|  |
| --- |
|  |
| Using DHCP Failover Auto Config Sync |
| A guide to a tool for automating synchronization of scope configurations in a DHCP failover setup |

|  |
| --- |
|  |

Using DHCP Failover Auto Config Sync

# Introduction

DHCP is one of the critical components of an IT environment today. Ensuring its continuous availability is one of the top priorities of any IT administration. In Windows Server 2012, DHCP server can be configured to provide high availability by pairing two DHCP servers in a failover relationship. Two DHCP servers in a failover relationship synchronize the IP address lease information on a continual basis there by keeping their respective databases up-to-date with client information and in sync with each other.

However, if the user makes any changes in any property/configuration (e.g. add/remove option values, reservation) of a failover scope, he/she needs to ensure that it is replicated to the failover server. Windows Server 2012 provides functionality for performing this replication using DHCP MMC as well as PowerShell. But these require initiation by the user. This requirement for explicitly initiating replication of scope configuration can be avoided by using a tool which automates this task of replicating configuration changes on the failover server. **DHCP Failover Auto Config Sync** (DFACS) is a PowerShell based tool which automates the synchronization of configuration changes. This document is a guide to using DFACS.

# DHCP Server Failover Feature

The DHCP failover feature can be used in two relationship modes:

**Load Balance (Active-Active):** Two independent DHCP servers share the responsibility for servicing clients in a scope or a set of scopes as per a configured load balance ratio. In case anyone of the servers fails the other assumes the complete responsibility for servicing the clients.

**Hot Standby (Active-Passive):** A DHCP server can be designated as a standby server for a primary DHCP server. The standby server assumes the load in case primary server goes down.

Both these modes increase the redundancy of DHCP service in the network and make it more fault-tolerant. This failover feature can be used in different topologies like hub and spoke topology or ring topology.

*The feature has been explained in greater detail on* [*http://technet.microsoft.com/en-us/library/hh831385.aspx*](http://technet.microsoft.com/en-us/library/hh831385.aspx)

# Replication of scope configurations

The first time failover is configured on a server, the scopes involved are replicated to the failover/partner server. Post that, any changes in the configuration of these scopes on any one of the servers need to be replicated on the other by invoking the “**Replicate scope**” or “**Replicate Relationship**” action in DHCP MMC (***Invoke-DhcpServerv4FailoverReplication*** cmdlet in DHCP PowerShell) in order to ensure that clients get the same configuration irrespective of the DHCP server that serves their request. The admin can automate this by using a tool that replicates scope configuration changes on a periodic or event driven basis.

# DHCP Failover Auto Config Sync (DFACS)

DFACS is a tool which tracks any scope configuration changes and replicates them on the failover server. The tool uses the configuration change events logged by the DHCP server in the operational channel to determine if there has been a configuration change in any of the scopes of a failover relationship. If it finds any such change it replicates that change to the failover partner server. In addition to the configuration sync being triggered by configuration change events, the tool also periodically performs synchronization of configuration changes to the failover partner server.

DFACS integrates seamlessly with the Windows Task Scheduler. This ensures the following:

* An instance of DFACS is always running unless explicitly terminated. The Task Scheduler starts an instance of it at system startup.
* DFACS can be provided suitable user credentials and can run even in remote server management scenarios where no users may login to the machine.

The tool can run in two modes:

* **Default Replication mode**: The tool monitors and synchronizes configurations of all scopes of all failover relationships that the server is a part of.
* **Selective Replication mode**: The tool monitors and synchronizes configurations of all scopes of only specified failover relationships that the server is a part of.

*Note: The Selective Replication mode can be used to make exclusions only at the relationship level and not at the scope level.*

DFACS, by its design, can be used only in cases where configuration changes for scopes in a failover relationship are always made on only one of the DHCP servers in the failover relationship. Running DFACS on both servers to cater to the same failover relationship will cause one of the instances of DFACS to terminate. Nevertheless, it can run on the two servers if it is configured to run in **Selective Replication** mode and to cater to different failover relationships on each of them. The **Selective Replication** mode can be particularly useful in topologies where the primary server can be in failover relationships with a number of servers and changes for only selective relations are to be considered. Some complex topologies where Selective Replication mode can come handy are shown below:

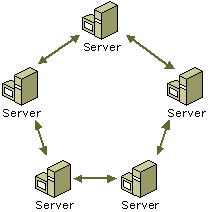
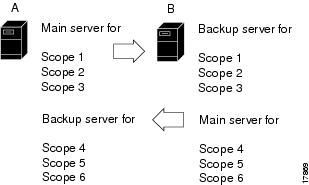


Fig. 1. Some failover setups where Selective Replication mode of DFACS can be useful

## How to use the tool

DFACS comes as a packaged zip file and consists of two PowerShell scripts and an xml file. The xml file contains values for settings like periodic retry interval and name of the log file. Using the xml file, the administrator can also set the tool to run in a **Selective Replication** mode and specify the failover relations that are to be included/excluded in/from the sync process.

The procedure for installing and running DFACS has been described in the steps below:

1. Extract the contents of the tool package (DhcpFailoverAutoConfigSyncTool.zip) to a folder.
2. Ensure that the settings for DFACS in the xml file have been set as desired. (See [Changing the settings of the tool](#_Changing_the_settings) for details)
3. Open Windows PowerShell in administrative mode by right clicking on PowerShell button and selecting “Run as Administrator” option.
4. Change current directory in PowerShell to the folder where the tool package contents have been extracted.
5. Ensure security is removed from both downloaded scripts ( install.ps1, DhcpFailoverAutoConfigSyncTool.ps1). To do this you can use PS command let “Unblock-File <FileName>” or right click on file, go to Properties and under Security click “Unblock”.
6. Ensure the execution policy has been set to ‘unrestricted’. The status of the execution policy can be retrieved by executing *Get-ExecutionPolicy*. It can be set to ‘unrestricted’ by executing *Set-ExecutionPolicy -ExecutionPolicy Unrestricted*.
7. Ensure the account running DFACS has permissions to modify the registry path: HKLM\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters\DHCPAutoSync and also account is part of group “WinRMRemoteWMIUsers\_\_”
8. Run the script: .\**install.ps1**. This will install DFACS as a task in the task scheduler.

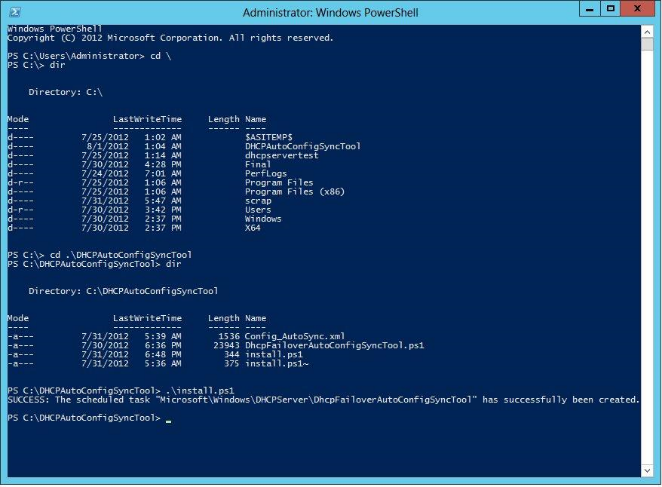
**

Fig. 2. Installing DHCP Failover Auto Config Sync using PowerShell

1. To run the tool, start Windows Task Scheduler and navigate in the tree view of the navigation pane to Task Scheduler Library->Microsoft->Windows->DHCPServer.

*Refresh the folder in the navigation pane if the task scheduler is already running. The folder DHCPServer might be located at the bottom of the list.*

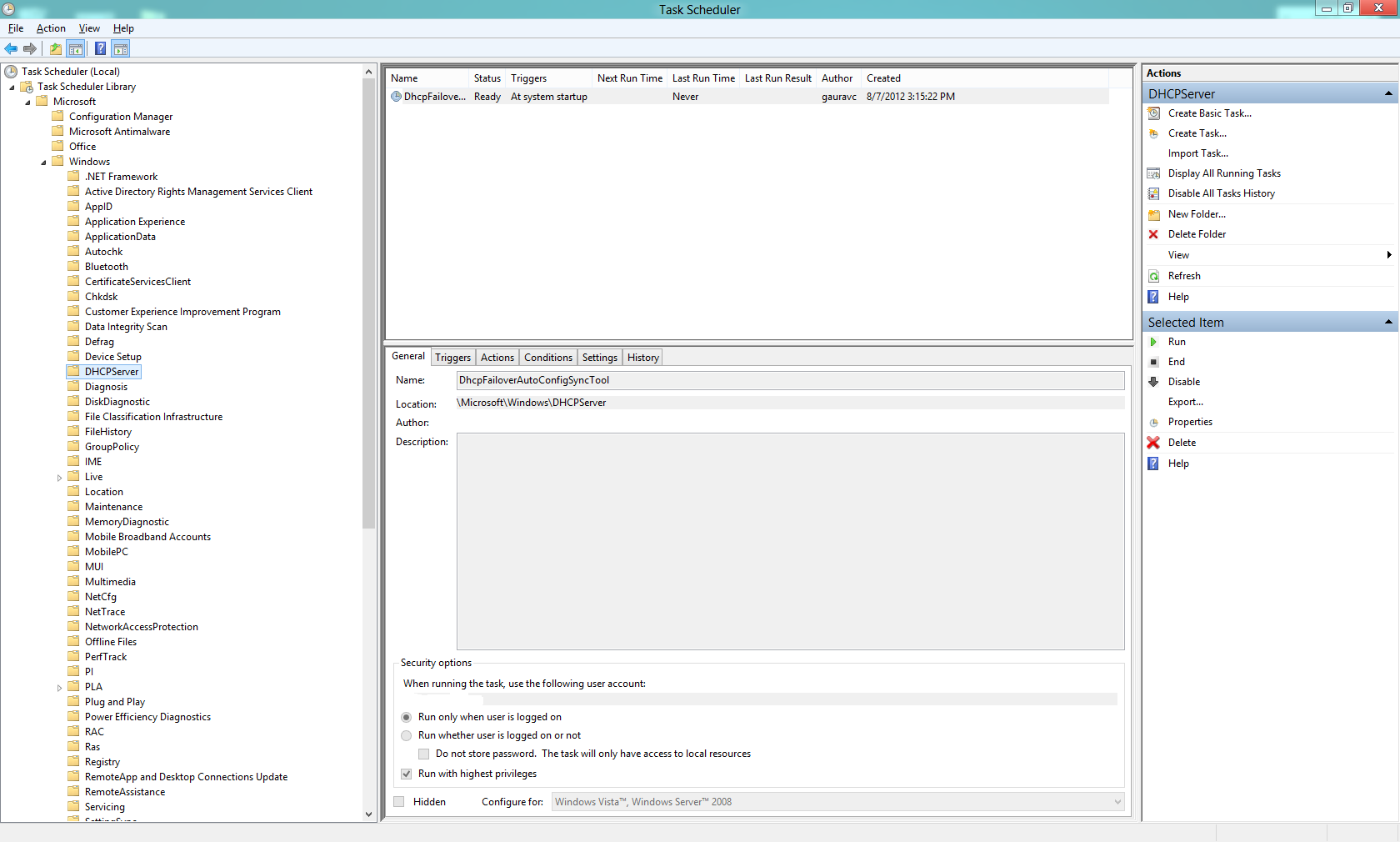


Fig. 3. A Task for DFACS created in the task scheduler

1. Right click on the task DHCPFailoverAutoConfigSyncTool and click on Properties.
2. Under Security Options, in the General tab, select ‘Run whether user is logged on or not’. Click OK and provide the appropriate credentials when prompted.

*The account must be a part of the DHCP administrators group and have the required privileges to start the tool on the machine on system startup and to replicate the changes on the failover partner.*

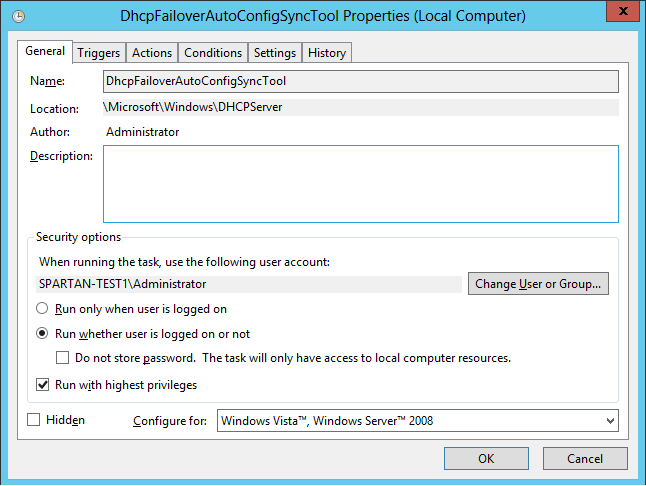
**

Fig. 4. Select ‘Run whether user is logged on or not’ in the General Tab of Properties

1. Right Click on the task DHCPFailoverAutoConfigSyncTool and click Run.
2. The tool logs the record of all the synchronizations done in the log file (by default created in the folder where the tool package was extracted). This can be useful in troubleshooting.

## Changing the settings of the tool

The xml file can be used to configure some important settings of DFACS. The file along with the configurable settings has been shown below:

<PSDhcpAutoSync>

<! -- File where console logs are created -->

<LogFileName>.\DhcpAutoSyncLogfile.txt</LogFileName>

<!--

Periodic Retry Interval (in minutes)

This is the duration between two successive Failover Replication attempts

-->

<PeriodicRetryInterval>30</PeriodicRetryInterval>

<!--

**Default Replication Mode:**

By default, the tool auto synchronizes the changes across all

Failover relations on this server

**Selective Replication Mode:**

If you choose to include only specific Failover relation(s) that

should be synchronized by this tool, do the following

a) Uncomment <FailoverRelationships> node given below

b) Add the Failover relationship names under <Include> node,

the ones you wish the tool should auto synchronize.

[This means, all the other relationships will be ignored by the tool]

c) Add the Failover relationship names under <Exclude> node,

the ones you wish the tool should Exclude from auto synchronization.

[This means, all the other relationships will be

considered by the tool for auto synchronization]

-->

<!--

<FailoverRelationships>

<Include>

<Relation>FailoverServer1-FailverServer2</Relation>

</Include>

<Exclude>

<Relation>FailoverServer1-FailoverServerver3</Relation>

</Exclude>

</FailoverRelationships>

-->

</PSDhcpAutoSync>

The tags and the settings that can be used to configure are:

* **<LogFileName>** tag contains name/path of log file where all logs are dumped.
* **<PeriodicRetryInterval>** tag contains the frequency time in minutes at which the tool automatically synchronizes pending configuration changes. A very small periodic retry interval will lead to more CPU usage by the tool.
* **<Include>** tag contains name of the relations to be included for consideration in automatic sync process on this server. If nothing is mentioned in **<Include>** tag, all relations other than the relations mentioned in **<Exclude>** tag will be considered.

# Usage Guidelines

* The configurations of the scopes involved should be in sync prior to starting the tool.
* Any change in the xml configuration file will require the tool to be restarted to take effect.
* When running in selective replication mode where relationships to be excluded are mentioned; creation of a new failover relationship (which is intended to be included in the sync process) will require the tool to be restarted to take effect.
* The task Scheduler can also be made to keep a history log of the operations of the task DHCPFailoverAutoConfigSyncTool task. This is a common setting for all the tasks in the Task Scheduler. Details can be found at <http://technet.microsoft.com/en-us/library/cc722006.aspx>.
* Use DFACS only on one of the servers in a failover relationship. It is on this server that any changes in the configuration of the scopes involved must be made. Any attempt to run the tool on both the servers to synchronize scope configuration changes of their failover relationship will abort that instance of the tool which was started later. Use Selective Replication mode if DFACS is to cater to different failover relationships on the two servers.
* DFACS uses the event log file of DHCP server. The size of this event log file should hence be large enough so that no change log gets erased before it is read.
  + Go to ‘Event Viewer’ application.
  + In the left pane click on Applications and Services Logs > Microsoft > Windows > DHCP-Server.
  + Right click on “Microsoft-Windows-Dhcp-Server/Operational” log and click on “Properties”.
  + Change Maximum log size to around 10 MB i.e. 10240 KB and click Apply and Ok.
* Ensure that PeriodicRetryInterval is not less than 1 minute as it can lead to a high CPU usage.
* DFACS can also be run in a command shell window. To do this right click on the task DHCPFailoverAutoConfigSyncTool in the Task Scheduler and click on Properties. Go to the Actions tab and click on Edit. Delete the ‘-WindowsStyleHidden’ argument from the add arguments text box and click OK. End the DHCPFailoverAutoConfigSyncTool task and Start it again. This would make DFACS run in a visible window. Closing the visible window would terminate the tool.

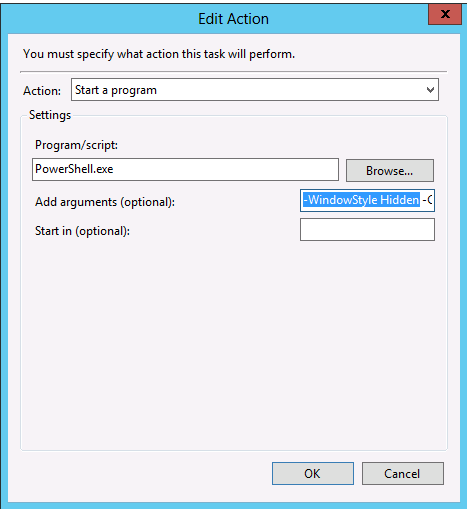


Fig. 5. By removing the ‘-WindowsStyleHidden’ argument, the tool can be made to run in a visible window

* If DFACS is to be stopped on the current server for starting an instance of it on the failover server the following steps must be observed:
* The DHCPFailoverAutoConfigSyncTool task must be stopped on the current server.
  + The registry entry for the tool must be deleted from the current server. The registry entry can be deleted using Registry Editor. It resides at *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters\DHCPAutoSync*
* For the tool to continue functioning, any changes in the credentials being used by the tool must be manually updated in the credentials stored with the Task Scheduler.

*For eg. If the password of the credentials has to be changed due to expiry, the new password must also be provided to the instance of the tool in the Task Scheduler.*

* For more information on the usage, use .\DhcpFailoverAutoConfigSyncTool.ps1 –h

# Limitations

DFACS has the following limitations which are important for consideration while using it:

* It cannot be used in cases where configuration changes for scopes in a failover relationship are being made on either of the DHCP servers.
* Following scope configuration changes are not instantaneously synchronized by the tool as there are no events logged for these changes in DHCP operational event log. However, these changes will get synchronized in the periodic synchronization process.
  + Scope IP range change in scope properties.
  + Activation/Deactivation of policies under scope.
  + Deletion of scope options.
* Configuration changes made to server level configuration (e.g. server level options, policies etc) are not synchronized by this tool.