

# L1 Monitoring Tasks

## **ABSTRACT**

This document will help you to handle L1 tickets of Unix/Windows servers.

## Unix Tasks

### 1. How to check disk usage:

- Login to the server using putty through SSH console.
- Use command → `df -h /mnt/wr76`



critical Alert for FW critical Alert for RE critical Alert for RE critical Alert for clear Alert for  
ms\_mediaserviceinfr ms\_mediaserviceinfr ms\_mediaserviceinfr ms\_mediaserviceinfr ms\_mediaserviceinfr

```
suryapj@cxint-soa01:~  
login as: suryapj  
suryapj@10.2.8.21's password:  
Last login: Fri Apr 18 07:06:27 2014 from 10.72.218.53  
[suryapj@cxint-soa01 ~]$ df -h  
Filesystem      Size  Used Avail Use% Mounted on  
/dev/sda3        15G   8.4G  5.0G   63% /  
tmpfs            1.9G   0  1.9G   0% /dev/shm  
/dev/sdal        248M   49M  188M  21% /boot  
10.10.14.9:/volumes/Inside_Media/cxint_media_70  
32T   22T   11T   69% /wfs  
[suryapj@cxint-soa01 ~]$
```

### 2. How to check CPU usage:

- Login to the server using putty through SSH console.
- Use command → `top`



critical Alert for FW critical Alert for RE critical Alert for clear Alert for  
ms\_mediaserviceinfr ms\_mediaserviceinfr ms\_mediaserviceinfr ms\_mediaserviceinfr

```
suryapj@cxint-soa01:~  
[suryapj@cxint-soa01 ~]$ top  
top - 11:11:33 up 79 days, 13:33, 1 user, load average: 0.00, 0.00, 0.00  
Tasks: 103 total, 1 running, 102 sleeping, 0 stopped, 0 zombie  
Cpu(s): 2.5%us, 0.2%sy, 0.0%ni, 97.3%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st  
Mem: 3925040k total, 2504176k used, 1420864k free, 179044k buffers  
Swap: 1572856k total, 23904k used, 1548952k free, 649860k cached  


| PID  | USER     | PR | NI | VIRT  | RES  | SHR  | S | %CPU | %MEM | TIME+    | COMMAND       |
|------|----------|----|----|-------|------|------|---|------|------|----------|---------------|
| 9896 | root     | 20 | 0  | 2995m | 1.3g | 6148 | S | 5.3  | 34.4 | 1441:46  | java          |
| 1661 | activemq | 20 | 0  | 113m  | 488  | 404  | S | 0.3  | 0.0  | 63:52.19 | tanukiwrapper |
| 1725 | suryapj  | 20 | 0  | 15028 | 1200 | 940  | R | 0.3  | 0.0  | 0:00.01  | top           |
| 1    | root     | 20 | 0  | 19344 | 708  | 500  | S | 0.0  | 0.0  | 0:02.22  | init          |
| 2    | root     | 20 | 0  | 0     | 0    | 0    | S | 0.0  | 0.0  | 0:00.00  | kthreadd      |
| 3    | root     | RT | 0  | 0     | 0    | 0    | S | 0.0  | 0.0  | 0:07.51  | migration/0   |
| 4    | root     | 20 | 0  | 0     | 0    | 0    | S | 0.0  | 0.0  | 1:37.43  | ksoftirqd/0   |
| 5    | root     | RT | 0  | 0     | 0    | 0    | S | 0.0  | 0.0  | 0:00.00  | migration/0   |
| 6    | root     | RT | 0  | 0     | 0    | 0    | S | 0.0  | 0.0  | 0:09.32  | watchdog/0    |
| 7    | root     | RT | 0  | 0     | 0    | 0    | S | 0.0  | 0.0  | 0:10.28  | migration/1   |
| 8    | root     | RT | 0  | 0     | 0    | 0    | S | 0.0  | 0.0  | 0:00.00  | migration/1   |
| 9    | root     | 20 | 0  | 0     | 0    | 0    | S | 0.0  | 0.0  | 1:22.34  | ksoftirqd/1   |
| 10   | root     | RT | 0  | 0     | 0    | 0    | S | 0.0  | 0.0  | 0:08.85  | watchdog/1    |
| 11   | root     | 20 | 0  | 0     | 0    | 0    | S | 0.0  | 0.0  | 4:57.46  | events/0      |
| 12   | root     | 20 | 0  | 0     | 0    | 0    | S | 0.0  | 0.0  | 6:05.85  | events/1      |
| 13   | root     | 20 | 0  | 0     | 0    | 0    | S | 0.0  | 0.0  | 0:00.00  | cgroup        |


```

### 3. To check robot running or not:

- Login to the server using putty through SSH console.
- Use Command → `service nimbus status`

### 4. To check server uptime:

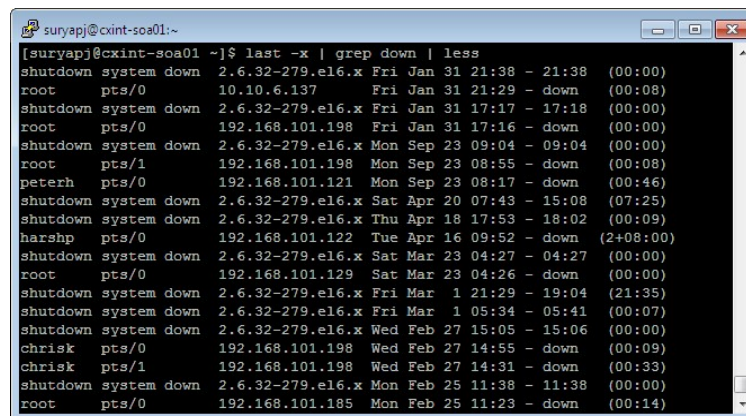
- Login to the server using putty through SSH console.
- Use command → `w` & Uptime

```
[kanalarasank@cxdmz-ftp01 ~]$ w
13:46:45 up 80 days, 19:21, 1 user, load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU WHAT
kanalara pts/0    10.72.218.51    13:42    0.00s  0.04s  0.02s w
[kanalarasank@cxdmz-ftp01 ~]$
```

```
[kanalarasank@cxdmz-ftp01 ~]$ uptime
13:47:16 up 80 days, 19:21, 1 user, load average: 0.00, 0.00, 0.00
[kanalarasank@cxdmz-ftp01 ~]$
```

### 5. To check server last reboot time:

- Login to the server using putty through SSH console.
- Use command → `last -x | grep down | less`



```
suryapj@cint-soa01:~$ last -x | grep down | less
shutdown system down 2.6.32-279.el6.x Fri Jan 31 21:38 - 21:38 (00:00)
root pts/0 10.10.6.137 Fri Jan 31 21:29 - down (00:08)
shutdown system down 2.6.32-279.el6.x Fri Jan 31 17:17 - 17:18 (00:00)
root pts/0 192.168.101.198 Fri Jan 31 17:16 - down (00:00)
shutdown system down 2.6.32-279.el6.x Mon Sep 23 09:04 - 09:04 (00:00)
root pts/1 192.168.101.198 Mon Sep 23 08:55 - down (00:08)
peterh pts/0 192.168.101.121 Mon Sep 23 08:17 - down (00:46)
shutdown system down 2.6.32-279.el6.x Sat Apr 20 07:43 - 15:08 (07:25)
shutdown system down 2.6.32-279.el6.x Thu Apr 18 17:53 - 18:02 (00:09)
harshp pts/0 192.168.101.122 Tue Apr 16 09:52 - down (2+08:00)
shutdown system down 2.6.32-279.el6.x Sat Mar 23 04:27 - 04:27 (00:00)
root pts/0 192.168.101.129 Sat Mar 23 04:26 - down (00:00)
shutdown system down 2.6.32-279.el6.x Fri Mar 1 21:29 - 19:04 (21:35)
shutdown system down 2.6.32-279.el6.x Fri Mar 1 05:34 - 05:41 (00:07)
shutdown system down 2.6.32-279.el6.x Wed Feb 27 15:05 - 15:06 (00:00)
chrisk pts/0 192.168.101.198 Wed Feb 27 14:55 - down (00:09)
chrisk pts/1 192.168.101.198 Wed Feb 27 14:31 - down (00:33)
shutdown system down 2.6.32-279.el6.x Mon Feb 25 11:38 - 11:38 (00:00)
root pts/0 192.168.101.185 Mon Feb 25 11:23 - down (00:14)
```

### 6. To check the server var log error messages:

- Login to the server using putty through SSH console.
- Use Command → `sudo cat /var/log/messages`



critical Alert for FW critical Alert for RE critical Alert for RE critical Alert for RE critical Alert for  
ms\_mediaserviceinfr ms\_mediaserviceinfr ms\_mediaserviceinfr ms\_mediaserviceinfr ms\_mediaserviceinfr



RE critical Alert for RE critical Alert for RE critical Alert for RE critical Alert for RE critical Alert for  
ms\_mediaserviceinfr ms\_mediaserviceinfr ms\_mediaserviceinfr ms\_mediaserviceinfr ms\_mediaserviceinfr



RE critical Alert for clear Alert for  
ms\_mediaserviceinfr ms\_mediaserviceinfr

```
suryapj@bkdmz-tm01:~
[suryapj@bkdmz-tm01 ~]$ sudo cat /var/log/messages | grep -i error | tail -10
[sudo] password for suryapj:
Apr  4 08:39:28 bkdmz-tm01 named[1547]: error (network unreachable) resolving './D
NSKEY/IN': 2001:503:c27::2:30#53
Apr  4 08:39:28 bkdmz-tm01 named[1547]: error (network unreachable) resolving './N
S/IN': 2001:503:c27::2:30#53
Apr  4 08:39:28 bkdmz-tm01 named[1547]: error (network unreachable) resolving './D
NSKEY/IN': 2001:7fe::53#53
Apr  4 08:39:28 bkdmz-tm01 named[1547]: error (network unreachable) resolving './N
S/IN': 2001:7fe::53#53
Apr  4 08:39:28 bkdmz-tm01 named[1547]: error (network unreachable) resolving 'dlv
.isc.org/DNSKEY/IN': 2001:500:71::29#53
Apr  4 10:39:29 bkdmz-tm01 named[1547]: error (network unreachable) resolving './D
NSKEY/IN': 2001:500:1::803f:235#53
Apr  4 10:39:29 bkdmz-tm01 named[1547]: error (network unreachable) resolving './N
S/IN': 2001:500:1::803f:235#53
Apr  4 10:39:29 bkdmz-tm01 named[1547]: error (network unreachable) resolving './D
NSKEY/IN': 2001:500:3::42#53
Apr  4 10:39:29 bkdmz-tm01 named[1547]: error (network unreachable) resolving './N
S/IN': 2001:500:3::42#53
Apr  4 10:39:29 bkdmz-tm01 named[1547]: error (network unreachable) resolving 'dlv
.isc.org/DNSKEY/IN': 2001:4f8:0:2::20#53
[suryapj@bkdmz-tm01 ~]$
```

Solution:-

## 7. How to check Physical memory usage:

- Login to the server using putty through SSH console.
- Use command → free -m  
Free -k  
Free -g  
K=kb m=mb g=gb

```

suryapj@bkdmz-ftp01:~$ free
              total        used         free       shared    buffers     cached
Mem:           1020644      956396       64248            0       160604      428012
-/+ buffers/cache:      367780       652864
Swap:          1572856        7552      1565304
[suryapj@bkdmz-ftp01 ~]$

```

```

[kanalarasank@cxdmz-ftp01 ~]$ free -k
              total        used         free       shared    buffers     cached
Mem:           1020644      881508       139136            0       153216      473980
-/+ buffers/cache:      254312       766332
Swap:          1572856        8216      1564640
[kanalarasank@cxdmz-ftp01 ~]$

```

```

[kanalarasank@cxdmz-ftp01 ~]$ free -g
              total        used         free       shared    buffers     cached
Mem:              0            0            0            0            0            0
-/+ buffers/cache:            0            0
Swap:              1            0            1
[kanalarasank@cxdmz-ftp01 ~]$

```

```

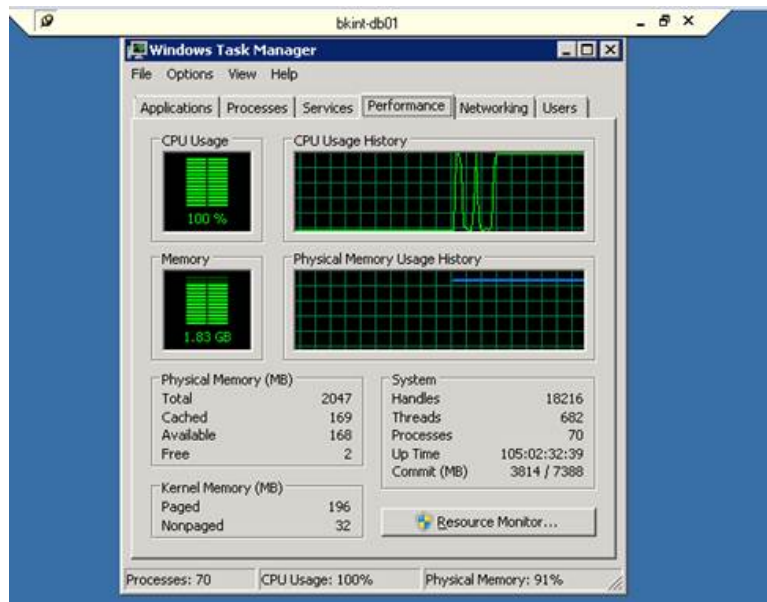
[kanalarasank@cxdmz-ftp01 ~]$ free -m
              total        used         free       shared    buffers     cached
Mem:              996         860          136            0          149          462
-/+ buffers/cache:          247          748
Swap:             1535           8         1527
[kanalarasank@cxdmz-ftp01 ~]$

```

## Windows Tasks

### CPU alert:

- Login to server and check in task manager (To check the alert is real or false)



- Type “**Get-process**” in windows power shell and check which process is using more CPU,

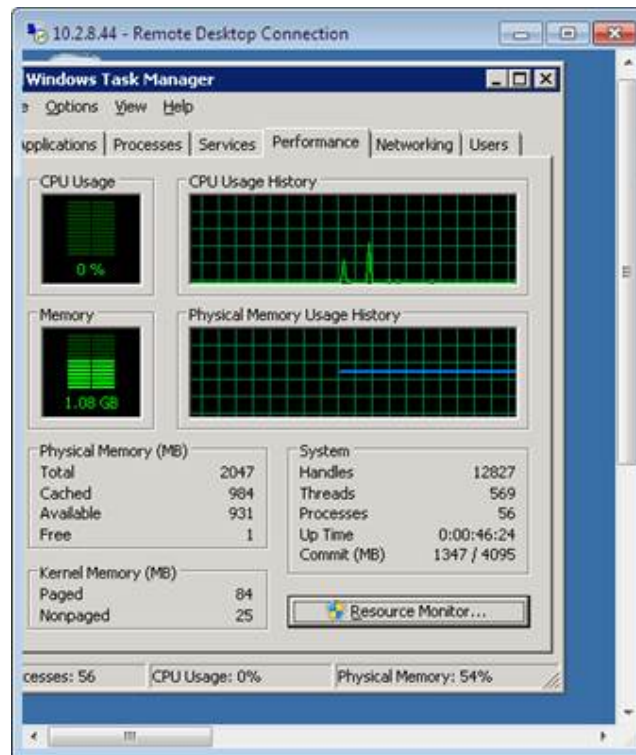
Windows PowerShell

```
PS C:\> get-process
```

Handles	NPM(K)	PM(K)	WS(K)	UM(M)	CPU(s)	Id	ProcessName
305	30	35536	25756	210		8328	AssetDoc
231	12	5244	3172	41		6664	cdm
21	4	2148	164	38		4024	cmd
21	4	2208	136	38		8064	cmd
33	5	2088	1368	27		2364	conhost
34	5	1332	400	46		3448	conhost
37	5	2124	4372	47	0.02	3584	conhost
33	5	2084	1352	27		5360	conhost
33	5	2144	1332	27		6180	conhost
51	6	1412	412	26		6424	conhost
39	5	1456	276	56		6508	conhost
146	11	3636	1464	39		6392	controller
839	16	3832	1292	55		336	csrss
73	9	8036	136	48		400	csrss
200	8	2352	408	47		1908	csrss
328	10	2488	3532	49		3700	csrss
253	11	3284	372	59		8112	csrss
185	9	2312	5276	46		8532	csrss
175	10	2400	512	40		8604	csrss
206	16	4456	2108	56		2140	dllhost
74	7	1792	188	54		7676	dwm
81	7	1964	232	54		8056	dwm
73	7	1764	220	54		8648	dwm
67	7	1548	3856	49	0.00	8932	dwm
70	7	1688	2824	49		9004	dwm
671	41	30800	15756	206		1064	explorer
516	34	14940	6052	186		3872	explorer
506	34	15052	29300	184	0.59	4604	explorer

## Memory alert:

- Login to server and check in task manager (To check the alert is real or false)



- Type “Task list” in command prompt for memory usage



```

C:\>tasklist

Image Name                      PID Session Name        Session#    Mem Usage
-----
System Idle Process             0 Services             0           24 K
System                          4 Services             0          308 K
smss.exe                       248 Services             0          476 K
csrss.exe                      336 Services             0       1,292 K
wininit.exe                    380 Services             0          176 K
csrss.exe                      400 Console               1          136 K
winlogon.exe                   444 Console               1          180 K
services.exe                   492 Services             0       6,204 K
lsass.exe                      500 Services             0      11,536 K
lsn.exe                        508 Services             0       3,780 K
svchost.exe                    608 Services             0       4,040 K
svchost.exe                    688 Services             0       5,496 K
LogonUI.exe                    768 Console               1          856 K
svchost.exe                    776 Services             0      33,812 K
svchost.exe                    824 Services             0      38,692 K
svchost.exe                    904 Services             0      10,724 K
svchost.exe                    944 Services             0       7,356 K
svchost.exe                    984 Services             0       6,944 K
svchost.exe                   1052 Services             0       3,280 K
spoolsv.exe                    1052 Services             0       2,772 K

```

## Reboot alert:

- Check in, Event viewer > windows logs > system > check filter with event id “1074 or user 32”



critical Alert for FW critical Alert for RE critical Alert for RE critical Alert for  
ms\_mediaserviceinfr ms\_mediaserviceinfr ms\_mediaserviceinfr ms\_mediaserviceinfr

**Event Viewer**

File Action View Help

Event Viewer (Local)

- Custom Views
- Windows Logs
  - Application
  - Security
  - Setup
  - System**
- Forwarded Events
- Applications and Services Logs
- Subscriptions

**System** Number of events: 5,459

Filtered: Log: System; Source: ; Event ID: 1074. Number of events: 33

Level	Date and Time	Source	Event ID	Task Category
Information	02/01/2014 10:10:55	USER32	1074	None
Information	26/11/2013 16:21:36	USER32	1074	None
Information	26/11/2013 16:21:35	USER32	1074	None
Information	12/11/2013 14:18:44	USER32	1074	None
Information	17/09/2013 13:15:44	USER32	1074	None
Information	11/09/2013 15:38:53	USER32	1074	None

**Event 1074, USER32**

General Details

The process C:\Windows\system32\winlogon.exe (BKINT-MXPAPP01) has initiated the restart of computer BKINT-MXPAPP01 on behalf of user TCLM\ckammermann for the following reason: No title for this reason could be found  
Reason Code: 0x500ff  
Shutdown Type: restart  
Comment:

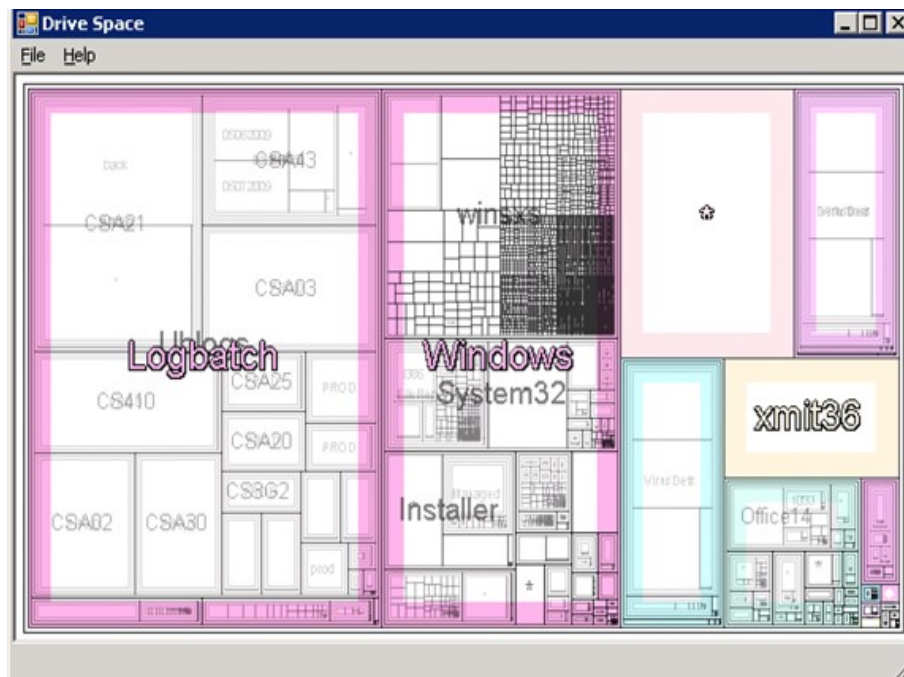
Log Name: System  
Source: USER32  
Event ID: 1074  
Level: Information  
User: TCLM\ckammermann

Logged: 26/11/2013 16:21:36  
Task Category: None  
Keywords: Classic  
Computer: BKINT-MXPAPP01.tclm.local

## To check drive space:



- Open “drivespace.exe” in server and check which drive is using more space



### Ping alert:

- Open command prompt and type “ping server ip address”

```
C:\Windows\system32\cmd.exe
C:\Users\SivaMuru>ping 10.20.8.62
Pinging 10.20.8.62 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

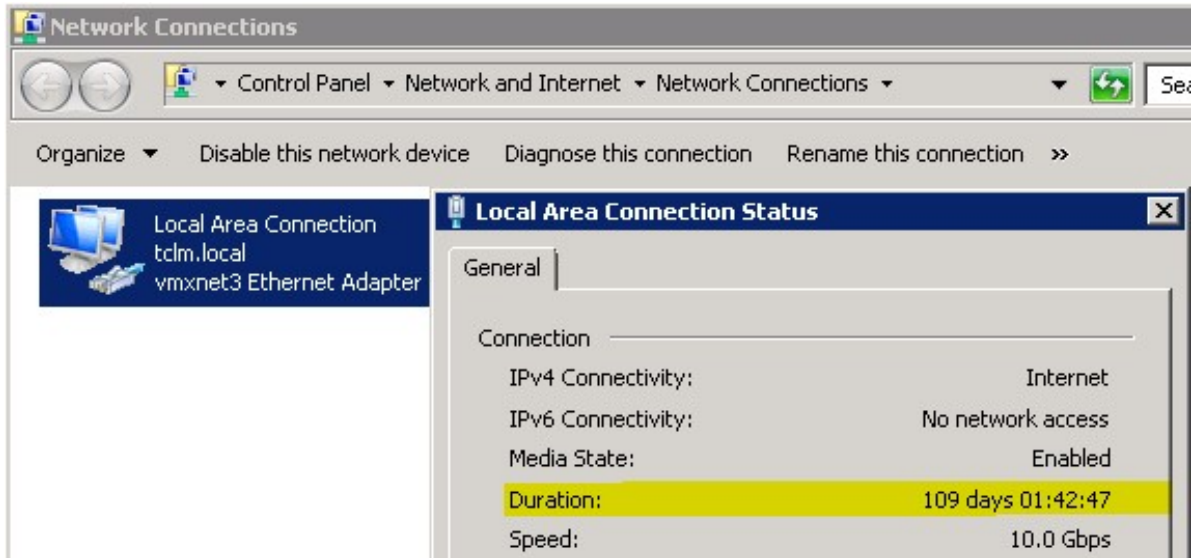
Ping statistics for 10.20.8.62:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\SivaMuru>ping 10.2.18.24
Pinging 10.2.18.24 with 32 bytes of data:
Reply from 10.2.18.24: bytes=32 time=138ms TTL=126
Reply from 10.2.18.24: bytes=32 time=138ms TTL=126
Reply from 10.2.18.24: bytes=32 time=139ms TTL=126
Reply from 10.2.18.24: bytes=32 time=138ms TTL=126

Ping statistics for 10.2.18.24:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 138ms, Maximum = 139ms, Average = 138ms

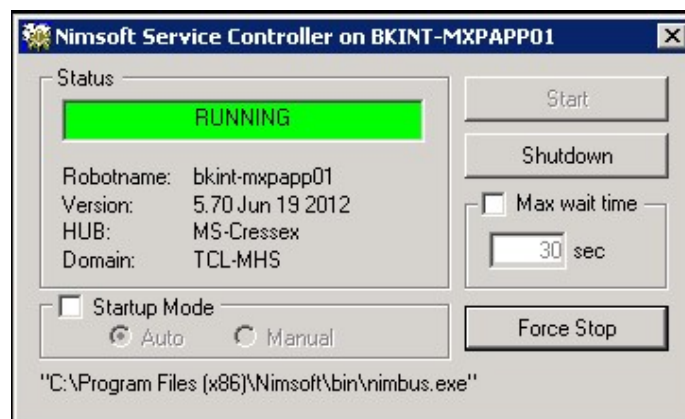
C:\Users\SivaMuru>
```

- Check the uptime of server in network connections by typing “Ncpa.cpl” in run



### **Robot alert:**

- Log into the server and open “**Nimsoft service controller**” and check the status of robot status



### **Service stopped alert:**

Log into server, type “**services.msc**” in run and check the service status.

Services

File Action View Help

Services (Local)

Services (Local)

ActiveX Installer (AxInstSV)

Description:  
 Provides User Account Control validation for the installation of ActiveX controls from the Internet and enables management of ActiveX control installation based on Group Policy settings. This service is started on demand and if disabled the installation of ActiveX controls will behave according to default browser settings.

Name	Description	Status	Startup Type	Log On As
ActiveX Installer (...)	Provides Us...		Manual	Local Syste...
Adaptive Brightness	Monitors a...		Manual	Local Service
Adobe Acrobat U...	Adobe Acro...	Started	Automatic	Local Syste...
Application Experi...	Processes a...	Started	Manual	Local Syste...
Application Identity	Determines ...		Manual	Local Service
Application Infor...	Facilitates t...	Started	Manual	Local Syste...
Application Layer ...	Provides su...		Manual	Local Service
Application Mana...	Processes in...		Manual	Local Syste...
Background Intelli...	Transfers fil...	Started	Automatic (D...	Local Syste...
Base Filtering Engi...	The Base Fil...	Started	Automatic	Local Service
BitLocker Drive En...	BDESVC hos...		Manual	Local Syste...

## Disk Usage



critical Alert for  
ms\_mediaserviceinfr



FW critical Alert for  
ms\_mediaserviceinfr



RE critical Alert for  
ms\_mediaserviceinfr



clear Alert for  
ms\_mediaserviceinfr