Monitor DHCP Scopes and Detect Man-in-the-Middle Attacks with PRTG and PowerShell

By Lockstep Group

Published: 2015-12-31 · Archived: 2026-04-05 21:39:01 UTC

DHCP is one of those services that many systems administrators set and forget. Often, the reasoning is that they have plenty of addresses (perhaps even 3 or 4 times the amount of devices), and it should never fill up. Any administrator that has ever dealt with a sudden deficiency of available addresses knows that this can make for a very bad day. After the crisis is dealt with (perhaps by lowering the lease time for addresses), he may ask himself: “How can I monitor my DHCP scopes so this never happens again?”

Additionally, the administrator may not be aware that full DHCP scopes can allow Man-In-The-Middle attacks on his network. An attacker can create enough DHCP requests to fill the DHCP scope. He can then put a rogue DHCP server on the network and any new DHCP requests will get fulfilled by his rogue DHCP server. The attacker will change the default gateway and DNS address to point to his machine which causes traffic to route through his machine allowing him to sniff unencrypted traffic.

The prudent Administrator will look for ways to decrease downtime and detect security risks. There are a number of options available for detecting when your DHCP scopes are running out of addresses; however, monitoring DHCP scopes isn’t as straight forward as one might imagine. Most administrators have the following options at their disposal:

1. *Manually track available addresses. Perhaps he makes this a daily check for the operations team.*
    - While this option is the easiest to implement since he only has to write some procedures for less senior staff to follow, he is now relying on a manual process prone to human error. This doesn’t detect MITM attacks in real time.
2. *Write a PowerShell script (or the language of your choice) to run periodically and search the event logs for event ID’s 1020 (Low Address Warning) and 1063 (Scope Full). It may email him when it finds these events.*
    - If the administrator already is comfortable with PowerShell and the nuances of building scheduled tasks that run PowerShell scripts, this can be implemented fairly quickly. Additionally, it provides a form of real-time alerting. It does require the administrator to build a script that gathers and parses Windows event logs, though. This can detect MITM attacks, but doesn’t provide a single pane of glass for all scopes.
3. *Use monitoring software such as PRTG along with a custom PowerShell script to not only alert on low addresses, but also build usage statistics over time.*
    - The administrator gets real-time alerts when the scope reaches a pre-defined threshold. Additionally, he gets ongoing scope statistics so he can see track peak usage, daily averages, and trending data. If an attacker fills his DHCP scopes, he can detect this and mitigate any potential MITM attack quickly.

This blog post will focus on using PRTG Network Monitor which has a free tier that can be used if your company has no network monitoring software. If your company already uses PRTG, then this will be very easy to implement.

Monitoring DHCP Scopes using PRTG and PowerShell

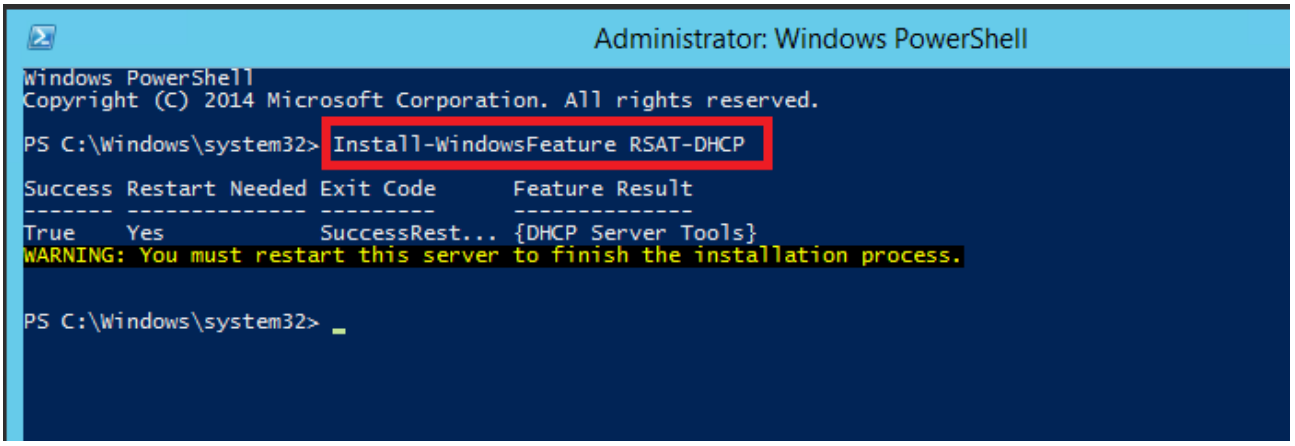
Note — The following process has only been tested with both the PRTG server and the DHCP server running Windows Server 2012 R2. I would like to thank Brian Addicks and Josh Sanders for their help in making this script ready for public consumption. I also recommend you look at this Lockstep Solutions Blog post if you don't have experience creating custom sensors in PRTG. The Extreme Basics of PRTG custom sensors with PowerShell

The overall process includes the following basic steps:

1. Install the DHCP Role Management Tools on the PRTG server
2. Add the custom script to the PRTG Server for use as a custom script sensor
3. Create the custom script sensor in PRTG

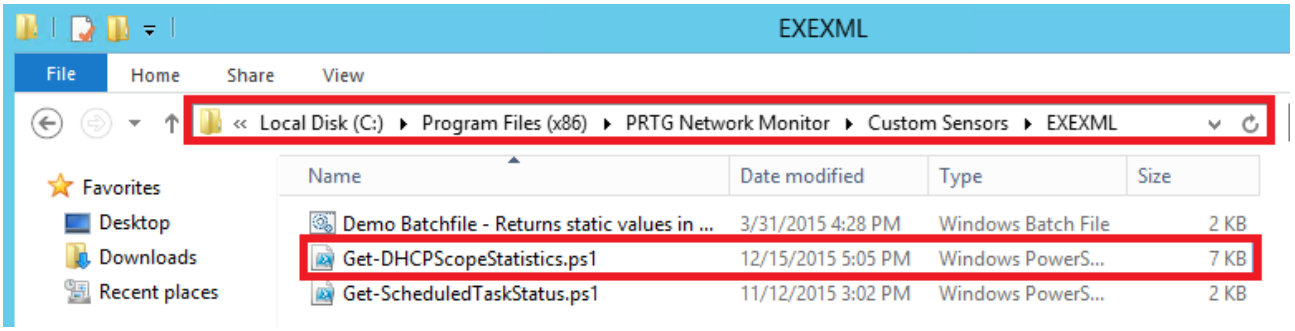
Install the DHCP Role Management Tools on the PRTG Server

1. Open PowerShell with Administrative Privileges and enter the following command.
    1. ***Install-WindowsFeature RSAT-DHCP*** (This installs only the DHCP management tools)



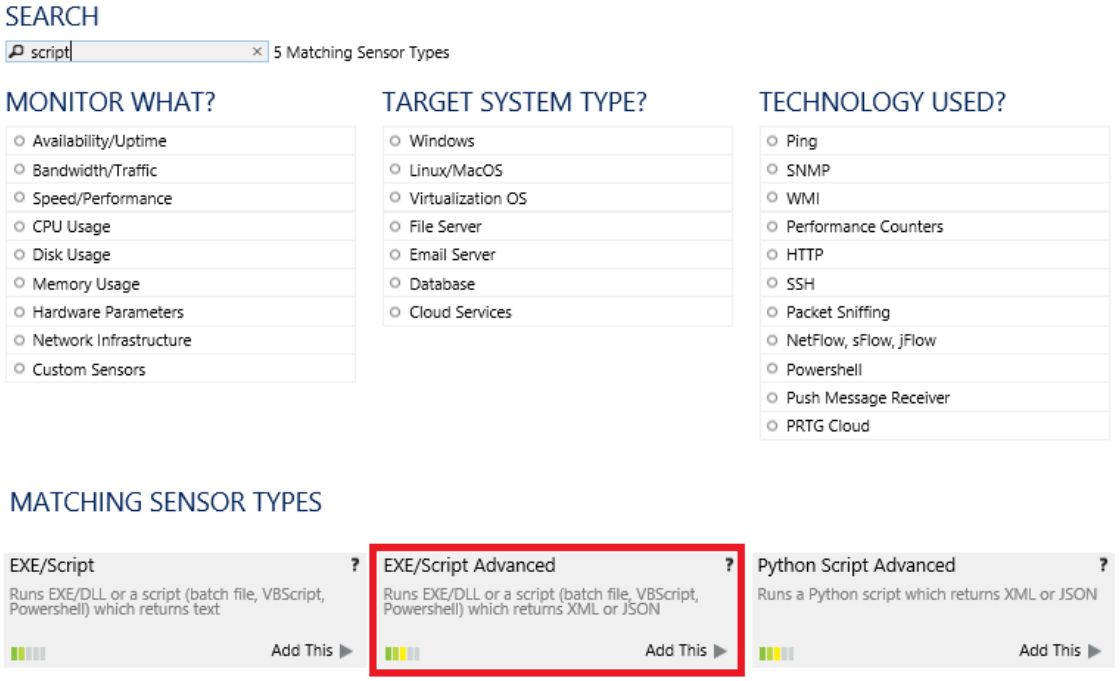
Add the custom script to the PRTG Server for use as a custom script sensor

1. Download the sensor script by filling out the form at the bottom of this post.
2. Copy the Get-DHCPScopeStatistics.ps1 script to "*C:\Program Files (x86)\PRTG Network Monitor\Custom Sensors\EXEXML*" on the PRTG server

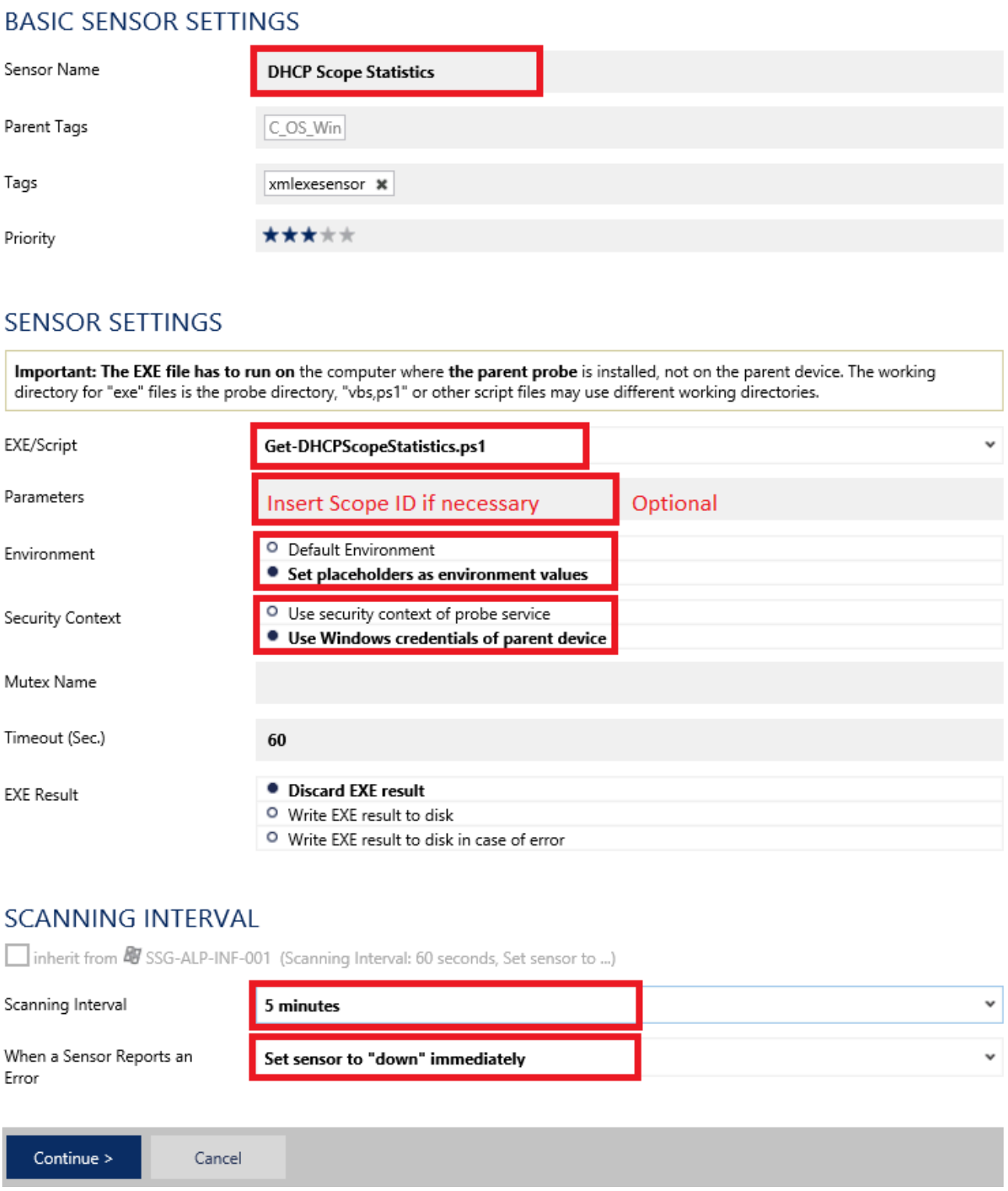


Create the custom script sensor in PRTG

1. In PRTG, **Right-Click the Windows DHCP server** being monitored
2. Click **Add Sensor**
3. Choose **EXE/Script Advanced**



4. Insert the correct options as follows
    1. Sensor Name: **DHCP Scope Statistics**
    2. EXE/Script: **Get-DHCPScopeStatistics.ps1**
    3. Parameters: ***-ScopeID <Scope ID>, <Scope ID>***
        - IMPORTANT – PRTG will support up to 50 channels per sensor. This sensor will create 2 channels per DHCP scope, so if you need to monitor more than 25 DHCP scopes on a server, you will need to create multiple sensors and specify the Scope ID's separated by comma. If you have less than 25 scopes, you can leave this field blank to monitor all scopes.
    4. Environment: **Set placeholders as environment values** (This allows the device name to be passed to the script automatically)
    5. Security Context: **Use Windows credentials of parent device**
    6. Scanning Interval: **5 minutes or more**
    7. When a Sensor Reports an Error: **Set sensor to "down" immediately**
5. Click **Continue**



Final Result

Notice that each scope has two channels that can be tuned individually. You may need to tune the Percentage Used channel to alert earlier. The default is when 95% of all addresses in the scope are used.

[activecampaign form=8]