

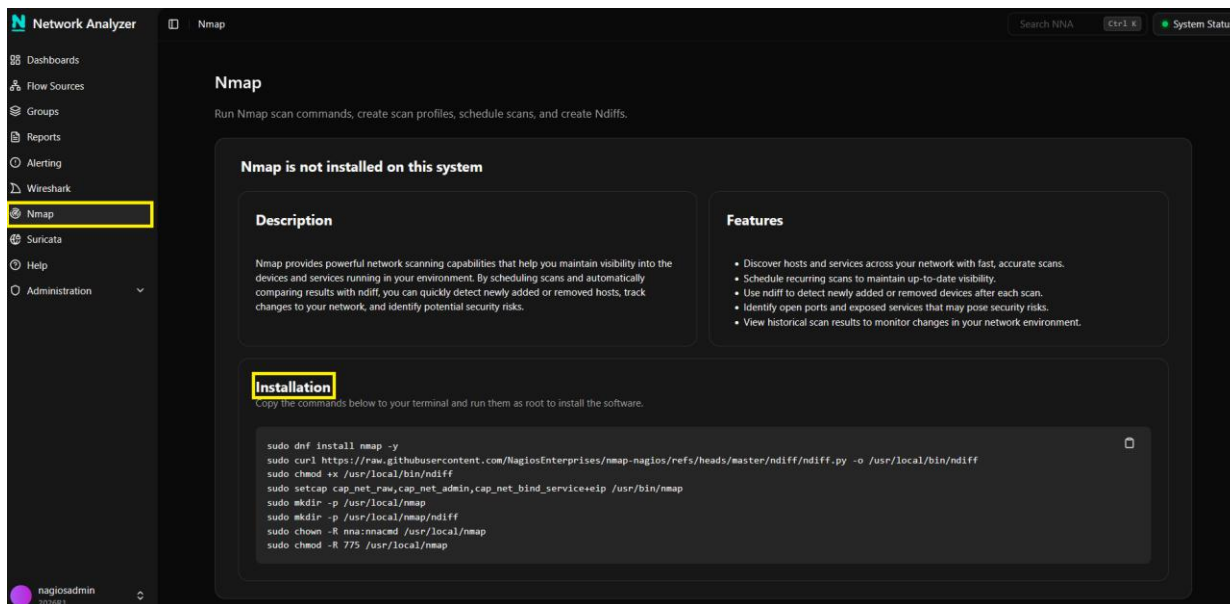
# How To Use Nmap With Nagios Network Analyzer 2026

## Purpose

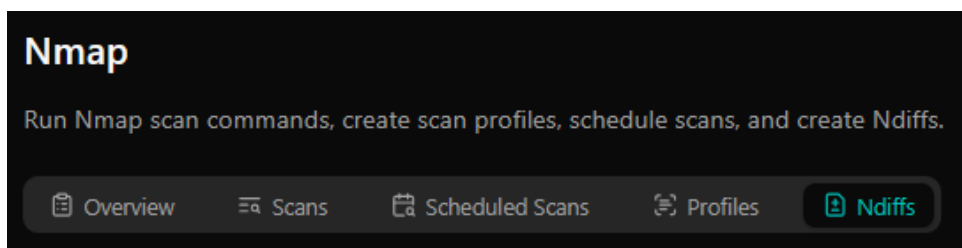
This document describes how to install Nmap alongside Nagios Network Analyzer 2026, and how to use the built-in integration capabilities to execute scans, schedule scans, set up scan Profiles, and create Ndiffs to compare scans you have run.

## Initial Setup

To begin, navigate to the **Nmap** section of the UI, and run the commands in the **Installation** section from the command line of your Network Analyzer server.



After the installation is completed, refresh the Nmap page. You will now see several tabs of options:



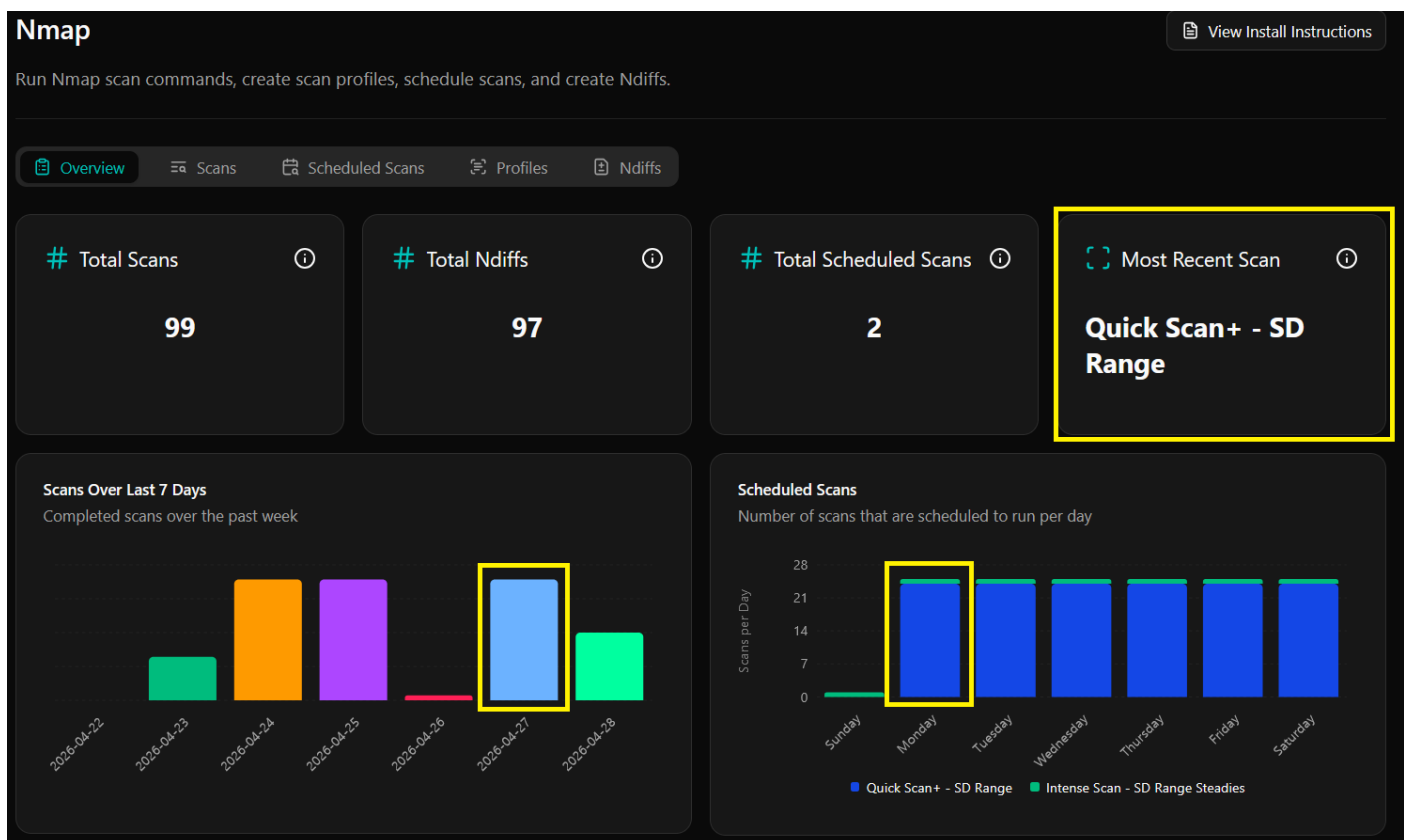
**Note:** after installation, you can click the **View Install Instructions** link on the upper right of the Nmap menu to review the instructions.

# How To Use Nmap With Nagios Network Analyzer 2026

## Overview Tab

The **Overview** tab provides a summary of Total Scans, Total Ndiffs, Total Scheduled Scans, and the Most Recent Scan ID. It also includes a bar graph of total scans over the last 7 days, and one showing the total number of hours scans are scheduled for on each day of the week.

You can click the **Most Recent Scan ID** panel to drill down to details on the most recent scan, and on the bars of the **Scans Over Last 7 Days** and **Scheduled Scans** graphs to drill down to filtered scan details.



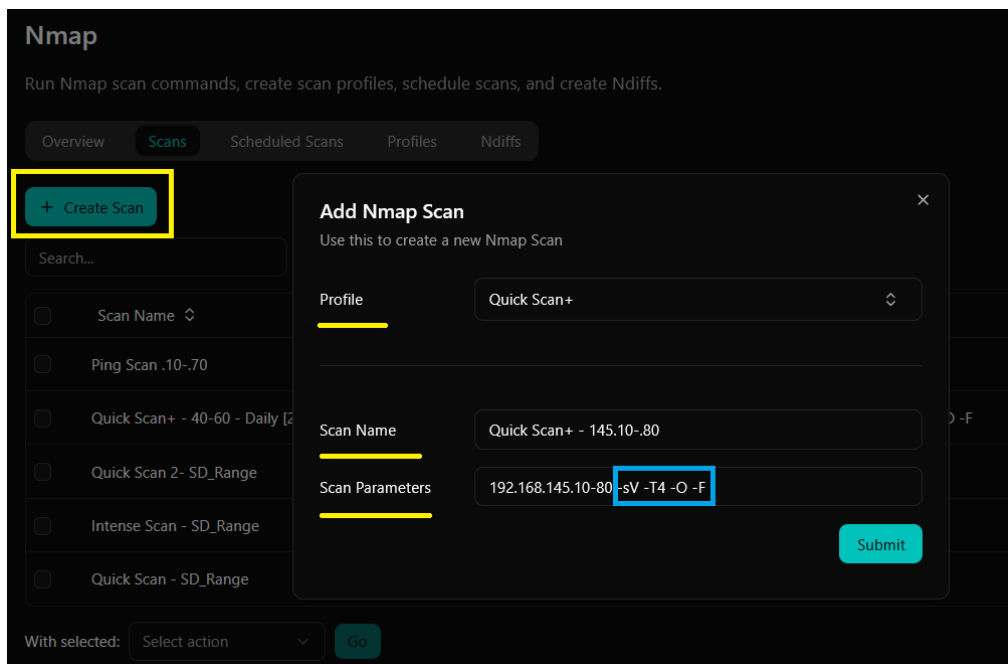
# How To Use Nmap With Nagios Network Analyzer 2026

## Scans Tab

In the **Scans** tab you can create, view, export, and manage Nmap scans.

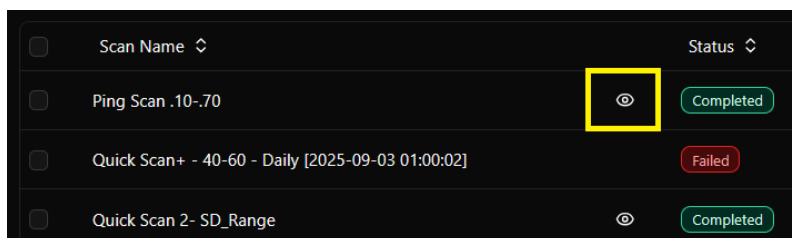
### Creating a Scan

To create a scan, click the **+Create Scan** button, then select a [Profile](#), enter a friendly **Scan Name** to help you identify the scan later in the Scans list and when creating Ndiffs, and enter your scan parameters. Note that some Scan Parameters (such as the [Nmap options](#) highlighted with a blue box in the screenshot below) will be automatically populated based on the **Profile** you select. Once you've updated all the settings, click **Submit** to run the scan immediately.



### Viewing a Scan

To view a completed scan, click the eye icon next to its name in the list.



# How To Use Nmap With Nagios Network Analyzer 2026

This will bring you to the scan details page, where you can view information on the **Hosts** and **Services** discovered by the scan, as well as **Scan Info**, and the **Raw Output** of the scan. Note that you can also click the **clipboard** icon to copy information to the your clipboard, and click the **Actions** icon to the right of various entries to initiate a [Suricata](#) search of the data.

The screenshot shows the 'Intense Scan - Overnights' details page. At the top, there are tabs for 'Hosts', 'Services', 'Scan Info', and 'Raw Output', with 'Hosts' selected. Below the tabs are three summary cards: 'Targets scanned' (127 IP addresses), 'Hosts found' (12 hosts), and 'Percentage up' (9%). A table below displays scan results with columns for IP Address, MAC Address, Operating System, State, Port, Protocol, Service, and Version. The first row shows IP 192.168.141.127 with OS Microsoft Windows 10 (94%) and state OPEN on port 22. The second row shows IP 192.168.141.126 with OS Linux 5.0 - 5.4 (100%) and state OPEN on port 80. The third row shows IP 192.168.141.125 with state CLOSED on port 443. A 'Search Suricata' button is visible next to the third row. A yellow box highlights the 'Hosts' tab and the 'Search Suricata' button.

## Stopping a Running Scan

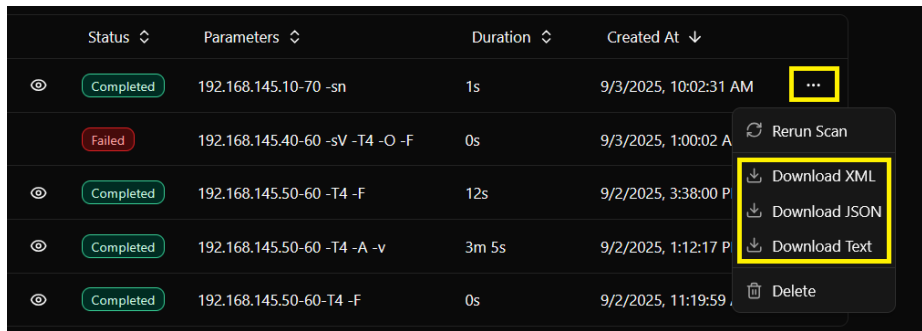
To stop a scan that is currently running, click the **Actions** icon on the far right of the scan entry, then select **Stop Scan**.

The screenshot shows a list of scans in Nagios Network Analyzer. The columns are Status, Parameters, Duration, and Started At. The first scan is 'In Progress' with parameters '192.168.168.201-210 -sV -T4 -O -F -e ens18', duration '12s', and started at '2/16/2026, 10:59:16 AM'. A yellow box highlights the 'Actions' icon (three dots) for this scan. A dropdown menu is open, showing options: 'Rerun Scan', 'Stop Scan', 'Create Scheduled Scan', 'Download XML', 'Download JSON', 'Download Text', and 'Delete'. The 'Stop Scan' option is highlighted with a yellow box.

# How To Use Nmap With Nagios Network Analyzer 2026

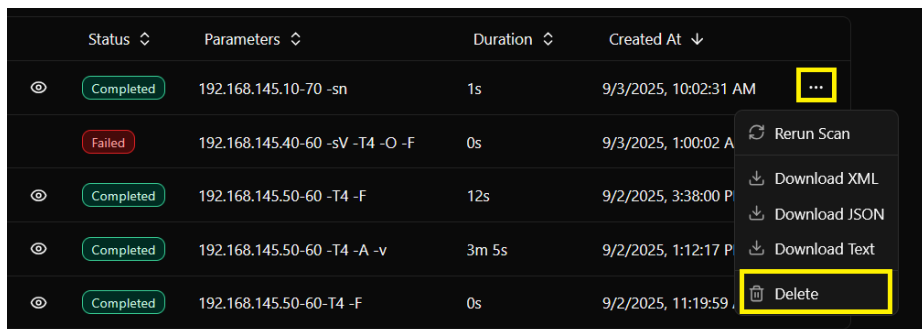
## Exporting a Scan

To export a scan, click the **Actions** icon on the far right of the scan entry, then select either XML, JSON, or Text to download the file.



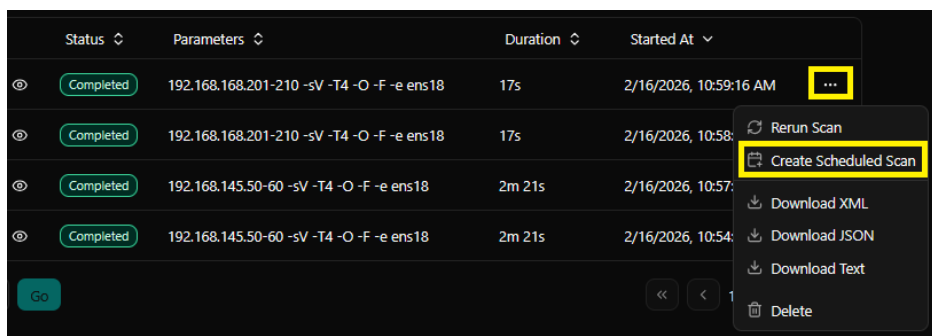
## Deleting a Scan

To delete a scan, click the Actions icon, and select **Delete**.



## Creating a Scheduled Scan

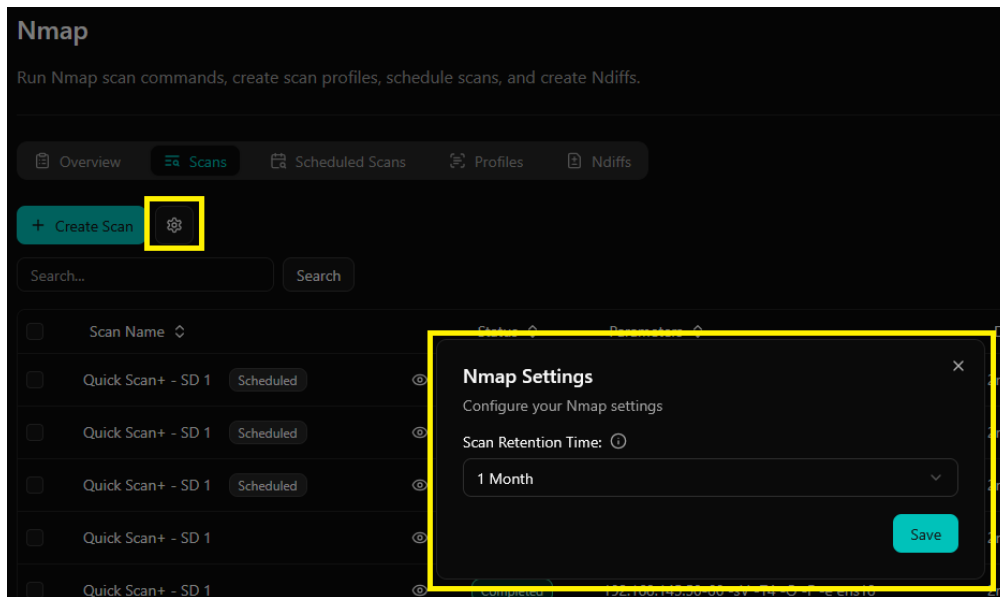
To use a regular scan as the basis for a new Scheduled Scan, click the Actions icon, then click Create Scheduled Scan (full scheduled scan details can be found in the following section).



# How To Use Nmap With Nagios Network Analyzer 2026

## Setting the Global Scan Retention Time

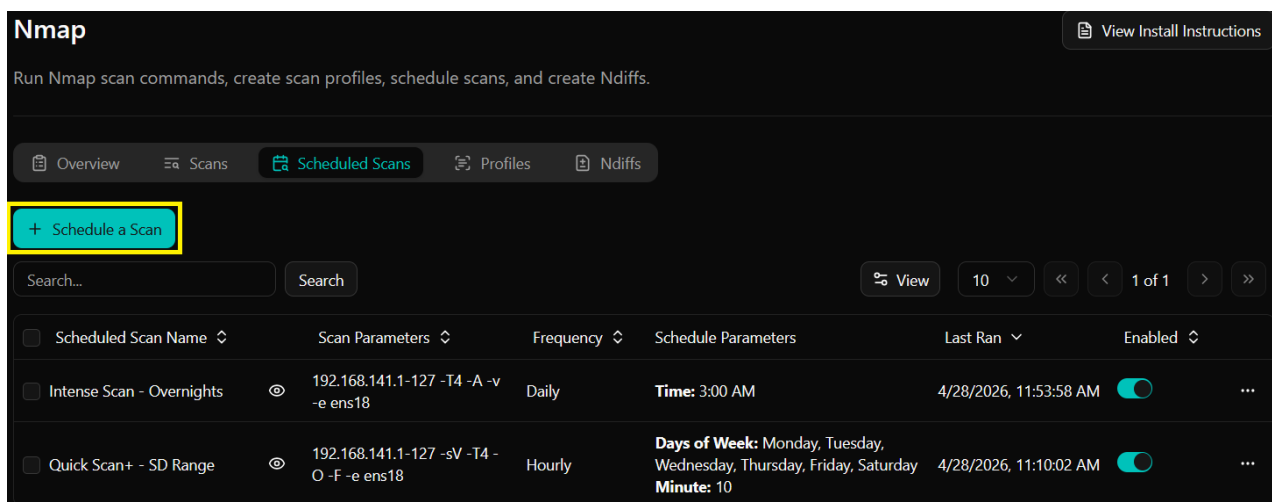
To automatically, *permanently* delete scans and their associated Ndiffs from the system once they reach a certain age, click the **gear** icon beneath the main Nmap menu tab bar:



Select a Scan Retention Time, then click **Save**. By default, this is set to *Never Delete*.

## Scheduled Scans Tab

It is also possible to schedule scans to run automatically on a frequency of your choosing in the **Scheduled Scans** tab. To schedule a scan, click the **+ Schedule Scan** button.



# How To Use Nmap With Nagios Network Analyzer 2026

Next, choose a **Profile**, give your scheduled scan a friendly **Name**, and adjust the **Scan Parameters** as needed. The **Schedule** can be anything from once a minute to once a year, or a custom cron expression.

In this example, we've scheduled a scan of a small IP range, using the Quick Scan + Profile, to run once an hour, on the 10<sup>th</sup> minute of the hour, on Fridays, Saturdays, and Sundays.

We've also checked the **Automatic Ndiffs** box so that an Ndiff comparing each new scan to the last is automatically generated:

**Add Scheduled Scan**

Use this to create a new Scheduled Scan

Profile: Quick Scan+

Name: Quick Scan+ - Weekends

Scan Parameters: 162.168.145.01-90 -sV -T4 -O -F -e ens18

Schedule: Hourly

Hourly at 10 minutes

Days: Saturday, Sunday, Friday

Between: --:-- -- to --:-- --

Enabled:

Automatic Ndiffs:

Submit

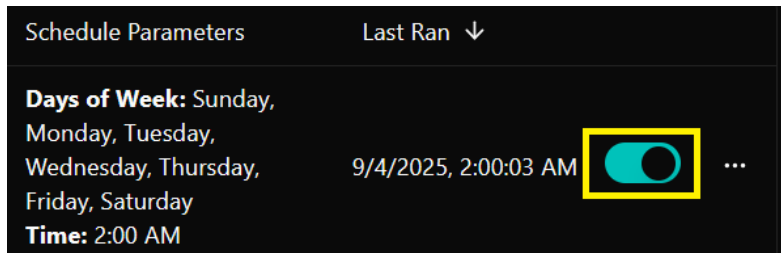
Once you've set your scan options, click **Submit**. You'll see the new scan appear in the list:

Scheduled Scan Name	Status	Scan Parameters	Frequency	Schedule Parameters	Last Ran
Quick Scan+ - 40-60 - Daily	Enabled	192.168.145.40-60 -sV -T4 -O -F	Daily	Days of Week: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday Time: 2:00 AM	9/4/2025, 2:00:03 AM
Quick Scan+ - Weekends	Enabled	192.168.145.01-90 -sV -T4 -O -F	Every Three Hours	Days of Week: Friday, Saturday, Sunday Minute: 5	Never

# How To Use Nmap With Nagios Network Analyzer 2026

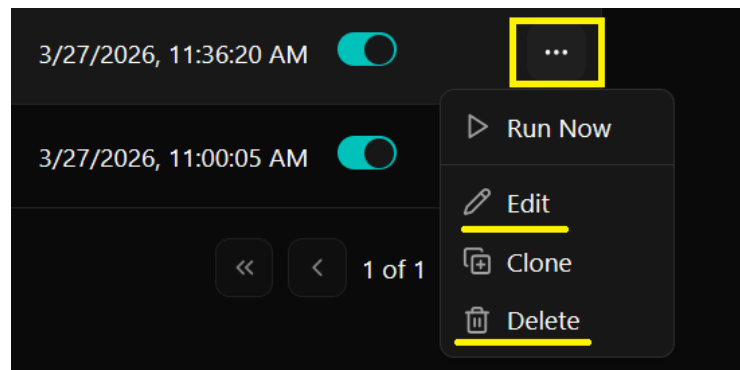
## Enabling and Disabling Scheduled Scans

The toggle on the far right of scans can be used to quickly **enable** or **disable** scheduled scans:



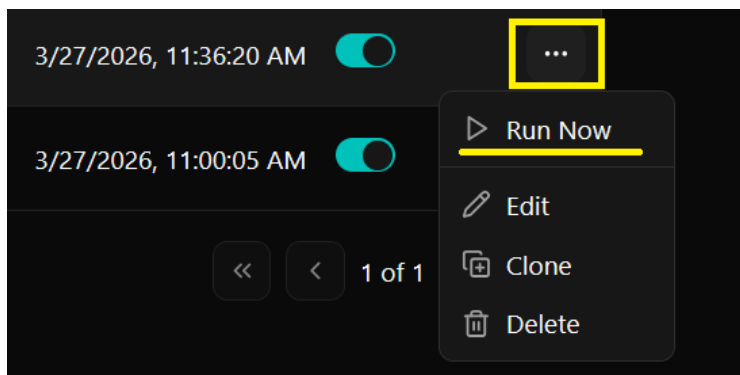
## Editing and Deleting Scheduled Scans

To edit or delete a scan, click the Actions dropdown on the far right and select your option:



## Running Scheduled Scans Now

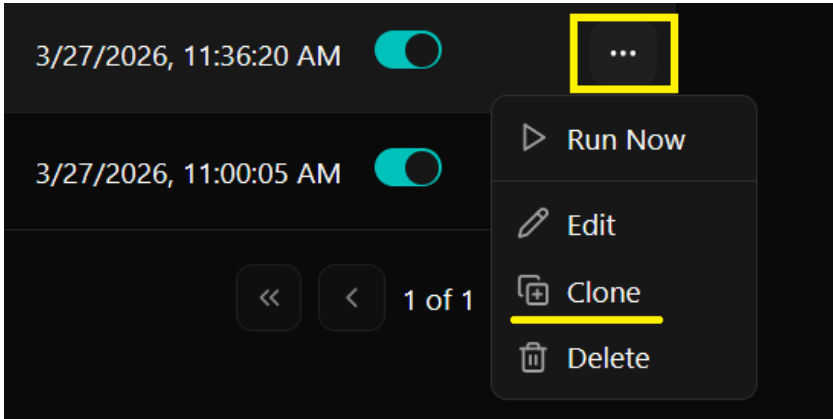
To force a scheduled scan to run immediately, click the Action dropdown and select **Run Now**:



# How To Use Nmap With Nagios Network Analyzer 2026

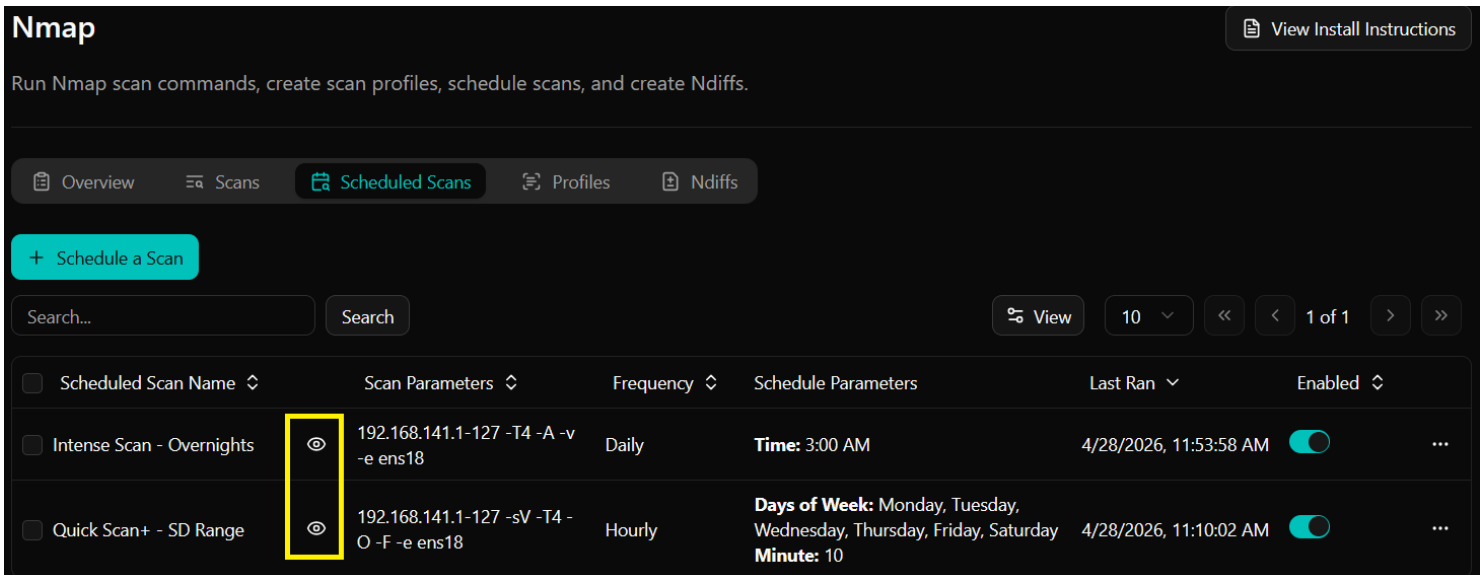
## Cloning Schedule Scans

To clone a scheduled scan, click the Actions dropdown and select **Clone**:



## Viewing Scheduled Scan Details

To drill down into the details of a scheduled scan, click the eye icon on the target scan:



# How To Use Nmap With Nagios Network Analyzer 2026

Here you will find an **Overview** of high-level results from the most recent scan, as well as **Scan History** and **Host History** tabs which provide additional specific details:

**Intense Scan - Overnights**

Scan Parameters: 192.168.141.1-127 -T4 -A -v -e ens18 Times Ran: 2 Last Run: 4/28/2026, 12:01:58 PM

Overview Scan History Host History

Search 10 << < 1 of 1 > Search... View 10 << < 1 of 1 > >>

Date	Scans	Status	Parameters	Duration
All Scans	2	<input type="checkbox"/>		
4/28/2026	2	<input type="checkbox"/>	192.168.141.1-127 -T4 -A -v -e ens18	15s
		<input type="checkbox"/>	192.168.141.1-127 -T4 -A -v -e ens18	3m 47s

With selected: Select action Go << < 1 of 1 > >>

## Profiles Tab

You can create, edit, and run scans using Profiles in the **Profiles** tab.

Profiles provide a way to pre-configure sets of Nmap parameters so that you can quickly apply those options and settings when executing future scans. You'll notice that several useful Profiles such as Intense Scan and Quick Scan are pre-loaded for you as a starting point.

## Creating a Profile

To create a new Profile, click **+Create Profile**.

**Nmap**

Run Nmap scan commands, create scan profiles, schedule scans, and create Ndiffs.

Overview Scans Scheduled Scans Profiles Ndiffs

+ Create Profile

Search... Search

# How To Use Nmap With Nagios Network Analyzer 2026

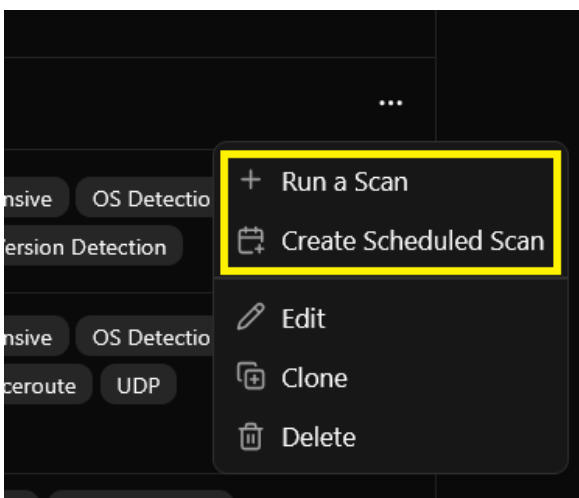
Give the Profile a friendly name to help you identify it in the list when scheduling future scans, and optionally enter a **Description** and add **Tags** to help users understand its use case and find it quickly in searches of the Profiles list.

Next, choose your **Nmap Options**. Each option in the list includes a tooltip to help you understand the multitude of possibilities.

## Running and Scheduling Scans via a Profile

If you'd like to execute a scan right from the Profiles tab, simply locate the desired Profile, click the Actions icon, and click **+Run a Scan**. This will start a new scan using the parameters of the Profile.

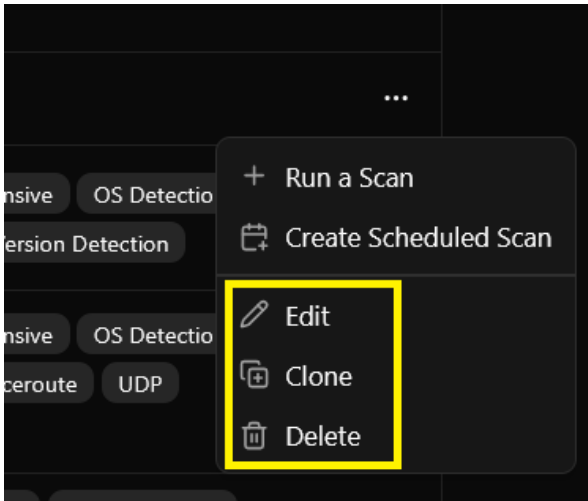
You can also set up a scheduled scan by clicking **Create Scheduled Scan** in the Actions dropdown.



# How To Use Nmap With Nagios Network Analyzer 2026

## Editing, Cloning, and Deleting Profiles

- To **edit** a Profile, click the Actions icon on the far right and click **Edit**.
- To **clone** a Profile, click the Actions icon on the far right and click **Clone**.
- To **delete** a Profile, click the Actions icon on the far right and click **Delete**.

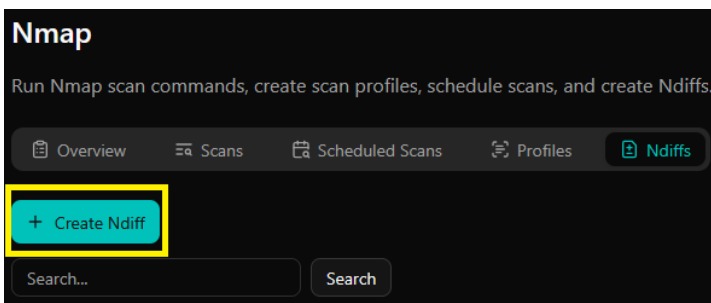


## Ndiffs Tab

Ndiffs allow you to compare previously run scans and view a diff to compare them in the user interface, or download a copy for external analysis.

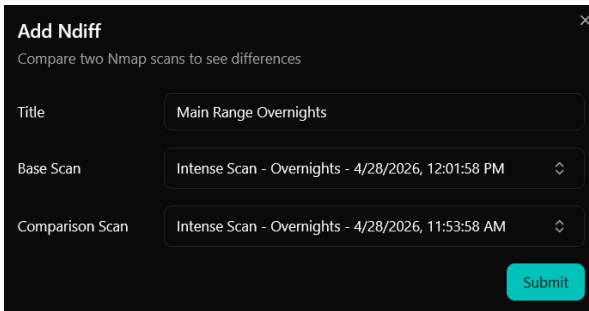
### Creating an Ndiff

To create a new Ndiff, click the **+ Create Ndiff** button.



# How To Use Nmap With Nagios Network Analyzer 2026

Next, enter a **Title** for the diff, and choose the two scans you'd like to compare, then click **Submit**.

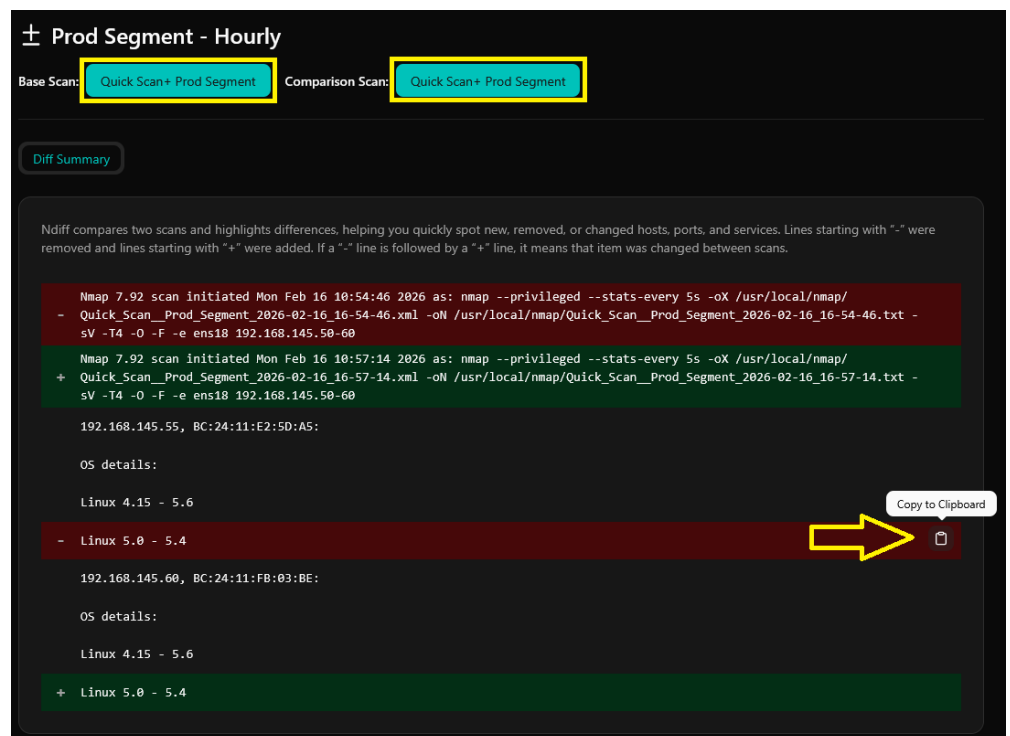


## Viewing an Ndiff

To view a completed Ndiff, click the eye icon to the right of its name in the list.

<input type="checkbox"/> Ndiff Name	Status	Scan 1	Scan 2
<input type="checkbox"/> SD-Range-2_Day	<input checked="" type="checkbox"/> Completed	Quick Scan - SD_Range	Quick Scan 2- SD_Range
<input type="checkbox"/> ndiff-2	<input checked="" type="checkbox"/> Completed	Quick Scan - SD_Range	Quick Scan 2- SD_Range

This will bring you to the **Diff Summary** page, where you can see partial results of the scan. You can hover over any block of the results to copy the section to your clipboard, or click the name of either scan at the top to drill down to the details of that individual scan:



```
± Prod Segment - Hourly
Base Scan: Quick Scan+ Prod Segment Comparison Scan: Quick Scan+ Prod Segment

Diff Summary

Ndiff compares two scans and highlights differences, helping you quickly spot new, removed, or changed hosts, ports, and services. Lines starting with "-" were removed and lines starting with "+" were added. If a "-" line is followed by a "+" line, it means that item was changed between scans.

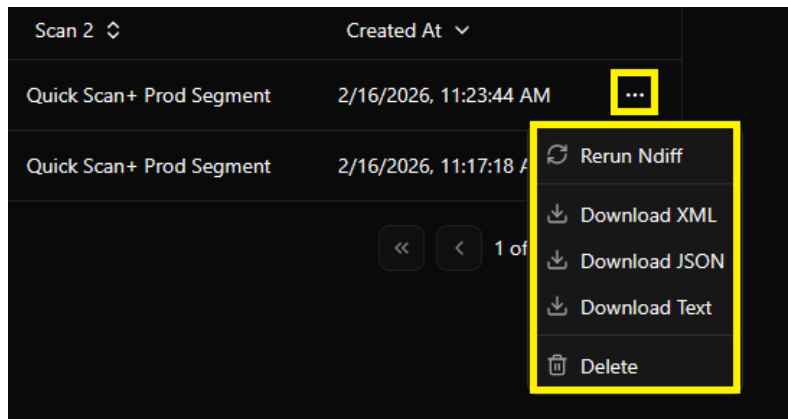
- Nmap 7.92 scan initiated Mon Feb 16 10:54:46 2026 as: nmap --privileged --stats-every 5s -oX /usr/local/nmap/Quick_Scan_Prod_Segment_2026-02-16_16-54-46.xml -oN /usr/local/nmap/Quick_Scan_Prod_Segment_2026-02-16_16-54-46.txt -sV -T4 -O -F -e ens18 192.168.145.50-60
+ Nmap 7.92 scan initiated Mon Feb 16 10:57:14 2026 as: nmap --privileged --stats-every 5s -oX /usr/local/nmap/Quick_Scan_Prod_Segment_2026-02-16_16-57-14.xml -oN /usr/local/nmap/Quick_Scan_Prod_Segment_2026-02-16_16-57-14.txt -sV -T4 -O -F -e ens18 192.168.145.50-60

192.168.145.55, BC:24:11:E2:5D:A5:
OS details:
Linux 4.15 - 5.6
- Linux 5.0 - 5.4
192.168.145.60, BC:24:11:FB:03:BE:
OS details:
Linux 4.15 - 5.6
+ Linux 5.0 - 5.4
```

# How To Use Nmap With Nagios Network Analyzer 2026

## Re-running, Downloading, and Deleting Ndiffs

- To **re-run** an Ndiff, click on the Actions icon on the far right, then select **Rerun Ndiff**.
- To **download** an Ndiff, click the Actions icon on the far right, then select XML, JSON, or Text. The downloaded file will contain complete details, rather than the partial details shown in the Diff Summary.
- To **delete an** Ndiff, click the Actions icon on the far right of the listing, then click **Delete**.



## Finishing Up

This completes the documentation on how to use Nmap with Nagios Network Analyzer 2026. If you have additional questions or other support-related questions, please visit us at our Nagios Support Forum, Nagios Knowledge Base, or Nagios Library:

[Visit Nagios Support Forum](#)

[Visit Documentation Hub](#)

[Visit Nagios Library](#)