Applying UDP monitoring  
Powershell Script



Table of Contents

[UDP monitoring with custom script 3](#_Toc447783816)

[Overview 3](#_Toc447783817)

[Requirements 3](#_Toc447783818)

[Background 4](#_Toc447783819)

[Modify the script for your customer environment 4](#_Toc447783820)

[To upload the policy in N-central 4](#_Toc447783821)

[To run the policy in N-central 7](#_Toc447783822)

# UDP monitoring with custom script

## Overview

Using a powershell script to gather information about UDP backup jobs and present the information in N-central through a custom monitoring service. You will see a count of failed jobs so you can get proper alerting.

It is important to understand some of the limitations and how to properly use the script.

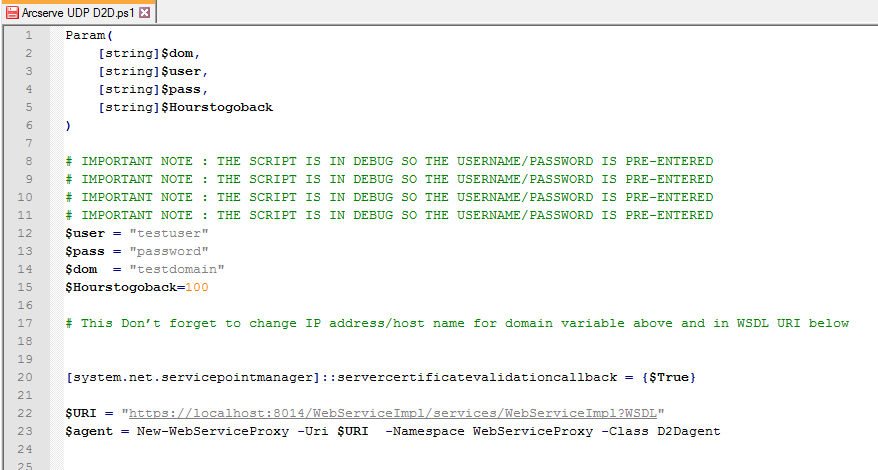
## Requirements

* The Arcserve UDP ps1 script
* The Arcserve UDP custom monitoring service
* Additionally, the script requires Powershell 2.0 and Microsoft .net 4

# Background

## Modify the script for your customer environment

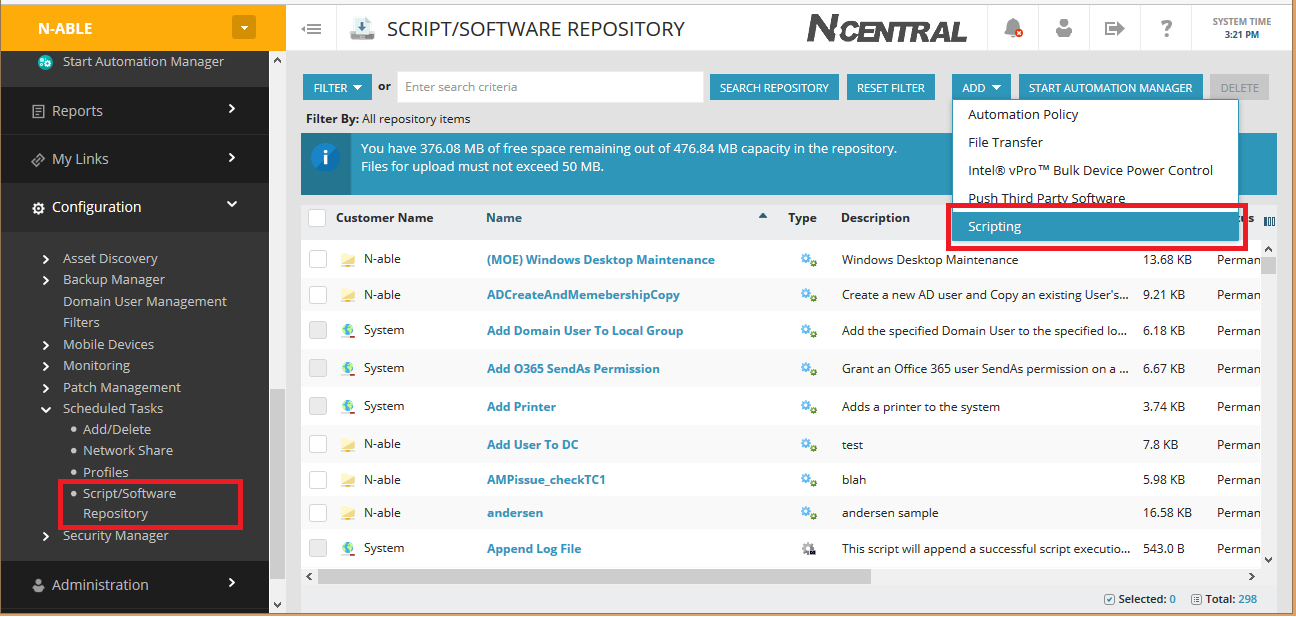
1. This is how the policy look



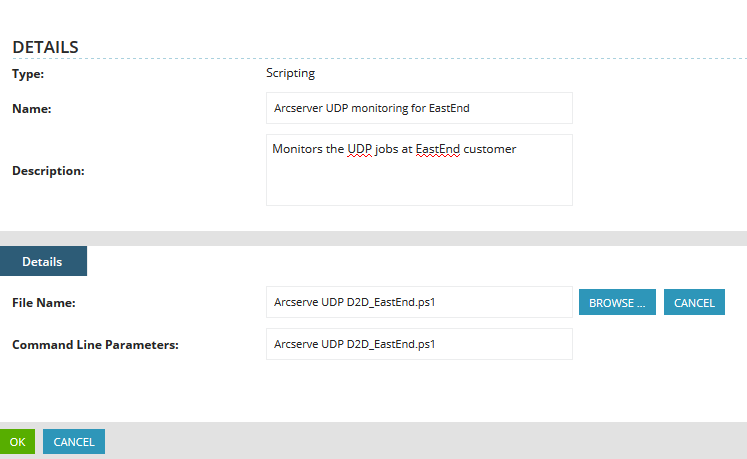
1. You will need to change the User, Pass, and Dom variables so the script can be executed in each customer environment you have. This credential should be a domain admin account.
2. By default, the script goes back 100 hours to check the job statuses.

## To upload the policy in N-central

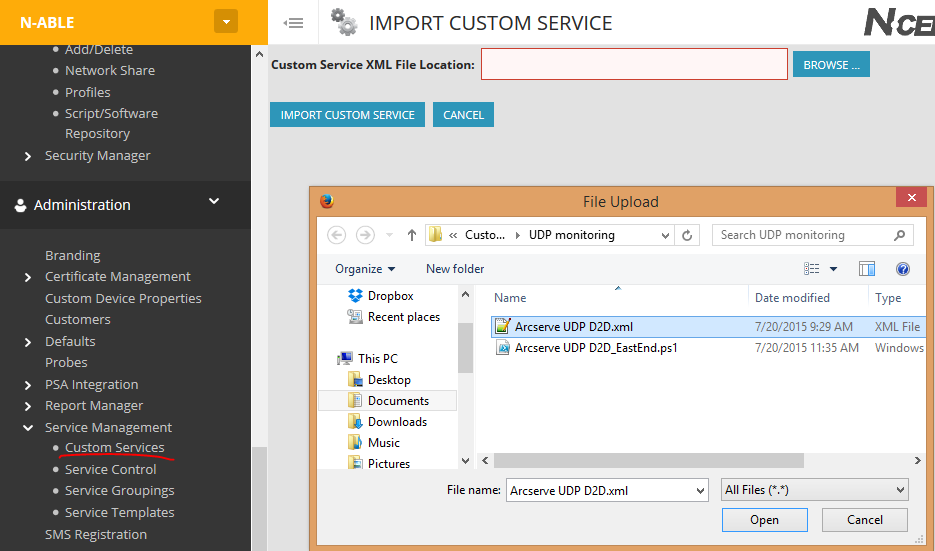
1. Go to your SO (Orange) level. You can upload the powershell script into the N-central under Configuration - Script/Software Repository – Add – Scripting.



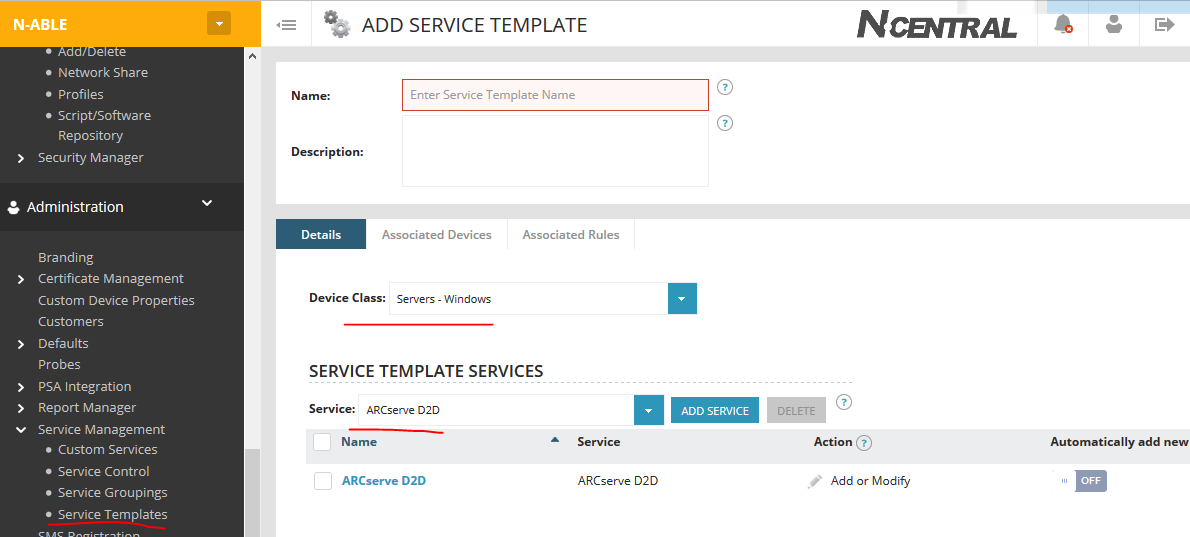
1. Make sure you name your scripts with correct identifications because they use different domain credentials within the scripts.



1. Now import the customer service by going to SO level, Administration – Service Management – Custom Services - Import.



1. Create a service template to include this custom service. SO level - Administration – Service Management – Service Templates – Add - find the Arcserve D2D service. (Note: pay attention to the device class, if you have UDP on both servers, workstations and laptops, you will need 3 service templates in total)

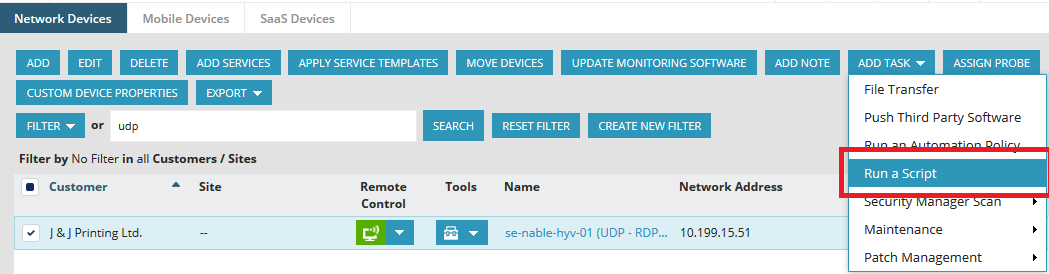


## To run the policy in N-central

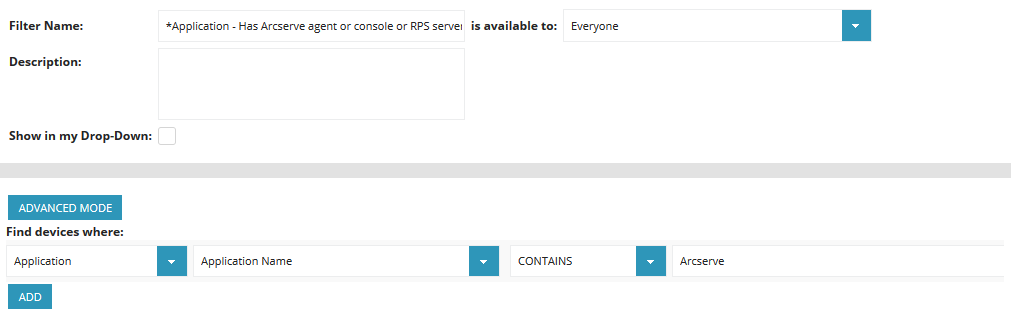
Note:

* + If backup is done through the UDP agent, run the script on each individual device that has the agent installed.
  + If backup is done agentless, run the script on the RPS server

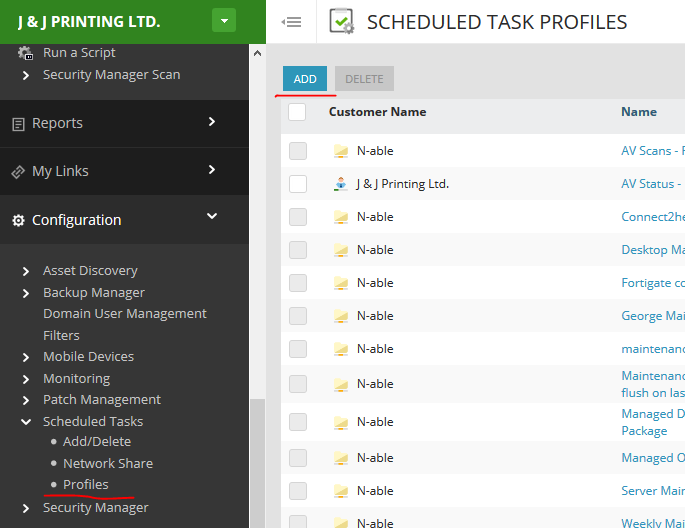
1. Once uploaded, you can target the devices and execute the script through either a scheduled task or a scheduled task profile. If you use scheduled task, simple select the devices that you know UDP agents are present or are RPS servers, then run the script with a re-curring schedule.



1. If using scheduled task profile, you will want to create a filter to automatically pickup systems with UDP agent and UDP RPS servers. A typical filter could be easily look at all devices that contains Arcserve application name.



1. After creating a filter from the SO level, you can go to the customer level where the UDP agents or RPS are located, create a scheduled task profile to run the powershell script with a re-curring schedule.



1. Now we will combine the filter, scheduled task profile, service template all into a rule so the monitoring and script can run automaticlaly whenever UDP is detected on all devices.

Go to the Customer level where you want to setup UDP monitoring and have customized the script with the customer environment username - on the left pane, go to Monitoring, create a new Rule.

First, select the filter created under devices to target.

Then jump to the Schedule Tasks Profiles tab within the rule, attach the Arcserve UDP schedule task profile. Finally, go under Monitoring Options select Service template created. Then you are done.