بسم الله الرحمن الرحیم

عنوان تحقیق

Policy based assignment (PBA) DHCP

استاد محترم: جناب آقای مهندس منصوری

نگارنده: یوسف رشیدی

جهت درس: MCSA 2016

هدف کلی تحقیق

انواع Policy در DHCP

اهداف جزئی

۱. آشنایی با PBA

۲. آشنایی با انواع دسته بندی

۳. آشنایی با مزایای DHCP Policy

هدف کاربردی

اختصاص اتوماتیک ۱. IP Address ۲. Subnet Mask ۳. Default Gateway ۴. Domain Name System برای کاربران یک شبکه با استفاده از Policy

Policy based assignment (PBA) DHCP

مقدمه

در مقاله قبلی در مورد سرور DHCP در ویندوز سرور ۲۰۱۶، گفتگو کردیم. این مقاله در مورد یک ویژگی جدید دیگر در سرور DHCP در سیاست‌های ویندوز سرور ۲۰۱۶ بحث می‌کند. این ویژگی همچنین به عنوان آدرس IP مبتنی برسیاست (PBA) به اختصار یاد می‌شود.

سناریوهای زیر را در نظر بگیرید که مدیران با آن مواجه هستند:

Subnet شما ترکیبی از انواع مختلفی از client ، کامپیوتر رومیزی، چاپگر، گوشی‌های IP و غیره دارد. شما از انواع مختلفی از client ها برای دریافت آدرس‌های IP از نشانی IP مختلف در داخل این زیرشبکه استفاده خواهید کرد.

در یک زیرشبکه که ترکیبی از کامپیوترهای کابلی و تلفن همراه دارد، ممکن است بخواهید مدت‌زمان کوتاه‌تر اجاره را به کامپیوترهای موبایل تخصیص دهید (به عنوان مثال ۴ ساعت) و مدت‌زمان اجاره طولانی‌تر را به کامپیوترهای سیمی اختصاص دهید (به عنوان مثال ۴ روز).

استقرار شما نیازمند این است که شما کسی را کنترل کنید که به شبکه شما دسترسی داشته باشد، یعنی شما می‌خواهید سرویس DHCP را برای یک سری از مشتریان شناخته‌شده (براساس آدرس MAC) برای هر زیرشبکه تامین کنید.

با استفاده از کارمندان خود (گوشی‌های هوشمند، تبلت) در محل کار، شما می‌خواهید دسترسی به اینترنت و یا دسترسی به شبکه را براساس نوع دستگاه کنترل کنید.DHCP Policies مدیریت DHCP را با یک اهرم بسیار مفید برای رسیدن به این سناریوها فراهم می‌کند.

به عنوان مثال ویندوز سرور ۲۰۰۸، یک Admin آدرس IP و مقادیر دیگر را برای یک دامنه و زیرشبکه پیکره بندی می‌کند. همه Client ها که در این محدوده / subnet هستند یک آدرس IP

از این دامنه آدرس IP دریافت می‌کنند و گزینه‌های پیکربندی شده برای این حوزه را دریافت می‌کنند. اگر یک مدیر سرور DHCP نیاز داشته باشد تا دامنه آدرس IP را به یک کلاس خاص از Client ها یا دستگاه‌ها ارایه دهد همانطور که مطرح‌شده هیچ راهی برای یک مدیر جهت دستیابی به آن وجود ندارد (مگر اینکه از شروط فردی استفاده کند که برای مدیریت بسیار فشرده می باشد). بنابراین، Policies DHCP در ویندوز سرور ۲۰۱۶ به مدیر کمک می‌کند تا دقیقاً به آن دست یابد.(یک مکانیسم دقیق‌تری برای تعیین آدرس‌های IP و گزینه‌ها)

Policies DHCP چیست؟

با ویندوز سرور ۲۰۱۶ می‌توانید Policy هایی در مورد سرور DHCP ایجاد کنید. یک Policy شامل ۲ بخش اصلی conditions and settings است. Conditions به شما این امکان را می‌دهد که Client ها را گروه‌بندی کنید. تنظیمات پارامترهای پیکربندی شبکه مانند آدرس IP، گزینه‌ها، مدت‌زمان اجاره می باشند ، که به Client ها در پاسخ سرور DHCP ارایه می‌شوند. Condition را می‌توان براساس مجموعه‌ای از زمینه‌ها مشخص کرد که DHCP Client در درخواست ارایه می کند. مدل Policy نسبتاً ساده است: هر درخواست DHCP Client به Condition یک Policy ارزیابی می‌شود. اگر یک درخواست Client منطبق با Condition در Policy باشد، تنظیمات مربوط به یک Policy از طریق واکنش سرور DHCP برای Client فراهم خواهد شد.در ویندوز سرور ۲۰۱۶، می‌توانید پنج معیار مختلف مشخص کنید (یک مجموعه ثابت) که براساس آن می‌توان گروهی از Client ها را جدا کنید.

۱. MAC Address
۲. Vendor Class
۳. User Class
۴. Client Identifier
۵. Relay Agent Information (and its sub options – remote id, circuit id and subscriber id)

تنظیمات (Settings)

هنگامی که یک Client با شرایط یک Policy منطبق می‌شود، سرور DHCP براساس تنظیمات یک Policy به Client پاسخ می‌دهد. تنظیمات مربوط به یک Policy می‌تواند DNS یا IP باشد. یک مدیر می‌تواند این Policy را پیکربندی کند تا نشانی IP را از Scope فرعی مشخص‌شده در محدوده آدرس IP کلی ارایه دهد. همچنین می‌توانید ارزش‌های گزینه متفاوتی را برای Client هایی که این Policy را استفاده می‌کنند، فراهم کنید.

Policy ها را می‌توان به صورت گسترده یا برای یک دامنه خاص تعریف شوند. یک Policy گسترده سرور برای همه محدوده‌ها در سرور DHCP قابل‌استفاده هستند. با این حال، یک Policy گسترده سرور نمی‌تواند دامنه آدرس IP مرتبط داشته باشد.

علاوه بر دامنه آدرس IP و گزینه‌هایی که می‌توانند با یک Policy مرتبط باشند، تنظیمات قابل‌توجه دیگر برای یک Policy وجود دارد. شما می‌توانید آدرس IP را برای یک Policy تنظیم کنید. این به شما این امکان را می‌دهد که مدت‌زمان اجاره طولانی‌تر یا کوتاه‌تر برای مشتریانی که با شرایط Policy همخوانی دارند، پیکربندی کنید. همچنین می‌توانید نحوه عملکرد سیستم DNS برای تطبیق مشتریان با شرایط Policy را پیکربندی کنید.

یک Policy می‌تواند تنها محدوده آدرس IP (بدون هیچ گزینه) یا تنها گزینه (هیچ محدوده آدرس IP) را به عنوان یک تنظیمات داشته باشد.

آشنایی با multiple policies

شما می‌توانید بیش از یک Policy را در scope یا حتی در عرض سرور پیکربندی کنید. هر Policy یک دستور پردازش اختصاص‌داده‌شده را دارد. در حالی که پردازش درخواست مشتری، سرور DHCP، درخواست‌های مشتری علیه شرایط در Policy های مختلف را براساس نظم پردازش

Policy ارزیابی می‌کند. با دستور پردازش ۱ که در ابتدا پردازش می‌شود. Policy های سطح scope اول بوسیله سرور DHCP و پس از آن Policy های گسترده سرور پردازش می‌شوند.

اگر یک مشتری شرایط بیش از یک Policy را برآورده کند، تنظیمات را به روش تجمعی از Policy های مختلف اعمال می‌کند. یک Policy باید با تمام مقادیر انتخابی که قبلاً در گزینه‌های سطح scope پیکربندی کرده‌اید پیکربندی شود. اگر یک مشتری از یک گزینه درخواست کند که در Policy حاضر نباشد اما در گزینه‌های سطح scope پیکربندی شده باشد، مقدار گزینه سطح scope به مشتری در پاسخ کارگزار برگردانده می‌شود.

کارگیری سیاست‌های DHCP

چند راه برای جداسازی مشتریان براساس نوع دستگاه وجود دارد. یک راه برای انجام این کار، استفاده از کلاس / شناسه فروشنده است. این رشته به گزینه ۶۰ با بیشتر مشتریان DHCP فرستاده می‌شود تا فروشنده را شناسایی کرده و در نتیجه نوع دستگاه را شناسایی کند. راه دیگر جداسازی مشتریان براساس نوع وسیله با استفاده از پیشوند آدرس MAC است. سه بایت اول یک آدرس MAC، oui نامیده می‌شود و فروشنده یا تولید کننده دستگاه را شناسایی می‌کند.

با ایجاد Policy DHCP با شرایط مبتنی بر clients based یا MAC، حالا شما می‌توانید مشتریان را در subnet به چنین روشی جدا کنید، که دستگاه‌های یک برند خاص تنها از دامنه آدرس IP مشخص‌شده در محدوده آن استفاده کنند. همچنین می‌توانید مجموعه‌ای از گزینه‌های مختلف را به این مشتریان بدهید.

پس از تخصیص آدرس‌های IP از محدوده آدرس IP خاص به یک کلاس از دستگاه‌ها، می‌توانید مسیریاب خود را پیکربندی کنید تا ترافیک شبکه را از این نشانی IP به طور متفاوت کنترل کند. در واقع، شما می‌توانید به کنترل دسترسی شبکه برای یک کلاس از وسایل دست یابید. با پیکربندی

گزینه‌های مسیر در یک Policy DHCP، شما می‌توانید جریان ترافیک شبکه را از انواع خاصی از دستگاه‌ها نیز کنترل کنید.

اجازه دهید به شما بگوییم که باید مدت‌زمان کوتاه‌تر اجاره را برای دستگاه‌های Wi - Fi و طولانی‌تر برای دستگاه‌های کابلی پیکربندی کنید. نقاط دستیابی (APs) به طور معمول قادر به رفتار به عنوان یک عامل تقویت‌کننده DHCP (یا DHCP relay agent) هستند. شما می‌توانید یک Policy را با شرایطی ایجاد کنید که براساس ارزش گزینه اطلاعات relay agent باشد.

اگر شما نیاز دارید که فیلتر کردن مبتنی بر MAC را در سطح scope انجام دهید، می‌توانید یک Policy سطح scope با استفاده از نشانی MAC به عنوان معیار در شرایط ایجاد کنید. چندین سناریو وجود دارد که در آن Policy های DHCP می‌تواند شرایط تامین آدرس‌های IP و تنظیمات را برآورده کند.

Introduction

In the recent blogs about DHCP server in Windows Server 2012, we discussed DHCP Failover – a new mechanism for achieving high availability of the Windows DHCP server and DHCP PowerShell – the new command line interface for managing Windows DHCP server. This blog discusses another new feature in DHCP Server in Windows Server 2012 – DHCP Policies. This feature is also referred as Policy based IP address and option assignment or just Policy Based Assignment (PBA) for short.

Envision the following scenarios that are faced by administrators:

-Your subnet has a mix of different types of clients – desktop computers, printers, IP phones etc. You would like different types of clients to get IP addresses from different IP address ranges within the subnet. For example, IP phones should get IP addresses from the

range 10.10.10.10 - 10.10.10.50 (in the 10.10.10.0/24 subnet), a different TFTP server and bootfile name option.

–In a subnet which has a mix of wired and mobile computers, you may want to assign shorter lease durations to mobile computers (e.g. 4 hours) and longer lease durations to wired computers (e.g. 4 days)

–Your deployment requires that you control who gets access to your network i.e. You want to provide DHCP service to a set of known clients (based on MAC address) for each subnet.

–With employees bringing in their own devices (smartphones, tablets) at work, you want to handle network traffic or control network access based on type of device.

DHCP Policies provide the DHCP admin with a very useful lever to achieve these scenarios.

As of Windows Server 2008 R2, an admin configures an IP address range and option values for a scope/subnet. All clients which are in that scope/subnet get an IP address from this IP address range of the scope and get options configured for the scope. If an administrator of the DHCP server needs to further apportion the IP address range of a scope to be delivered to a specific class of clients or devices or needs to give out different option values to different types of clients - as the aforementioned scenarios demand – there was no way for an admin to achieve that (unless you used individual reservations, which are effort intensive to manage). So, essentially, granularity at which you could assign IP addresses and options existed only up to the scope level. The DHCP policies in Windows Server 2012 help the

administrator achieve exactly that – a more granular mechanism to assign IP addresses and options.

What are DHCP policies?

With Windows Server 2012, you can create policies on the DHCP server. A policy consists of 2 main parts – conditions and settings. Condition(s) specified in a policy allows you to group clients. Settings are the network configuration parameters (IP address, options, and lease duration) that are provided to the clients in the DHCP server response. Conditions can be specified based on a set of fields which are present in the DHCP client request. The policy model is fairly simple: every DHCP client request is evaluated against the conditions in a policy. If a client request matches the conditions in the policy, the settings associated with a policy will be provisioned to the client via the DHCP server response.

Conditions

In Windows Server 2012, you can specify five different criteria (a fixed set) based on which one can segregate or group clients:

MAC Address

Vendor Class

User Class

Client Identifier

Relay Agent Information (and its sub options – remote id, circuit id and subscriber id)

The operators that can be used in the conditions are equals and not equals. You can also use a trailing wild card with MAC address, Vendor Class, User Class and Client identifier conditions to perform a

partial match. Combine the equals or not equals with a wild card in the value specified in the condition and you effectively achieve a starts with or does not start with condition.

You can either have a single condition in a policy or a set of conditions which can be ORed or ANDed. For example, "Vendor Class Equals Cisco IP Phone 7940" is a condition (Cisco IP Phone 7940 is the value of Vendor Class for Cisco IP Phone version 7940). Also a grouping such as "User Class Equals LabComputers" AND "MAC Address Not Equals 00-11-22*" is a group of two conditions. Each policy is created with either a single condition or a set of such conditions. An incoming client requesting for an IP address and options from the DHCP server is said to satisfy a policy if the client satisfies the cumulative set of conditions in the policy.

A client which does not match conditions of any policy, is leased an IP address from the rest of the IP address range of the scope (exclusive of all the policy IP address ranges) and given option values configured at the scope.

Settings

When a client matches the conditions of a policy, the DHCP server responds to the clients based on the settings of a policy. Settings associated to a policy can be an IP address range and/or options. An administrator could configure the policy to provide an IP address from a specified sub-range within the overall IP address range of the scope. You can also provide different option values for clients satisfying this policy.

Policies can be defined server wide or for a specific scope. A server wide policy – on the same lines as server wide option values – is

applicable to all scopes on the DHCP server. A server wide policy however cannot have an IP address range associated with it.

In addition to the IP address range and options which can be associated with a policy, there are two other noteworthy "settings" for a policy. You can set the IP address lease period for a policy. This allows you to configure a longer or shorter lease duration for clients which match the policy conditions. You can also configure how DNS registrations should be handled for clients matching the policy conditions. Any DNS registration behavior of the DHCP server which can be configured server wide or on a per scope basis – for example, turn on/off the DNS registration (and deregistration) or DNS name protection – can be configured on a per policy basis.

A policy can have only an IP address range (no options) or only options (no IP address range) as a setting.

A word about multiple policies

You can configure more than one policy within a scope or even server wide. Every policy has an admin assigned processing order. While processing client requests, the DHCP server evaluates the client requests against the conditions in the different policies based on the processing order of the policy – with processing order 1 policy being processed first. Scope level policies are processed first by the DHCP server followed by server wide policies.

If a client satisfies the conditions of more than 1 policy, it will get the settings in an aggregated manner from the different policies it satisfied. What this implies is if, for example - policy-1 has an option value for option 3 (router) and policy-2 has an option value for option 6 (DNS server) and if a client request matched the condition set of both policies, the server will respond with router value of policy-1 and

DNS server value of policy-2. However, in this example, if policy-1 also had an option value for DNS server, the client will get both (router and DNS server) option values from policy-1 if policy-1 is higher up in processing order i.e. the DNS server option value in policy-2 is overridden.

A policy does not have to be configured with all option values that you have already configured at the scope level options. If a policy client has requested an option which is not present in the policy but has been configured in the scope level options, the scope level option value would be returned to the client in the server response.

Employing DHCP policies

There a couple of ways to segregate clients based on the type of device. One way to do this is by using vendor class/identifier. This string sent in option 60 by most DHCP clients identify the vendor and thereby the type of the device. Another way to segregate clients based on device type is by using the MAC address prefix. The first three bytes of a MAC address is called OUI and identify the vendor or manufacturer of the device.

By creating DHCP policies with conditions based on Vendor Class or MAC address prefix, you can now segregate the clients in your subnet in such a way, that devices of a specific type get an IP address only from a specified IP address range within the scope. You can also give different set of options to these clients.

After assigning IP addresses from a specific IP address range to a class of devices, you can configure your router to handle network traffic from this IP address range differently. In effect, you can achieve network access control for a class of devices. By configuring route options (default gateway - option id 3, classless static routes -

option id 121) on a DHCP policy, you can also control flow of network traffic from specific types of devices.

Let's say you need to configure shorter lease durations to Wi-Fi devices and longer ones to wired devices. Access Points (APs) are typically capable of behaving as a DHCP relay agent (or are connected to one) which can be configured with Option 82 - DHCP relay agent option. Presence of a specific value in the relay agent option in this case would indicate a Wi-Fi device. You can create a policy with a condition based on the relay agent information option value which segregates these WiFi clients and configure this policy for a shorter lease duration. The rest of the clients in the scope will continue to get the longer lease duration configured at the scope.

Another scenario, if you need to perform MAC-based filtering at the scope level, you could create a scope-level policy using MAC Address as the criteria in the condition.

There are several such scenarios which DHCP policies can cater to in terms of provisioning of IP addresses and settings. We will be talking more about some of these scenarios in upcoming blog posts.

You can find the step-by-step guide for configuring DHCP policies here.

In conclusion, DHCP policies in Windows Server 2012 enables grouping of clients/devices using the different criteria and delivering targeted network configuration to them. We hope that you will find policy based assignment useful to your deployment needs! We would love to hear any feedback you have to share on the same.

باتشکر فراوان از توجه شما استاد عزیز