DWS Management Console

DWS MMC 3.0 client

Contents

Requirements

- Microsoft .NET 2.0
- Microsoft Management Console (MMC) 3.0
  - MMC 3.0 is native for Windows Server 2003 R2 and Vista
  - MMC 3.0 for Windows Server 2003 and XP
    - http://support.microsoft.com/?kbid=907265

Installation

Run install.bat found in the same directory as this document. To start DWS MMC, double-click the Microsoft Common Console Document, dws.msc. Custom consoles can be created by making a new MSC file:

- Start → Run → MMC
- File → Add/Remove Snap-in…

- Add, DHCP Web Services Console

DWS MMC can be uninstalled by running uninstall.bat.

Usage

DWS MMC allows users to consume DHCP Web Services from a Windows OS platform. DWS MMC can support multiple user 'profiles' within a console MSC file. When new profiles and servers are added, the MMC will save the associated connection data within its MSC file. The DWS MMC can manage any DHCP server accessible through DWS.

Profiles

A profile contains a user account ID and a DHCP Web Services connection URL. This allows DWS MMC the ability to support multiple user accounts within one console document. Once a profile is created, it will be saved to the MSC file when the DWS MMC is closed, thus allowing profile data to be saved across console shutdowns. To create a new DWS profile:

- Right click the DWS root node and select '**Create Profile…**'
    - **Profile Name**: Identifying name of profile
    - **DWS URL**: The directory URL of DHCP Web Services, for example, the value of URL would be https://server/dws/, if the URL path containing DhcpOperations.asmx and DhcpSecurity.asmx files.
    - **Username**: User account authorized to use DWS
    - **Domain**: User's Active Directory domain

DHCP Servers

Once a profile is created, management of one or more DHCP server can begin. The set of DHCP servers DWS can manage depends on the installation and setup of DWS itself (See DWS-Install document). Also, the user account assigned in the profile must have some authorizations set for the DHCP Server (See Permissions section); otherwise the user may not see any subnets once they add a DHCP server to the MMC. To add a DHCP server:

- Right click profile node, '**Manage DHCP Server…**'
- **DHCP Server IP**: IP address of DHCP server to manage

Server-wide Dynamic DNS configurations can be changed by right clicking a server node and selecting **properties**.

Search the DHCP server's client lease database: right click a server node and select '**Search…**'

DHCP servers added to the DWS MMC will be saved to the MSC file, allowing servers to be saved across console shutdowns.

Subnets

DHCP subnets are networks in which connected network devices (DHCP clients) are served IP and network configurations from DHCP server. To create a new subnet:

- Right click server node, '**Create Subnet…**'
- **Name**: A name for subnet
- **Description**: A description of subnet
- **Range**
  - The range of IP address belonging to subnet will be served IP and network configurations
  - **Start IP**: Start IP address of range that the DHCP server will manage
  - **End IP**: End IP address of range that the DHCP server will manage
- **Mask**: Network mask of subnet
- **Lease Time**: Lease time duration of dynamic clients
- **State**: Refers to state of service for subnet. Enabled – Subnet is serving client, Disabled – Subnet is not serving clients

DHCP subnets can be changed by right clicking the subnet node and selecting **properties**. Within properties, Dynamic DNS (DNS tab) and BOOTP (Advanced tab) can be changed.

Search the subnet's client lease database: right click a subnet node and select '**Search…**'

Address Pools

Address pools node contains a pool that makes up the subnet's default IP range and zero or more exclusion pools. The default pool can be type Dhcp, Bootp, or Both, configured in the subnet properties advance tab. Exclusion pools are address ranges within the subnet and mark exclusion IP addresses that should not be served leases by the DHCP server. To create a new pool:

- Right click Address Pools node, select '**New Exclusion Range…**'
  - **Start IP**: Start IP address of exclusion pool
  - **End IP**: End IP address of exclusion pool

Leases

Leases node is mostly a read only node, showing information about client leases that have been established within the network via DHCP. A client lease can be deleted by right clicking the client lease and selecting delete. This node will also show reservations that have been made in the same DHCP subnet and whether the reservation is active or not.

Reservations

The reservation node shows the current IP reservations made within the DHCP subnet. To create a new reservation:

- Right click Reservations node, select 'Add Reservation…'
    - **Name**: Name identifier of client, usually the client's hostname
    - **IP Address**: IP address that should be assigned to client
    - **MAC Address**: Hardware address that identifies client to DHCP server
    - **Description**: A description for client
    - **Client Type**: DHCP, BOOTP, or Both allowed client type for this reservation

An IP reservation can be changed by right clicking the reservation and selecting **properties**.

DHCP Options

DHCP options are network related configurations that are sent to a DHCP client upon receiving a lease from the DHCP server. DHCP options can be assigned values at three levels of the DHCP server and are hierarchic. The three levels are server, subnet, and reservation. If an option's value is set at the server level, then subnets and reservations under that server will receive the same option value. Option values can be set via the Options node under the server or subnet nodes in the MMC. To set a reservation's options, right click the reservation, select **properties**, and chose the Options tab.

Some common option and values type are:

DHCP Option	Data Type	Example values
003 – Router	Array of IP addresses	192.168.0.1
006 – DNS Servers	Array of IP addresses	192.168.0.5, 192.168.0.6
015 – DNS Domain Name	String	unf.edu

See http://www.faqs.org/rfcs/rfc2132.html for more information on DHCP options.

There is also a concept of option classes, which includes three types: DHCP, BOOTP, and Routing and Remote clients. An option can be assigned a value for a specific type of client class. For example, if the router option was set within the BOOTP class. Then only BOOTP client types would receive that router option value when receiving a lease from DHCP server.

Permissions and Security Trimming

Users whom have been granted global administrator rights within DWS will see permission nodes throughout the DWS MMC tree. Permission nodes allow administrators to assign various authorizations to sections of the DHCP server to users. Those users can then manage that section (or scope) of the DHCP server.

The authorizations layer of DHCP Web Services allows scope-sensitive, role-based access controls over the DHCP server. In general, this means it allows user accounts various access rights to DHCP objects within the server that normally only a server administrator could manipulate. More specifically, authorization scopes, in this application, are defined at three levels in a DHCP server: at the **server**,

subnet and **IP range** levels. Each of these scopes contains three possible role assignments: **Owner**, **Manager**, and **Auditor**. There are four operations that generally represent the operations that can occur when managing a DHCP server: Create, Read, Update, and Delete. The **Owner** role is assigned all operations, the **Manager** role is assigned Read and Update, and the **Auditor** role is assigned only the Read operation. User accounts are assigned roles within scopes, which means those accounts would have particular rights to DHCP objects for a particular layer of the DHCP server, but not others. So, if a user is assigned the **Manager** role, he is allowed to Read and Update DHCP objects, but not Create nor Delete those objects. And because this authorization layer is scope-sensitive, if that same user is authorized to manage only one subnet, he can only Read and Update objects on that specific subnet. It is important to mention that these authorization scopes are hierarchical in nature, which means the user can manage all DHCP objects underneath the highest layer for which he has authorization. Using the previous example, the user that is authorized to manage only a subnet, also has access to the lower IP range level. In addition to the previously mentioned authorization scopes is one specialized scope that contains two special Global roles: Global Administrator and Global Auditor. These roles have full control or read-only access, respectively, over all servers that are managed through DHCP Web Services. The table below shows the list of DHCP operations with the minimum access role and scope assignments needed to execute that operation.

DHCP Operation	Role	Scope
EnumSubnets	Auditor	IP Range
CreateSubnet	Owner	Subnet
DeleteSubnet	Owner	Subnet
UpdateSubnet	Manager	Subnet
UpdateSubnetRange	Manager	Subnet
CreateSubnetExclusion	Manager	Subnet
DeleteSubnetExclusion	Manager	Subnet
SubnetFindAllClients	Auditor	IP Range
SubnetFindOneClient	Auditor	IP Range
ServerFindAllClients	Auditor	Server
ServerFindOneClient	Auditor	Server
EnumPools	Auditor	Subnet
EnumLeases	Auditor	IP Range
CreateLease	Owner	IP Range
UpdateLease	Manager	IP Range
DeleteLease	Owner	IP Range
CreateReservation	Owner	IP Range
UpdateReservation	Manager	IP Range
DeleteReservation	Owner	IP Range
EnumReservations	Auditor	IP Range
SetOptionValue	Manager	Scope Specific

RemoveOptionValue	Manager	Scope Specific
EnumOptionValues	Auditor	Scope Specific
GetOptionValue	Auditor	Scope Specific

Authorizations are enforced using two methods. The first is a direct allow/deny method. If a user does not have sufficient authorization access to complete an operation, like **CreateSubnet**, the operation will throw an unauthorized exception. Otherwise, the operation will allow the creation to occur. The second method is security trimming. In this approach, DHCP operations that return a set of DHCP objects are 'trimmed' to exclude objects to which the user does not have access. For example, if a user has read access to a range of IP addresses within a subnet, and executes the **EnumClients** operation, the operation would normally return all client leases within that subnet. With security trimming, however, the caller will only receive client leases within the range of IP addresses to which he has been granted read access. Furthermore, the set of client leases could be empty if the user does not have access to read any leases within a subnet.

Searching

Searching allow users to query a DHCP server for client leases based on regular expression patterns. The search filter allows three terms to be used in a query: client hostname, client IP address, and client MAC address. The search filter matches based on a logical AND condition of non-empty terms. The regular expression patterns should follow the .NET regular expression language definition, http://msdn2.microsoft.com/en-us/library/az24scfc(VS.80).aspx.

Examples:

Terms	Patterns	Results
IP:	^192.168.2.*$	Client leases that contain first 3 bytes 192.168.2 AND their MAC address ends with byte D8
Mac:	*D8$	
Name:		
IP:		Client leases containing hostnames ending in unf.edu
Mac:		
Name:	^*.unf.edu$	