Split-brain Avoidance works by pinging from the passive server to the active server across the Public network. If the active server responds, the passive does not failover, even if the channel connection is lost. WAN installations require different IP addresses on the Public network for the local and remote servers.

1. To enable Split-brain Avoidance, open the **Server Monitoring** page in the Ipswitch Advanced Management Client.
2. Click **Configure Failover**
3. Select *Prevent failover if channel heartbeat is lost but Active server is still visible to other servers (recommended)*.
   The active server must respond within the time period value specified in the *Failover timeout* to prevent a failover from occurring. If the active server responds in a timely manner, the failover process ceases. If the active server does not respond, the failover proceeds.

> ***Note:*** *You must configure Management IP addresses on the Public network cards of each server to allow the passive server to send a ping. Management IP addresses are additional IP addresses assigned to the network card connected to the Public network.*

Configuring Management IP Addressing

Management IP addresses are used to allow the passive server to communicate, because unlike the Public IP address, they are not filtered. Management IP addresses are necessary when configuring Network Isolation Protection.

Procedure

To configure a Management IP address on the Public network card, perform the following procedure:

1. Open the network properties for the Public network connection.
2. Double-click **TCP/IP** to display the properties.
3. Click **Advanced**.
4. Enter an additional (currently unused) IP address from a subnet other than the Public or Ipswitch Channel subnet in the IP address table.
5. Reposition the IP addresses in the list so that the additional (Management) IP address appears first, and the Public network address (by which clients connect to the server) appears second.
6. Click **OK** on all three dialogs to accept the configuration changes to the network connection.
7. After completing all of the steps, click **OK**.
8. Launch the Ipswitch Advanced Management Client and select **Server: Monitoring** > **Configure Pings** > **Ping Routing** and add the newly assigned IP addresses to the *Ping Routing* table.

Chapter 5

Network Protection

Overview

Ipswitch Failover proactively monitors the ability of the active server to communicate with the rest of the network by polling defined nodes around the network at regular intervals, including (by default) the default gateway, the primary DNS server, and the Global Catalog server. If all three nodes fail to respond, for example, in the case of a network card failure or a local switch failure, Ipswitch Failover can initiate a switchover, allowing the passive server to assume an identical network identity as the active server.

The Ipswitch Advanced Management Client **Network Monitoring** page allows you to view the status of the network and to make adjustments to the IP addresses used to ping multiple servers within the network.

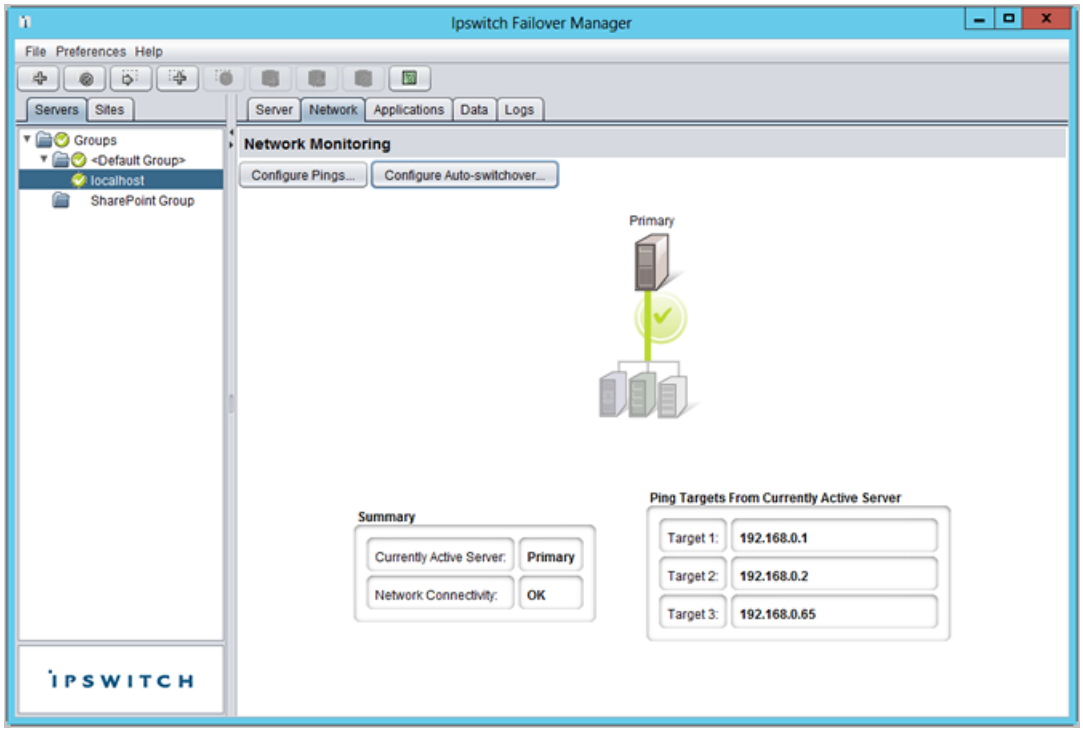

Figure 104: Network Monitoring

Configure Public Network Monitoring

The Public network monitoring feature, previously discussed, is enabled by default during the installation of Ipswitch Failover. This feature integrates the polling of the particular waypoints around the network through the

active server's Public connection to ensure connectivity with the Public network is operational. By default, the IP addresses of the default gateway, the primary DNS server, and the Global Catalog server are all selected. When one or more of the automatically discovered waypoints are co-located on a physical machine (leading to duplication of IP addresses), the ability to specify additional waypoints manually becomes an advantage.

Procedure

To configure Public Network Monitoring:

1. To specify a manual target for the Public network checking, click **Configure Pings** to invoke the **Ping Configuration** dialog.

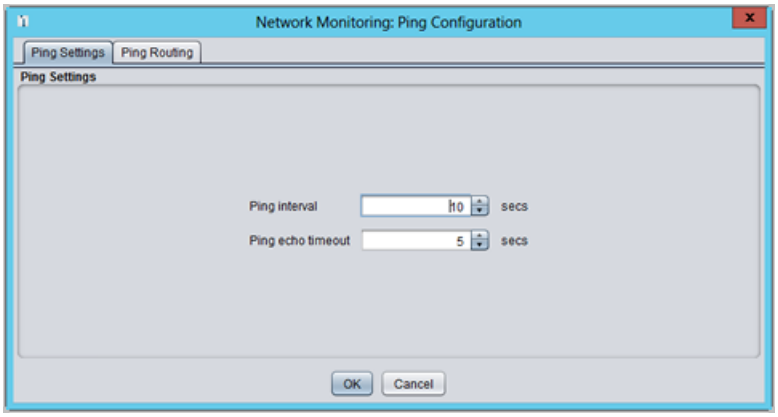

Figure 105: Network Monitoring: Ping Configuration: Ping Settings

2. Select the *Ping Routing* tab to add to or modify the existing target IP addresses for each server to ping.

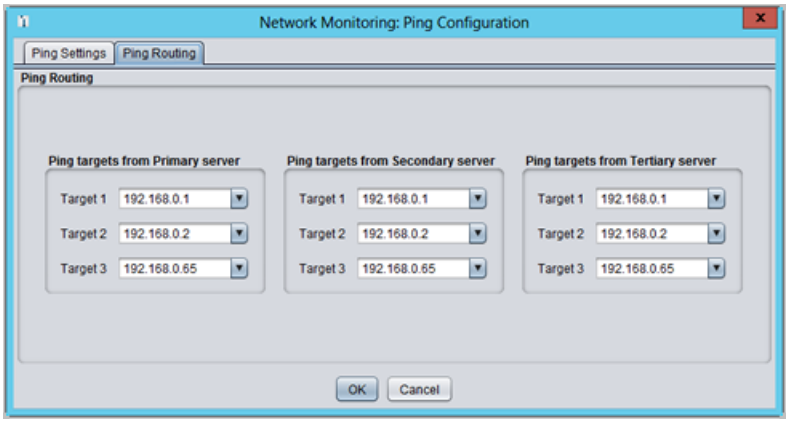

Figure 106: Network Monitoring: Ping Configuration: Ping Routing

In a WAN Pair environment, the target addresses for Public network monitoring on the Secondary server may be different to those automatically selected on the Primary server. Again, the ability to override automatically discovered selections is provided by manually specifying the target address.

Public Network Monitoring is carried out by the active server effectively pinging the target addresses at regular time intervals. The time interval is set by default to every 10 seconds but the frequency may be increased or decreased as required.

Each target is allowed 5 seconds (default) to respond. On slower networks where latency and network collisions are high, increase this interval by changing the *Ping echo timeout* value.

The failure of all three targets to respond is allowed up to the *Max pinged echoes missed before auto-switchover* threshold value. If the failure count of all three targets exceeds this value, Ipswitch Failover initiates an auto-switchover.

Enabling Automatic Switchover in a WAN

The default setting for Automatic Switchover when deployed in a WAN is *Disabled*. Should it be necessary to configure Automatic Switchover in a WAN, use the procedure below:

Procedure

To enable Automatic Switchover in a WAN:

1. In the Ipswitch Advanced Management Client, select the *Network* tab to display the *Network Monitoring* page.
2. Click **Configure Auto-switchover**.
3. Select the *Auto-switchover if client network connectivity lost for* check box.
4. Configure the number of pings to wait before performing the auto-switchover.
5. Click **OK**.

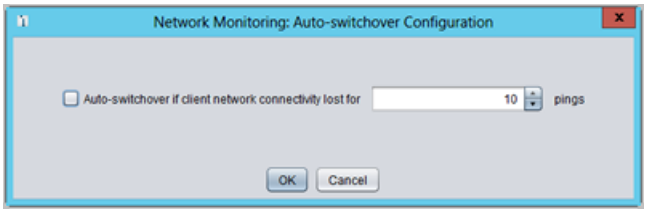

Figure 107: WAN Auto-Switchover Configuration

Setting Max Server Time Difference

Ipswitch Failover generates a warning if the Primary and Secondary server system clocks are not synchronized. The threshold for time difference can be configured using the *Server: Summary* page.

Procedure

To set Max Server Time Difference:

1. Select the *Server: Summary* tab and click **Configure** to display the *Server: Summary Configure* dialog.
2. Type a number (seconds) or use the arrow buttons to select an alert threshold value for time difference between servers, which is checked at handshake following startup.
3. Click **OK**.

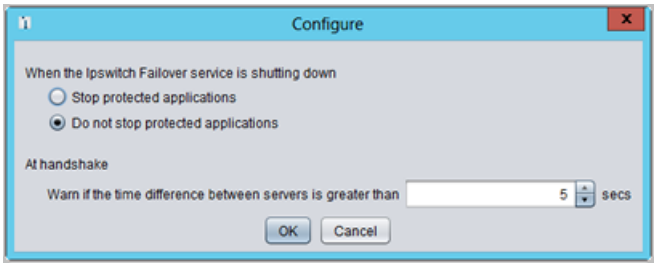

Figure 108: Server: Summary Configure dialog

Chapter 6

Application Protection

Applications Environment

Ipswitch Failover incorporates an Application Management Framework (AMFx) to manage Ipswitch Failover plug-ins.

The AMFx provides additional functions while maintaining the traditional stability of Ipswitch software. Use the AMFx to install and remove plug-ins on the fly while Ipswitch Failover continues to provide protection to currently installed applications.

The AMFx also employs sponsorship for protected applications' files and services. With sponsorship, multiple plug-ins can share files or services. When removing a plug-in, sponsorship prevents removal of a shared file or service that is still required by a remaining plug-in.

Ipswitch Failover uses the System plug-in to monitor the server performance. With the System plug-in, you can configure a variety of counters and assign actions when associated rules are exceeded.

Applications: Summary

The Ipswitch Advanced Management Client **Applications: Summary** page displays the current status of the Cluster, including the identity of the active server, the application state and health, details of application types and their corresponding running status and health. The lower portion of the page provides an *Applications Log* that allows viewing of application events as they occur.

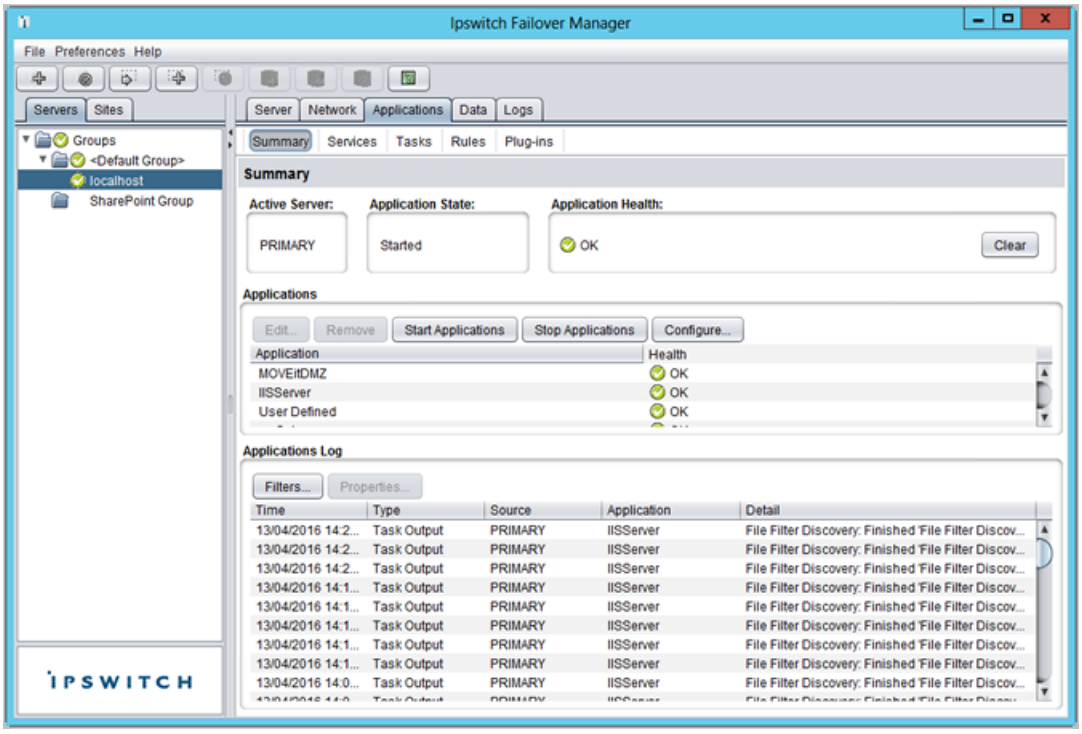

Figure 109: Applications: Summary

This page also provides controls to edit, remove, start, and stop applications, and to configure all protected applications.

View Application Status

After an application starts and is running you can view its status in the *Applications* pane of the **Applications: Summary** page.

Edit Individual Applications

You can configure the amount of time to wait for applications to start or stop before taking action or reporting a failure.

Procedure

To configure these timeout settings, select the application (in the *Applications* pane) and do one of the following:

1. Right-click on the application and select **Edit** from the menu or click **Edit** at the top of the pane.
   The **Edit Application** dialog appears.

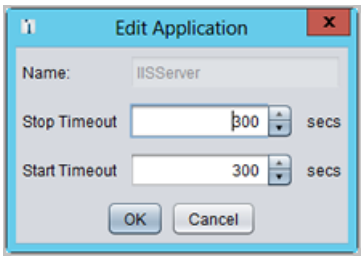

Figure 110: Edit Application

Note: *Default application timeout settings for plug-ins is 300 sec and for user-defined applications is 180 sec.*

2. Enter new values into the *Stop Timeout* and *Start Timeout* text boxes or use the arrow buttons to adjust the values (seconds).
3. Click **OK** to accept the new settings or click **Cancel** to close the dialog without making any changes.

Remove an Application

Application removal is a simple process and can be performed without having to stop Ipswitch Failover.

Procedure

To remove an application:

1. Select the application (in the *Applications* pane).
2. Right-click on the application and select **Remove** from the menu or click **Remove** at the top of the pane.

   A confirmation message appears.
3. Click **Yes** to remove the selected application, or click **No** to dismiss the message without deleting the application.

Configure Applications

You can configure protected applications and enable or disable protection and monitoring. This feature allows you to perform application maintenance without stopping Ipswitch Failover or taking the whole server offline. During installation, Ipswitch Failover creates default settings for application configurations. The Ipswitch Advanced Management Client **Applications: Summary** page allows you to change the settings.

Procedure

To configure applications:

1. Click **Configure** (at the top of the *Applications* pane) to change these settings.

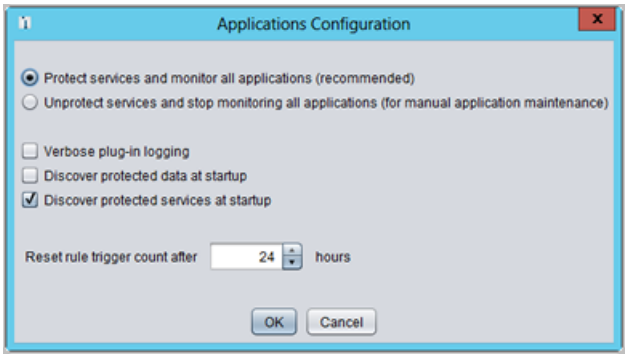

Figure 111: Applications Configuration

2. Select *Protect services and monitor all applications (recommended)* or *Unprotect services and stop monitoring all applications (for manual application maintenance)*.

   Optionally select any or all of the following:

   - Verbose Plug-in logging
   - Discover protected data at startup

- Discover protected services at startup

3. Additionally, you can type a new value into the *Reset rule trigger count after* text box or use the arrow buttons to adjust the values (hours).
4. Click **OK** to accept the new settings or click **Cancel** to close the dialog without making any changes.

View the Applications Log

The *Applications Log* is very useful in troubleshooting the protected application environment.

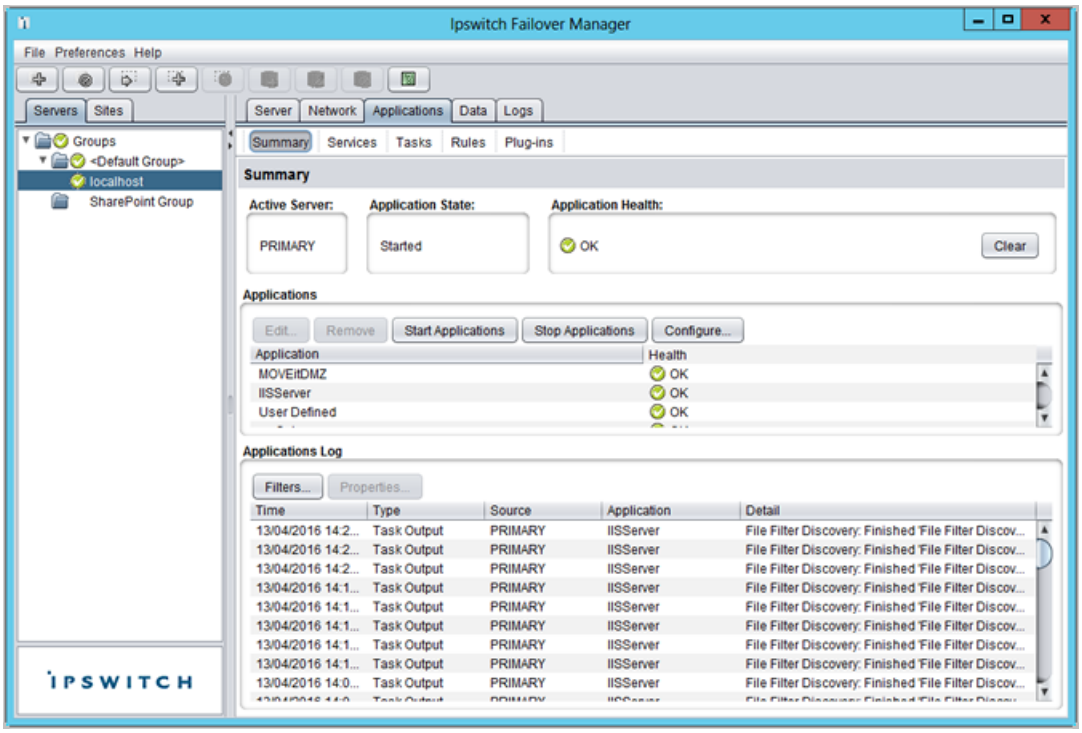

Figure 112: Applications Log

The *Applications Log* provides information about the behavior of all protected applications and includes events such as changes to task status, rule triggering, task outputs, and application warnings. The order that entries are displayed can be sorted either ascending or descending by clicking on the column title.

You also can filter *Applications Log* entries to reduce the number of events displayed, and use the *Applications Log* to troubleshoot application errors. For example, if an application fails, you can right-click on the associated event in the *Application Logs* and select *Properties* to open the Log and investigate the failure.

Filter Application Log Entries

By default, all events are displayed in the *Application Log* pane. To filter the events displayed, perform one of the following steps:

- Right-click on the entry and select **Filters** from the menu
- Click **Filters** at the top of the pane

The **Application Log Filters** dialog appears.

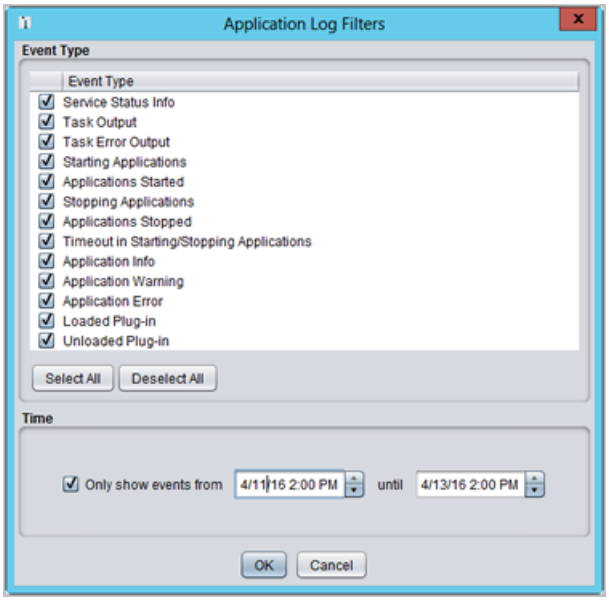

Figure 113: Application Log Filters

Use the check boxes (select to display or clear to hide) to filter *Application Log* entries by at least one *Event* Type. To display only entries within a particular time range, select the check box associated with *Only show events from* and type values into the two date/time text boxes or use the up and down arrow keys to adjust the dates and times. Click **OK** to accept the filter criteria or click **Cancel** to close the dialog without changing the filter criteria.

Applications: Services

The Ipswitch Advanced Management Client **Applications: Services** page shows services specified by plug-ins or by the user, and any services related by dependency.

Change the Order of Services

You can change the order of services using **Up** and **Down** arrows (near the top of the page or on the right-click menu) to change the order in which they appear in the list of services. It is important to understand that the exact order in which services are started and stopped is influenced by a number of key factors:

Procedure

To change the starting and stopping order of protected services:

- The order in which application services are started can be specified by plug-ins.
- Service dependencies must be respected. For example, if service B is listed after service A in the User Defined group, and service A depends on service B, then service B is started first.
- A service can be used by multiple applications (the same service can have more than one sponsor). A service is started when the first application to reference it is started.
- The order of stopping services is the reverse of the order of starting service.

Applications: Tasks

Tasks are a generalization and extension of the start, stop, and monitor scripts in earlier versions of this product.

Task types are determined by when the tasks are run, and include the following:

- **Network Configuration** — This is the first type of task run when applications are started, and is intended to launch `Dnscmd`, `DNSUpdate` or other network tasks. Where multiple `DNScmds` are required, these can be contained in a batch script, which is then launched by the task. Network Configuration tasks are the only types of task that can vary between Primary and Secondary servers.
- **Periodic** — These tasks are run at specific configurable intervals.
- **Pre/Post Start** — These tasks are run before and after services are started on the active server.
- **Pre/Post Stop** — These tasks are run before and after services are stopped on the active server.
- **Pre/Post Shadow** — These tasks are run before and after a shadow copy is created on the active server by the Data Rollback Module (not available in this version).
- **Rule Action** — These tasks can be configured to run in response to a triggered rule, or when a service fails its check.

Tasks can be defined and implemented by plug-ins or by the user, or they can be built-in tasks defined by Ipswitch Failover. User defined tasks are implemented as command lines, which can include launching a batch script. Examples of built-in tasks include monitoring a protected service state on the active and passive servers. An example of a plug-in-defined task is the discovery of protected data and services for a particular application.

The Ipswitch Advanced Management Client **Applications: Tasks** page provides a list of tasks and associated status information, as well as features to quickly manage tasks.

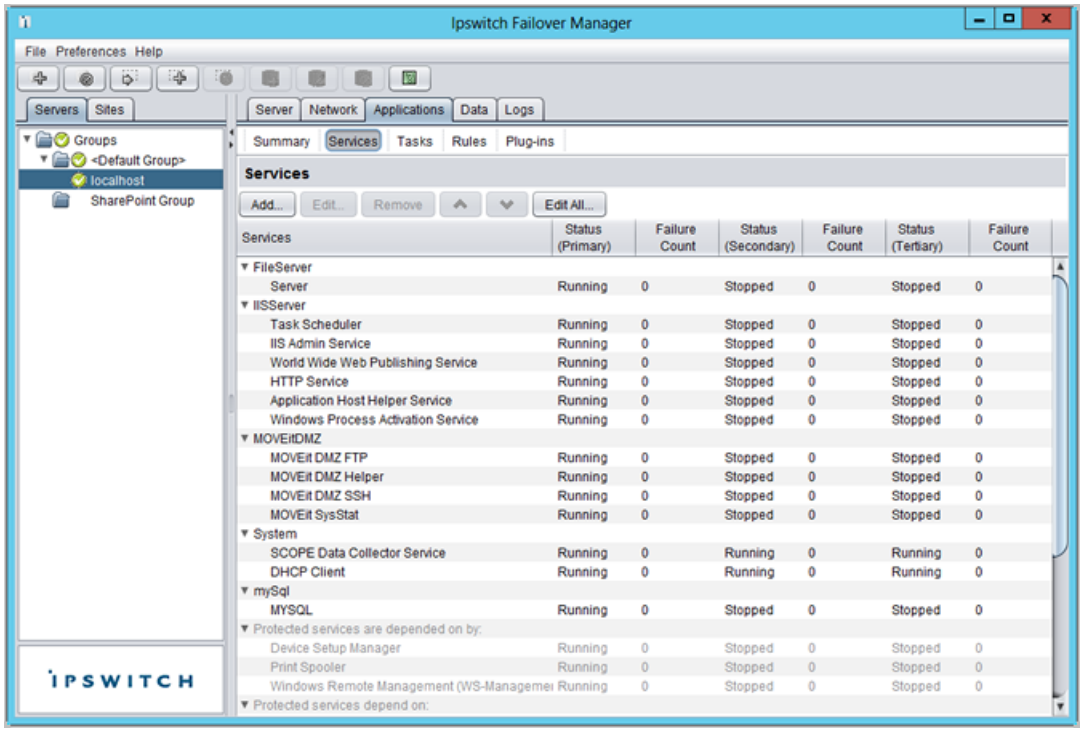

Figure 114: Applications: Tasks page

Change the Order of Tasks

You can change the order of tasks using **Up** and **Down** arrows (near the top of the page or on the right-click menu) to change the order in which they appear in the list of tasks.

View, Add, and Remove User Accounts

You can view, add, and remove user accounts through the Ipswitch Advanced Management Client.

Procedure

- Click **User Accounts** (near the top of the **Applications: Tasks** page).
  The **User Accounts** dialog appears.

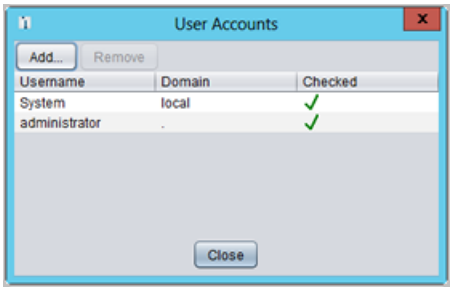

Figure 115: User Accounts

The **User Accounts** dialog contains a list of all currently configured user accounts, including *Username*, *Domain*, and *Checked* (username/password credential validation) status.

Add User Account

To add a user account:

Procedure

1. Click **Add**.
   The **Add User** dialog appears.

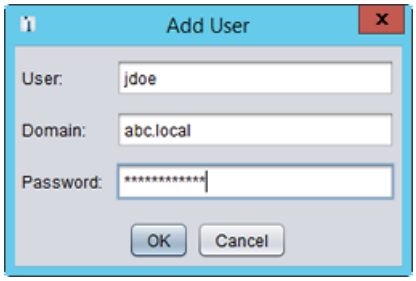

Figure 116: Add User Account

2. Type the name of the *User*, the associated *Domain*, and a *Password* into the corresponding text boxes.
3. Click **OK** to add the new user, or click **Cancel** to close the dialog without adding the user.

> ***Note:*** *Because this information is used for executing tasks that require credentials, be sure to populate these fields with information identical to the Windows credentials.*

Remove User Account

To Remove a user, select the user account from the list in **User Accounts** dialog.

Procedure

1. Click **Remove**.
   A confirmation message appears.
2. Click **Yes** to remove the user, or click **No** to close the dialog without removing the user.

Chapter 7

Data Protection

Data: Replication

Ipswitch Failover can protect many permutations or combinations of file structures on the active server by the use of custom inclusion and exclusion filters configured by the administrator.

> ***Note:*** *The Ipswitch Failover program folder holds the send and receive queues on the active and passive servers, and therefore should be explicitly excluded from the set of protected files.*

You can view replication status and manage data replication through the **Data: Replication** page.

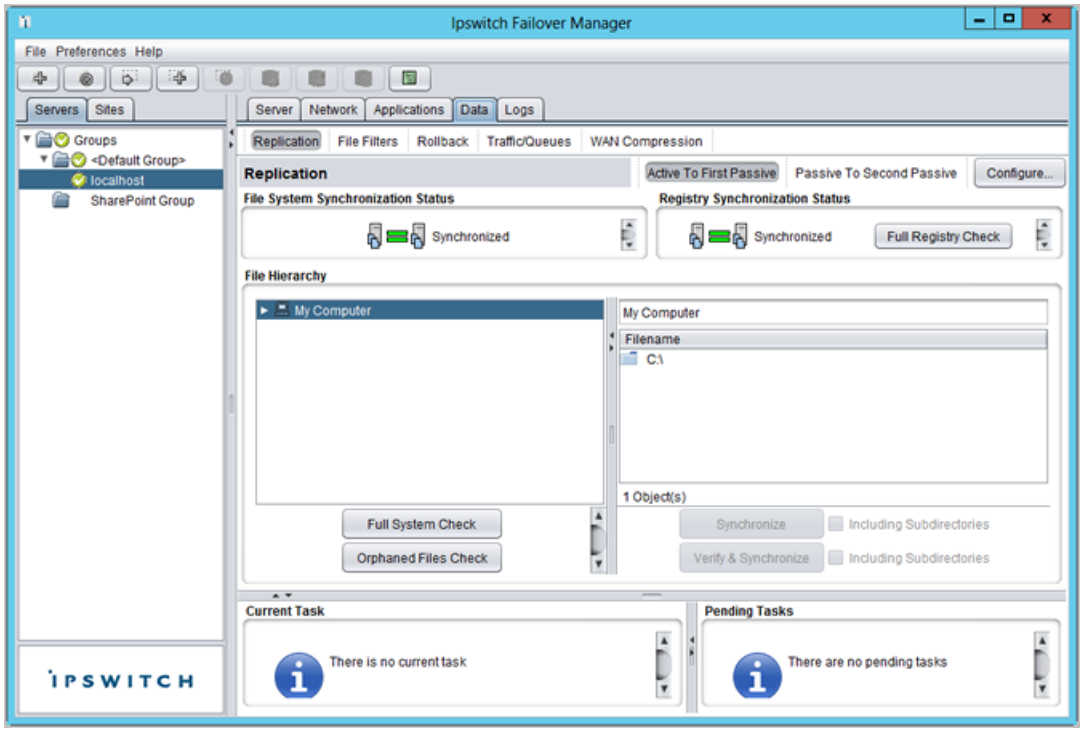

Figure 117: Data: Replication page

Initiate a Full System Check

Certain system events, such as preceding a switchover or following a failover or split-brain syndrome, may require running a full system check to ensure that the entire protected file set is synchronized and verified. A

full system check performs a block-level check identical to that performed during initial synchronization and verification, and of the same files identified by the file filters.

Procedure

To initiate a full system check:

1. Click **Full System Check** in the left pane of the *File Hierarchy* pane.

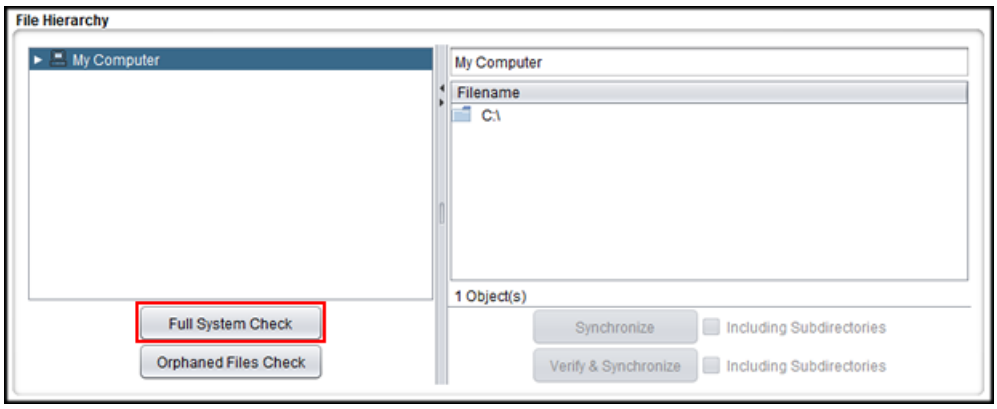

Figure 118: Data: Replication File Hierarchy pane

2. A Caution message opens and asks "*Are You Sure You Want To Initiate A Full System Check?*" and explains that depending on the amount of protected data, this task may take a long time to complete (a number of hours).

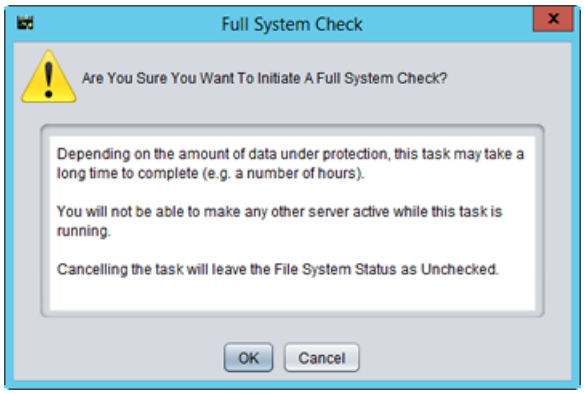

Figure 119: Full System Check Caution Message

3. Click **OK** to initiate the Full System Check, or click **Cancel** to close the message without starting the Full System Check.

> ***Note:*** *Once a Full System Check is initiated, allowing it to run to its conclusion is strongly recommended because canceling leaves the file system status Unchecked. Depending on the amount of data, resynchronization may take substantial time to complete. Switchover is not permitted until after the task is complete and the File System Status is Synchronized.*

Fast Check

The Fast Check process is used by Ipswitch Failover to rapidly verify files between servers prior to starting applications. Fast Check compares file time stamps and attributes rather than the check sums of the data thereby

accelerating the startup and synchronization process. If the time stamp or attribute check fails, than the normal verification and synchronization process will initiate. Additionally, you can configure the length of time to wait for Fast Check to complete before starting applications.

Fast Check is beneficial after a graceful shutdown where severs were synchronized before shutdown. Fast Check allows the server to check the file synchronization rapidly and start to service clients. If Fast Check detects files that are out-of-sync, it initiates the full verify and synchronization process to resynchronize your data.

Configure Fast Check

When combined with Controlled Shutdown, Fast Check provides the ability to perform scheduled unattended restarts of the servers.

Procedure

To enable Fast Check:

1. Navigate to **Data** > **Replication**.
2. Click the **Configure** button.
3. Select the *Fast Check* tab.
4. Select the manner in which Fast Check should operate using the Fast Check radio buttons.
5. Configure *Maximum Application Delay*. This is the length of time Ipswitch Failover will delay the startup of the application while it attempts to establish replication between active and all passive nodes.
6. Click **OK**.

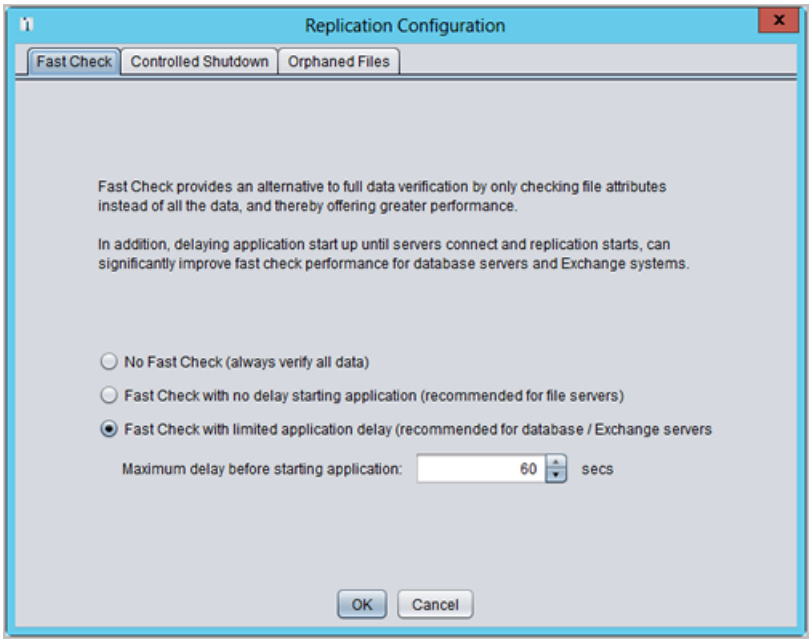

Figure 120: Configure Fast Check

Note: *When Fast Check is configured in addition to Controlled Shutdown, Ipswitch Failover can be configured to perform an unattended restart. For more information about Controlled Shutdown, see Controlled Shutdown.*

Manually Initiate File Synchronization

When an out-of-sync file or folder is detected, a red icon is displayed indicating the Out-of-sync status. You can re-synchronize the out-of-sync file(s) manually using a process that is quicker and simpler than the Full System Check.

Procedure

To manually re-synchronize:

1. Select one or more files and folders from the list in the right pane of the *File Hierarchy* pane. Multiple files and folders can be selected from this file list by using the standard Windows multiple selection techniques, **Shift** + click and **Ctrl** + click.
2. When one or more folders are selected, also select the *Including Subdirectories* check box to ensure that all files within the folder(s) are also synchronized.
3. Click **Synchronize**. As the synchronization runs, you may see its progress in the *Current Task* pane at the bottom left of the **Data: Replication** page. When the synchronization process successfully completes, a green icon indicates synchronized status.

   You also can right-click on a folder in the tree view (in the left pane of the *File Hierarchy* pane) to quickly select *Synchronize* or *Verify and Synchronize* from a menu. Both options automatically include subdirectories.

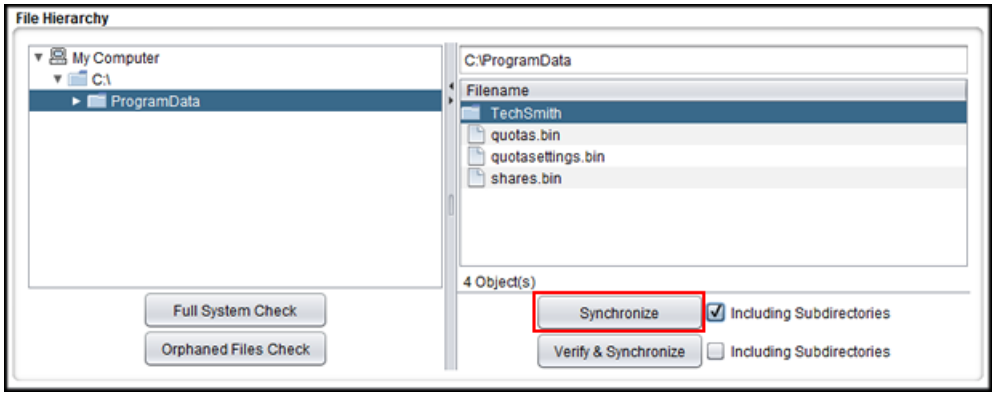

Figure 121: Manual Selection to initiate file synchronization

Manually Initiate Verify and Synchronize

To perform manual verification and synchronization, the process is identical to the one described in *Manually Initiate File Synchronization* except that the process is started by clicking **Verify and Synchronize**.

Procedure

To manually verify and synchronize:

1. Select one or more files and folders from the list in the right pane of the *File Hierarchy* pane. Multiple files and folders can be selected from this file list by using the standard Windows multiple selection techniques, **Shift** + click and **Ctrl** + click.
2. When one or more folders are selected, also select the *Including Subdirectories* check box to ensure that all files within the folder(s) are also verified and synchronized.
3. Click **Verify and Synchronize**. As verify and synchronization runs, you may see its progress in the *Current Task* pane at the bottom left of the **Data: Replication** page. When the verify and synchronization process successfully completes, a green icon indicates verified and synchronized status.

You also can right-click on a folder in the tree view (in the left pane of the *File Hierarchy* pane) to quickly select *Verify and Synchronize* from a menu. This option automatically includes subdirectories.

Each verification and synchronization request (manually or automatically scheduled) is defined as a task with subsequent tasks queued for processing after the current task is completed. Each task is listed in the *Pending Tasks* list to the right of the *Current Tasks* frame.

Note: *Individual tasks can be canceled, but canceling automatically triggered tasks can lead to an Unchecked system. A warning is presented detailing the possible consequences of canceling tasks.*

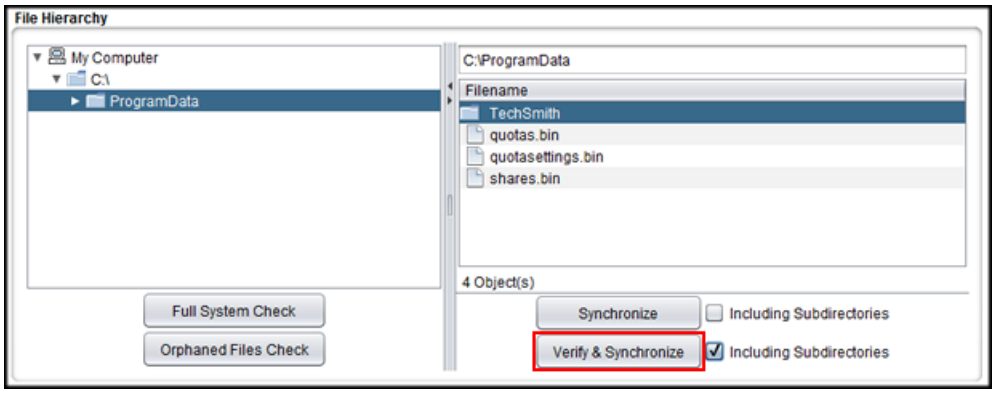

Figure 122: Manual Selection to Initiate Verify and Synchronize

Orphaned Files Management

Ipswitch Failover provides the opportunity to check the system for orphaned files and either notify the administrator or to delete the orphaned files. Orphaned files are those files in a protected set that exist on the passive server but do not exist in the protected set on the active server in a pair.

Orphaned File Check can either delete or log files on the passive server that exist within the protected set; they were “orphaned” because Ipswitch Failover was not running when content changes were made on the active server.

Note: *Orphaned File Check does not delete files on the passive server if there is no file filter to include the content as this would be unsafe.*

Special Cases

Filters for files, file types, or other wildcards

Folder root filters

Orphaned File Check will manage the entire contents of that folder (for example, `D:\folder\**`). This deletes all passive files within the folder that do not exist on the active server, and includes content created only on the passive server.

Exclusion file filters

Orphaned File Check will not delete any files excluded from the protected set by exclusion filters. This rule safeguards users and applications.

Filters for files, file types, or other wildcards

Orphaned File Check is not managing the contents of the folder (for example, `D:\database\*.log`), only the selected files.

Orphaned File Check will only process files that match the filter and will not delete files with any other extension within the folder `D:\database`

Orphaned files are those files in a protected set that exist on the passive server but do not exist in the protected set on the active server in a pair.

Prior to initiating an orphaned files check, you must configure the options for actions to take in the event orphaned files are found. By default, Orphaned Files Check is configured to delete orphaned files. Should you want to log the files presence, see *Configure Orphaned Files Check*.

Configure Orphaned Files Check

Prior to initiating an orphaned files check, you must configure the options for actions to take in the event orphaned files are found. By default, Orphaned Files Check is configured to delete orphaned files. Should you want to log the files presence, follow the steps below.

Procedure

To Configure Orphaned Files Check options:

1. Navigate to the **Data: Replication** page and click on the **Configure** button.
2. Select the *Orphaned Files* tab.
3. Select the *Detect orphaned files* check box and in the *On detection, take the following action* drop-down menu select *Delete* to automatically delete the orphaned files or *Log to file* to add the files list to the log file.

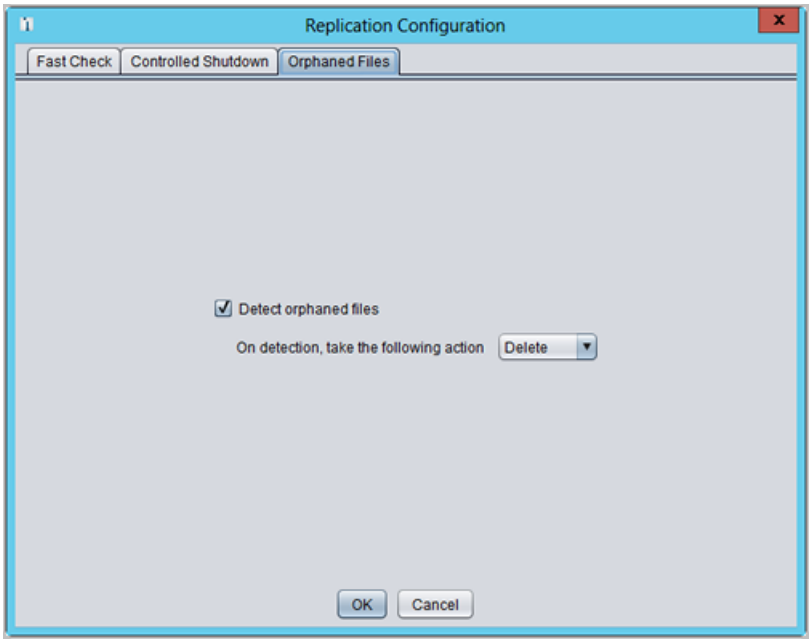

Figure 123: Orphaned Files Configuration Options

4. After selecting the options, click **OK** to close the dialog.
5. Click the **Orphaned Files Check** button.

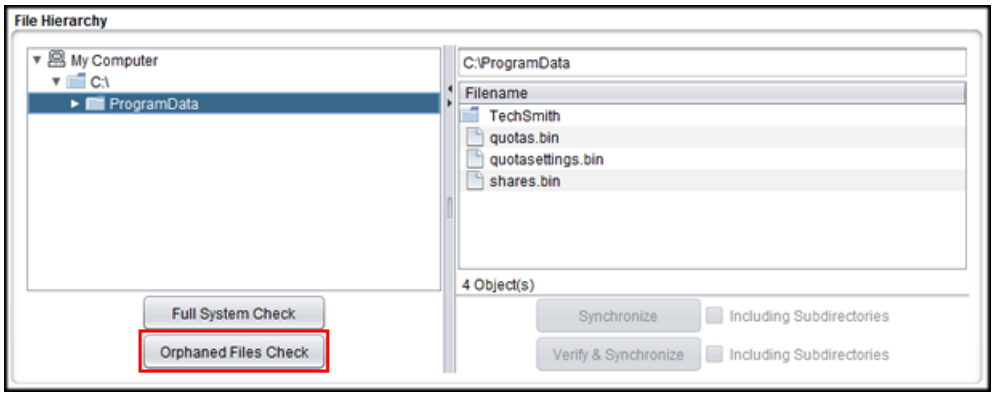

Figure 124: Initiate Orphaned Files Check

Reference

Appendix A

Other Administrative Tasks

Post Installation Configuration

Upon completion of installation of Ipswitch Failover, you should perform the following Post Installation tasks.

Configure the VmAdapter Plug-in

After installation of Ipswitch Failover is complete:

Procedure

Configure the VmAdapter Plug-in:

1. Launch the Failover Management Service UI for the server pair and login.
2. Navigate to **Settings** > **Application Protection** > **Plug-ins**.
3. Select the `VmAdapterNFPlugin.dll`
4. Click the **Edit** button.
   The *Edit Plug-in* dialog is displayed.
5. For the Primary server, enter the Destination for VM migration of the Primary server by providing the following information:
   - Host (name or IP address as in vCenter)
   - Datastore
   - Resource Pool
6. For the Secondary server, enter the Destination for VM migration of the Secondary server by providing one of the following:
   - Host (name or IP address as in vCenter)
   - Datastore
   - Resource Pool
7. If integration with vSphere HA monitoring is desired, select the *Integrate with vSphere HA monitoring* check box.

Note: *This option requires vSphere HA Application monitoring for the cluster and VM.*

8. Click **OK**.

Adding an Additional Network Interface Card

Ipswitch Failover allows for installation using a single NIC on each Ipswitch Failover server in the Pair or Trio. When installed with a single NIC, Ipswitch recommends that to prevent experiencing a single point-of-failure, an additional NIC be installed or configured on each server in a Pair or Trio with one NIC configured as the Public NIC and another configured for the Ipswitch Channel.

Procedure

To add an additional network interface card (NIC) to allow moving the Channel IPs to a dedicated NIC:

Adding an additional NIC to a physical server will require that Ipswitch Failover be shutdown while the NIC is added and the server must be restarted. If the server is a virtual server, the shutdown is not necessary. Ipswitch recommends that the NIC be added on the passive (Secondary) server, and then a switchover be performed making the Secondary server active, and then adding an additional NIC to the passive (Primary) server.

This procedure assumes that Ipswitch Failover is installed as a Pair with the Primary server active and the Secondary server passive.

1. Shutdown Ipswitch Failover on the passive server.
2. Navigate to **Start** -> **Control Panel** -> **Administrative Tools** -> **Services**.
3. Select the *Ipswitch Failover Service* and change the *Start up* to *Manual*.
4. Add a virtual NIC to the Secondary server.
5. Restart the server.
6. Navigate to **Control Panel** -> **Network and Internet** -> **Network and Sharing** -> **Change Adapter Settings**.
7. Right-click the newly added NIC and select *Properties*.
8. Right-click the newly added NIC and select *Internet Protocol Version 4 (TCP/IPv4)* and click **Properties**.
9. Configure the NIC so that it does not use DHCP by temporarily entering an unused IP address (for example, 1.1.1.1).
10. Click **OK** -> **Ok** -> **Close**.
    If the NIC is not enabled, enable it now.
11. Open the Configure Server wizard, select the *Channel* tab, and double click the *Channel IP Routing* you are moving to the new NIC. Select the new NIC in the drop down list and click the **Edit** button.
12. Navigate to **Start** -> **Control Panel** -> **Administrative Tools** -> **Services**.
13. Select the *Ipswitch Failover* service and change the *Start up* to *Automatic*.
14. Start Ipswitch Failover on the passive (Secondary) server.
15. Perform a switchover to make the Secondary server active and the Primary server passive.
16. Shutdown Ipswitch Failover on the (Primary) passive server.
17. Navigate to **Start** -> **Control Panel** -> **Administrative Tools** -> **Services**.
18. Select the *Ipswitch Failover* service and change the *Start up* to *Manual*.
19. Add a virtual NIC to the Primary server.
20. Restart the server.
21. Right-click the newly added NIC and select *Properties*.
22. Select *Internet Protocol Version 4 (TCP/IPv4)* and click **Properties**.

23. Configure the NIC so that it dows not use DHCP by temporarily entering a unused IP address (for example, 2.2.2.2).
24. Click **OK** -> **Ok** -> **Close**.
    If the NIC is not enabled, enable it now.
25. Open the Configure Server wizard, select the *Channel* tab, and double click the *Channel IP Routing* you are moving to the new NIC. Select the new NIC in the drop down list and click the **Edit** button.
26. Start Ipswitch Failover on the passive (Primary) server.
27. Allow the server to synchronize. Once synchronized, perform a switchover.

Business Application Groups

Ipswitch Failover offers the ability to group application servers together creating a Business Application Group. Business Application Groups are a grouping of servers that share a common purpose such as Microsoft Exchange servers, BlackBerry Enterprise servers, or Microsoft SQL servers for monitoring and management purposes. With the Business Application Plug-in installed, Ipswitch Failover provides the ability to manage groups of servers as a single entity and perform switchovers of a complete group from one site to another.

Installing the Business Application Plug-in

The Business Application Plug-in (`BusinessApplicationNFPlugin.dll`) is installed after installing Ipswitch Failover.

Prerequisites

Prior to installing and configuring the Business Application Plug-in, complete the following:

- If you are not using the same host name for all servers in a Cluster, you must configure Alternate IP addresses on all servers in the Secondary sites.
- Configure persistent static routes for the Ipswitch Channel between the servers within a Business Application Group site as explained below:
  - Configure persistent static routes between all of the Primary servers within the Business Application Group at the Primary HA site.
  - Configure persistent static routes between all of the Secondary servers within the Business Application Group at the Secondary HA site.
  - Configure persistent static routes between all of the servers within the Business Application Group at the DR site.

Note: *Add persistent routes with a lower metric to allow them to be attempted first.*

1. Download the `Z-SW-BusinessApplicationPlugin.201.5.[n].zip` file to a temporary location on the active server in the cluster.

   Note: *The `BusinessApplicationNFPlugin.dll` must be downloaded and installed on each cluster server to be included in the Business Application Group.*

2. Extract the archive `.zip` file.
3. Launch the Ipswitch Advanced Management Client and navigate to the **Applications: Plug-ins** page.

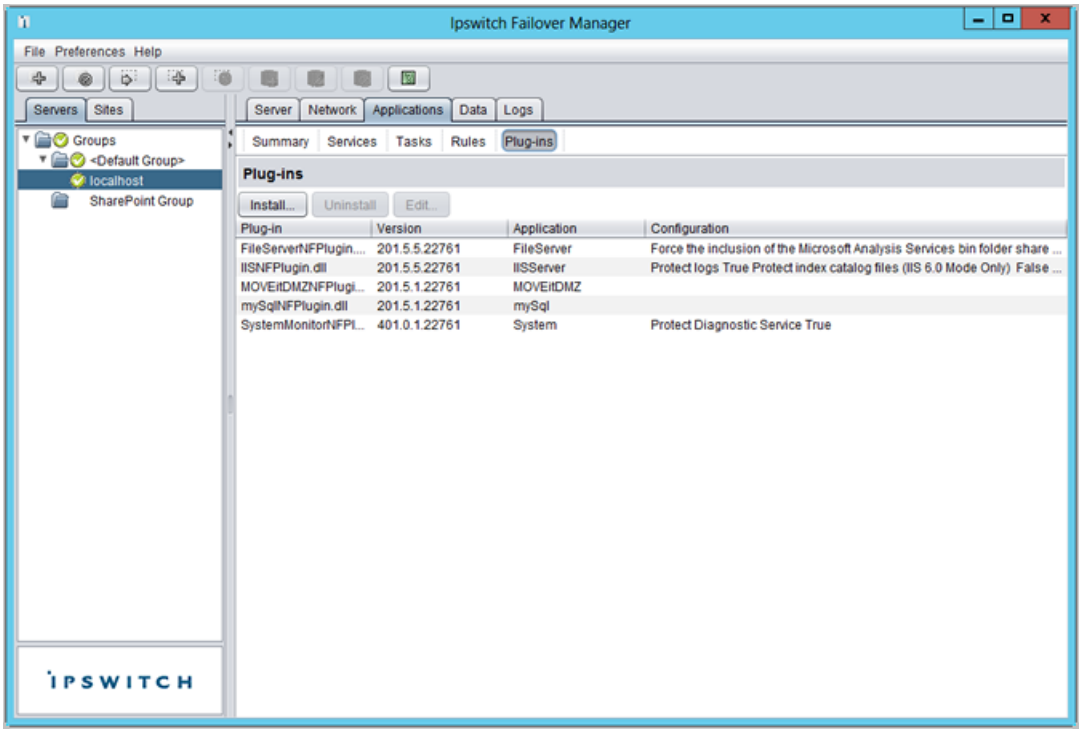

Figure 125: Applications: Plug-ins Page

4. Click **Install**.
5. Browse to the location of the `BusinessApplicationNFPlugin.dll` file and select the file.

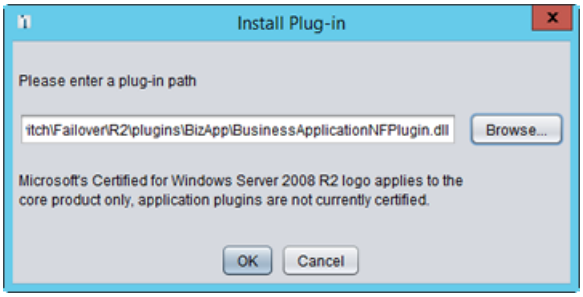

Figure 126: Install Plug-in Dialog

6. Click **OK**.
7. Repeat the process on each Cluster to be included in the Business Application Group.

> ***Important:*** *Once the Business Application Plug-in has been installed, Ipswitch recommends that you do* ***NOT*** *edit the Business Application Plug-in directly but rather use the* ***Edit Business Application Group Wizard*** *to make changes to the plug-in parameters.*

Creating a Business Application Group

When the Ipswitch Failover Business Application Plug-in is installed it is initially in an unconfigured state. The Unconfigured icon appears in the left pane of the Ipswitch Advanced Management Client under Servers. All servers listed in the Unconfigured category are available as Business Application Group candidates and may be

added to a Business Application Group. Add the appropriate servers to a Business Application Group to monitor or manage servers with a common function or purpose as a group.

Prerequisites

The Ipswitch Advanced Management Client requires that you have access to a minimum of two Ipswitch Failover clusters displayed in the *Servers* pane as Unconfigured to create a new Business Application Group.

1. Launch the Ipswitch Advanced Management Client.
2. Navigate to **File** > **Add Business Application Group**.
   The **Business Application Group Wizard** is displayed.

Figure 127: Business Application Group Wizard

3. Review the information in the **Create Business Application Group Wizard** and click **Next**.
   The **Enter Basic Group Information** page is displayed.

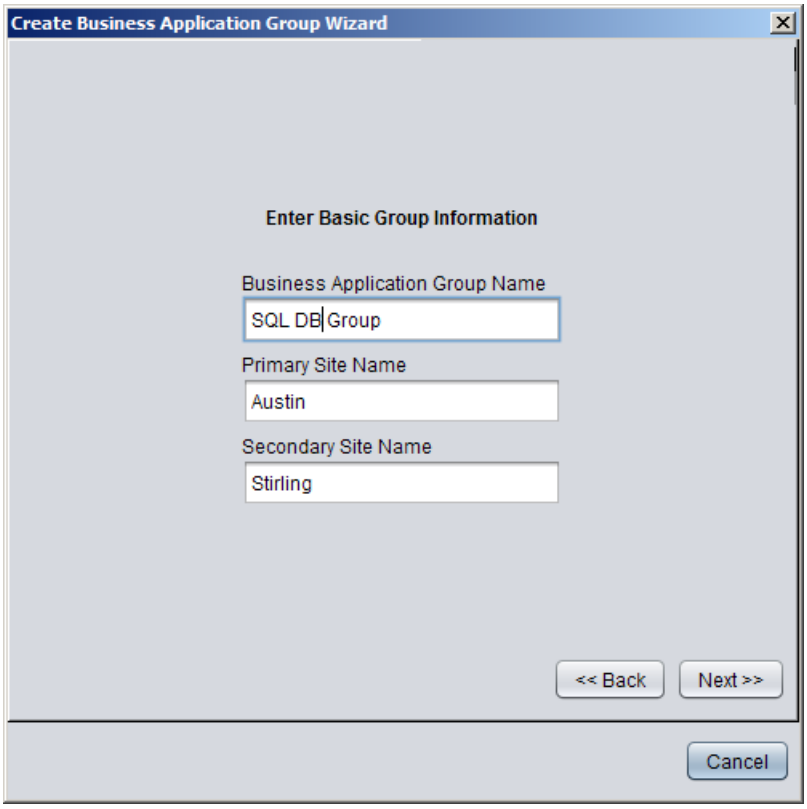

Figure 128: Enter Basic Group Information Page

4. Enter a name for the Business Application Group into the text field.

   Note: *The name of the Business Application Group cannot exceed 15 characters.*

5. Add the name of the Primary Site.
6. Add the name of the Secondary (DR) site and click **Next**.
   The **Add Servers to Business Application Group** page is displayed. A list of available servers is displayed in the left pane of the dialog.

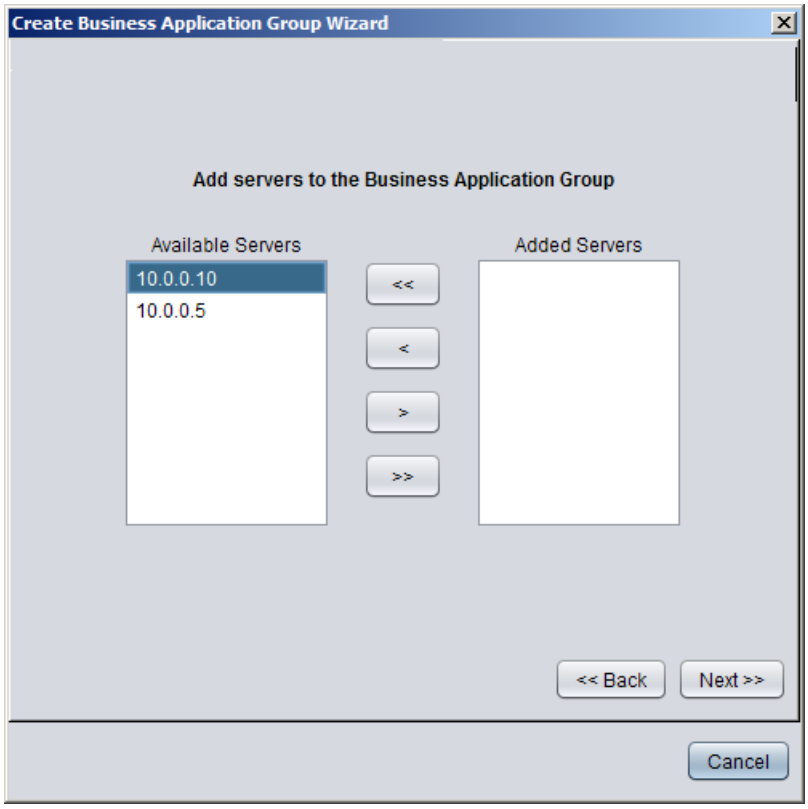

Figure 129: Add Servers to Business Application Group Page

7. Select the servers to join the Business Application Group and click the > button to add the servers to the Business Application Group. Click **Next**.
   The **Select First Server to Switch** page is displayed.
8. Select the server you want to be the first to switch within the Business Application Group. Click **Next**.

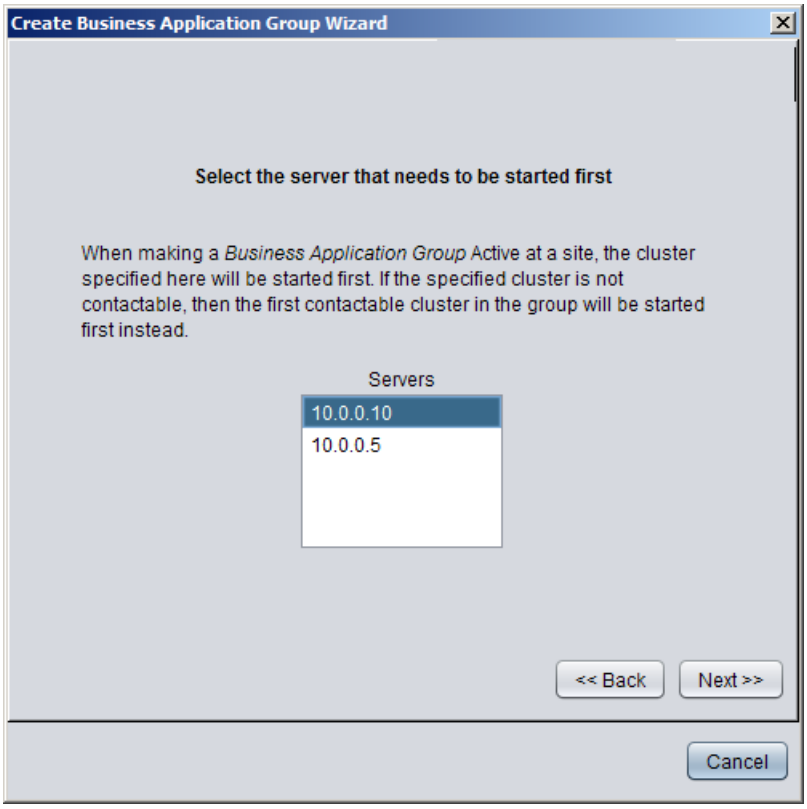

Figure 130: Select First Server to Switch Page

Note: *Ipswitch Failover will attempt to switch the server indicated in step 8 above but in the event that the server is unavailable, Ipswitch Failover will continue to switch other servers in the Business Application Group.*

The **Create Business Application Wizard Complete** page is displayed.

9. The **Create Business Application Wizard Complete** page informs you that you have successfully created a Business Application Group and can now take advantage of Ipswitch Failover's Site Switchover capabilities discussed in *Site Switchover*. Click **Finish**.

Figure 131: Create Business Application Wizard Complete Page

Editing a Business Application Group

Failover Management Service allows you to edit the configuration of an existing Business Application Group.

1. Navigate to **File** > **Edit Business Application Group** or click on the **Edit Business Application Group** button.
   The **Edit Business Application Group Wizard** is displayed.

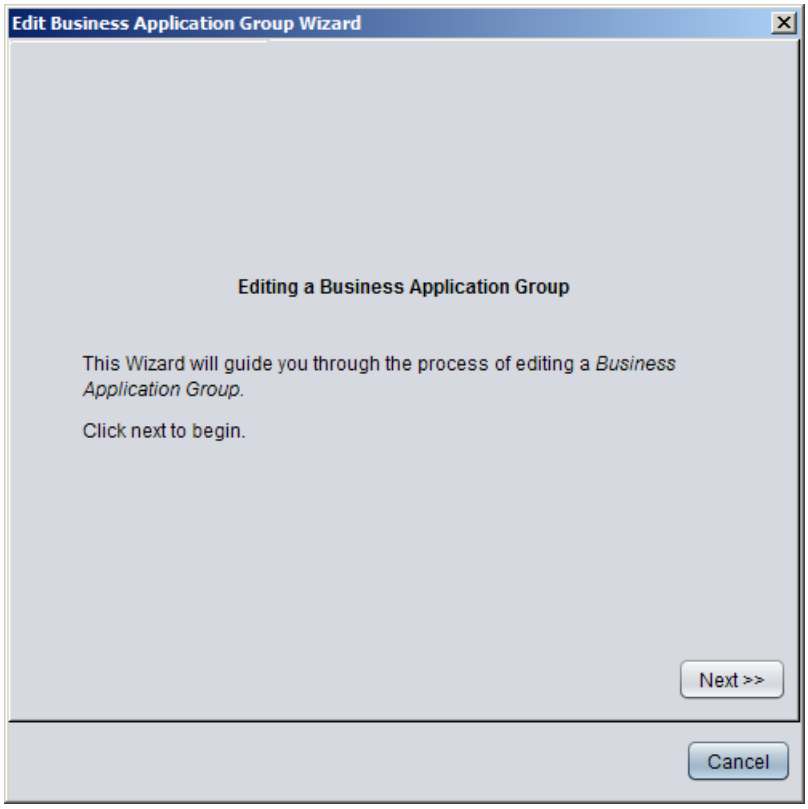

Figure 132: Edit Business Application Group Wizard

2. Click **Next**.
   The **Enter Basic Group Information** page is displayed.

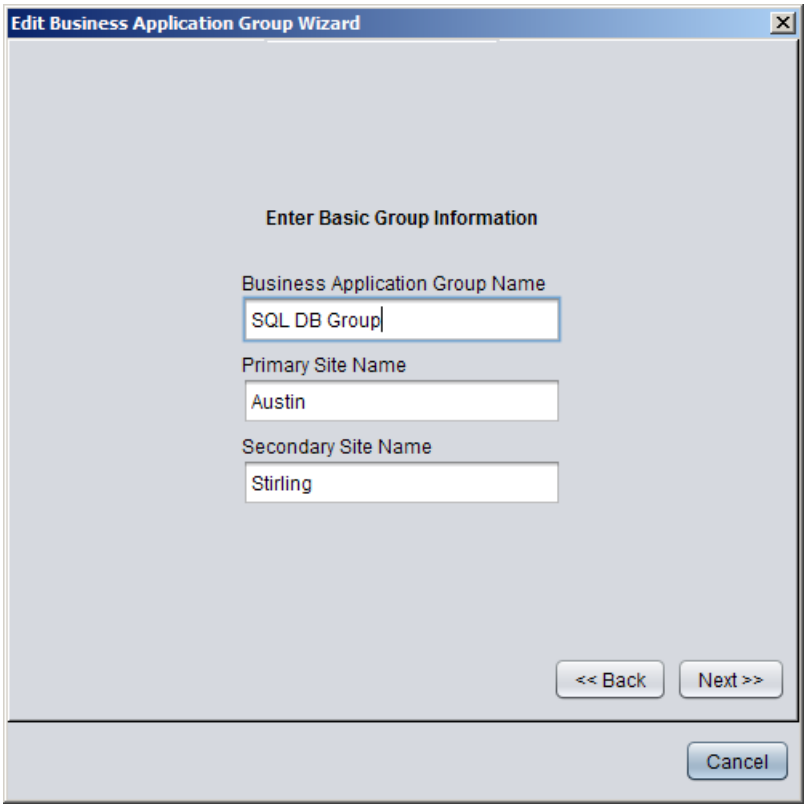

Figure 133: Enter Basic Group Information

3. Edit the name of the Business Application Group, Primary Site, and/or the Secondary Site and click **Next**. The **Select First Server to Switch** page is displayed.

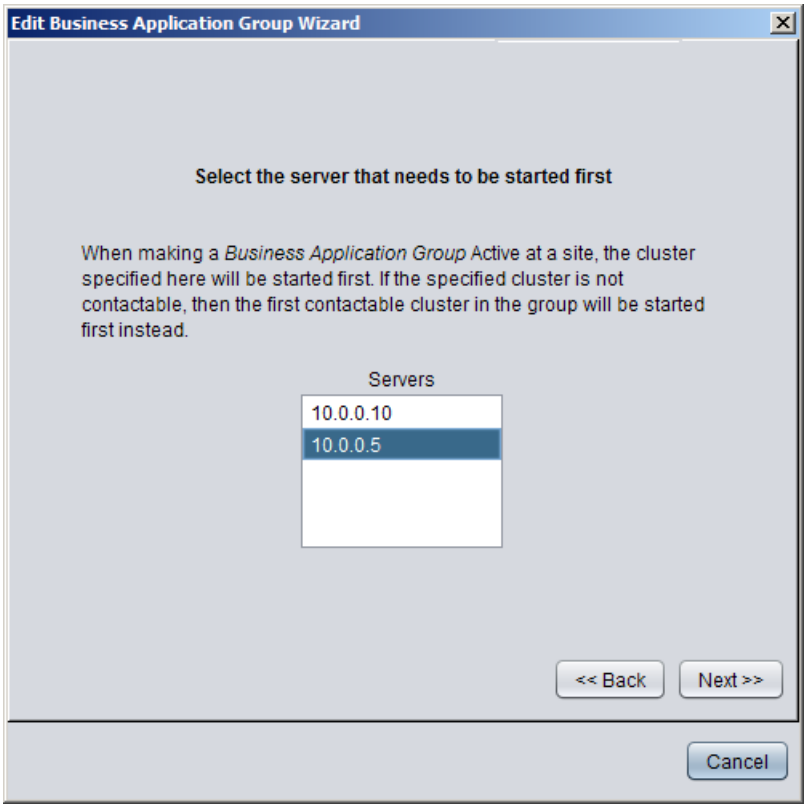

Figure 134: Select First Server to Switch Page

4. Select the server you want to be the first to switch within the Business Application Group and click **Next**. The *Edit Business Application Wizard* page is displayed.
5. Click **Finish**.

Dissolve a Business Application Group

The Dissolve Business Application Group feature of the Ipswitch Advanced Management Client allows you to remove a Business Application Group without removing the servers from the Ipswitch Advanced Management Client.

1. Using the Ipswitch Advanced Management Client, select the Business Application Group to be dissolved.

> ***Note:*** *If you do not intend to recreate the Business Application Group, you must remove the Business Application Plug-in from each server in the Group.*

2. Navigate to **File** > **Dissolve Business Application Group**.

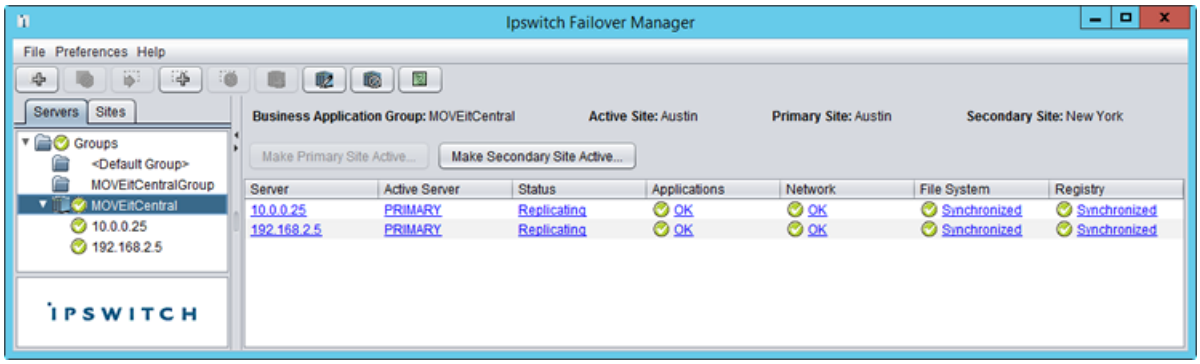

Figure 135: Dissolve Business Application Group - Tool bar Button

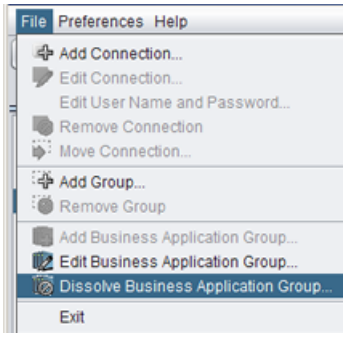

Figure 136: Dissolve Business Application Group - File Menu

A dialog is displayed asking if you are sure you want to dissolve the Business Application Group.

Figure 137: Dissolve Business Application Group - Confirmation Dialog

3. Click **Yes** to dissolve the Business Application Group.

Business Application Switchover

Ipswitch Failover provides the ability to perform a managed switchover of a Business Application Group thereby allowing the administrator to transfer the load of the active servers in the Business Application Group to a secondary site with a single operation.

In the event that one of the servers in the Business Application Group should fail, the administrator can perform a managed switchover to the secondary site thereby maintaining continuous availability for users. Additionally, for maintenance and management purposes, the administrator can perform a managed switchover to the secondary site for all servers in the Business Application Group with the click of a single button.

The **Business Application Group Summary** page provides an overview of all servers within the Business Application Group. Selecting an individual server within the group displays information that is specific to the selected server.

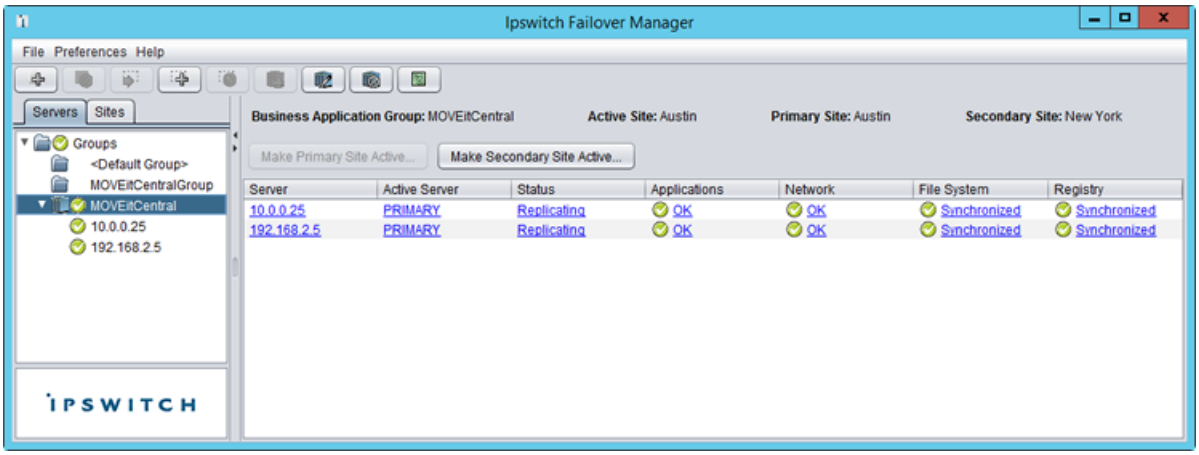

Figure 138: Business Application Group Summary Page

Performing a Business Application Switchover

1. Launch the Ipswitch Advanced Management Client.
2. Select the *Servers* tab in the left pane.
3. In the *Servers* pane, select the Business Application Group to switch.
   The **Business Application Group Summary** page is presented.
4. To perform a managed switchover, click:

Option	Description
Make Secondary Site Active	Switches the active operational load from the current (Primary) site to an alternate Secondary site
Make Primary Site Active	Switches the active operational load from the current (Secondary) site to the Primary site

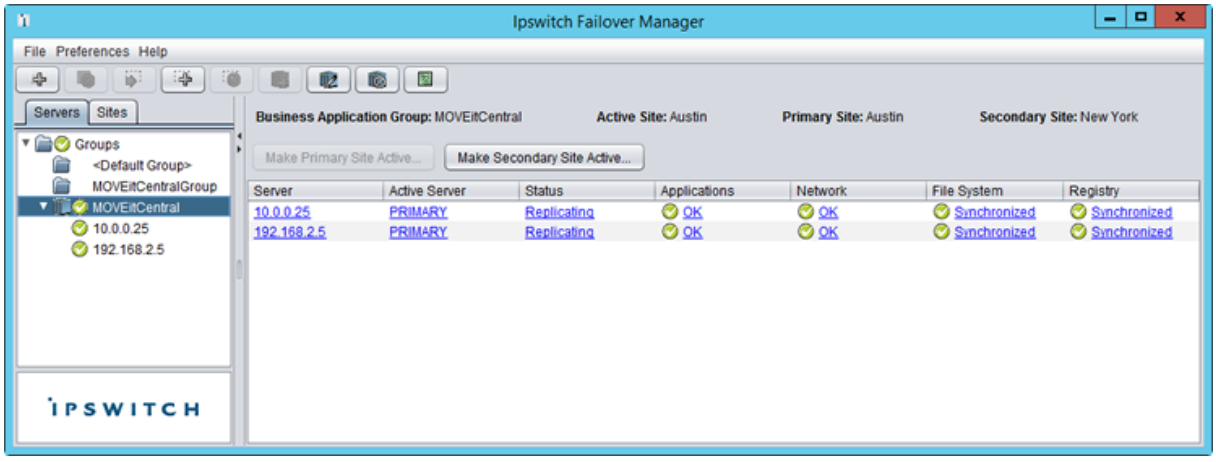

Figure 139: Business Application Group Summary Page

The active servers at the current site become passive and the passive servers at the opposing site become active.

Site Switchover

When Ipswitch Failover is deployed for Disaster Recovery in a pair, Ipswitch Failover can be configured to perform a managed switchover at the site level.

When the Business Application Plug-in is installed and Business Application Groups are configured, Ipswitch Failover can provide a single button action to switch the active load of all Business Application Groups in a single site to a Standby Site and back again as required.

This feature can be used when a Business Application Group member server has failed, an application running on one of the servers has failed and cannot be restored, or a total site outage has occurred.

If the server that fails is the server configured to switch first, the Ipswitch Advanced Management Client will be unable to connect to the host name and after a retry, will attempt to connect via the Alternate IP address. If the Alternate IP address has not been configured, then the connection will drop out of the group and commands to switchover cannot be sent.

In the event of a WAN outage, the administrator needs to ensure that if the standby site is made active, then the administrator must shut down the previously active site to prevent both sites from being simultaneously active. To prevent both sites from being active at the same time, the administrator should shut down the active site prior to making the Standby Site active. A site switchover assumes that the Primary Site has experienced a total failure and that the servers in the Primary Site are not longer running. If this is not the case, the administrator is responsible for shutting down the previously active site.

Performing a Site Switchover

Procedure

1. Launch the Ipswitch Advanced Management Client.
2. Select the *Sites* tab in the left pane.

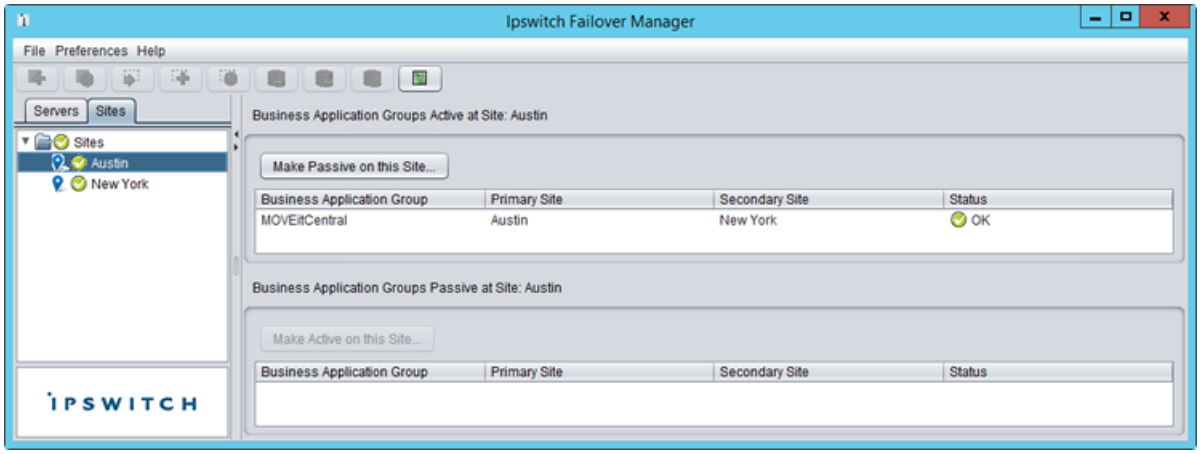

Figure 140: Ipswitch Failover Sites Overview Page

3. Select the Site to change.
4. Click:

Option	Description
Make Passive on this Site	The currently active site
Make Active on this Site	The currently passive site

Note: *If you select the currently active site, only the* ***Make Passive on this Site*** *button is available. If you select the currently passive site, only the* ***Make Active on this Site*** *button is available.*

Perform a Site Switchover when the First Server to Switch is Unavailable

In the event that the First to Switch server in the Business Applications Group can not be contacted to perform a switchover, you can perform a switchover by performing the steps below:

Procedure

1. Launch the Ipswitch Advanced Management Client.
2. Login to Ipswitch Failover on the Disaster Recovery server of the First to Switch Cluster.
3. Navigate to the **Server: Summary** page.
4. Select the Disaster Recovery server icon.
5. Click the **Make Active** button.
   The Disaster Recovery server of the First to Switch Cluster becomes active.

Uninstall the Business Application Plug-in

The Ipswitch Advanced Management Client allows you to uninstall the Business Application Group Plug-in on-the-fly without stopping Ipswitch Failover.

Prerequisites

If the Business Application Plug-in must be uninstalled for any reason, you must first dissolve the Business Application Group and then uninstall the Business Application Plug-in. After uninstalling the Business Application Plug-in, you can then reinstall the plug-in and create a new Business Application Group.

1. After dissolving the Business Application Group, select the server to have the Business Application Plug-in uninstalled.
2. Navigate to the **Applications: Plug-ins** page of the Ipswitch Advanced Management Client.
3. Select the server on which to uninstall the Business Application Plug-in.
4. Select the `BusinessApplicationNFPlugin.dll`
5. Click **Uninstall**.
   The Business Application Plug-in is uninstalled.

Note: *When upgrading the Business Application Plug-in on a server in a Business Application Group, you must upgrade the Business Application Plug-in on all other servers in the Business Application Group.*

Configure Event Log Files

To configure default settings for log files, click **Configure** to invoke the **Event Log Configuration** dialog. Select the *General* tab to configure the log file. This dialog allows you to define where the exported comma separated variable file is stored and the name of the file by entering the path and filename manually or browsing to a location using the browse feature. Click **Browse** to open an Explorer type interface and navigate to the appropriate location.

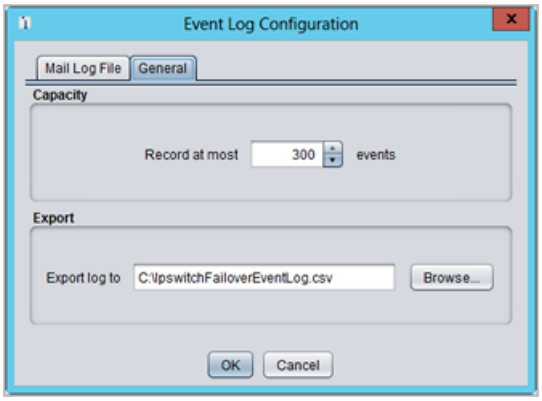

Figure 141: Event Log Configurations: General

The length of the event list can also be adjusted using the *Record At Most* option. The default is to record 300 events but changing the value increases or decreases the length of the log list accordingly. After the logs are configured, click **OK** to commit the changes.

Review Event Logs

The events that Ipswitch Failover logs are listed chronologically (by default) in the *Event Log* pane, the first log appears at the top and subsequent logs below it. The display order for the events can be sorted either descending or ascending by clicking on the column heading.

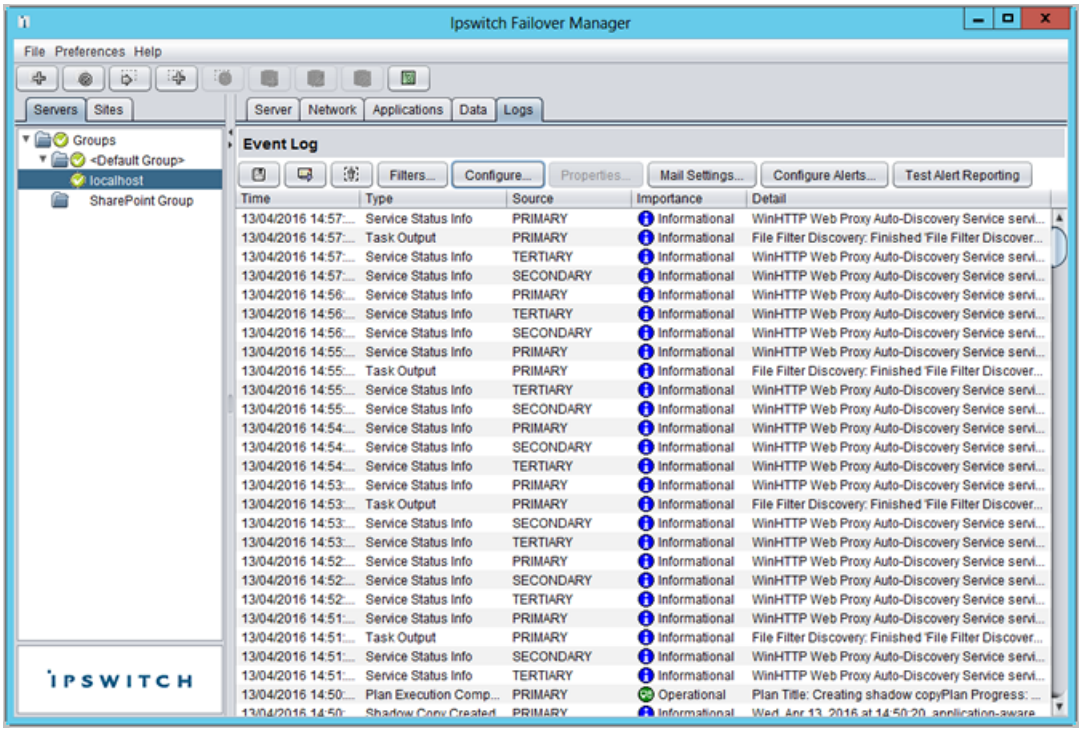

Figure 142: Event Log page

The events listed in the *Event Log* pane show the time the event happened, its importance, the type of event that triggered the log, and its detail.

Since the detail in the data grid is truncated, it may be necessary to review the log in more detail by double-clicking its entry in the pane.

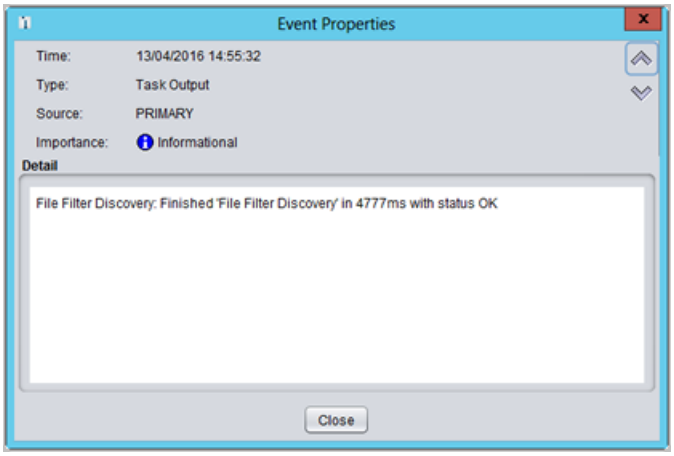

Figure 143: Event Log Properties

The **Event Properties** dialog gives the full detail and trace of the log that caused the event along with the source of the error aiding in troubleshooting. Further logs can be reviewed without having to close this window by using the **Up** and **Down** arrows of the dialog box to scroll through the list of logs. This can help identify the source of the problem when many simultaneous events occur. The **Event properties** dialog may be closed by clicking **Close**.

There are four categories of importance of events that Ipswitch Failover by default is configured to log:

Table 3: Ipswitch Failover Event Categories

Icon	*Definition*
	These are critical errors within the underlying operation of Ipswitch Failover and can be considered critical to the operation of the system.
	Warnings are generated where the system finds discrepancies within the Ipswitch Failover operational environment that are not deemed critical to the operation of the system.
	System logs are generated following normal Ipswitch Failover operations. Review these to verify the success of Ipswitch Failover processes such as file synchronization.
	Information events are similar to system logs but reflect operations carried out within the graphical user interface rather than operations carried out on the Ipswitch Failover Server service itself such as logging on etc.

The list of logs that Ipswitch Failover records may be filtered to hide less important logs by clicking **Filters** to invoke the **Event Log Filters** dialog, selecting the *Show Events of at Least* check box in the *Importance group*, selecting the importance level from the drop down list, and clicking **OK**. Only logs equal to or above the selected severity are displayed.

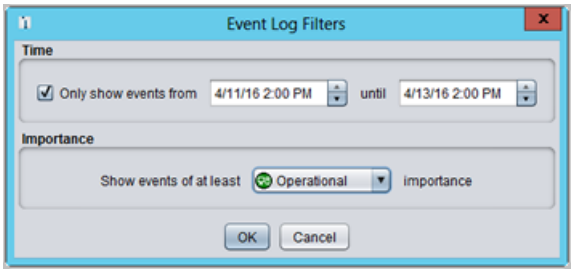

Figure 144: Event Log Filters

You can filter logs to display a subset of entries between a specific date and time range by selecting the *Only Show Events From* check box and adjusting the start and end date, time, and clicking **OK**.

Table 4: Event Log Buttons

Icon	*Definition*
	**Remove all entries from the event log** — Click to clear the list.
	**Export event log as comma-separated text** — Click to export the list to a comma separated variable file. Configure the data export file name and path through the **Event Log Configuration** dialog (click **Configure**).
	**Mail event log to recipients immediately** — Click to email the list to recipients immediately.

Appendix B

Troubleshooting

Two Active Servers

The occurrence of two active servers is not by design and when detected, must be resolved immediately. When there are two identical active servers live on the same network, Ipswitch refers to the condition as Split-brain syndrome.

Symptoms

Split-brain syndrome can be identified by the following symptoms:

1. Two servers in the Cluster are running and in an active state. This is displayed on the task bar icon as P/A (Primary and active) and S/A (Secondary and active).
2. An IP address conflict may be detected in a Cluster running Ipswitch Failover on the Public IP address.
3. A name conflict may be detected in a Cluster running Ipswitch Failover. In a typical WAN environment, the Primary and Secondary servers connect to the network using different IP addresses and no IP address conflict occurs. If the servers are running with the same name, then a name conflict may result. This happens only when both servers are visible to each other across the WAN.
4. Clients (for example, Outlook) cannot connect to the server running Ipswitch Failover.

Causes

Two active servers (Split-brain syndrome) can be caused by a number of issues. It is important to determine the cause of the Split-brain syndrome and resolve the issue to prevent reoccurrences of the issue. The most common causes of two active servers are:

- Loss of the Ipswitch Channel connection (most common in a WAN environment)
- The active server is too busy to respond to heartbeats
- Mis-configuration of the Ipswitch Failover software

Resolutions

After split-brain syndrome has occurred, the server with the most up-to-date data must be identified.

Note: *Identifying the wrong server at this point can result in data loss. Be sure to reinstate the correct server.*

The following can help identify the server with the most up-to-date data:

1. Review the date and time of files on both servers. The most up-to-date server should be made the active server.
2. From a client PC on a LAN, run `nbtstat -A 192.168.1.1` where the IP address is the Public IP address of your server. This can help identify the MAC address of the server currently visible to clients.

Note: *If the two active servers have both been servicing clients, perhaps at different WAN locations, one and only one server can be made active. Both servers contain recent data, which cannot be merged using Ipswitch Failover. One server must be made active and one server passive before restarting replication. After replication is restarted, ALL data on the passive server is overwritten by the data on the active server. It may be possible to extract the up-to-date data manually from the passive server prior to restarting replication. Consult the Microsoft knowledge base for information regarding various tools that may be used for this purpose. For further information, contact your Ipswitch Support representative.*

To Resolve Two Active Servers (Split-Brain Syndrome), perform the following steps:

1. Identify the server with the most up-to-date data or the server you prefer to make active.
2. Shutdown Ipswitch Failover on all servers (if it is running).
3. On the server you select to make passive, right-click the task bar icon, and select **Configure Server Wizard**.
4. Click the *Machine* tab and set the server role to passive.

Note: *Do not change the Identity of the server (Primary or Secondary).*

5. Click **Finish** to accept the changes. Reboot this server.
6. Start Ipswitch Failover (if required) and verify that the task bar icon now reflects the changes by showing **P**/**-** (Primary and passive) or **S**/**-** (Secondary and passive).
7. On the active server, right-click the task bar icon and select **Server Configuration Wizard**.
8. Click the *Machine* tab and verify that the server role is set to active.
9. Click **Finish** to accept the changes. Reboot this server.

Important: *As the server restarts, it connects to the passive server and starts replication. When this happens data on the passive server is overwritten by the data on the active server.*

10. Start Ipswitch Failover (if required) and verify that the task bar icon now reflects the changes by showing **P**/**A** (Primary and active) or **S**/**A** (Secondary and active).
11. Log into the Ipswitch Advanced Management Client .
12. Verify that the servers have connected and replication has started.

Two Passive Servers

The Primary and Secondary servers are both passive at the same time.

Symptoms

The first indication that Ipswitch Failover may be experiencing two passive servers is when users are unable to connect to protected applications. This situation can prove serious to your business, and must be addressed immediately. If you have already configured alerts, you are notified that replication is not functioning properly.

Causes

- Two passive servers generally results from some kind of sudden failure on the active server — for example, unexpected termination of the Ipswitch Failover R2 Service, a transient power failure, a server reset triggered from hardware power or reset buttons, or any other type of unclean shutdown. Following an unclean shutdown, an active server automatically assumes the passive role to isolate itself from the network until the failure can be investigated.
- The active server suffers a failure before completion of the handshake, which establishes the Ipswitch Channel. In this situation, the passive server has no way of detecting that the active server is not responding when the failure occurs - no channel connection was established, so it is impossible for the passive server to determine the condition of the active server. The active server may suffer a transient failure as described above; and the passive server cannot respond by failing over into the active role. This leaves both servers in the passive role.
- Both Primary and Secondary server experience a power outage simultaneously (for example, because they are using the same power source and neither is attached to a UPS). In this situation, a failover is not possible. When the servers are restarted, each displays the following error message: `Cannot start replication because previous run did not shutdown properly. Check configuration.`

> ***Note:*** *If an attempt is made to start Ipswitch Failover without reconfiguring one server as active, Ipswitch Failover responds with the warning:* `No active server amongst [PRIMARY, SECONDARY]`

Resolution

To resolve two passive servers, perform the following steps:

1. Determine which server to make active.
2. If Ipswitch Failover is running on either server, shut it down. Leave any protected applications running on the server you selected to make active.
3. On the server you selected to make active, open the **Configure Server Wizard**, and select the active role. Do NOT change the Identity (Primary / Secondary). Save the changes and exit the wizard.
4. On the server you selected to make passive, open the **Configure Server Wizard**, and confirm that the role is passive. Do NOT change the Identity (Primary / Secondary). Exit the wizard.
5. Reboot all servers. This ensures that all protected application services are stopped on the passive servers and started on the active server..
6. Start Ipswitch Failover on both servers.

Invalid Ipswitch Failover License

The Ipswitch Failover License is generated from the HBSIG of the host machine. This unique key is generated by examining the Fully Qualified Domain Name (FQDN), Machine SID, and software installed on the server. A valid license key must match the HBSIG.

Symptoms

During normal operations, you receive an error message stating your Ipswitch Failover License key has expired or Ipswitch Failover fails to start after rebooting the server or stopping Ipswitch Failover.

Causes

A license key can become invalid for any of the following reasons:

- Taking a server out of a domain and adding it to another domain.
- The Ipswitch Failover License has expired - If a licensing problem arises during an implementation, Ipswitch may provide a temporary or time-limited license so that the implementation can proceed. Temporary or time-limited licenses have a defined expiration date, and prevents Ipswitch Failover from starting when the date is exceeded.
- Windows Management Instrumentation (WMI) hung or not running. Ipswitch Failover uses WMI to validate the license on the Primary server and if WMI is hung or not running validation cannot complete.

Resolutions

1. If the invalid license error is due to changes in the domain status of the Primary server, or expiration of a temporary or time-limited Ipswitch Failover License key, simply generate request a new license key for the Primary server.
2. If the invalid license error is not due to expiration of a temporary or time-limited Ipswitch Failover License key, review the Windows Services and ensure that WMI is running. If WMI is running, stop the WMI Service, restart it, and then attempt to start Ipswitch Failover.

Synchronization Failures

When Ipswitch Failover is started, a Full System Check runs to ensure that:

- All protected Registry Keys and values from the active server are present on the passive servers.
- All protected File/Folder structures from the active server are present on the passive servers.

After the Full System Check finishes, the File System Status and the Registry Status should be in a *Synchronized* status. There may be cases when the File System Status or the Registry Status is shown as *Out-of-sync* or *Synchronized and busy processing*. Some of the cases are described below, with possible reasons and workarounds.

Services Running on the Passive Server

Symptoms

File System Status is *Out-of-sync* or *Synchronized and busy processing*.

Causes

A service that is running on the passive server may open a protected file for exclusive access. If Ipswitch Failover attempts to update a file which has been opened in this way, the following error is logged by the Apply component:

```
[N29]The passive Ipswitch Failover server attempted to access the file:
{filename}. This failed because the file was in use by another application.
Please ensure that there are no applications which access protected files
running on the passive.
```

Services that keep files locked on the passive server might be:

- Protected application services
- File-level anti-virus tool services
- The NNTP service in an Ipswitch Failover for IIS deployment (if the `\Inetpub` folder is shown as *Out-of-sync*)
- IISAdmin service in an Ipswitch Failover for IIS deployment (if `C:\WINDOWS\system32\inetsrv\MetaBase.xml` is shown as *Out-of-sync*). IISAdmin service starts on the passive after a reboot of the server and must be stopped manually.

Resolutions

Until the file is closed on the passive server, Ipswitch Failover reports that the file's status, and hence the *File System Status*, is *Out-of-sync*.

To resolve an *Out-of-sync* system status, take the actions below:

1. Ensure Protected Application services are set to *Manual* on both servers and that they are not running on the passive server(s).
2. Ensure that the *Recovery Actions* set from the Service Control Manager (SCM) for the Protected Application services are *Take No Action* (otherwise, the Protected Application services are restarted by the SCM).
3. Ensure that file-level anti-virus is not part of the protected set as the file-level anti-virus and the corresponding services are running on both servers.
4. Ensure the NNTP service is not running on the passive server in an Ipswitch Failover for IIS deployment (if `\Inetpub` folder is shown as *Out-of-sync*). This is valid for some of the Exchange implementations as well, where IIS Admin is protected.
5. Ensure that IISAdmin is not running on the passive server in an Ipswitch Failover for IIS deployment (if `C:\WINDOWS\system32\inetsrv\MetaBase.xml` is *Out-of-sync*) if IISAdmin service is started on the passive.

Ipswitch Channel Incorrectly Configured

Symptoms

If the Ipswitch Channels are not properly configured, they cannot initiate the handshake to establish communications through the channel connection. Failure to establish the channel connection prevents a Full System Check and leaves the File System Status and Registry Status as *Out-of-sync*.

Causes

The most common Ipswitch Channel configuration errors are:

- Channel IP addresses configured in different subnets (in LAN configurations)
- In a WAN configuration, no static routes between the channel NICs

Resolutions

To resolve an Ipswitch Channel configuration error:

1. Verify that channel IP addresses are properly configured.

2. In a WAN configuration, verify that static routes between channel NICs are properly configured.

3. Ensure that NetBIOS settings on the channel NICs have been disabled.

Incorrect or Mismatched Disk Configuration

Common disk configuration errors which may affect a Cluster:

Symptoms

When Ipswitch Failover starts, the complete set of File Filters is checked for consistency. If any of the entries points to a non-existent drive letter or to a non-NTFS partition, the list of File Filters is reset to the default value of `C:\Protected\**`. This is a safety measure; Ipswitch Failover requires the same drive letter configuration on the Primary and Secondary servers, and only supports protection of NTFS partitions.

Causes

Different partition structures on the Primary and Secondary servers, resulting in one or more file filters pointing to drives which cannot be protected on all servers. For example:

- The Primary server has drive `G:`, which is a valid NTFS partition; but there is no corresponding drive on the Secondary server
- The Primary server has drive `G:`, which is a valid NTFS partition; but the equivalent drive on the Secondary server is a CD / DVD drive or a FAT / FAT32 partition, which cannot be protected by Ipswitch Failover.

In either case, if a file filter is configured to protect a directory on drive `G:`, the entire filter set is rejected and the filters are reset to the default value of `<Windows drive>\Protected\**`

Resolutions

If this occurs, follow the steps documented in IKB-500 — The set of File Filters is reset to C:\Protected**. What should I do next?

The Passive Server has Less Available Space than the Active Server

Free up some additional disk space on the passive server. Make sure you are not deleting data from the protected set as you might lose data in the event of a switchover. This may require you to update the disk subsystem on the passive server. When complete, you must manually start replication.

Symptoms

Replication stops and the following error is reported:

```
[N27]Failed to write information for the file: {filename} to the disk.
Either the disk is full or the quota (for the SYSTEM account) has been
exceeded.
```

Causes

The passive server has less available disk space than the active server and this prevents replication of updates to the passive server because the quantity of updates from the active server exceeds the available disk space on the passive server.

Resolution

Free up some additional disk space on the passive server. Make sure you are not deleting data from the protected set as you might lose data in the event of a switchover. This may require you to update the disk subsystem on the passive server. When complete, you must manually start replication.

Unprotected File System Features

Symptoms

Another possible reason why Ipswitch Failover cannot synchronize certain files or directories is the presence in the replication set of so-called “unprotected” file system features.

The default behavior for Ipswitch Failover in the presence of Unprotected Features from category 2 (Extended Attributes and file encryption) is to log an error and set the File System Status to *Out-of-sync*. If these types of files are present in the replication set, replication continues, but the system remains *Out-of-sync*.

Causes

Ipswitch Failover does not synchronize if the replication set contains files with unprotected file system features. Unprotected file system features are described by category in IKB-321 — Ipswitch for File Server: Unprotected Features of the Windows 2008 File System.

Resolutions

Two methods of dealing with these Unprotected Features are described in IKB-321 — Ipswitch for File Server: Unprotected Features of the Windows 2008 File System. If these features are not essential for the normal operation of your file system, zipping and unzipping the affected files within their parent directory removes the Unprotected Features, allowing the Ipswitch Failover to synchronize the file system.

Registry Status is Out-of-Sync

The Registry may be reported as Out-of-Sync when one or more Registry keys fail to synchronize. There are at least two possible reasons.

Resource Issues

Symptoms

Ipswitch Failover logs the following error message:

```
Call to RegOpenKeyEx failed: on <Reg_Key> : Insufficient system resources
exist to complete the requested service
```

Causes

One or both of the servers are running low on virtual memory.

Resolutions

This is usually a sign that the server does not have enough virtual memory left. Restart the server to correct this problem.

Registry Security Issues

Symptoms

Ipswitch Failover is unable to read/sync/replicate the registry.

Causes

If a protected registry key has permissions that deny Write access to the System account, Ipswitch Failover may be unable to synchronize or replicate it.

Resolutions

Change the permissions on the affected registry key to grant the System account *Full Control*.

Channel Drops

Performance Issues

Symptoms

The message `java.io.IOException: An existing connection was forcibly closed by the remote host` appears in the active server's `NFLog.txt` file, and the channel connection between the servers is lost.

Causes

This condition is unusual and generally points to an application, or Windows itself, experiencing a fault on one of the passive servers. The most likely issue here is a sudden reboot / restart of the passive server and may be due to one of the following causes:

- The server is configured for automatic software update management and some updates force a server reboot.
- There is a software or Operating System issue which occasionally results in a BSOD and system restart.
- The Ipswitch Failover R2 service itself experiences problems and may hang or terminate unexpectedly.

Resolutions

- Determine the likely source of the hang or reboot by examining the Windows event logs.
- Alternatively, if the server does not show any evidence of a system restart or application hang, the issue may be due to one or both of the channel NICs forcing a channel disconnection.

Passive Server Does Not Meet Minimum Hardware Requirements

Symptoms

The data rate between the servers is very high during a Full System Check and the channel drops.

Causes

A The passive server does not meet the recommended hardware requirements for Ipswitch Failover or it meets them but is much less powerful than the other server(s) in the Cluster. The underpowered server cannot apply the received replication data from the active or passive server at the rate that the data is sent to the is passive server

Resolutions

To avoid reinstalling your Ipswitch Failover solution, it is best to tackle this issue by upgrading the hardware (for example, memory and or CPU) on the passive server. It is important to establish the identity (Primary or Secondary) of the affected server before you perform the upgrade.

Hardware or Driver Issues on Channel NICs

Symptoms

The Ipswitch Channel drops or disconnects and reconnects intermittently.

Causes

- Old/wrong drivers on the channel NICs
- If the physical connection used for the Ipswitch Channel connection uses a hub or Ethernet switch, a hardware fault may cause the channel to drop
- Defective Ethernet patch or crossover cables
- Improper configuration of the NICs used for the channel connection
- ISP problems in a WAN environment

Resolutions

1. Verify that channel NIC drivers are the correct/latest versions. This is a known issue with HP/Compaq ProLiant NC67xx/NC77xx Gigabit Ethernet NICs but may affect other NIC types as well. See IKB-116 — Ipswitch Failover and Gigabit Ethernet NIC drivers. (NC77XX).
2. Verify hubs and Ethernet switches are operating properly. Identify and replace any defective components.
3. Test for defective Ethernet patch or crossover cables and replace if defective.
4. Correctly configure the NICs used for the channel connection.
5. Verify the physical link to identify any ISP problems.

Firewall Connection

In both a LAN or WAN deployment of Ipswitch Failover, the channel may be connected via one or more Internet firewalls. Since firewalls are intended to block unauthorized network traffic, it is important to ensure that any firewalls along the route of the channel are configured to allow channel traffic.

Symptoms

The Ipswitch Channel cannot connect or connects and disconnects continuously.

Causes

In a WAN deployment, port #57348 (or any other port configured for the Ipswitch Channel) is closed on one or more firewalls on the route between the channel NIC on the active server and its counterpart on the passive server.

Resolutions

Open port #57348 (and any other port configured for the Ipswitch Channel) on all firewalls on the route between the channel NIC on the active server and its counterpart on the passive server.

Incorrect Ipswitch Channel Configuration

Symptoms

IP conflicts are encountered on one of the channel IP addresses. The Ipswitch Channel does not connect or connects and disconnects.

Causes

Identical IP addresses at each end of the channel, IP addresses in different subnets without static routing at each end of the channel, or a channel NIC configured for DHCP when a DHCP server is not available.

During installation, Ipswitch Failover configures the channel NICs with user provided information. Providing incorrect information or incorrectly modifying the channel NIC configuration after installation can cause the Ipswitch Channel to fail communicating.

On rare occasions, if the servers in a Cluster have NICs of the same type in a different order, both the name and IP address of a channel NIC on the Primary server may be transferred to the Public NIC on the Secondary server; or the name and IP address of the Public NIC may be transferred to a channel NIC. If this happens, it can be hard to reconcile the names of the NICs with their physical identities, making it difficult to assign the correct IP address to each NIC on the Secondary server.

Resolution

It is part of the normal Ipswitch Failover installation process to manually assign the correct IP addresses to each NIC on the Secondary server. If there is no channel connection between the servers, verify that the IP addresses on the Secondary server's channel NICs are correctly configured. Verify the settings for the Public NIC, since any configuration error here may not be apparent until a switchover is performed or a failover occurs.

It is possible to capture the identities of all of the NICs on the Secondary server prior to installing Ipswitch Failover, by opening a Windows Command Prompt on that server and executing the following command:

```
ipconfig /all > ipconfig.txt
```

This saves the current name, TCP/IP configuration, and MAC address of each NIC on the Secondary server to a file called `ipconfig.txt`, which is present on the server after the Plug and Play phase of the Ipswitch Failover install is complete. At this point, it is possible to compare the pre-install and post-install state of each NIC by running `ipconfig /all` from a Windows command prompt and comparing the output of this command with the content of the file `ipconfig.txt`. The MAC address of each NIC is tied to the physical identity of each card, and never changes - so it is possible to identify each NIC by its MAC address and determine its original name and network configuration, even if these have been updated by the Plug and Play process.

Subnet/Routing Issues — In a LAN

Symptoms

The Ipswitch Channel disconnects or fails to connect in a LAN deployment.

Causes

The Ipswitch Channel may disconnect or fail to connect due to the Public NIC and/or one or more channels sharing the same subnet.

Resolutions

If Ipswitch Failover is deployed in a LAN environment, the Public IP address and the channel IP address on a server should be in separate subnets. If there are multiple redundant channels, each should have its own subnet. Verify the network configuration for each NIC and correct any issues.

Subnet/Routing Issues — In a WAN

Symptoms

The Ipswitch Channel disconnects or fails to connect in a WAN deployment.

Causes

When the Ipswitch Channel disconnects or fails to connect in a WAN deployment it may be because the static route is not configured or is configured incorrectly.

When Ipswitch Failover is deployed in a WAN, it is generally not possible for the Public IP address and the channel IP addresses to be in different subnets, since there is usually a single network path between the two

servers. To ensure that channel traffic is routed only between the endpoints of the channel, it is necessary to configure a static route between these endpoints.

Resolutions

Refer to IKB-466 — How to Create a Static Route for the Ipswitch Channel Connection where the channel and Principal Public) IP addresses are on the same subnet in a WAN environment, for a detailed discussion about WAN channel routing issues, and for instructions on how to configure a static route for the Ipswitch Channel.

MaxDiskUsage Errors

Disk Usage and Disk Quota Issues

Ipswitch Failover uses queues to buffer the flow of replication data from the active server to the passive server. This configuration provides resilience in the event of user activity spikes, channel bandwidth restrictions, or channel drops (which may be encountered when operating in a WAN deployment). Some types of file write activity may also require buffering as they may cause a sharp increase in the amount of channel traffic. The queues used by Ipswitch Failover are referred to as either the send queue or the receive queue with each server in the Cluster maintaining both a send queue and receive queue for each channel connection.

Send Queue

Ipswitch Failover considers the send as 'unsafe' because the data in this queue is awaiting replication across the channel to the passive server and is vulnerable to loss in the event of a failover. As a result of failover, some data loss is inevitable, with the exact amount depending upon the relationship between current channel bandwidth and the required data transmission rate. If the required data transmission rate exceeds current channel bandwidth, the send queue fills; if the current channel bandwidth exceeds the required data transmission rate, the send queue empties. This situation is most commonly seen in a WAN environment, where channel bandwidth may be restricted. In a LAN with normally high bandwidth on a dedicated channel, the size of the send queue is zero or near zero most of the time.

Note: *On a server that is not protected with Ipswitch Failover, all data is technically 'unsafe' because it is possible to lose all data if the server fails.*

Receive Queue

The target queue on the passive server is called the receive queue and is considered safe. Ipswitch Failover considers the receive queue safe because the data in this queue has already been transmitted across the channel from the active to the passive server, and is not lost in the event of a failover, since all updates to the passive server are applied as part of the failover process.

The queues (on both servers) are stored on-disk, by default in the `<Ipswitch Failover Install Directory>\R2\log`, with a quota configured for the maximum permitted queue size (by default, 10 GB on each server). Both the queue location and the quota are configurable.

There are two ways to set the queue size:

- With Ipswitch Failover started, open the Ipswitch Advanced Management Client and select **Data: Traffic/Queues**. Click the **Configure** button. Configure the value for the *Max Disk Usage* and click **OK**. It is necessary to shut down and restart Ipswitch Failover (specify that the stopping of protected applications is not necessary) for the change to take effect.
- With Ipswitch Failover shut down on the active server, open the **Configure Server Wizard** and select the *Logs* tab. Set the value of *Maximum Disk Usage* and click **Finish**.

Note: *Ipswitch Failover is a symmetrical system, and can operate with either server in the active role. For this reason, the queue size is always set to the same value for both servers.*

MaxDiskUage Errors

If Ipswitch Failover exceeds its pre-configured queue size, it reports an error message. There are several possible reasons for this, with the most common ones shown below.

When Ipswitch Failover reports `[L9] Exceeded the maximum disk usage (NFChannelExceededMaxDiskUsageException)`, the following conditions exist:

- On the active server, it indicates that the size of the send queue has exceeded the disk quota allocated for it.
- On a passive server, it indicates that the size of the receive queue or send queue has exceeded the disk quota allocated for it.

Neither of these conditions is necessarily fatal, or even harmful; but it is important to try to determine the sequence of events, which led to the condition appearing in the first place.

[L9]Exceeded the Maximum Disk Usage on the ACTIVE Server

Symptoms

Replication stops and restarts or stops completely (if the event occurs while a Full System Check is in progress) and the Ipswitch Failover *Event Log* displays the error `[L9]Exceeded the maximum disk usage`, originating from the ACTIVE server.

Causes

As stated previously, if there is a temporary interruption in the Ipswitch Channel, or there is insufficient channel bandwidth to cope with the current volume of replication traffic, the send queue may begin to fill. If the situation persists, the size of the queue may eventually exceed the configured disk quota.

Resolutions

Assuming there are no other channel connection issues (see IKB-992 — Ipswitch Channel Drops) you can increase the amount of disk space allotted to the queues to prevent this situation recurring. The default setting is 10 GB, which may be insufficient on servers with a large volume of replication traffic and/or limited channel bandwidth. If you have sufficient disk space, set the queue size to zero (unlimited). This allows Ipswitch Failover to utilize any free disk space to store the queues.

[L9]Exceeded the Maximum Disk Usage on a PASSIVE Server

Symptoms

Replication stops and restarts or stops completely (if the event occurs while a Full System Check is in progress) and the Ipswitch Failover *Event Log* displays the error `[L9]Exceeded the maximum disk usage`, originating from a PASSIVE server.

Causes

- In this situation, the bottleneck lies between the Ipswitch Channel NIC and the disk subsystem on a passive server. When replication traffic passes across the channel faster than it can be written to disk on the passive server, it is buffered temporarily in the passive server's receive queue. As before, if this situation persists, the size of the queue may eventually exceed the disk quota allotted.

- If the passive server is much less powerful than the active server, in terms of processor speed, RAM or disk performance, it may lag behind the active server during periods of high replication activity. If you suspect this is the case, it may be useful to monitor one or more Windows performance counters to determine which component is experiencing sustained high activity. Intensive page file use or persistently large disk queue length may indicate a problem, which can be solved by upgrading one or more physical components of the server.
- Note that any server can be active or passive. If the Secondary server is more powerful than the Primary server, hardware-related issues might only occur while the Secondary server is in the active role.

Resolutions

If you have multiple physical disks on each server, it may be worth locating the Ipswitch Failover send and receive queues on a separate physical disk, away from the Windows directory, the Windows page file, and any protected files to help alleviate disk performance issues. To do this:

1. Shut down Ipswitch Failover.
2. Open the **Server Configuration Wizard** and select the *Logs* tab.
3. Set the intended path for *Message Queue Logs Location* and click **Finish**.
4. Start Ipswitch Failover on all servers.

> ***Note:*** *The selected path is applicable only to the specific server where the change was performed.*

5. You may alleviate the symptoms of this problem by simply increasing the amount of disk space allotted to the queues. If you have reason to suspect that a hardware issue is the root of the problem, it is better to correct that problem at the source if possible.
6. It is also possible for the size of the receive queue to increase sharply in response to certain types of file write activity on the active server. This is most obvious when Ipswitch Failover is replicating a large number of very small updates (typically a few bytes each) - the volume of update traffic may be far greater than the physical size of the files on the disk, and so the receive queue in particular may become disproportionately large. This pattern of disk activity is often seen during the population of Full-Text Catalogs in Microsoft SQL Server.
7. Increase the amount of disk space available for the queues, as described above; it may be also help to alleviate the issue by moving the queues to their own physical disk, or upgrading memory or the disk subsystem.
8. Ipswitch Failover requires a certain amount of system resources for its own basic operations and requires some additional resources for processing replication traffic. This is in addition to the resources used by Windows and other applications running on the server (including critical applications protected by Ipswitch Failover). It is always a good idea to ensure that there are sufficient resources for all of the applications and services running on such a server to provide maximum performance, stability, and resilience in the face of changing client, server, and network activity.

[L20]Out of disk space (IPChannelOutOfDiskSpaceException)

Symptoms

Replication stops and the Ipswitch Failover *Event Log* displays the error `[L20]Out of disk space`, originating from either server.

Causes

This is similar to the `[L9]Exceeded the maximum disk usage` scenario, with one important difference - one of the queues has exceeded the amount of physical disk space available for it, without reaching its quota limit. So, for example, if the maximum queue size is set to 10 GB, but only 3 GB of physical disk space remains, this message is reported if one of the queues exceeds 3 GB in size.

Resolutions

The strategy for dealing with this is simple - it is necessary either to free up more disk space, or to move the queues to a disk with sufficient free space to accommodate queue sizes up to the limit configured for Maximum Disk Usage.

Application Slowdown

Any piece of software installed on a server or workstation consumes a finite amount of system resources when it runs, and it must share the resources it uses with any other applications, which are running at the same time. If the total resource requirement for the applications exceeds the available physical resources, the operating system gracefully attempts to provide resources but some applications may be under-resourced. This may mean that an application cannot obtain enough memory to operate normally, or that a process is required to wait to access the hard disk.

In a situation where applications are competing for resources, it is likely that one or more applications suffer from poor performance. Operations performed by the application may take longer than usual to complete, and in turn, may affect the time required to log in to a remote client, or to open or save a file. This is true for both servers running Ipswitch Failover and for servers running any other application. Ipswitch Failover is able to monitor system performance counters and provide warnings if predefined thresholds are exceeded, but it does not actively manage system resources for other applications. Like any other application, it also requires a finite amount of resources for its own operations in addition to the resources used by the operating system and the protected application.

It is very important to ensure that the machines hosting Ipswitch Failover meet recommended hardware requirements and are powerful enough to cope with the load imposed by Ipswitch Failover, the protected application, and any other critical applications. Ipswitch SCOPE Data Collector Service provides users with the information to make this decision at install time, and can monitor server performance while Ipswitch Failover is running.

Poor Application Performance

Symptoms

The servers are unable to accommodate the load placed upon them during normal operation.

Causes

This may be due to the active server's resource usage in one or more areas being close to the maximum possible before Ipswitch Failover was installed.

Resolutions

Ipswitch SCOPE Data Collector Service is designed to report on these types of conditions, and can provide warnings if CPU usage or memory usage exceeds a certain percentage of the available resource. The information provided by Ipswitch SCOPE Data Collector Service means that the risk of application slowdown could be minimized by performing any recommended hardware upgrades on the active server before Ipswitch Failover is installed.

Servers Could Accommodate the Initial Load but the Load has Increased

Symptoms

Application response times have slowed in response to increased user activity.

Causes

It is also possible that the servers may be able to operate normally when Ipswitch Failover is first installed, with performance decreasing because of an increase in user activity - for example, the number of users on your Exchange system may increase, or the typical usage pattern for a user may become more intense. This may be a gradual and sustained increase over time; or it may be transient if some specific event triggers a temporary surge in user activity.

Resolution

If the situation is sporadic, it may correct itself when the load decreases. If the increase is sustained and permanent, it may be necessary to upgrade the server hardware to compensate.

One Server is Able to Cope, but the Other Cannot

Symptoms

Applications operate normally when the Primary server is active but slow when the Secondary server is active (or vice versa).

Causes

If there is a large discrepancy in the processing power between the servers, it may be that one of the servers can handle the operational load, and the other cannot. The load on a server is generally higher when it is in the active role and the protected application(s) started, so it is possible that applications run successfully when the Primary server is active, but may experience performance issues when the Secondary is active (or vice-versa). Problems may arise even when the more powerful server is active, such as when resource intensive tasks are running.

Resolutions

It is good practice to ensure that all servers have approximately equivalent processing power, RAM and disk performance. It may be necessary to upgrade the hardware so that servers have roughly the same performance.

Scheduled Resource Intensive Tasks

Symptoms

Resource-intense scheduled tasks impact performance at certain times.

Causes

System performance may be fine until two or more resource-hungry processes run simultaneously; or, one process may perform actions, which increase the load on Ipswitch Failover by triggering additional (and sometimes unnecessary) replication traffic. Typical examples might be processes such as backups, database maintenance tasks, disk defragmentation or scheduled virus scans.

Resolution

As far as possible, it is good practice to schedule such operations so that they do not overlap, and to schedule them outside regular working hours, when the load imposed on the server by users accessing the protected application is likely to be smaller.

Appendix C

Ipswitch SCOPE Data Collector Service Overview

Using Ipswitch SCOPE Data Collector Service

Daily Usage

The Ipswitch SCOPE Data Collector Service collects configuration and performance data for pre-implementation analysis, license key generation, and assisting in support of Ipswitch Failover.

The Ipswitch SCOPE Data Collector Service runs as a service that requires no user intervention to log daily configuration and performance data. There is no need for any day-to-day user interaction with Ipswitch SCOPE Data Collector Service. Log files can be collected and sent to Ipswitch Support for analysis if desired.

Collecting Log Files

The Ipswitch SCOPE Data Collector Service can be used both pre and post implementation of Ipswitch.

Pre-Implementation

Ipswitch SCOPE Data Collector Service maintains a single file which is needed to obtain a pre-implementation report and to generate a license key. The data file created by Ipswitch SCOPE Data Collector Service may be available as soon as 15 minutes after installing the collector service, but on systems with many shared files and folders the collection process can take an hour or more. If you require a full performance report you should wait at least 24 hours before collecting the file and sending it to Ipswitch Support. The file contains the latest configuration data and the most recent 24 hours worth of performance data.

Post-Implementation

To receive configuration or performance analysis you must collect the `Candidate for Upload files` and manually forward to Ipswitch Support for analysis and report creation.

Configuring Ipswitch SCOPE Data Collector Service

The SCOPE Configuration Tool

Ipswitch strongly recommends contacting Ipswitch Support staff to change these settings.

Procedure

- To use the SCOPE Configuration Tool, select **Start** > **All Programs** > **Ipswitch** > **SCOPE** > **SCOPE Configuration Tool**.

  The SCOPE Configuration Tool opens in a new window.

The SCOPE Configuration Tool consists of two tabs: **General** and **Data Files** The features of each tab are described in the associated sections of this document.

Additionally, a link to *Ipswitch SCOPE Data Collector ServiceOnline Help* can be found in the lower left corner of the window.

Configure the General tab

. The **General** tab allows you to start the Ipswitch SCOPE Data Collector Service Windows service, to upload collected Ipswitch SCOPE Data Collector Service data, to download configuration settings from the and to locate the `.CAB` file for manual uploading.

Procedure

1. Select the **General** tab.

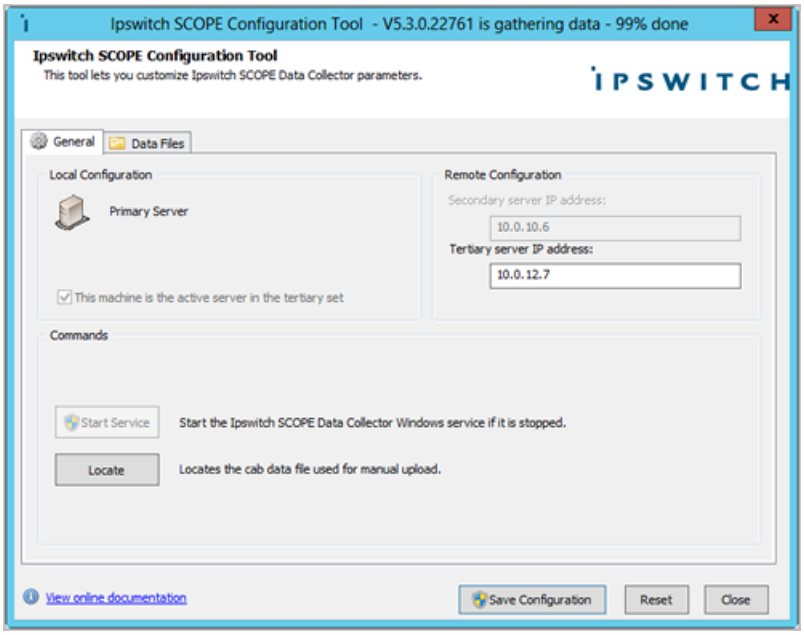

Figure 145: SCOPE Configuration Tool - General tab

Option	Description
Start Service	Starts the Ipswitch SCOPE Data Collector Service Windows service if it is stopped.
Locate	Locates the `.cab` files for manual upload.

When you click **Upload**,Ipswitch SCOPE Data Collector Service gathers all data. Do not close the application until it has finished gathering the data. After all data is gathered, Ipswitch SCOPE Data Collector Service uploads it.

2. After making configuration changes, click **Save Configuration** to save your changes, or click **Reset** to restore the default configuration.

Configure the Data Files tab

The *Data Files* section allows you to configure the file locations for Ipswitch SCOPE Data Collector Service.

Procedure

1. Select the **Data Files** tab.

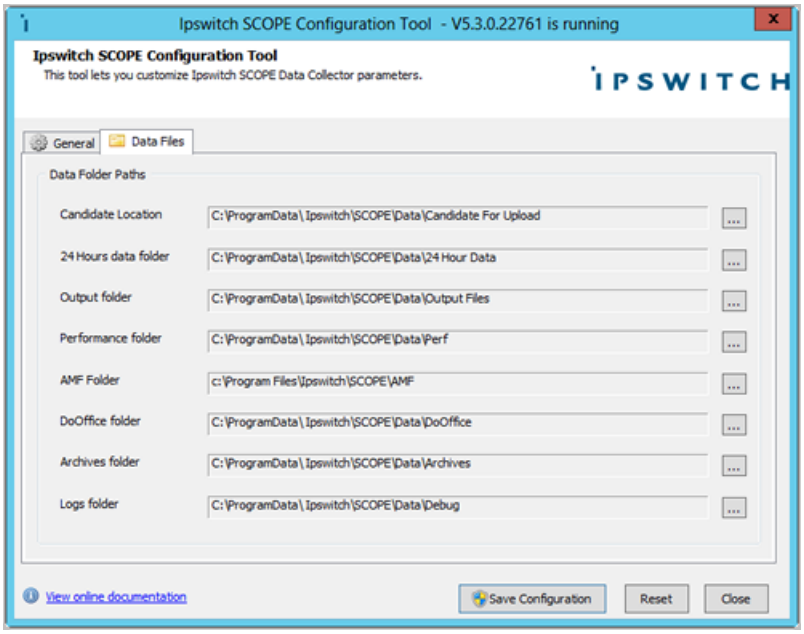

Figure 146: SCOPE Configuration Tool - Data Files tab

   Use the **Data Files** page to change the location where data files are stored.

2. After making configuration changes, click **Save Configuration** to save your changes, or click **Reset** to restore the default configuration.

Glossary

Active

The functional state or role of a server when it is visible to clients through the network, running protected applications, and servicing client requests.

Active Directory (AD)

Presents applications with a single, simplified set of interfaces so users can locate and use directory resources from a variety of networks while bypassing differences between proprietary services. Ipswitch Failover switchovers and failovers require no changes to AD resulting in switchover/failover times typically measured in seconds.

Active–Passive

The coupling of two servers with one server visible to clients on a network and providing application service while the other server is not visible and not providing application service to clients.

Advanced Configuration and Power Interface (ACPI)

A specification that dictates how the operating system can interact with the hardware especially where power saving schemes are used. The Primary, Secondary, and Tertiary servers must have identical ACPI compliance.

Alert

A notification provided by Ipswitch Failover sent to a user or entered into the system log indicating an exceeded threshold.

Asynchronous

A process whereby replicated data is applied (written) to the passive server independently of the active server.

Basic Input/Output System (BIOS)

The program a personal computer's microprocessor uses to get the computer system started after you turn it on. It also manages data flow between the computer's operating system and attached devices such as the hard disk, video adapter, keyboard, mouse, and printer.

Cached Credentials

Locally stored security access credentials used to log into a computer system when a Domain Controller is not available.

Channel Drop

An event in which the dedicated communications link between servers fails, often resulting in the passive server becoming active and consequently creating a split-brain syndrome.

Channel NIC (Network Interface Card)

A dedicated NIC used by the Ipswitch Channel.

Checked

The status reported for user account credential (username/password) validation.

Cloned Servers

Servers that have identical configuration settings, names, applications, Security Identifiers (SIDs) and IP addresses, following the installation of Ipswitch Failover.

Cloning Process

The Ipswitch Failover process whereby all installed programs, configuration settings, and the machine name, Security Identifier (SID), and IP addresses are copied to another server.

Cluster

A generic term for an Ipswitch Failover Pair or Trio and the set of machines (physical or virtual) involved in supporting a single protected server. An Ipswitch Failover Cluster can include the machines used in a VMware or Microsoft cluster.

Connection

Also referred to as Cluster Connection. Allows the Failover Management Service to communicate with an Ipswitch Failover Cluster, either on the same machine or remotely.

Crossover Cable

A network cable that crosses the transmit and receive lines.

Data Replication

The transmission of protected data changes (files and registry) from the active to the passive server via the Ipswitch Channel.

Data Rollback Module

An Ipswitch Failover module that allows administrators to rollback the entire state of a protected application, including files and registry settings, to an earlier point-in-time. Typically used after some form of data loss or corruption.

Degraded

The status reported for an application or service that has experienced an issue that triggered a Rule.

Device Driver

A program that controls a hardware device and links it to the operating system.

Disaster Recovery (DR)

A term indicating how you maintain and recover data with Ipswitch Failover in event of a disaster such as a hurricane or fire. DR protection can be achieved by placing the Secondary server at an offsite facility, and replicating the data through a WAN link.

DNS (Domain Name System) Server

Provides a centralized resource for clients to resolve NetBIOS names to IP addresses.

Domain

A logical grouping of client server based machines where the administration of rights across the network are maintained in a centralized resource called a domain controller.

Domain Controller (DC)

The server responsible for maintaining privileges to domain resources; sometimes called AD controller in Windows 2003 and above domains.

Dualed

A way to provide higher reliability by dedicating more than one NIC for the Ipswitch Channel on each server.

Failover

Failover is the process by which the passive server assumes the active role when it no longer detects that the active server is alive as a result of a critical unexpected outage or crash of a server.

Full System Check (FSC)

The internal process automatically started at the initial connection or manually triggered through the Manage Server GUI to perform verification on the files and registry keys and then synchronize the differences.

Fully Qualified Domain Name (FQDN)

Also known as an absolute domain name, a FQDN specifies its exact location in the tree hierarchy of the Domain Name System (DNS). It specifies all domain levels, including the top-level domain, relative to the root domain. Example: somehost.example.com., where the trailing dot indicates the root domain.

Global Catalog

A global catalog is a domain controller that stores a copy of all Active Directory objects in a forest. The global catalog stores a full copy of all objects in the directory for its host domain and a partial copy of all objects for all other domains in the forest.

Graceful (Clean) Shutdown

A shutdown of Ipswitch Failover based upon completion of replication by use of the Failover Management Service, resulting in no data loss.

Group

An arbitrary collection of Ipswitch Failover Clusters used for organization.

Hardware Agnostic

A key Ipswitch Failover feature allowing for the use of servers with different manufacturers, models, and processing power in a single Ipswitch Failover Cluster.

Heartbeat

The packet of information issued by the passive server across the channel, which the active server responds to indicating its presence.

High Availability (HA)

Keeping users seamlessly connected to their applications regardless of the nature of a failure. LAN environments are ideally suited for HA.

Hotfix

A single, cumulative package that includes one or more files that are used to address a problem in a product.

Identity

The position of a given server in the Ipswitch Failover Cluster: Primary, Secondary, or Tertiary.

Install Clone

The installation technique used by Ipswitch Failover to create a replica of the Primary server using NTBackup or Wbadmin and to restore the replica to the Secondary and/or Tertiary servers.

Ipswitch Channel

The IP communications link used by the Ipswitch Failover system for the heartbeat and replication traffic.

Ipswitch Failover

The core replication and system monitoring component of the Ipswitch solution.

Ipswitch License Key

The key obtained from Ipswitch, Inc. that allows the use of components inIpswitch Failover; entered at install time, or through the Configure Server Wizard.

Ipswitch Pair

Describes the coupling of the Primary and Secondary servers in an Ipswitch Failover solution.

Ipswitch Plug-ins

Optional modules installed into an Ipswitch Failover server to provide additional protection for specific applications.

Ipswitch SCOPE

The umbrella name for the Ipswitch process and tools used to verify the production servers health and suitability for the implementation of an Ipswitch solution.

Ipswitch SCOPE Report

A report provided upon the completion of the Ipswitch SCOPE process that provides information about the server, system environment, and bandwidth.

Ipswitch Switchover/Failover Process

A process unique to Ipswitch Failover in which the passive server gracefully (switchover) or unexpectedly (failover) assumes the role of the active server providing application services to connected clients.

Ipswitch Trio

Describes the coupling of the Primary, Secondary, and Tertiary servers into an Ipswitch solution.

Low Bandwidth Module (LBM)

An Ipswitch Failover module that compresses and optimizes data replicated between servers over a WAN connection. This delivers maximum data throughput and improves application response time on congested WAN links.

Machine Name

The Windows or NETBIOS name of a computer.

Management IP Address

An additionally assigned unfiltered IP address in a different subnet than the Public or Ipswitch Channel IP addresses used for server management purposes only.

Many-to-One

The ability of one physical server (hosting more than one virtual server) to protect multiple physical servers.

Network Monitoring

Monitoring the ability of the active server to communicate with the rest of the network by polling defined nodes across the network at regular intervals.

Pair

See Ipswitch Failover Pair above.

Passive

The functional state or role of a server when it is not delivering service to clients and is hidden from the rest of the network.

Pathping

A route-tracing tool that works by sending packets to each router on the way to a final destination and displays the results of each hop.

Plug-and-Play (PnP)

A standard for peripheral expansion on a PC. On starting the computer, PnP automatically configures the necessary IRQ, DMA and I/O address settings for the attached peripheral devices.

Plug-in

An application specific module that adds Ipswitch Failover protection for the specific application.

Pre-Clone

An installation technique whereby the user creates an exact replica of the Primary server using VMware vCenter Converter or other 3rd party utility prior to the initiation of installation and uses the replica as a Secondary and or Tertiary server.

Pre-Installation Checks

A set of system and environmental checks performed as a prerequisite to the installation of Ipswitch Failover.

Primary

An identity assigned to a server during the Ipswitch Failover installation process that normally does not change during the life of the server and usually represents the production server prior to installation of Ipswitch Failover.

Protected Application

An application protected by the Ipswitch Failover solution.

Public IP Address

An IP address used by clients to contact the server through drive mappings, UNC paths, DNS resolved paths, etc. to gain access to the server's services and resources.

Public Network

The network used by clients to connect to server applications protected by Ipswitch Failover.

Public NIC

The network card which hosts the Public IP address.

Quality of Service (QoS)

An effort to provide different prioritization levels for different types of traffic over a network. For example, Ipswitch Failover data replication may have a higher priority than ICMP traffic, as the consequences of interrupting data replication are more obvious than slowing down ICMP traffic.

Receive Queue

The staging area on a passive server used to store changes received from another server in the replication chain before they are applied to the disk/registry on the passive server.

Remote Desktop Protocol (RDP)

A multi-channel protocol that allows a user to connect to a computer running Microsoft Terminal Services.

Replication

The generic term given to the process of intercepting changes to data files and registry keys on the active server, transporting the changed data across the channel, and applying them to the passive server(s) so the servers are maintained in a synchronized state.

Role

The functional state of a server in the Ipswitch Failover Cluster: active or passive.

Rule

A set of actions performed by Ipswitch Failover when defined conditions are met.

Secondary

An identity assigned to a server during the Ipswitch Failover installation process that normally does not change during the life of the server and usually represents the standby server prior to installation of Ipswitch Failover.

Security Identifier (SID)

A unique alphanumeric character string that identifies each operating system and each user in a network of Windows 2008/2012 systems.

Send Queue

The staging area of the active server used to store intercepted data changes before being transported across Ipswitch Channel to a passive server in the replication chain.

Server Monitoring

Monitoring of the active server by the passive server, using a heartbeat message, to ensure that the active server is functional.

Shared Nothing

A key feature of Ipswitch Failover in which no hardware is shared between the Primary or Secondary servers. This prevents a single point of failure.

SMTP

A TCP/IP protocol used in sending and receiving e-mail between servers.

SNMP

Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing devices on IP networks.

Split-Brain Avoidance

A unique feature of Ipswitch Failover that prevents a scenario in which Primary and Secondary servers attempt to become active at the same time leading to an active-active rather than an active-passive model.

Split-Brain Syndrome

A situation in which more than one server in an Ipswitch Failover Cluster are operating in the active mode and attempting to service clients, resulting in the independent application of different data updates to each server.

Storage Area Network (SAN)

A high-speed special-purpose network or (subnetwork) that interconnects different kinds of data storage devices with associated data servers on behalf of a larger network of users.

Subnet

Division of a network into an interconnected but independent segment or domain, intended to improve performance and security.

Switchover

The graceful transfer of control and application service to the passive server.

Synchronize

The internal process of transporting 64KB blocks of changed files or registry key data, through the Ipswitch Channel, from the active server to the passive server to ensure the data on the passive server is a mirror image of the protected data on the active server.

System Center Operations Manager (SCOM)

System Center Operations Manager is a cross-platform data center management server for operating systems and hypervisors.

System State

Data that comprises the registry, COM+ Class Registration database, files under Windows File Protection, and system boot file; other data may be included in the system state data.

Task

An action performed by Ipswitch Failover when defined conditions are met.

Tertiary

An identity assigned to a server during the Ipswitch Failover installation process that normally does not change during the life of the server and usually represents the disaster recovery server prior to installation of Ipswitch Failover.

Time-To-Live (TTL)

The length of time that a locally cached DNS resolution is valid. The DNS server must be re-queried after the TTL expires.

Traceroute

A utility that records the route through the Internet between your computer and a specified destination computer.

Trio

An Ipswitch cluster comprising three servers, a Primary, Secondary and Tertiary, in order to provide High Availability and Disaster Recovery.

Ungraceful (Unclean) Shutdown

A shutdown of Ipswitch Failover resulting from a critical failure or by shutting down Windows without first performing a proper shutdown of Ipswitch Failover, resulting in possible data loss.

Unprotected Application

An application that is not monitored nor its data replicated by Ipswitch Failover.

Virtual Private Network (VPN)

A private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures.

Windows Management Instrumentation (WMI)

A management technology allowing scripts to monitor and control managed resources throughout the network. Resources include hard drives, file systems, operating system settings, processes, services, shares, registry settings, networking components, event logs, users, clusters, and groups.