NetCrunch は追加エージェントをインストールすることなく、Microsoft Windows を監視することができます。しかし、セキュリティルールが厳格なため、初期設定のみでリモート監視ができるかは、ユーザーの Windows 環境に依存します。

監視サーバー

NetCrunch サーバーは、Windows Server 2008 R2、Windows Server 2012/R2 にインストールすることができます。ユーザーが Active Directory 環境で多数のサーバーを管理している場合、Active Directory ドメインに参加したマシンに、NetCrunch をインストールすることを推奨します。推奨理由としては、容易に設定することができるためです。

監視対象システム

サーバー

サーバーでは一般的にファイアウォールが有効なため、リモート管理がブロックされています。まずこの項目を変更する必要があります。最も簡単な方法としては、Active Directory グループポリシーで管理する方法です。その他の方法を採用する場合、ユーザーは AdRem Software 社が用意するスクリプトを使用して、個々のサーバーを設定する必要があります。（Web サイトからダウンロード: http://www.adremsoft.com/download/SetWinForNC.zip）

ワークステーション

ユーザーが対象のワークステーションを Active Directory で管理している場合、サーバーと同様に、監視設定する必要があります。（Active Directory グループポリシーの編集、もしくはスクリプトの実行）

ワークグループに所属しているワークステーションを監視する場合、Windows Vista 以降に追加された UAC（ユーザーアクセス制御）のために、設定が困難となっています。この機能のために、ローカルアドミニストレーショングループから管理者権限を継承しているリモート接続を許可しません。この場合、ユーザーはローカルのビルトイン Administrator アカウントを利用することや必要な権限を直接アカウントに割り当てること、必要な権限を持つアカウントを作成することを選択することができます。

設定方法の概要

1. **アクセス権限の設定**
   NetCrunch はユーザーアカウントに **DCOM**、**WMI**（root\cimv2）と（Read Access）、レジストリキー（*HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib*）へのアクセ

ス権限が必要となります。ユーザーはローカル Administrators グループへ使用するユーザーを追加することでこの権現を割り当てることが可能です。

2. **ファイアウォール設定**
   ファイアウォールルールとして、RCP、パフォーマンスモニタ、名前付きパイプ、WMI のトラフィックを許可しなければなりません。

3. **PerfMon 監視の有効化**
   Remote Registry サービスはスタートアップの種類を自動として、実行中でなければなりません。

4. **UAC のリモート制限を無効化**
   UAC（ユーザーアクセス制御）のリモート制御をドメイン参加していないサーバーのために無効にする必要があります。設定変更した場合、コンピュータの再起動が必要になります。以下のレジストリキーの値を 1 に変更します:

   *KEY_LOCAL_MACHINE**SOFTWARE**Microsoft**Windows**CurrentVersion**Policies**System*\LocalAccountTokenFilterPolicy

ACTIVE DIRECTORY ドメインでの設定方法

この手順は管理ツールの *グループポリシー管理* と *Active Directory のユーザー、コンピュータ* の知識が必要となります。

もしユーザーが Active Directory を用いて、多数のサーバーを管理している場合、Active Directory ドメインに参加しているサーバー上に、NetCrunch をインストールして、監視専用のアカウントを作成することが最も容易な方法となります。**この場合、NetCrunch のインストールを中断して、まず Active Directory の設定をしなければなりません。**設定の変更が全てのサーバーに反映された後、NetCrunch をインストールしてください。設定の反映には**約 2 時間程度**、必要になることがあります。

この方法で、NetCrunch は Active Directory に参加している全てのサーバーの検出と監視設定が自動的に行われます。他のドメインやワークグループのサーバーについては、個別に設定が必要になります。（設定方法は*その他の Windows サーバー*の項を参照ください。）

アクセス権限の設定

STEP 1 – 監視専用ユーザーの作成

NetCrunch サーバーで使用する監視専用ユーザーを Active Directory ユーザーアカウント（例では、*nc-mon-user*）として作成します。NetCrunch のインストール中、このユーザー認証情報を求められることがあります。

STEP 2 – ユーザーの権限を設定

NetCrunch サーバーがインストールされているサーバーを含む全ての監視対象 Windows マシンで監視するためには、ユーザーアカウントは管理者権限が必要となります。設定方法としては、ユーザーが利用している Active Directory 構成に依存して、2 種類の方法があります:

監視対象の全てのマシンが単一のドメインに参加している場合

Active Directory の定義済み Domain Admins グループにユーザーアカウントを作成する。

監視対象のマシンが一部のサブセットであるか、複数のドメインがある場合

各監視対象の Windows マシン上でローカル Administrators グループを変更するために、グループポリシーを使用します。

a) Monitoring Users という名前の Active Directory グループを作成します。そのグループに作成したユーザーアカウント（*nc-mon-user*）を追加します。

> グローバルグループはフォレストのいくつかのドメインのリソースへの許可を設定するために利用するため、複数のドメインフォレストの中に、デフォルト Active Directory グループ（*Global*）はこのグループに対して、十分な権限が必要である。

b) グループポリシーオブジェクト（GPO）を新しく作成して、名前を付けます。例えば *Local Administrators group membership for NetCrunch* です。

c) Monitoring Users グループメンバーシップのルール作成
手順:
コンピュータの構成→ポリシー→ Windows の設定→セキュリティの設定→制限されたグループ
ローカル Administrators グループへ Monitoring Users を追加します。

d) Active Directory ドメイン上の組織ユニット（OU）へ適用するために、Link *Local Administrators group membership for NetCrunch* GPO にリンクします。

ファイアウォールの設定方法

1. 新しいグループポリシーオブジェクトを作成して、名前を付けます。例えば *Windows Firewall rules for monitoring by NetCrunch* です。

2. 監視したい Windows マシンのビルトインファイアウォールタイプの両方を設定するために、GPO に 2 つの異なるブランチを使用します:
   a. **XP と Server 2003 R2 の場合**
      手順:
      コンピュータの構成→管理用テンプレート→ネットワーク→ネットワーク接続→Windows ファイアウォール→ドメインプロフィール
      以下を”有効”に設定:
      Windows ファイアウォール: 着信ファイルとプリンタの共有の例外を許可する
      Windows ファイアウォール: 着信リモート管理の例外を許可する

   b. **Vista/7/8 と Server 2008/2008R2/2012 の場合**
      手順:
      コンピュータの構成→ポリシー→Windows の設定→セキュリティの設定→セキュリティが強化された Windows ファイアウォール
      受信の規則に事前定義された規則から以下の規則を追加:
      ファイルとプリンタの共有
      リモート管理

      > デフォルトでは、Windows 標準のファイアウォールは送信トラフィックをブロックしません。もしデフォルトから変更を加えている場合、送信の規則の事前定義済みリストから同名のルールを追加する必要があります。

3. Active Directory ドメイン上の組織ユニット（OU）へ適用するために、*Windows Firewall rules for monitoring by NetCrunch*GPO にリンクします。

セキュリティを強化する方法として、NetCrunch サーバーのアドレスのみ、リモート管理ルールの許可アドレスに指定することを推奨します。

パフォーマンスカウンタ監視の有効化

1. 新しいグループポリシーオブジェクトを作成して、名前を付けます。例えば、*Windows services for monitoring by NetCrunch* です。
2. *Remote Registry* サービスを設定します。
   手順:

   コンピュータの構成→ポリシー→Windows の設定→セキュリティの設定→システムサービス

Remote Registry サービスのスタートアップの種類を*自動*に設定します。

3. Active Directory ドメイン上の組織ユニット（OU）へ適用するために、*Windows services for monitoring by NetCrunch*GPO にリンクします。

ポリシーを更新した直後に、このサービスはコンピュータ上で即座にスタートします。

その他の WINDOWS サーバーの設定

全てのコマンドは管理者用コマンドプロンプトから実行しなければなりません。

完全なスクリプトは WEB サイトからダウンロード:

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

アクセス権限の設定

以下のコマンドをコマンドプロンプトで実行して、*nc-mon-user* アカウントを作成して、ローカル Administrators グループに追加します。

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

ファイアウォールの設定

Windows Server 2003 と Server 2003 R2 の場合:

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

Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 の場合

NetCrunch サーバーの IP アドレスにのみ有効なルールを作成することができます。

コマンドプロンプトで実行する場合、%IP%は NetCrunch サーバーの IP アドレスを入力します。

```
netsh advfirewall firewall add rule name="NC-Mon" dir=in action=allow remoteip=<IP アドレス>
netsh advfirewall firewall add rule name="NC-Mon" dir=out action=allow remoteip=<IP アドレス>
```

PERFMON 監視の有効化

Remote Registry サービスのスタートアップの種類を自動に設定して、サービスを起動します。

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

UAC リモート制御を無効化

Modify UAC behaviorfor 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
```

NETCRUNCH が使用している WINDOWS テクノロジのサマリ

Windows テクノロジは多層構造を持っており、それぞれの層が組み合わさっています。例えば、RPC は名前付きパイプの上で動作しており、Remote Registry は RPC を必要としており、WMI もまた、通信のために RPC を使用している DCOM を使用しています。全ての機能が適切なファイアウォールとセキュリティ設定を必要とします。NetCrunch で使用されるテクノロジと必要な設定のリストを以下に記載します。

1. **RPC と名前付きパイプ –** (*ファイル共有の有効化とファイアウォールの設定が必要です。*)
2. **Remote Registry –** (*ファイアウォール設定と Remote Registry サービスの実行が必要です。*)
3. **WMI と DCOM –** (*ファイアウォール設定、DCOM と WMI のセキュリティ設定が必要です。*)

本項に記載した通り、監視で使用するユーザーがローカル Administrators グループのメンバーである場合は、単純な設定となります。監視のために最も単純な方法は、必ずしもセキュアではありません。もしセキュリティの懸念点がある場合、アカウントを監視に必要な権限のみ割り当てることができます。