1 Introduction

This document describes steps required to deploy Network Performance Monitor solution (NPM) in a test environment. Network Performance Monitor offers near real time monitoring of network performance parameters like loss and latency. Network performance monitor generates alerts as and when a threshold has breached for a network link. These thresholds can be learnt automatically by the system (ideal-state) or can be configured by the administrator using custom alert rules.

The solution makes use of active probes to assess the health of the network. OMS agents installed at various point in the network, exchange TCP packets with one another and in the process learn the round trip time and packet loss if any. Periodically each agent also performs a trace route to other agents to find what are various routes in the network that must be tested. Using this data, the agents are able to deduce the network latency and packet loss figures. The tests are repeated every three seconds and data is aggregated for a period of three minutes by the agents before uploading it to OMS.

In spite of talking to each other very frequently the agents do not generate a whole lot of network traffic while conducting the tests. The reason being that agent rely only on TCP SYN-SYNACK-ACK handshake packets to determine the loss and latency and no data packets are exchanged. Also every agent does not talk to every other agent every time and the communication topology of agents is optimised to further reduce the network traffic.

Deploying NPM involves four basic steps.

1. Enabling the solution on your OMS workspace
2. Installing the OMS agents
3. Configuring the OMS agents
4. Configuring the solution.

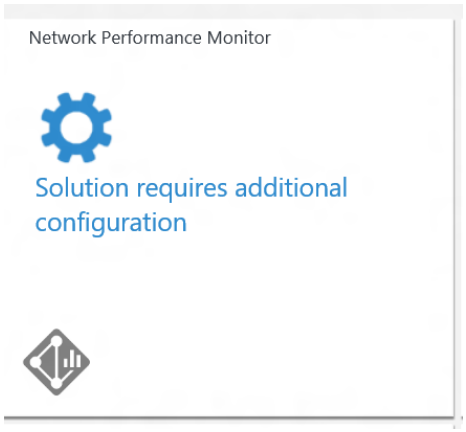
These steps have been described in detail below.

2 Enabling Solution on your OMS workspace

During private preview the solution is listed as “Coming soon” in OMS solution gallery and is not available to general public. We specifically invite a select set of customers to try out the solution and solution is enabled specifically for their workspaces. Chances are that if you are receiving this guide from us the solution has already been enabled on your workspace. If not, please share your workspace ID with us and we will enable the solution.

Mail you workspace ID to netmonpms@microsoft.com and we will enable the solution on your workspace. You should not proceed further till you get a confirmation mail from us.

Once the solution has been enabled you will see a new tile titled “Network Performance Monitor” appear in your OMS home page. You can start deploying the solution even though the solution gallery is still showing it as “coming soon”.



Before you can proceed further you need to download and install OMS agents (See Below). You must install at least two OMS agents for solution to work correctly.

3 Deploying with SCOM

If you have connected on premise SCOM with OMS, you do not need to manually install agents on the machines. Once the NPM solution is enabled on your OMS workspace the required management packs for NPM will automatically flow down to the machines that are connected to OMS via SCOM.

If you are deploying using SCOM you should **ignore step 4** and jump directly to **step 5**

In case you want to connect SCOM with OMS but haven't figured out how to do it yet; click on the link below.
https://technet.microsoft.com/en-us/library/mt484104.aspx

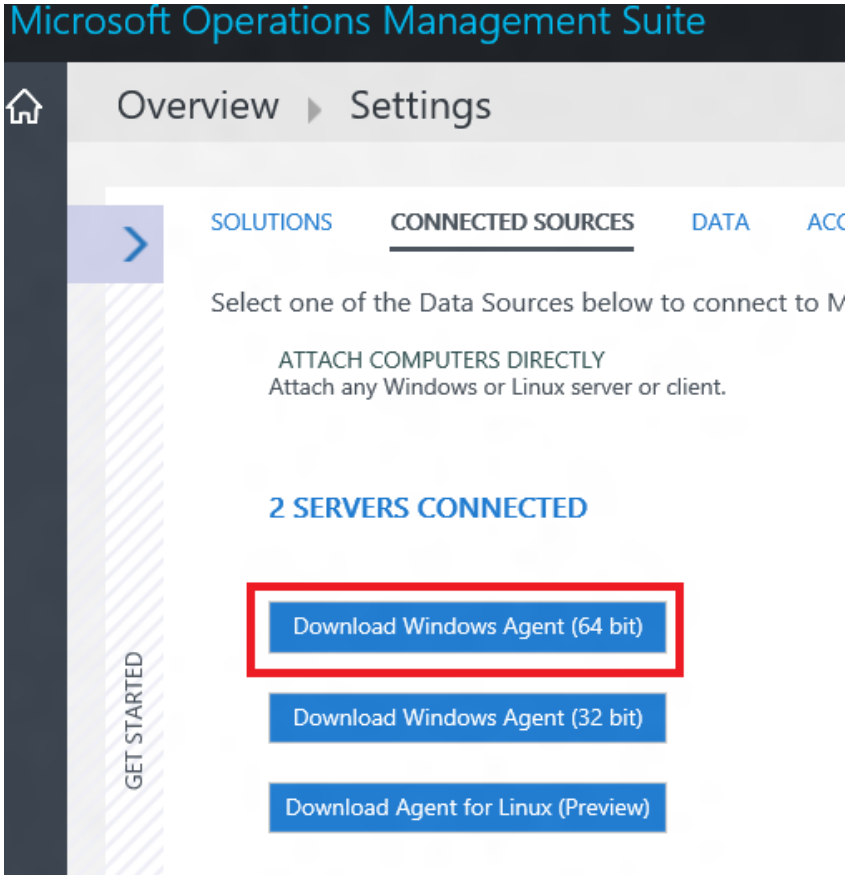
4 Installing the OMS agents

In order to work with OMS you need to install OMS agents on your servers. OMS agent is a lightweight binary that runs on your hosts and periodically sends monitoring data to the cloud service. OMS agent only collects the data that is required by the solutions subscribed by you.

In case you have been using OMS for a while and have already deployed OMS agents then you can directly skip to next step. However, remember that if you have created a new OMS workspace for testing this solution then you will have to configure these agents with new workspace ID or install new agents as described below.

4.1 Download Agent Installer

In OMS portal go the Settings -> Connected Sources and download the OMS agent for windows server by clicking on the appropriate button.



Please note that at the moment we support only agents running on windows server 2008 onwards. Agents for other platforms including windows clients, Linux are a work in progress and will be available going forward.

4.2 Where to install the agents

Before you install agents you should take into consideration the topology of your network and what parts of the network you want to monitor. We recommend that you deploy more than two agents for each subnet that you want to monitor. In other words, for every subnet that you want to monitor select two or more servers and install the agent on them.

If you are unsure about the topology of your network, simply install the agents on critical workloads for which you want to monitor the network performance. For example, one might want to keep a track of network connection between Web Server and SQL backend. So one would install the agent on both Web Server as well as SQL server.

It may be noted that agents monitor network connectivity (Links) between hosts and not the hosts themselves. Hence to monitor a network link you must install agents on both endpoints of that link.

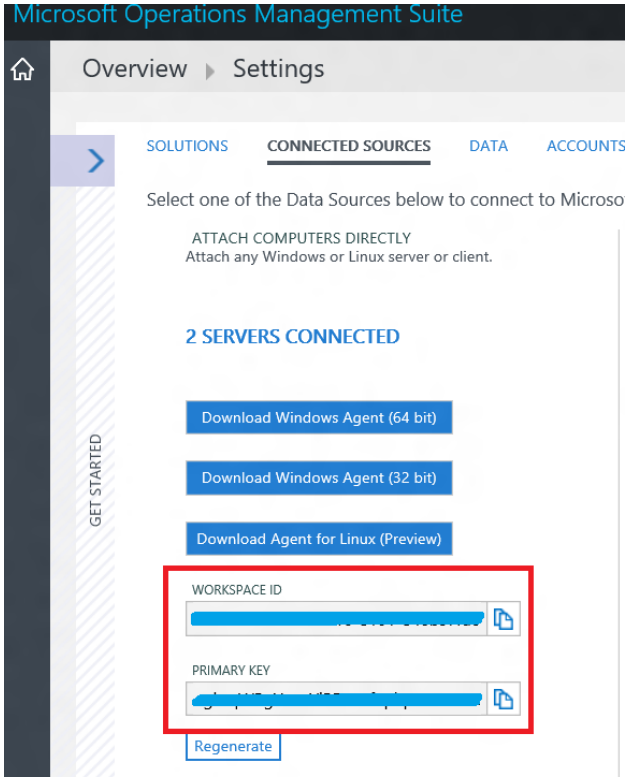
Make sure that you have installed the agents on at least two machines. Otherwise the solution will not have enough data and will remain in configuring state till the time you install and configure more agents.

4.3 Installing the agents

Copy the installer downloaded from OMS portal on the machine where you want to install the agent.

Double click on the installer package to start the installation. While installing the agent you will be requested to enter a workspace ID and Primary key. You will find these on your OMS settings page.

Copy these values from the portal and input them into the installer.



5 Configuring the agents

Once the agents have been installed you will need to open firewall ports to on the machines to make sure that the agents are able to talk to each other. We have provided a power shell script to help you with this task. Run the script named EnableRules.ps1 given in the zip file along with this guide in a power shell window with elevated privileges (administrative privileges). The script should be run without any parameters.

This script creates few registry keys required by NPM and creates windows firewall rules to allow agents to create TCP connections with each other.

Note that the script will configure only windows firewall locally. If you have a network firewall you should make sure that it is allowing traffic destined for TCP port 8084 (default NPM port).

6 Configuring the solution

Once the agents have been installed and configured they will automatically discover the subnets that they are connected to and report these to the cloud service.

The NPM tile on the OMS home page would still say “Solution requires configuration”.

Click on the solution tile to bring up the configuration page of NPM solution.

6.1 Understanding the Default network

On the configuration page you will see a single network named “Default”. In absence of any user defined networks all the auto-discovered subnets are placed in the Default network.

Whenever you create a network and you add a subnet to it. The same subnet is automatically removed from the “Default” network. If you delete a network all its subnets are automatically returned back to default network.

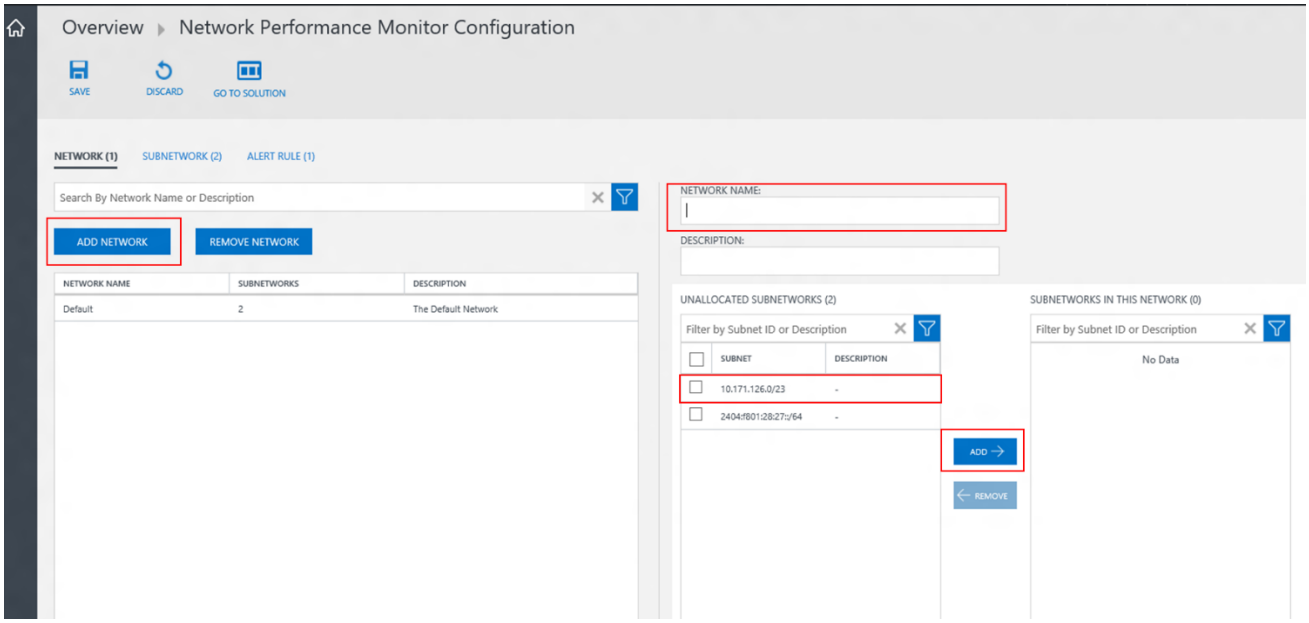
In other words, Default network is the container for all the subnets that are not contained in any user defined Network. You cannot edit or delete the Default network. It will always remain in the system. However, you can create more networks as per your business requirements.

In the most likely case the subnets in your organization will be arranged in more than one network and you should create one or more network to logically group your subnets.

6.2 Create new networks

A network in NPM is a container for a bunch of subnets. You can create network with any name that meets your business requirements and the add subnets to the network. For example, you can create a network named *Building1* and then add all the subnets that are present in *building1* to this network or you can create networks named *DMZ* and then add all subnets belonging to demilitarized zone to this network.

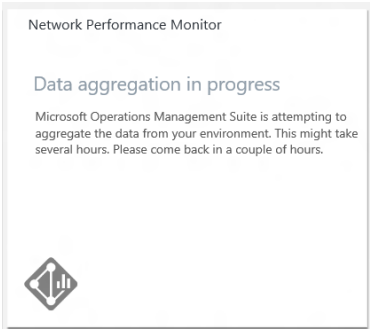
To create a new network, click on the “ADD NETWORK” button and the enter the network name and description on the right hand side. Select one or more subnets and add these to the network by clicking the “ADD ->” button.



Please note that you can't add same subnet to more than one network. If you want to move a subnet from one network to another you must first remove it from one network and then add it to another network explicitly.

6.3 Wait for data aggregation

Once you have saved the configuration for first time the solution will start collecting network packet loss and latency figures between the nodes on which agents are installed. This process usually takes few minutes. During this state you'll see the solution tile in OMS home page shows "Data aggregation in process"



Once the data has been uploaded you should be able to see the solution dashboard with data and graphs.

At this point deployment is complete and you can start to play around with the solution.

Please note that private preview has a limitation because of which any configuration change (addition/deletion of networks etc.) does not reflect immediately on the dashboard. It may take several minutes before solution dashboard is updated with the changes that you have made in the solution configuration.

7 Common Tasks

Below are few task that you may want to try out and provide feedback on.

- Find network link with most loss
- Find network link with most latency
- Create a new alert rule
- Drill down on an alert generated by the system to find the root cause of the problem.
- Stop monitoring a particular subnetwork.
- Stop monitoring a particular node.
- Search of the network Performance Monitor data through OMS search. Example queries are on solution dashboard.

Please reach out to netmonpms@microsoft.com if you have question or run into any issue blocking your deployment.