NetCrunch 7 can monitor Microsoft Windows systems without installing additional agents. However, due to tightened security rules, remote monitoring is possible only after initial configuration which depends on your Windows environment.

MONITORING SERVER

NetCrunch Server can be installed on Windows Server 2003 R2, Windows Server 2008/2008 R2, or Windows Server 2012. If you manage most of servers by Active Directory, it is better to install NetCrunch on a machine within Active Directory domain. It just makes configuration easier.

MONITORED SYSTEMS

SERVERS

Most servers systems come with the firewall being enabled, which blocks remote administration. This is the first thing you need to fix. It's easy to configure – especially if managed by Active Directory Group Policies. Otherwise, you need to configure servers one by one – you can do it using simple script (download it from: http://www.adremsoft.com/download/SetWinForNC.zip).

WORKSTATIONS

If you manage your workstations by Active Directory, preparing them for monitoring will be the same as for the servers (by Active Directory Group Policies).
Monitoring of workstations in Workgroups is a little harder to configure, because starting from Windows Vista, all later systems use UAC (User Account Control). It does not allow remote connections to inherit administration rights from local *Administrators* group. In this case you can choose to use built-in local *Administrator* account, or create new account and manually assign necessary rights directly to this account.

CONFIGURATION STEPS OVERVIEW

1. **Setting Access Rights**
   NetCrunch needs user account for monitoring which has proper access rights to **DCOM**, **WMI** (*root\cimV2*) and (*Read Access*) to registry key *HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib.* The easiest way you can do it is by adding this user to the local *Administrators* group.

2. **Setting Firewall Rules**
   Firewall rule must allow traffic of RPC, Performance Monitoring, Named Pipes and WMI.

3. **Enabling PerfMon monitoring**
   Remote Registry service must be running and its startup type should be set to *Automatic*.

4. **Disable UAC remote restrictions**
   User Account Control remote restrictions needs to be disabled on non-Domain servers.
   This requires changing value of registry key:
   KEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy

CONFIGURING ACTIVE DIRECTORY DOMAIN

> The procedure below requires a working knowledge of *Active Directory Users and Computers* and *Group Policy Management* Administrative Tools

If you manage most of servers by Active Directory the best solution is installing NetCrunch on a server in the Active Directory domain, and creating dedicated user for monitoring. **In this case, you should abort your installation now and configure your Active Directory first.** You can resume your NetCrunch installation after your configuration is propagated to all servers – it takes approximately **2 hours**.

In this way NetCrunch will be able to discover all servers in AD and automatically setup monitoring for them. Other servers in untrusted domains or workgroups can be configured separately (*see Configuration of Separate Windows Server chapter*).

SETTING ACCESS RIGHTS

STEP 1 – CREATE USER FOR MONITORING

Create Active Directory user account (for example *nc-mon-user*) that will be used by NetCrunch Server for monitoring. You will be asked later for this user credentials during the NetCrunch installation.

STEP 2 – SET UP RIGHTS FOR THE USER

The user account needs administrative rights to all monitored Windows computers (including the server where NetCrunch Server is installed). There are two different ways to accomplish this, depending on your Active Directory architecture and your needs:

IF IN SINGLE DOMAIN WHERE YOU WANT TO MONITOR ALL MACHINES

Add created user account to predefined *Domain Admins* Active Directory group.

IF MULTIPLE TRUSTED DOMAINS OR ONLY SUBSET OF COMPUTERS NEEDS MONITORING

You need to use Group Policy to modify local Administrators groups (on each monitored Windows machine).

a) Create Active Directory group named *Monitoring Users* and add previously created user account (*nc-mon-user*) to this group.

> In multi-domain forest, default Active Directory group scope (which is *Global)* should be sufficient for this group, because global groups can be used to assign permissions to resources in any domain in a forest.

b) Create a new Group Policy Object (GPO) and name it for example *Local Administrators group membership for NetCrunch.*

c) Create rule for *Monitoring Users* group membership.
Go to:
Computer Configuration → Policies → Windows Settings → Security Settings → Restricted Groups
and add *Monitoring Users* to local *Administrators* group using section *This group is a member of*

d) Link *Local Administrators group membership for NetCrunch* GPO to appropriate Organization Unit(s) (OU) in your Active Directory domain(s).

SETTING FIREWALL RULES

1. Create a new Group Policy Object and name it for example *Windows Firewall rules for monitoring by NetCrunch*.

2. Use two different branches in GPO to configure both built-in firewall types in Windows machines which you want to monitor:
   a. **For XP and Server 2003 R2,**
   Go to:
   Computer Configuration → Administrative Templates → Network → Network Connections → Windows Firewall → Domain Profile
   and set these settings to "Enabled":
   Windows Firewall: Allow inbound file and printer sharing exception
   Windows Firewall: Allow inbound remote administration exception

   b. **For Vista/7/8 and Server 2008/2008 R2/2012,**
   Go to:
   Computer Configuration → Policies → Windows Settings → Security Settings → Windows Firewall with Advanced Security
   and add these rules to *Inbound Rules*, choosing them from predefined list:
   File and Printer Sharing

Remote Administration

> By default, Windows built-in firewall doesn't block outgoing traffic – if you have changed this behavior, add rules with the same names from predefined list to *Outbound Rules*.

3. Link *Windows Firewall rules for monitoring by NetCrunch* GPO to appropriate Organization Unit(s) (OU) in your Active Directory domain(s).

For a security reasons, it is recommended to customize remote administration rules to narrow the list of allowed IP addresses to the address of your NetCrunch Server only.

ENABLING PERFMON MONITORING

1. Create a new Group Policy Object and name it for example *Windows services for monitoring by NetCrunch*.
2. Setup *Remote Registry* service.
   Go to:

   Computer Configuration → Policies → Windows Settings → Security Settings → System Services

   and set *Remote Registry* Windows service startup mode to *Automatic*.

3. Link *Windows services for monitoring by NetCrunch* GPO to appropriate Organization Unit(s) (OU) in your Active Directory domain(s).

Right after the policy refresh, the service should immediately start on every computer.

CONFIGURING OF SEPARATE WINDOWS SERVERS

All commends below must be executed from the administrator’s command line.

COMPLETE SCRIPT CAN BE DOWNLOADED FROM:

http://www.adremsoft.com/download/SetWinForNC.zip

SETTING ACCESS RIGHTS

Create *nc-mon-user* account using shell commands and add it to local *Administrators* group.

```
net user /add nc-mon-user <Password>
net localgroup Administrators /add nc-mon-user
```

SETTING FIREWALL RULES

For Windows Server 2003 and Server 2003 R2:

```
netsh firewall set service type=fileandprint scope=all profile=all
netsh firewall set service type=remoteadmin scope=all profile=all
```

For Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012 you can create rule for IP address of NetCrunch server only.

```
netsh advfirewall firewall add rule name="NC-Mon" dir=in action=allow remoteip="%IP%"
netsh advfirewall firewall add rule name="NC-Mon" dir=out action=allow remoteip="%IP%"
```

ENABLING PERFMON MONITORING

Setup *Remote Registry* service startup and start the service.

```
WMIC SERVICE where name=”RemoteRegistry” call ChangeStartMode StartMode=Automatic
WMIC SERVICE where name=”RemoteRegistry” call StartService
```

DISABLING UAC REMOTE RESTRICTIONS

Modify UAC behavior for Windows Server 2008/2008 R2, and Windows Server 2012 (http://support.microsoft.com/kb/951016)

```
WMIC /Namespace: \\Root\Default Class StdRegProv Call SetDWORDValue hDefKey="&H80000002"
sSubKeyName="SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"
sValueName="LocalAccountTokenFilterPolicy" uValue=1
```

WINDOWS TECHNOLOGIES USED BY NETCRUNCH

Windows technologies have been built layer by layer. One at top of another – for example RPC is working on top of the Named Pipes, Remote Registry needs RPC, and WMI is using DCOM which is using also RPC for communication. Everything needs proper firewall and security settings. So here is short list of technologies used by NetCrunch that need proper configuration.

1. **RPC & Named Pipes** – (*Needs enabling File Sharing, firewall settings)*
2. **Remote Registry** – (*Needs firewall settings, and Remote Registry service running*)
3. **WMI & DCOM** – (*Needs Firewall settings, DCOM & WMI security settings*)

It is simple in case when the user designated for monitoring is a member of local *Administrators* group – as described in this document. This is the simplest way to configure servers for monitoring but not most secure. In case when security is a big concern it is possible to setup exact rights for monitoring account.