

Windows Server® "8" Beta

Understand and Troubleshoot DHCP Failover in Windows Server "8" Beta

Microsoft Corporation

Published: February 2012

Abstract

This Understand and Troubleshoot Guide (UTG) enables you to learn technical concepts, functionality, and troubleshooting methods for DHCP Failover in Windows Server "8" Beta. This UTG provides you with:

- A technical overview and functional description of this feature.
- Technical concepts to help you successfully install, configure, and manage this feature.
- User Interface options and settings for configuration and management.
- Relevant architecture of this feature, with dependencies, and technical implementation.
- Primary troubleshooting tools and methods for this feature.

Microsoft®

Copyright information

This document is provided “as-is”. Information and views expressed in this document, including URL and other Internet Web site references, may change without notice.

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

© 2012 Microsoft. All rights reserved.

Active Directory, Hyper-V, Microsoft, MS-DOS, Visual Basic, Visual Studio, Windows, Windows NT, Windows Server, and Windows Vista are trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.

Table of Contents

Windows Server "8" Beta Understanding and Troubleshooting Guide: DHCP Server Failover.....	1
About The Understanding and Troubleshooting Guide	1
Introducing DHCP Failover	1
Technical Overview	3
Installing/Enabling DHCP Failover	5
Installation Process	5
Management Considerations	8
Configuring and Managing DHCP Failover.....	10
Configuration and Management UI.....	10
Configuration Settings.....	10
Troubleshooting DHCP Failover.....	23
Server Event Channels.....	23
Failover Performance Counters	27
Windows PowerShell Support for DHCP Failover	27

Windows Server "8" Beta Understanding and Troubleshooting Guide: DHCP Server Failover

About The Understanding and Troubleshooting Guide

Understanding and Troubleshooting Guides enable you to learn about technical concepts, functionality, and general troubleshooting methods for new Windows features and enhancements. The Understanding and Troubleshooting Guide supports you in developing understanding of key technical concepts, architecture, functionality, and troubleshooting tools and techniques. This understanding will enable more successful testing and early adoption experiences during the pre-release product evaluation phase, and will support early ramp-up of help desk and technical support roles.

Introducing DHCP Failover

The Dynamic Host Configuration Protocol (DHCP) service provides IP addresses and other network configuration parameters to host computers and network devices. If this critical service becomes unavailable, it can result in a widespread loss of network connectivity. Since any prolonged network outage can have catastrophic impact on productivity, high availability of the DHCP service is essential to business continuity.

In Windows Server 2008 R2, there are two high availability options available for DHCP Server deployment.

- Deploying DHCP in a Windows failover cluster
- Split scope deployment

The Windows Server Enterprise Edition DHCP Server service is a cluster-aware application. By using clustering support for DHCP, administrators can implement DHCP server failover for a single site, achieving greater fault tolerance. The clustering deployment uses a single shared storage. This makes the storage a single point of failure, and requires additional investment in redundancy for storage. In addition, clustering involves relatively complex setup and maintenance.

Administrators can also enhance fault tolerance by combining DHCP server clustering with a split scope configuration. Split scopes provide another mode of redundancy for DHCP. Two DHCP servers back each other up by each hosting part of the IP address range of a scope. Split scope deployment does not provide IP address continuity and is unusable in scenarios where the scope is already running at high utilization of address space, which is very common with Internet Protocol version 4 (IPv4).

What Is DHCP Server Failover?

DHCP failover in Windows Server "8" Beta provides the ability for administrators to deploy a highly resilient DHCP service to support a large enterprise. The main goals of the feature are the following.

- Provide DHCP service availability at all times on the enterprise network
- If a DHCP server is no longer reachable, the DHCP client is able to extend the lease on its current IP address by contacting another DHCP server on the enterprise network

The DHCP server failover feature provides the ability to have two DHCP servers serve IP addresses and option configuration to the same subnet or scope, providing for continuous availability of DHCP service to clients. The two DHCP servers replicate lease information between them, allowing one server to assume responsibility for servicing of clients for the entire subnet when the other server is unavailable. It is also possible to configure failover in a load-balancing configuration with client requests distributed between the two servers in a failover relationship.

DHCP failover in Windows Server "8" Beta provides support for a maximum of two DHCP servers, and the failover relationship is limited to IPv4 scopes and subnets. Network nodes using Internet Protocol version 6 (IPv6) typically determine their own IPv6 address using stateless IP auto configuration. In this mode, the DHCP server delivers only the DHCP option configuration, and the server does not maintain any lease state information. A high availability deployment for stateless DHCPv6 is possible by simply setting up two servers with identical option configuration. Even in a stateful DHCPv6 deployment, the scopes do not run under high address utilization, which makes split scope a viable solution for high availability.



More Information:

The Microsoft implementation of DHCP failover is based on the Internet Engineering Task Force (IETF) draft for DHCP Failover Protocol

<http://www.ietf.org/proceedings/59/I-D/draft-ietf-dhc-failover-12.txt>

Purpose/Benefits

The Windows Server "8" Beta DHCP failover feature provides a high availability solution for IP address and configuration assignment. Deployment of this solution does not require the additional expense of hardware or third party storage software. There is no need to provide a dedicated network for high availability traffic, and the failover configuration is very simple for network administrators to configure.

Technical Overview

Prerequisites

The feature described in this guide requires that both DHCP servers in the failover configuration are running Windows Server "8" Beta, with the DHCP Server role installed. The Windows Server "8" Beta DHCP failover feature does not interoperate with legacy or third party DHCP servers.

Functional Description

The DHCP high availability feature in Windows Server "8" Beta is based on the DHCP failover protocol specification as defined in the IETF draft. Two servers are in a failover relationship for one or more scopes when they are configured with identical scope configuration and are setup to replicate lease information and manage response to client requests as defined in the failover protocol.

A unique failover relationship name is required to identify the failover setup between two servers. Since multiple failover relationships can exist with one or more DHCP servers, each relationship name is required to be unique on a server. The failover relationship name, with a maximum length of 126 characters, is exchanged between the two servers during initial configuration. The peer server in a failover relationship is referred to as the partner server. The partner server in a failover relationship is identified by a hostname or IP address based on the format entered by the administrator.

Administrators can deploy Windows Server "8" Beta DHCP servers as failover partners in either hot standby mode or load sharing mode.

Hot Standby Mode

In hot standby mode, two servers operate in a failover relationship where an active server is responsible for leasing IP addresses and configuration information to all clients in a scope or subnet, while a secondary server assumes this responsibility if the primary server becomes unavailable. A server is primary or secondary in the context of a subnet. For instance, a server that has the role of a primary for a given subnet could be a secondary server for another subnet.

Hot standby mode of operation is best suited to deployments where a central office or data center server acts as a standby backup server to a server at a remote site, which is local to the DHCP clients. In such deployments, it is undesirable to have the standby server, located remotely, service any clients unless the local DHCP server becomes unavailable.

Load Sharing Mode

In a load sharing mode deployment, which is the default mode of operation, the two servers simultaneously serve IP addresses and options to clients on a given subnet. The client requests are load balanced and shared between the two servers. The load sharing mode of operation is best suited to deployments where both servers in a failover relationship are located at the same physical site. Both servers respond to DHCP client requests based on the load distribution ratio configured by the administrator.

**More Information:**

Sharing of client request load is implemented using the DHC Load Balancing algorithm described in RFC 3074.

<http://tools.ietf.org/html/rfc3074>

DHCP failover implements a load-balancing scheme, defined in RFC 3074, in which a hash is computed from the MAC address contained in each client request. The setup process assigns hash buckets to each server in the failover relationship. Based on the hash of the MAC address, servers determine if they are designated to respond to the client or not. When a failover relationship is configured in load sharing mode, the administrator must specify the load-balancing ratio. The default value of load balancing ratio between the two servers is 50:50.

Maximum Client Lead Time (MCLT)

The DHCP failover protocol includes a setting for Maximum Client Lead Time (MCLT,) which defines the temporary lease period given by the failover server to a new client. This period also determines the amount of time that a server in a failover relationship will wait in partner down state before assuming control over the entire IP address range.

MCLT cannot be set to zero, and the default setting is 1 hour.

Reserve Addresses Percentage

In a failover relationship configured in hot standby mode, administrators can specify a percentage of the address range of the scope as reserved for the hot standby server. A number of addresses, in proportion to the percentage value configured, are assigned to the hot standby server. The hot standby server will use these addresses to service new clients after the primary server goes down, during the time interval before the standby server assumes control over the entire IP address range of a scope. The hot standby server assumes control over the entire IP address range only after it transitions into partner down state and a certain time (defined by MCLT) has elapsed after moving into the partner down state.

If an administrator sets this parameter to zero, no addresses are reserved for the hot standby server, and the failover partner server cannot grant new client leases until the time that the

hot standby assumes control over the entire IP address range. The default value for reserve address percentage is 5%.

Auto State Switchover Interval

A server that loses communication with a partner server transitions into a communication interrupted state. The loss of communication may be due to a network outage or the partner server may have gone offline. Since there is no way for the server to detect the reason for loss of communication with its partner, the server will continue to remain in communication interrupted state until the administrator manually changes the state to partner down.

Alternatively, DHCP failover has a provision for automatic transition to partner down state based on a time out interval. This is a configurable element called the auto state switchover interval. The default value for auto state switchover interval is 10 minutes.

Message Authentication for DHCP Failover

Windows Server "8" Beta implements failover message authentication using the Secure Hash Algorithm 2 (SHA-2) cryptographic standard. By default, DHCP failover uses the SHA-256 algorithm.



More Information:

For more information on hashing of data using CNG APIs, see the MSDN documentation:

[Creating a Hash With CNG](#)

<[http://msdn.microsoft.com/en-us/library/aa376217\(v=VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa376217(v=VS.85).aspx)>

To configure message authentication, the DHCP failover setup wizard prompts the administrator to provide a shared secret. As part of the failover relationship creation, the failover setup wizard provisions the shared secret for message authentication to each of the servers in the failover relationship.

Installing/Enabling DHCP Failover

Installation Process

The Windows Server "8" Beta DHCP Server role integrates with the Server Manager console for installation and uninstallation. The Server Manager console eases the task of installing and managing multiple server roles through the Add Roles and Features Wizard (ARFW).

Installation UI/Wizard

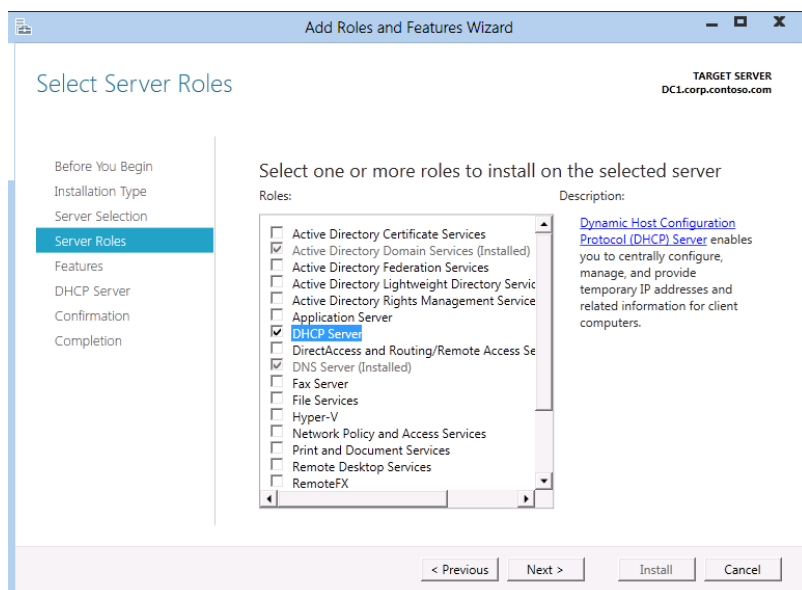


Figure 1 Add Roles Wizard

Verifying Installation

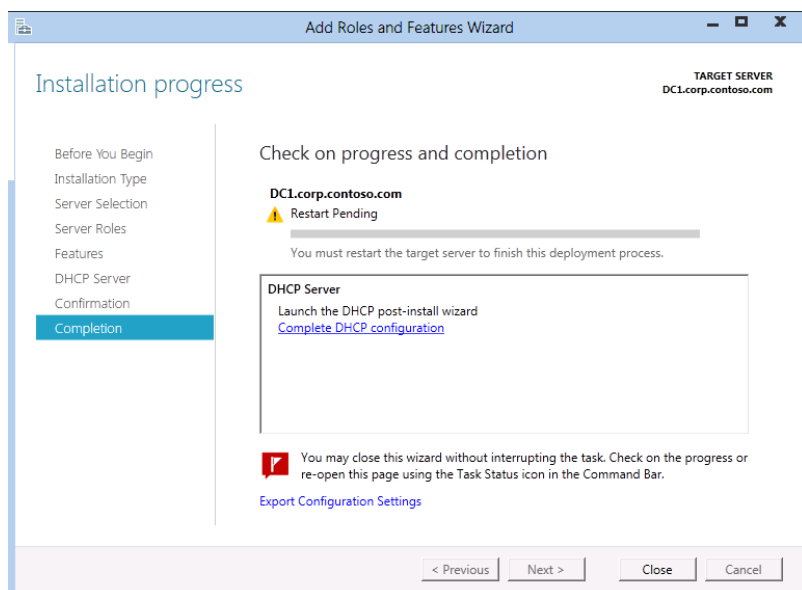


Figure 2 Installation Results

When installation is complete, click **Complete DHCP configuration**. The **DHCP Post-Install Configuration Wizard** will start. Click **Next**, supply credentials for Active Directory authorization, and then click **Commit**.

DHCP server security groups – DHCP Administrators and DHCP Users – are also added by the post-install configuration wizard.

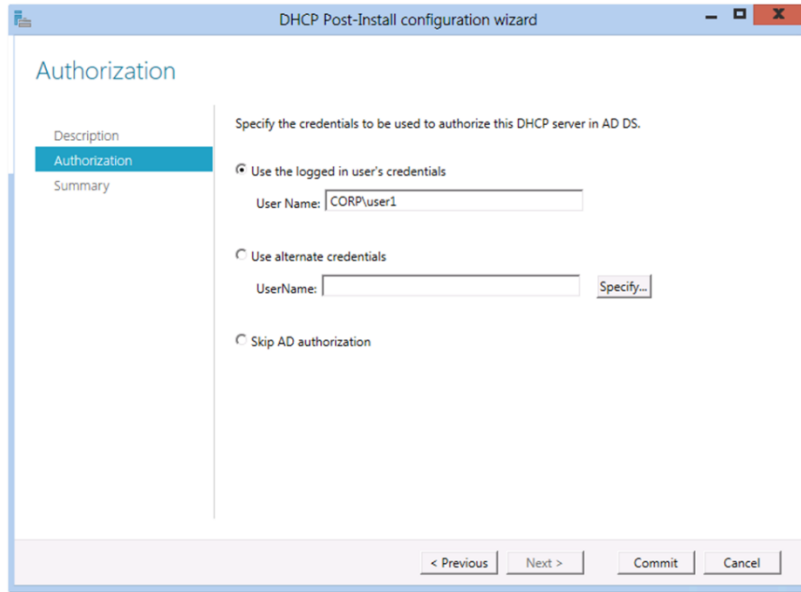


Figure 3 DHCP Post-Install configuration wizard



Note:

Enterprise Admin credentials are required to authorize DHCP in the Active Directory forest. Alternatively, you can delegate this ability to another user. See [Delegate ability to authorize DHCP servers to a non-enterprise administrator](#) for more information.

Uninstalling/Disabling

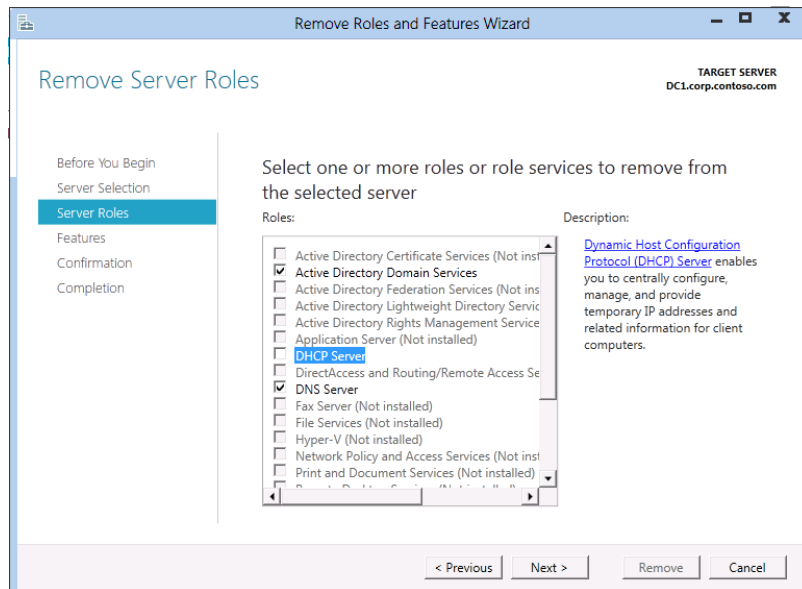


Figure 4 Remove Server Roles Wizard

Management Considerations

There are several management considerations for DHCP Server administration when failover replication is enabled. The following sections provide a description of each.

Time Synchronization

For DHCP failover to function correctly, time must be kept synchronized between the two servers in a failover relationship. Time synchronization can be maintained by deployment of the Network Time Protocol (NTP) or any other alternative mechanism. When the failover configuration wizard is run, it will compare the current time on the servers being configured for failover. If the time difference between the servers is greater than one minute, the failover setup process will halt with a critical error instructing the administrator to synchronize the time on the servers.

Each failover protocol message includes a time field, which is populated with the UTC time at which the sending server transmitted the message. On each received protocol message, the receiving server will perform a check of the time difference between the time stamp field in the packet and the time at the receiving server. If this time difference is found to be greater than one minute, the receiving server will log a critical event indicating that the two servers are not time synchronized.

A binding is a collection of configuration parameters managed by DHCP servers, including at least an IP address, associated with or "bound to" a DHCP client. A binding update

transaction refers to the set of information (contained in options), necessary to perform an update for a single IP address. Any change in state of an IP address lease (e.g. a new lease, renew, expiry, release) leads to a binding update message from the server on which the state change happened to a partner server. Any binding update message received by the server while time is out of synchronization is rejected with an error code. Determination of a time out-of-synch condition will not cause any change in the failover state of the server. Both servers will continue to operate in the same state as before determination of a time out-of-synch condition.

BOOTP Support

When BOOTP clients obtain an IP address from a DHCP server, they keep the assigned address indefinitely. The DHCP failover protocol is dependent on the temporary lease concept of DHCP and the associated client action of renewal of IP addresses based on the lease period. Since BOOTP clients do not follow this concept, and based on the very limited prevalence of BOOTP clients, DHCP failover is not supported for BOOTP. This implies that only scopes configured for DHCP alone can be setup for failover.

Policy Based IP Address and Option Assignment

Windows Server "8" Beta includes a new policy based IP address assignment feature, which allows a Windows DHCP administrator to group the DHCP clients by a specific attribute of the client, such as vendor class, user class, client identifier, or MAC address. By grouping the clients based on these attributes, an administrator is able to assign parameters such as IP address, default gateway, DNS server and other DHCP options to a specific grouping of clients. This allows the administrator to exercise greater control on the configuration parameters delivered to end hosts. This feature introduces the concept of multiple IP address ranges within a single scope. To accommodate this, DHCP failover address distribution in load sharing mode is done on a per IP address range basis.

Windows Firewall Rules

DHCP Server uses TCP port 647 to listen for failover messages between the two failover partner servers. For this traffic to be allowed by the Windows firewall, the following inbound and outbound firewall rules are added as part of the DHCP server role install.

- "Microsoft-Windows-DHCP-Failover-TCP-In"
- "Microsoft-Windows-DHCP-Failover-TCP-Out"

Configuring and Managing DHCP Failover

Configuration and Management UI

Configuration and management of DHCP failover settings is done via the DHCP Management console. The DHCP console in Windows Server "8" Beta includes a new **Configure Failover** menu item. This new menu item is available in the main DHCP IPv4 node and each of the IPv4 scope nodes. The **Configure Failover** option will only be displayed for scopes that are not already part of a failover relationship.

Configuration Settings

Setting up DHCP Failover

To configure failover for the entire server, launch the failover configuration wizard from the **Configure Failover** menu item on the IPv4 node in the DHCP Management console. To configure failover for only a subset of the scopes on a server, select the set of scopes to be configured for failover, and click on the **Configure Failover** menu option.

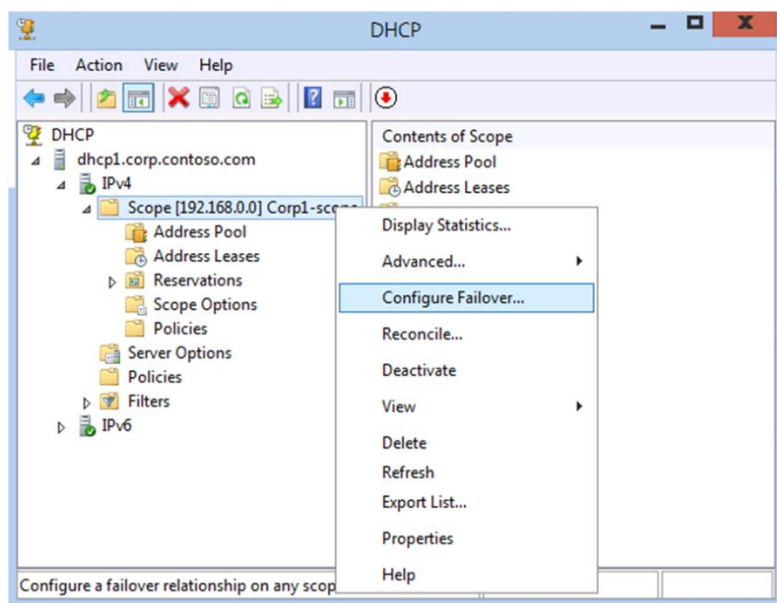


Figure 5 Configure Failover menu option

The Configure Failover wizard presents the administrator with an introductory screen, which allows selection of the scopes to configure for high availability. The **Select All** button provides the convenience of selecting all scopes, and is checked by default. If the administrator selects only specific scopes, the **Select All** checkbox will be cleared.

After clicking **Next** in the introduction dialogue, specify the partner server with which to setup a failover relationship. If there are existing failover relationships that this server has with other servers, they may be selected from the list of partner servers in the drop down box.

Enter the hostname or IP address of a partner server for the failover relationship, or browse to select from the list of authorized DHCP servers.

The **Reuse existing failover relationships setup with this server (if any)** checkbox will be checked if there are existing failover relationships on the server. If there is no existing failover relationship on the server, this checkbox will be unchecked and disabled.

Configure Failover

Specify the partner server for failover setup

Provide host name or IP address of the partner DHCP server with which failover should be set up.

You can select from the list of servers with which there is an existing failover set up or you can browse and select from the list of authorised DHCP servers.

Alternatively, you can also type the host name or IP address of the partner server.

Partner Server:

☒ Reuse existing failover relationships set up with this server (if any).

Figure 6 Select Partner Server

After the administrator clicks **Next**, the failover configuration wizard performs a series of checks, and may display errors encountered as noted in the table below.

Check Performed	Message displayed on error
Is the specified DNS name resolvable	Unable to resolve specified DNS name.
Is the IP address specified a valid IP address	The specified IP address <IP address> is invalid
Is the specified DHCP server reachable	The specified DHCP server is not reachable. Please provide a DHCP server that is reachable.
Is the specified server running Windows Server "8" Beta or above	The version of specified DHCP server does not support failover.

Check Performed	Message displayed on error
Is the logged in user a member of DHCP Administrators group on the partner server	You do not have permissions to perform this operation on the remote DHCP server.
Have either of the two servers already hit the maximum limit on the number of failover relationships	The <local/partner> server already has 31 (maximum allowed) failover relationships. A server cannot have more than 31 failover relationships.
Is DHCP server running on the partner server	DHCP server is not running on the specified server. Please ensure that DHCP server is running on the specified server.
Is time synchronized between the two servers	<p>The time difference between this server and the specified partner server is greater than the permissible value of x minutes. It is recommended to ensure that both servers are time synchronized before configuring failover. You could setup Network Time Protocol (NTP) service on both servers to ensure time synchronization.</p> <p>Note: The check for time sync is based on the registry value configured for permissible time difference. The registry value will be read from both the servers and the minimum of the values will be used to perform the check. If registry value has not been configured, the default value for permissible time difference will be used.</p>
Are any of the scopes selected for failover setup present on the partner server	Following scopes already exist on the specified partner server. These scope(s) will need to be deleted on the partner server before configuring failover.

If all prerequisite checks are successful, the following dialog allows the administrator to change the default values for relationship name, MCLT, failover mode, load-balance ratio, and auto-state switchover interval.

Configure Failover

Create a new failover relationship

Create a new failover relationship with dhcp2.corp.contoso.com

Relationship Name: 1.corp.contoso.com-dhcp2.corp.contoso.com

Maximum Client Lead Time: 0 hours 1 minutes

Mode: Load Balance

Load Balance Percentage

Local Server: 50%

Partner Server: 50%

☐ Auto State Switchover Interval: 10 minutes

☒ Enable Message Authentication

Shared Secret: [masked]

< Back Next > Cancel

Figure 7 Configure failover settings

Click **Next**, and after verifying the failover settings, click **Finish** to apply the configuration. The failover configuration wizard displays a progress screen as the various tasks listed below are completed.

- Create the scope(s) on the partner server and deactivate the scopes. At this point, there is no configuration on the scopes. The scope(s) only contain a scope id/name and subnet mask.
- Provision the scope with identical configuration (including address ranges) as this server
- Create the failover relationship and the associated failover configuration parameters on the partner server.
- Create the failover relationship and the associated failover configuration parameters on this server.
- Activate the scopes on the partner server.

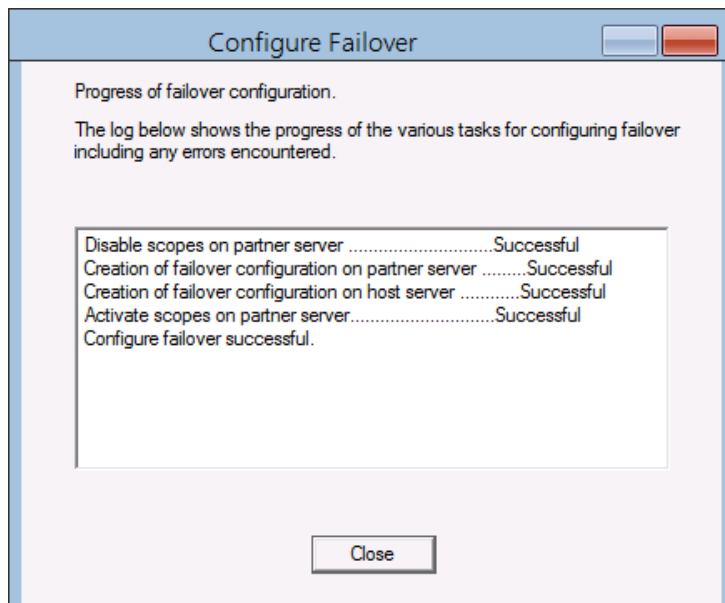


Figure 8 Failover Configuration Progress

If any of the configuration steps fail, the failover configuration wizard will log a message indicating the error encountered, and the rollback button will be automatically initiated. The rollback process will delete the scopes already created up to the point of failure from the partner server, and remove all the failover configuration from both the servers if a new failover relationship was being setup. In case of loss of communication with the partner server, the rollback will only be performed on the local server. A warning will be displayed indicating that the contact with the partner was lost and rollback could not be completed on the remote server.

Viewing and Changing Failover Configuration

You can delete, edit, and view status of all failover relationships on a DHCP server by accessing the Failover tab in the Properties of the IPv4 node in the DHCP console.

You can also view the failover properties of a scope by accessing the Failover tab in the properties of a scope in the DHCP console.

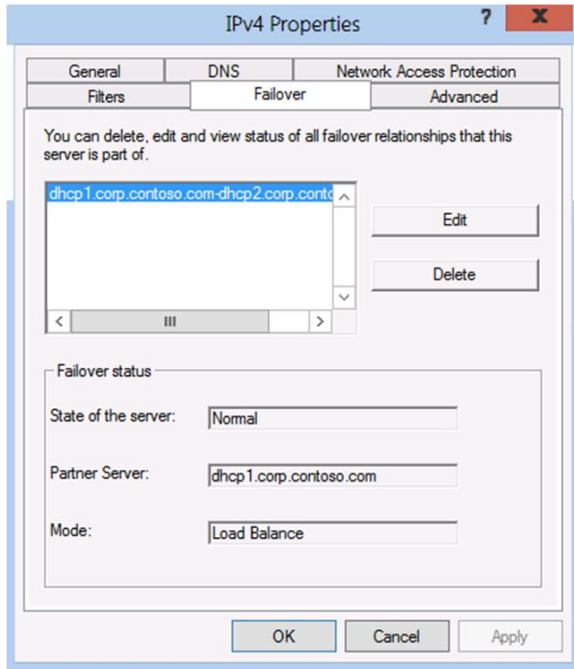


Figure 9 IPv4 Properties Failover Tab

Click **Edit** to view or modify the failover relationship settings.

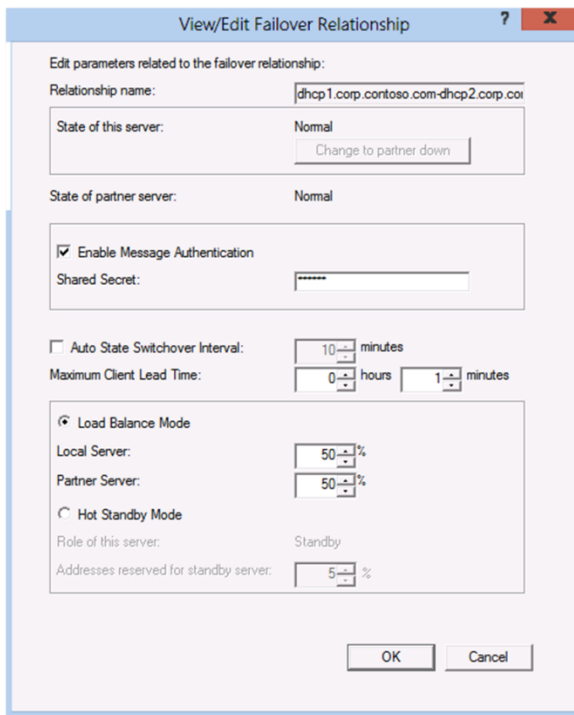


Figure 10 View/Edit Failover Relationship

Configuration Synchronization

In order to ensure that the clients get the same network configuration regardless of which DHCP server they contact, it is necessary to maintain identical configuration on both servers for the scope. The DHCP failover implementation is based on the DHCP failover Internet draft, which defines the lease synchronization protocol and the associated server behavior. However, it does not specify synchronization of server configuration changes between the two DHCP servers in a failover relationship.

The DHCP console in Windows Server "8" Beta provides an interface to replicate scope configuration at the following levels.

- IPv4 Node - Replicate all failover scopes
- Single failover scope - Replicate selected scope, Replicate all scopes of the failover relationship to which the selected scope belongs
- Multiple failover scopes - Replicate selected scopes

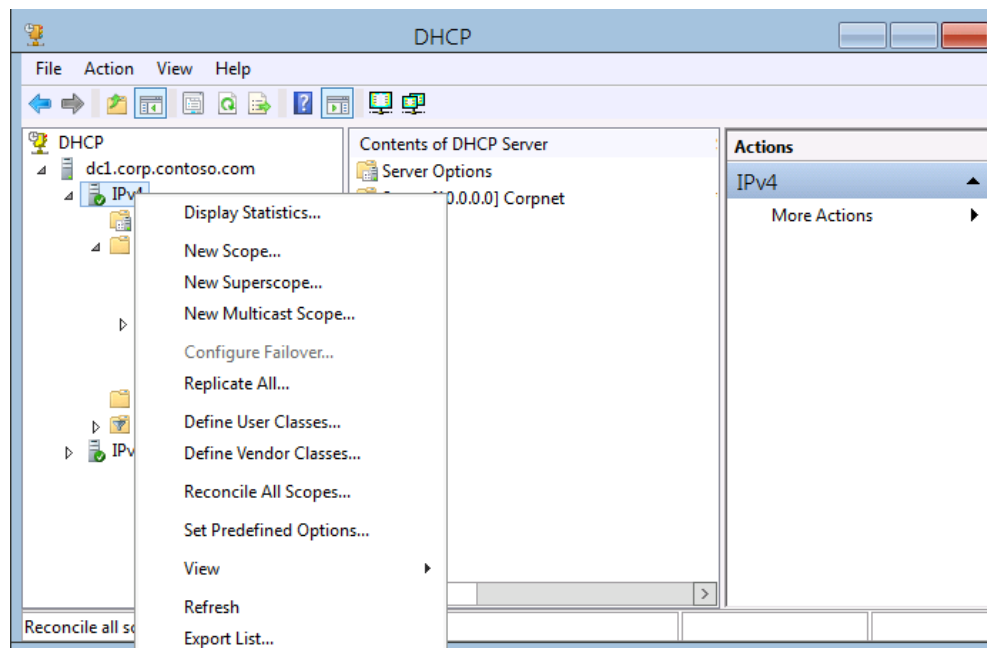


Figure 11 IPv4 Node - Replicate All Scopes

Scope replication will be initiated after user confirmation as shown in the figure below.

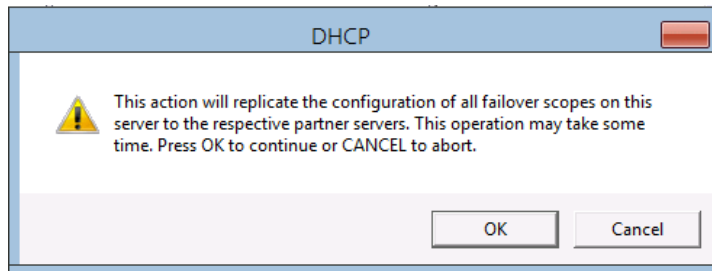


Figure 12 Confirm Scope Replication

The following settings are replicated per scope to the partner server by the replicate action:

Scope properties - Scope name, description, state (active/inactive), delay, superscope, scope delay

- NAP settings of a scope - NAP enabled or disabled, NAP profile setting
- IP address ranges - IP address range and exclusion range
- Scope option values including DNS registration setting
- Reservations - IP address, MAC Address, name and description, reservation option values
- Policies - Name, description, conditions, IP address range setting, option value settings

After user confirmation, a replication progress window is displayed to indicate the status of the replication to the partner server. Messages are logged to the screen to indicate progress of replication on a per-scope basis. The close button on the configuration replication progress window will be enabled when replication of all of the selected scopes to the respective partner servers is complete. On any failure, the configuration replication for the specific scope will be stopped, and replication of scope configuration of the next selected scope will be started.

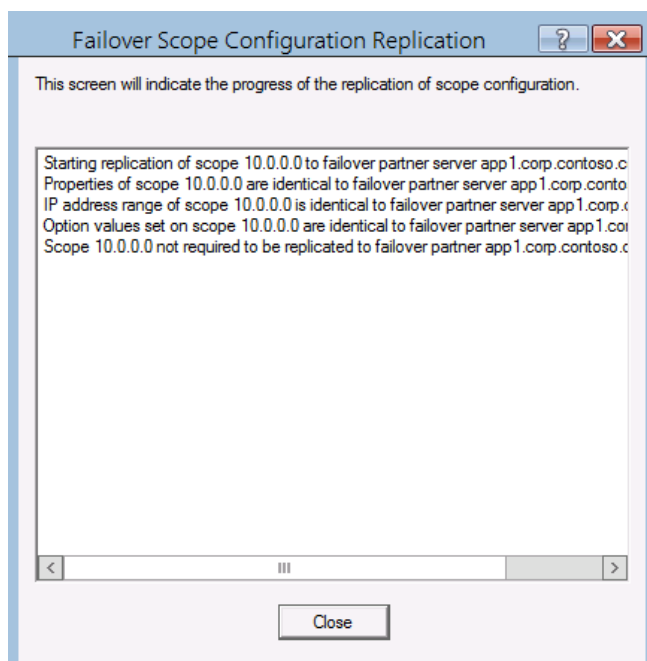


Figure 13 Replication Progress

The table below provides a summary of the messages displayed in the progress window with associated conditions.

Condition	Message
Beginning to replicate a specific scope	"Starting replication of scope <ScopeID> to failover partner server <IPAddress/DNSName of partner server>"
Successfully completed replicating a specific scope	"Scope <ScopeID> was successfully replicated."
Scope properties are compared and found to be identical	<p>Initial Message</p> <p>"Replication of scope properties to failover partner server initiated"</p> <p>Final message in case of success:</p> <p>"Scope properties of scope <ScopeID> are identical to failover partner server."</p>

Condition	Message
Scope properties are found to be different and were replicated successfully to partner	<p>Initial Message</p> <p>"Replication of scope properties to failover partner server initiated"</p> <p>Final message in case of success:</p> <p>"Properties of scope <ScopeID> are replicated to failover partner server."</p>
NAP settings are compared and found to be identical	<p>Initial Message</p> <p>"Replication of NAP settings to failover partner server initiated"</p> <p>Final message in case of success:</p> <p>"NAP settings of scope <ScopeID> are identical to failover partner server."</p>
NAP settings are found to be different and were replicated successfully to partner	<p>Initial Message</p> <p>"Replication of NAP settings to failover partner server initiated"</p> <p>Final message in case of success:</p> <p>"NAP settings of scope <ScopeID> are replicated to failover partner server."</p>
IP address ranges are compared and found to be identical	<p>Initial Message</p> <p>"Replication of IP address ranges to failover partner server initiated"</p> <p>Final message in case of success:</p> <p>"IP address range and exclusion IP address ranges of scope <ScopeID> are identical to failover partner server."</p>
IP address ranges are found to be different and are successfully replicated to partner	<p>Initial Message</p> <p>"Replication of IP address ranges to failover partner server initiated"</p> <p>Final message in case of success:</p> <p>"IP address range and exclusion IP address ranges of scope <ScopeID> are replicated to failover partner server."</p>
Scope option values are compared and found to be identical	<p>Initial Message</p> <p>"Replication of scope option values to failover partner server initiated."</p> <p>Final message in case of success:</p> <p>"Option values set on scope <ScopeID> are identical to failover partner server"</p>

Condition	Message
Scope option values are found to be different and are successfully replicated	<p>Initial Message</p> <p>"Replication of scope option values to failover partner server initiated."</p> <p>Final message in case of success:</p> <p>"Option values set on scope %s are replicated to failover partner server <ScopeID>"</p>
Reservations are compared and found to be identical	<p>Initial Message</p> <p>"Replication of reservations to failover partner server initiated."</p> <p>Final message in case of success:</p> <p>"Reservations in scope %s are identical to failover partner server <ScopeID>"</p>
Reservations are found to be different and are successfully replicated	<p>Initial Message</p> <p>"Replication of reservations to failover partner server initiated."</p> <p>Final message in case of success:</p> <p>"Reservations in scope <ScopeID> are replicated to failover partner server"</p>
Policies are copied to destination server	<p>Initial Message</p> <p>"Replication of policies to failover partner server initiated."</p> <p>Final message in case of success:</p> <p>"Policies in scope <ScopeID> are replicated to failover partner server"</p>
Failed to read configuration from sever	<p>"Failed to read Scope properties/IP Address Ranges/NAP settings/Option Values/Policies/Reservations from partner server <IPAddress/DNSName of partner server>. <Error code>: <Error string>"</p>

Condition	Message
Failed to update configuration from server	<p>"Failed to update Scope properties for scope <ScopeID> on partner server <IPAddress/DNSName of partner server>. <Error code>: <Error string>"</p> <p>"Failed to update IP Address ranges for scope <ScopeID> on partner server <IPAddress/DNSName of partner server>. <Error code>: <Error string>"</p> <p>"Failed to update NAP settings for scope <ScopeID> on partner server <IPAddress/DNSName of partner server>. <Error code>: <Error string>"</p> <p>"Option definition for option id <OptionID> is not present on partner server. Option value cannot be updated."</p> <p>"Failed to update option values for user class: <UserClass> vendor class: <VendorClass> in scope <ScopeID> on partner server <IPAddress/DNSName of partner server>. <Error code>: <Error string>"</p> <p>"Failed to copy policies for scope <ScopeID> on partner server <IPAddress/DNSName of partner server>. <Error code>: <Error string>"</p> <p>"Failed to add or modify reserved IP address <ReservedIP Address> on partner server <IPAddress/DNSName of partner server>. <Error code>: <Error string>"</p> <p>"Failed to update option values for user class: <UserClass> vendor class: <VendorClass> on reserved IP address <ReservedIP Address> on partner server <IPAddress/DNSName of partner server>. <Error code>: <Error string>"</p>
One of the selected scopes in a multi-select is not part of the failover relationship	"Selected scope <ScopeID> is not part of any failover relationship"

Removing a Scope from a Failover Configuration

If failover has been configured for a scope, the DHCP console includes a menu option "Deconfigure Failover". If this option is selected, the following warning dialog is displayed.

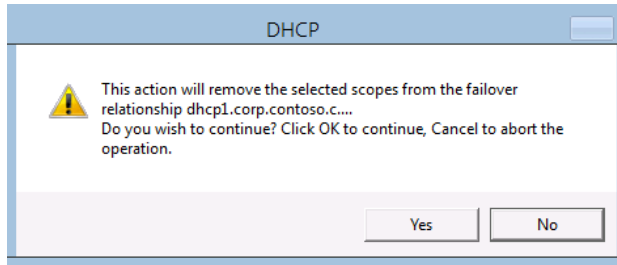


Figure 14 Deconfigure scope

If all the scopes of a failover relationship are being removed or deconfigured, the following warning dialog is displayed.

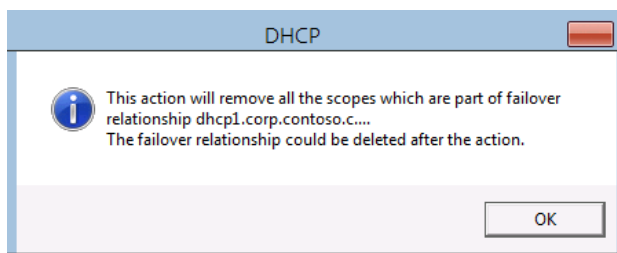


Figure 15 Deconfigure Failover

After the administrator acknowledges the warning dialogs, the deconfigure failover process performs the following steps.

- Check for status of each of the partner servers and issue an appropriate warning if both servers are in any state other than normal. The administrator is provided the option to continue to delete the failover relationship after acknowledging the warning. The warning message indicates that since the server is not in communication with its partner server, the deletion will only be performed locally. The administrator must perform similar deconfiguration on the partner server.
- Deactivate the scope(s) on the partner server so that no further addresses are leased out from the partner server.
- Remove the scope(s) from the failover relationship on this server.
- Delete the scope(s) from the partner server.

On successful completion of all the above steps, a message indicating successful completion of the deconfiguration is displayed.

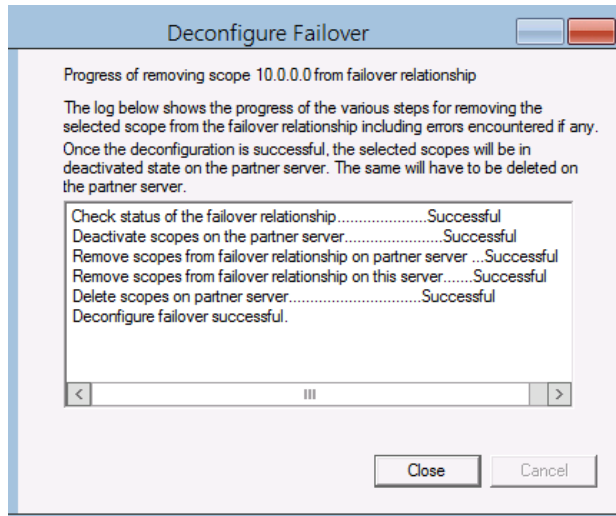


Figure 16 Deconfigure Failover Success

In case of any errors, the rollback action is automatically invoked. The rollback action performs the same steps in reverse order with corresponding messages being printed to the log. The rollback is performed for all the changes done up to the point of failure (complete rollback). In case of loss of communication with the partner server, the rollback will only be performed on the local server (i.e. the server which is being managed via the management console). A warning is issued that the contact with the partner server was lost and hence rollback could not be completed on the remote server.

Once rollback completes successfully or fails, the Close button is enabled.

Troubleshooting DHCP Failover

Windows Server "8" Beta introduces new event logging and performance counters to support troubleshooting of DHCP failover.

Server Event Channels

DHCP failover-specific events have been added for configuration audit and failover event logging.

Configuration Audit

The following information-level change events are logged to the DHCP server operational channel Microsoft\Windows\DHCP Server\Operational.

Event Type	OpCode	Description
Creation of Failover Relationship	CreateFailover	A failover relationship has been created between servers <server host name/IP address> and <server host name/IP address> with the following configuration parameters: Name: <value> Mode:<Load Balance/Hot Standby>, Maximum Client Lead Time: <value> seconds, Load Balance percentage on this server/Reserve Address percentage on standby server: <value>, Auto state switchover interval <value> seconds Standby server: <hostname or IP address of standby server>
Deletion of Failover Relationship	DeleteFailover	Failover relationship <relationship name> between <server IP address/hostname> and <server IP address/hostname> has been deleted
Addition of a scope to an existing failover relationship	AddFailoverScope	Scope <scope id> has been added to the failover relationship <relationship name> with server <partner server IP address>
Removal of a scope from an existing failover relationship	RemoveFailoverScope	Scope <scope id> has been removed from the failover relationship <relationship name> with server <partner server hostname/IP address>
Change MCLT	ChangeFailoverConfig	The failover configuration parameter MCLT for failover relationship <relationship name> with server <partner server hostname/IP address> has been changed from <old value> seconds to <new value> seconds
Change Auto state switchover interval	ChangeFailoverConfig	The failover configuration parameter Auto State switchover interval for failover relationship <relationship name> with server <partner server hostname/IP address> has been changed from <old value> seconds to <new value> seconds
Change Reserve Address percentage	ChangeFailoverConfig	The failover configuration parameter Reserve Address Percentage on standby server for failover relationship <relationship name> with server <partner server hostname/IP address> has been changed from <old value> to <new value>

Event Type	OpCode	Description
Change Mode of failover relationship	ChangeFailoverConfig	The failover configuration parameter Mode for failover relationship <relationship name> with server <partner server hostname/IP address> has been changed from <old value> to <new value>
Change Load Balance percentage	ChangeFailoverConfig	The failover configuration parameter Load Balance percentage for failover relationship <relationship name> with server <partner server hostname/IP address> has been changed from <old value> to <new value> on this server

Failover Event Logging

In addition to logging events for configuration changes, Event Tracing for Windows (ETW) events are logged for state transition of the server or its partner server. These events are logged to the DHCP server admin channel Microsoft\Windows\DHCP Server\Admin. The following data is provided as part of each state change event.

- Previous state of the server
- Current state of the server
- Failover relationship name
- Server hostname/IP address

In addition to logging its own change of state, the server will also log change of state of the partner server communicated by the state messages from the partner. The table below lists the values populated for the various fields in the event log.

Event Field	Value
Event ID	20252
Date and Time	Time of the state change
Computer	DHCP server host name
User	Network Service

Event Field	Value
Description	<p>The failover state of server <server IP address or hostname> for failover relationship <relationship name> changed from <Old State> to <New State>.</p> <p>Note: Server IP address/hostname would relate to the server whose state has changed. In case of state of change of partner, this would be the host name or IP address of the partner.</p> <p>Note: If the previous state of the server is not known (this happens in the case of new relationship creation and when communication is interrupted), the following description will be displayed for the event:</p> <p>The failover state of server <server IP address or hostname> for failover relationship <relationship name> changed to <New State>.</p>
OpCode	FailoverStateChange
Task Category	DHCP Failover
Level	<p>Error (in case of transitioning out of NORMAL state or in case of entry into PARTNER DOWN state)</p> <p>Information (in case of transitioning into NORMAL state)</p> <p>Warning (in case of transitions between other states)</p>
Keywords	

The following event is logged when a server detects that it is out of time synchronization with its partner server.

Event Field	Value
Event ID	
Date and Time	Time of detection of time being out of sync with partner server
Computer	DHCP server host name
User	Network Service
Description	The server detected that it is out of time synchronization with partner <server IP address or hostname> for failover relationship <relationship name>. The time is out of sync by <x> minutes.
OpCode	TimeOutOfSync
Task Category	DHCP Failover
Level	Error
Keywords	

An event will also be logged when connection is established and when a connection is lost between the failover servers.

Level	Opcode	Task Category	Description
Error	CommDown	DHCP Failover	Server has lost contact with failover partner server <IP address> for relationship <name>
Informational	CommUp	DHCP Failover	Server has established contact with failover partner server <IP address> for relationship <name>

Failover Performance Counters

Windows Server "8" Beta introduces new failover performance counters to the DHCP server counters, including the following.

- Binding Updates sent per minute
- Binding Acks received per minute
- Binding Updates received per minute
- Binding Acks sent per minute
- Number of pending outbound binding updates on this server
- Number of transitions into COMMUNICATION INTERRUPTED state
- Number of transitions into PARTNER DOWN state
- Number of transitions into RECOVER state
- Number of Binding Update queue running at 90% of the maximum queue size
- Number of Binding Updates dropped

Windows PowerShell Support for DHCP Failover

The following sections provide reference documentation of the Windows PowerShell cmdlets specific to DHCP Failover.

The Properties of a Failover Relationship

The following Windows PowerShell object represents the properties of a failover relationship:

<i>Type</i>	<i>Name</i>	<i>Description</i>
DhcpServv4Failover		
{		
String	Name	Unique name for the failover relationship
String	PartnerServer	IP Address or hostname of the partner server
String	Mode	Failover mode; possible values are { HotStandby LoadBalance}
String	ServerRole	In case of Hot standby, the role of the this server {Active, Standby} else NULL
Uint	LoadBalancePercent	If mode is LoadBalance, the % of load distribution 0-100 (indicates the % load allocated to this server) If mode is HotStandby, this should be unassigned.
Uint	ReservePercent	If mode is HotStandby; the % of addresses reserved on standby server (0-100) If mode is LoadBalance, this should be unassigned.
IPAddress[]	ScopeId	IDs of one or more Scopes that are part of the failover relationship.
TimeSpan	MaxClientLeadTime	Maximum amount of time that a server can extend a lease for a client's binding over the lease time known by the partner server
Bool	AutoStateTransition	Enable/Disable automatic transition from COMM_INTERRUPTED state to PARTNER_DOWN state {True, False}
TimeSpan	SafePeriod	Time periodthat the server will stay in COMM_INTERRUPTED state before auto transitioning into PARTNER_DOWN state
String	State	State of the failover relationship { NORMAL, COMMUNICATION_INTERRUPTED, PARTNER_DOWN, POTENTIAL_CONFLICT, STARTUP, RESOLUTION_INTERRUPTED, CONFLICT_DONE, RECOVER, RECOVER_WAIT, RECOVER_DONE, PAUSED, SHUTDOWN, INIT, NO_STATE }

Bool	EnableAuth	Enable/Disable message authentication {True, False}
}		

Displaying the Properties of a Failover Relationship

```
Get-DhcpServerv4Failover [-Name <string[]>]
Get-DhcpServerv4Failover -ScopeId <IPAddress[]>
```

Description

This cmdlet gets failover relationship properties configured on the server for the specific failover relationship name(s) or scope(s).

Input Parameters

The cmdlet accepts the following parameters

Parameter	Mandatory	Parameter Type	Description
Name	No	string	Name(s) of the failover relationships to retrieve
ScopeId	Yes	IPAddress	Scope identifiers of failover scopes

Output Parameters

The cmdlet displays the following output parameters

Parameter	Description
DHCPv4Failover	One or more objects containing the failover relationships on the server

Behavior

- If no relationship name is specified, the cmdlet returns all failover relationships defined on the server. When no failover relationships are present on the server and the name parameter is not specified, an empty collection will be returned. There will be no error returned in this case. If there is no failover relationship by the specified name, a non-terminating error is returned for the specific name.
- If ScopeId is specified, the cmdlet returns the failover relationships for the specified scopes. If a specified ScopeId is not part of a failover relationship, a non-terminating error is returned.

Adding a Failover Relationship

```
Add-DhcpServerv4Failover -PartnerServer <string> -Name <string> -ScopeId
<IPAddress[]> [--LoadBalancePercent <uint>] [-MaxClientLeadTime <TimeSpan>] [-
AutoStateTransition <Bool>] [-SafePeriod <TimeSpan>] [-SharedSecret <string>]
[-Force]
```

```
Add-DhcpServerv4Failover -PartnerServer <string> -Name <string> -ScopeId
<IPAddress[]> [-ReservePercent <uint>] [-ServerRole <string>] [-
MaxClientLeadTime <TimeSpan>] [-AutoStateTransition <Bool>] [-SafePeriod
<TimeSpan>] [-SharedSecret <string>] [-Force]
```

Description

This cmdlet adds a new IPv4 failover relationship to a DHCP Server. The first parameter set is for adding a failover relationship with load balance mode and the second one is for adding it in hot-standby mode.

Input Parameters

The cmdlet accepts the following parameters

Parameter	Mandatory	Parameter Type	Description
Name	Yes	string	Unique name of the failover relationship to add
PartnerServer	Yes	string	IP address or hostname of the partner server
LoadBalancePercent	No	UInt	Percentage of client requests to be served by the partner server for LoadBalance mode of operation Default: 50%
MaxClientLeadTime	No	TimeSpan	Maximum amount of time that a server can extend a lease for a client's binding over the lease time known by the partner server Default: 1 hour
AutoStateTransition	No	Bool	Enable/disable automatic transition from COMM_INTERRUPTED state to PARTNER_DOWN state {True, False} Default: False (If SafePeriod is specified, this would be set to true.)

Parameter	Mandatory	Parameter Type	Description
SafePeriod	No	TimeSpan	Time period that a server in COMM_INTERRUPTED state will wait before it transitions automatically to PARTNER_DOWN state Default: 1 hour (if AutoStateTransition is specified as True)
ScopeID	Yes	IPAddress	IDs of one or more scopes that are part of the failover relationship
ReservePercent	No	UInt	Percentage of scope IP addresses reserved on the partner server for hot standby mode of operation Default: 5%
ServerRole	No	String	Role of this server in hot standby configuration (Standby, Active) Default: Active
SharedSecret	No	String	Shared secret used for message authentication Default: NULL
Force	No	Switch	If specified, the default confirmation will not be sought when shared secret is specified

Behavior

- This cmdlet will create the failover relationship on both servers with the specified parameters. The scope IDs specified on the source server (local server) are setup identically on the partner server.
- If shared secret is specified, enableauth will be set to true.
- The user will be prompted for confirmation if shared secret is specified.

Adding a Failover Scope

```
Add-DhcpServerv4FailoverScope -Name <string> -ScopeId <IPAddress[]>
```

Description

This cmdlet adds the specified scope(s) to the failover relationship.

Input Parameters

The cmdlet accepts the following parameters

Parameter	Mandatory	Parameter Type	Description
Name	Yes	string	Unique name for the failover relationship to which scopes will be added
ScopeId	Yes	IPAddress	List of scopes to add to a failover relationship

Output Parameters

The cmdlet displays the following output parameters

Parameter	Description
DHCPServer4Failover	An object containing the newly created failover relationship

Behavior

- If there is no failover relationship by the specified name, a terminating error will be returned.
- If any of the specified scopes do not exist or are already part of any failover relationship, a non-terminating error will be returned.
- If the specified ScopeId already exists on the partner server, a non-terminating error will be returned

Removing a Failover Relationship

```
Remove-DhcpServerv4Failover -Name <string[]> [--Force] [-PassThru]
```

Description

This cmdlet removes the failover relationship from a DHCP server.

Input Parameters

The cmdlet accepts the following parameters

Parameter	Mandatory	Parameter Type	Description
Name	Yes	string	Unique name for the failover relationship

Parameter	Mandatory	Parameter Type	Description
Force	No	Switch	If specified, removes the failover relationship even if the failover relationship is not in NORMAL state. If not specified and the failover relationship is in a state other than NORMAL, a non-terminating error will be returned for that failover relationship
PassThru	No	Switch	If specified, causes an object to be returned

Behavior

If any of the failover relationship names specified do not exist on the server, a non-terminating error will be returned.

Removing a Failover Scope

```
Remove-DhcpServerv4FailoverScope -Name <string> --ScopeId <IPAddress[]> [-Force] [-PassThru]
```

Description

This cmdlet removes the specified scope(s) to the failover relationship.

Input Parameters

The cmdlet accepts the following parameters

Parameter	Mandatory	Parameter Type	Description
Name	Yes	string	Unique name for the failover relationship from which scopes will be removed
ScopeId	Yes	IPAddress	List of scopes to remove from a failover relationship
Force	No	Switch	If specified, removes the scope from the failover relationship even if the failover relationship is not in NORMAL state. If not specified and the failover relationship is in a state other than NORMAL, a terminating error will be returned.
PassThru	No	Switch	If specified, causes an object to be returned

Output Parameters

The cmdlet displays the following output parameters

Parameter	Description
DHCPServer4Failover	An object containing information for the removed Class. Returned only if – PassThru is specified

Behavior

For any specified scope which is not part of the specified failover relationship or which does not exist, a non-terminating error will be returned. This will be done before adding the valid scopes to the failover relationship.

Modifying a Failover Relationship

```
Set-DhcpServerv4Failover -Name <string> [--LoadBalancePercent <uint>]
[--ReservePercent <uint>] [-MaxClientLeadTime <TimeSpan>] [--
AutoStateTransition <Bool>] [-SafePeriod <TimeSpan>] [-SharedSecret <string>]
[-PartnerDown] [-Force]
```

Description

This cmdlet modifies the attributes of an existing failover relationship.

Input Parameters

The cmdlet accepts the following parameters

Parameter	Mandatory	Parameter Type	Description
Name	Yes	string	Name of the failover relationship to be modified
LoadBalancePercent	No	uint	Percentage of client request to be served by the partner server in case of LoadBalance mode of operation
ReservePercent	No	uint	Percentage of scope IP addresses reserved on the partner server in case of Hot standby configuration
MaxClientLeadTime	No	TimeSpan	Maximum amount of time that a server can extend a lease for a client's binding over the lease time known by the partner server
AutoStateTransition	No	Bool	<p>Enable/Disable automatic transition from COMM_INTERRUPTED state to PARTNER_DOWN state {True, False}</p> <p>If the user specifies a value for SafePeriod, this will default to true if not specified.</p> <p>If the user specifies AutoStateTransition to false and specifies a value for SafePeriod, a terminating error will be returned.</p>
SafePeriod	No	TimeSpan	<p>Time period that a server in COMMUNICATION INTERRUPTED state would wait till it transitions automatically to PARTNER DOWN state</p> <p>If the user sets AutoStateSwitchOver to true, SafePeriod will default to a value of 1 hour.</p>
ServerRole	No	String	Role of the partner server in case of a hot standby configuration. Values are {Standby, Active}
EnableAuth	No	Bool	<p>Enable/Disable message authentication</p> <p>Disabling message authentication will set shared secret to NULL.</p>
SharedSecret	No	String	Shared secret used for message authentication of failover messages
PartnerDown	No	Switch	If the failover relationship is in COMM_INTERRUPTED state, specifying this switch will change the state to PARTNER_DOWN. However, if the failover relationship is in any other state other than COMM_INTERRUPTED, an NTE will be returned.

Parameter	Mandatory	Parameter Type	Description
Force	No	Switch	If specified, the default confirmation will not be sought when shared secret is specified.

Output Parameters

The cmdlet displays the following output parameters

Parameter	Description
DHCPServer4Failover	Modified failover relationship object

Behavior

- If the failover mode of the relationship is set to LoadBalance, LoadBalancePercent, MaxClientLeadTime, SafePeriod, AutoStateTransition, SharedSecret, and State can be specified.
- If the failover mode of the relationship is set to HotStandby, ReservePercent, MaxClientLeadTime, SafePeriod, AutoStateTransition, SharedSecret, and State can be specified.

Specifying a parameter other than these will cause a terminating error.

- If SharedSecret is specified as a value other than null, EnableAuth will be set to true.
- If null is specified for SharedSecret, EnableAuth will be set to false in the data structure.
- If SharedSecret is specified, default confirmation will display warning the user that the shared secret may be transported in the clear on the network.

Replicating Failover Scopes

```
Invoke-DhcpServerv4FailoverReplication [-Name <string[]>] [-Force]
```

Description

This cmdlet provides a way to replicate scope configuration changes between failover partner servers.

Input Parameters

The cmdlet accepts the following parameters

Parameter	Mandatory	Parameter Type	Description
Name	No	string	Unique name for the failover relationship
Force	No	Switch	If specified, the user will not be prompted for confirmation

Output Parameters

The cmdlet displays the following output parameters

Parameter	Description
IPAddress	An array of IP addresses that identify the scopes which are replicated by the cmdlet

Behavior

- Replicates the configuration of all scopes that are part of the failover relationship to the partner server. If a failover relationship is not specified, all the failover scopes will be replicated to the respective partner servers.
- This cmdlet will seek user confirmation by default for this parameter set.

Displaying Failover Statistics

```
Get-DhcpServerv4ScopeStatistics [-ScopeId <IPAddress[]>] [-Failover]
```

Description

This cmdlet returns IPv4 scope statistics corresponding to the IPv4 Scope IDs specified for a DHCP Server. The cmdlet returns statistics for all IPv4 Scopes if no Scope ID is specified.

Input Parameters

The cmdlet accepts the following parameters

Parameter	Mandatory	Parameter Type	Description
Scopeld	No	IPAddress	An array of IPAddress objects
Failover	No	Switch	If specified, the failover related scope statistics will be returned in the scope statistics object. These object members will be 0 if the switch is not specified.

Output Parameters

The cmdlet displays the following output parameters

Parameter	Description
DhcpServerv4ScopeStatistics	An array of objects containing Scope statistics corresponding to the Scope IDs specified.

The PowerShell object for DHCPv4 scope statistics is as follows:

<i>Type</i>	<i>Name</i>	<i>Description</i>
DhcpServerv4ScopeStatistics		
{		
IPAddress	ScopeId	Scope identifier
string	SuperscopeName	Superscope Name
uint	AddressesFree	No. of free addresses that can be leased out to DHCPv4 clients in the Scope
uint	AddressesInUse	No. of addresses leased out to DHCPv4 clients in the Scope
uint	PendingOffers	No. of unconfirmed addresses in the Scope (offered to DHCPv4 clients but requests have not been received)
uint	ReservedAddresses	No. of addresses reserved in the Scope
real32	PercentageInUse	Scope address utilization percentage
uint	AddressesFreeOnThisServer	If this is a failover scope, this will indicate the number of addresses free on this server based on the ownership assignment of the free address pool. This field will be 0 if this is not a failover scope.
uint	AddressesFreeOnPartnerServer	If this is a failover scope, this will indicate the number of addresses free on partner server based on the ownership assignment of the free address pool. This field will be 0 if this is not a failover scope.
uint	AddressesInUseOnThisServer	If this is a failover scope, this will indicate the number of addresses leased/renewed by this server. This field will be 0 if this is not a failover scope.

uint	AddressesInUseOnPartnerServer	If this is a failover scope, this will indicate the number of addresses leased/renewed by partner server. This field will be 0 if this is not a failover scope.
}		