How to Configure DHCP Parameter Templates

https://campus.barracuda.com/doc/73719085/

Create DHCP parameter templates to simplify the configuration of multiple DHCP subnets. Specify time settings for leases and updates, configure networking settings, and apply them to your client address pools.

Before You Begin

Before configuring DHCP parameter templates, enable advanced pool configuration in the DHCP service setup. For more information, see How to Configure Advanced DHCP Settings.

Step 1. Configure Lease Constraints

1. Go to **CONFIGURATION** > **Configuration Tree > Box** > **Virtual Servers** > ***your virtual server*** > **Assigned Services** > **DHCP** > **DHCP Enterprise Configuration**.
2. In the left menu, expand **Configuration Mode** and click **Advanced View**.
3. In the left menu, select **Parameter Templates**.
4. Click **Lock**.
5. In the **Parameters** table, click **+** to add a parameter template.
6. Enter a **Name** for the template and click **OK**. The **Parameters** window opens.
7. In the **Lease Constraints** table, configure the following settings:
   - **Max Lease Time** – The maximum length of time in seconds that will be assigned to a lease. The only exceptions to this setting are Dynamic BOOTP lease lengths, which are not specified by the client.
   - **Def Lease Time** – The default length in seconds that is assigned to a lease.
   - **Min Lease Time** – The minimum length in seconds that is assigned to a lease.
   - **Reply Delay** – The minimum number of seconds since a client began trying to acquire a new lease before the DHCP server will respond to its request. The number of seconds is based on what the client reports, and the maximum value that the client can report is 255 seconds. If you specify *1* second, the DHCP server will not respond to the client's first request but will always respond to its second request. This setting can be used to set up a secondary DHCP server which never offers an address to a client until the primary server has been given a chance to do so. If the primary server is down, the client will bind to the secondary server, but otherwise clients should always bind to the primary.

     This does not, by itself, permit a primary server and a secondary server to share a pool of dynamically allocatable addresses.

Step 2. Configure Dynamic DNS Parameters

Configure dynamic DNS settings if DNS updates are enabled and **ddns-update** (see How to Configure DHCP with Dynamic DNS) is set to *interim*.

1. From the **Do Fwd Updates** list, select whether the DHCP server should attempt to update a DHCP client's A record if the client acquires or renews a lease.
   - **true** – Forward updates are enabled, and the DHCP server will also honor the setting of the client-updates flag.
   - **false** – The DHCP server only attempts to update the client's PTR record if the client supplies an FQDN that should be placed in the PTR record using the 'fqdn' option.
2. From the **Optimized Updates** list, select one of the following options:
   - **true** – The DHCP server will only update when the client information changes, the client gets a different lease, or the client's lease expires.
   - **false / not-set** – If set for a given client, the server will attempt a DNS update for that client each time the client renews its lease, rather than only attempting an update when necessary. This allows the DNS to heal from database inconsistencies more easily, but the DHCP server must do many more DNS updates.
3. Leave **Update Static Leases** as default (*false*) unless instructed otherwise.
   DNS updates for static IP addresses are not recommended because the DHCP server will not tell that the update has been done, and therefore will not delete the record when it is not in use. Also, the server must attempt the update each time the client renews its lease, which could have a significant performance impact in environments that place heavy demands on the DHCP server.
4. Enter the **DDNS Domainname** that should be appended to the client's hostname to form a FQDN.
5. In the **Rev DDNS Domainname** field, you can change the domain name (default= in-addr.arpa.) for use in the client's PTR record, that should be appended to the client's reversed IP address (e.g. 74.92.17.10.in-addr.arpa. for client 10.17.92.74).
6. In the **Dynamic BOOTP Lease Time** field, you can specify the length in seconds of leases dynamically assigned to BOOTP clients. At some sites, it may be possible to assume that a lease is no longer in use if its holder has not used BOOTP or DHCP to get its address within a certain time period. If a client reboots using BOOTP during the timeout period, the lease duration is reset to this length, so a BOOTP client that boots frequently enough will never lose its lease.
   Use this setting with extreme caution!
7. In the **Boot File Server** field, enter the host IP address of the server from which the initial boot file (specified in the file name statement) is to be loaded. If this setting does not apply to a given client, the IP address of the DHCP server is used.
8. In the **Boot File** field, enter the name of the initial boot file which is to be loaded by a client. The file name should be recognizable to the file transfer protocol used to load the file.

Step 3. Configure Miscellaneous Parameters

Configure address assignment for clients without host declaration, and specify domain lookup and ping checking behavior. Some BOOTP clients expect RFC1048-style responses, but do not follow RFC1048 when sending their requests. In this case, the client is not getting the options that you have configured for it and the server log the message '(non-rfc1048)' is printed with each BOOTREQUEST that is logged. To send RFC1048 options to such a client, you can set the *always-reply-rfc1048* option (**RFC1048 Conformance**) in that client's host declaration and the DHCP server will respond with an RFC-1048-style vendor options field.

1. From the **Boot Unknown Clients** list, select one of the following options:
   - **true / not-set** – Clients without host declaration are allowed to obtain IP addresses, as long as those addresses are not restricted by 'allow' and 'deny' statements within their pool declarations.
   - **false** – Clients without host declaration will not be allowed to obtain IP addresses.
2. From the **RFC1048 Conformance** list, select one of the following options:
   - **true** – Response in RFC 1048-style. This flag affects all clients that are covered by the respective scope.
   - **false** – Response NOT in RFC 1048-style.
3. From the **Hostname via Rev-DNS** list, select whether or not DHCP looks up the domain name corresponding to the IP address of each address in the lease pool and uses that address for the DHCP hostname option:
   - **true** – Lookup is done for all addresses in the current scope.
   - **false** – No lookups are done.
4. From the **Ping Check** list, select whether or not an ICMP echo request is sent to the address being assigned.

   If the DHCP server dynamically allocates an IP address to a client, it first sends an ICMP echo request (ping) to the address being assigned. It waits for a second, and if no response is heard, it assigns the address. If a response is heard, the lease is abandoned, and the server does not respond to the client. This setting introduces a default one-second delay in responding to DHCPDISCOVER messages, which can be a problem for some clients.

   - **true** – Ping check is done for all addresses in the current scope.
     - In the **Ping Timeout** field, specify how many seconds the DHCP server should wait for an ICMP echo response. If a response is not received before the timeout expires, it assigns the address. If a response is heard, the server does not respond to the client.
   - **false** – No ping checks are done.
   - **not-set** – (default) Deactivates the setting.
5. Click **OK**.
6. Click **Send Changes** and **Activate**.

Now you can apply your configured template to your DHCP subnets. Fore more information, see How

to Configure DHCP Subnets and Address Pools.

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.