

Windows Server 2008 NAP 設定手順書 DHCP 編

～テスト環境での DHCP NAP の強制～



免責事項

本書は伊藤忠テクノソリューションズ株式会社が行った Microsoft Windows Server 2008 製品候補版(RC0 及び RC1)に関する様々な検証をもとに記述したものです。製品化前の段階での検証であり、製品出荷時に仕様に変更になり、本書の内容と相違が発生する可能性があります。

本書は検証における結果をもとに記述していますが、その動作や手順は限られた検証環境での動作であり、他の検証環境や実環境における動作を明示的にも暗示的にも保証するものではありません。

また、本書の内容によりいかなる損害が発生した場合においても伊藤忠テクノソリューションズ株式会社はその責任を負いません。

本書に記載された製品名、ロゴ等は各社の商標、登録商標、もしくはトレードマークです。

目 次

はじめに.....	1
Network Access Protection とは	2
DHCP 構成	2
テスト環境.....	3
テスト環境論理図	3
環境作成手順	3
ドメインコントローラの作成.....	4
NPS のインストールと構成	5
概要	5
Windows Server 2008 RC1 のインストール	5
NPS と DHCP の役割のインストール.....	6
役割の追加ウィザード	6
DHCP サービスの構成	10
ネットワークポリシーサーバーの設定	11
AD への登録.....	11
クライアントの設定	14
動作確認.....	15
おわりに.....	17
付録 NPS と DHCP の分離構成.....	18
インストール手順.....	18
NAP 構成ウィザード.....	18
DHCP サーバーの設定	19
RADIUS Proxy の設定	19

はじめに

伊藤忠テクノソリューションズ株式会社は 2007 年から 2008 年にかけて Microsoft Windows Server 2008 に関する検証を製品候補版(RC0 及び RC1)を利用して実施しました。製品候補版の段階から数々の検証を実施し、製品発売前に Windows Server 2008 という Microsoft の次期サーバーOS について理解を深め、製品の発売と同時に構築作業が実施できるようにすることを目的としています。

本書は、様々な検証の中で実際に作業した結果をもとに、Network Access Protection(NAP)を DHCP 構成で実装する場合の手順を示したものです。

Network Access Protection(NAP)には様々な構成パターンが存在しますが、DHCP 以外の設定手順に関してはそれぞれの設定手順書を参照してください。

本書の手順に従い作業を行うことで、DHCP を利用した NAP を構成することができますが、この手順書の通りに作業した場合、各種の設定項目はデフォルトのままであり、追加の設定が必要になる場合があります。

また、本書は Active Directory 環境や Windows Server 2008 に関して一通りの知識を持った人を対象に記述されています。

そのため、本書は DHCP を利用した NAP を構成する手順を示すことが目的であり、その前提となる Windows Server 2008 のインストールや Active Directory の構築方法に関しては記載しません。

必要に応じて別途技術資料を参照してください。

本書の内容は Windows Server 2008 Enterprise Edition RC1 (x64) を利用して行った検証結果をもとに記載されています。本書内で特に記載がない限り、Windows Server 2008 と記述されている場合は Windows Server 2008 Enterprise Edition RC1 (x64)を指します。

Network Access Protection とは

Network Access Protection(NAP)は Microsoft の次期 OS Windows Server 2008 に搭載されたネットワーク検疫機能です。

NAP を利用することでセキュリティレベルの低いクライアント PC を社内ネットワークから分離することができます。

NAP には実現方法が 5 つ用意されており、それぞれに特徴があります。

- DHCP
- IP Sec
- VPN
- 802.1X
- TS Gateway

本書では一番手軽に導入できるであろう DHCP を利用した NAP を実現するための手順を扱います。

DHCP 構成

DHCP を利用して NAP を構成する場合、DHCP サーバーがクライアントの状態に応じて IP アドレスとサブネットマスクの組み合わせ、さらに静的ルーティングを利用して、修復サーバー以外には接続できないように制御します。

VLAN のようにサブネットを変更するわけではなく、静的ルーティングを利用して接続できるサーバーを制御します。

Windows Server 2008 だけあれば構成することができ、他のネットワーク機器等に依存しないため、NAP の基本的な動作を確認する際に役に立ちます。

ネットワークポリシーサーバー(NPS)と DHCP サーバーは分離することも可能ですが、本書ではより構築が容易な同居構成の手順を示します。

(分離構成の手順は付録に記載)

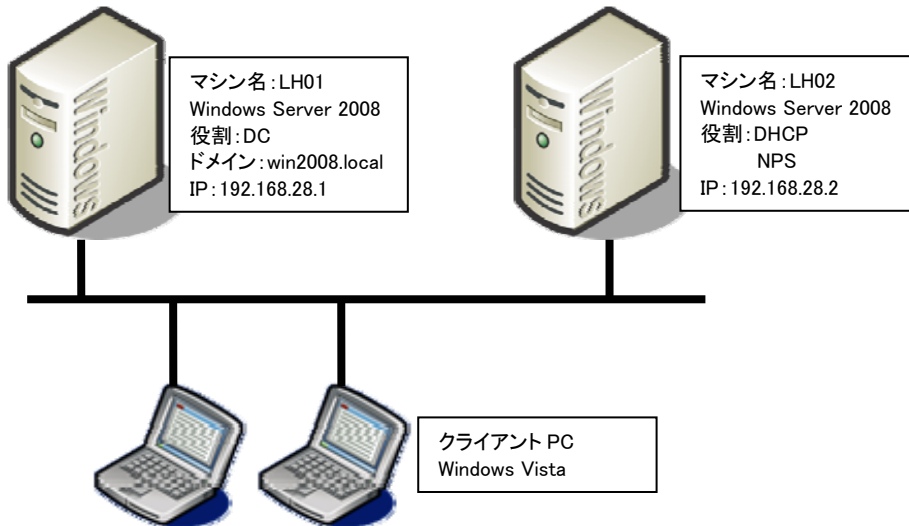
その他の方法に関してはそれぞれの設定手順書を参照してください。

NAP を設定するうえで必要となる各種の用語等に関しては本書では解説しません。必要に応じて各種の技術資料を参照してください。

テスト環境

テスト環境論理図

本書は以下の環境を想定しています。



本書の中では上記のマシン名やドメイン名を利用して手順を説明しています。実際に NAP 環境を構築する際にはご自身の環境に合わせて名前や IP アドレスを変更してください。本書では割愛していますが、必要に応じて WSUS や FCS といったセキュリティを保つためのサーバーを構成してください。

環境作成手順

NAP のテスト環境を作成するためには、最低限3つの役割のサーバーをセットアップする必要があります。

ドメインコントローラ(DC)

Windows Server 2008 RC1 が動作している LH01 を使用します。LH01 をドメインコントローラとして Active Directory ドメインサービスと DNS サービスを構成します。

注) NAP 環境においては Active Directory ドメインサービスは必須ではありません。しかしながら、Active Directory ドメインサービスを用いることで、コンピュータのグループによるアクセス管理やユーザーグループによるアクセス管理など、よりセキュアに使用することができます。なお使用する Active Directory ドメインサービスは、Windows Server 2008 でなくてもかまいません。Windows Server 2003 でも使用可能です。

ネットワークポリシーサーバーサービス(NPS)

Windows Server 2008 RC1 が動作している LH02 を使用します。LH02 にネットワークポリシーサーバーサービスを構成します。

DHCP サービス

NPS 用の LH02 に DHCP サービスを同居させます。NAP 用の DHCP サービスは Windows Server 2008 で構築する必要があります。

また、NAP を動作させるにはクライアント側の設定も必要です。

クライアントの設定

Windows Vista が動作しているクライアント上で、DHCP クライアントと NAP クライアントを構成します。

これらのサーバー、クライアントの設定を順次行うことで NAP が動作し、正常性が確認されたクライアントのみが社内ネットワークに接続できるようになります。

ドメインコントローラの作成

LH01 に Windows Server 2008 RC1 をインストールして次の役割を与えます。

Win2008.local という Active Directory のドメインコントローラ

Win2008.local という DNS ドメインの DNS サーバー

手順の概略は次のとおりです。

- Windows Server 2008 Enterprise Edition RC1 をインストールする

- TCP/IP の構成を行う

- Active Directory ドメインサービスをインストールする

- DCPROMO コマンドを実行して、ドメインコントローラに昇格させる

- (DNS サービスは同時にインストールする)

- 必要に応じて Active Directory でユーザー作成や、GPO を構成する

ドメインコントローラの実行に関する詳細手順は、ここでは省略します。

NPS のインストールと構成

概要

ネットワークポリシーサーバー(NPS)を動作させるには Windows Server 2008 RC1 が動作している必要があります。

手順の概略は次の通りです。

- Windows Server 2008 Enterprise Edition RC1 をインストールする
- TCP/IP の構成を行う
- win2008.local ドメインに参加する
- ネットワークポリシーサーバーサービスをインストールする
- DHCP サービスをインストールする
- DHCP サービスを構成する
- NPS を構成する

以下、手順の詳細を記述します。

Windows Server 2008 RC1 のインストール

コンピュータの電源を入れ Windows Server 2008 Enterprise Edition RC1 の DVD を入れます。画面の指示に従ってインストールを進めます。

インストールが完了したら、Windows にログオンして「ネットワーク接続の管理」から「ローカルエリア接続」のプロパティを開きます。

Internet Protocol Version 6(TCP/IPv6)のチェックボックスを外します。(本書の手順では IPv6 は使用しません)

Internet Protocol Version 4(TCP/IPv4)のプロパティを開いて、IP アドレス、サブネットマスク、デフォルトゲートウェイ、優先 DNS を設定して、OK をクリックして画面を閉じます。

ドメインコントローラに ping を実行してレスポンスが正常なことを確認します。

win2008.local ドメインに参加して、再起動します。

※OS のインストール、TCP/IP の設定、ドメインへの参加方法の詳細に関しては、Microsoft その他から提供されている技術文書を参照してください。

NPS と DHCP の役割のインストール

NPS と DHCP の役割を LH02 にインストールします。

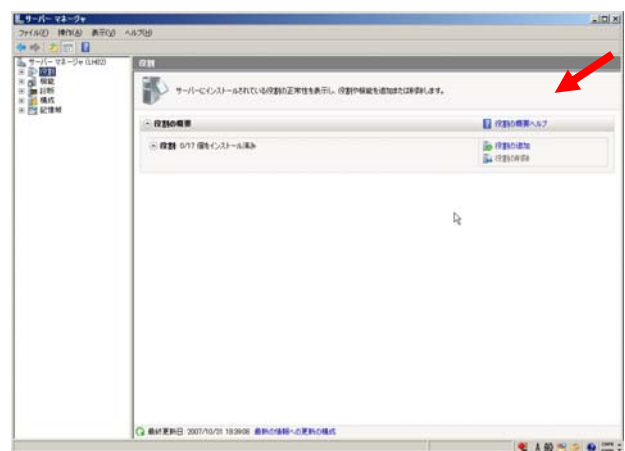
NPS と DHCP は別々にインストールすることも可能ですが、本書では同時にインストールする手順を示します。

役割の追加ウィザード

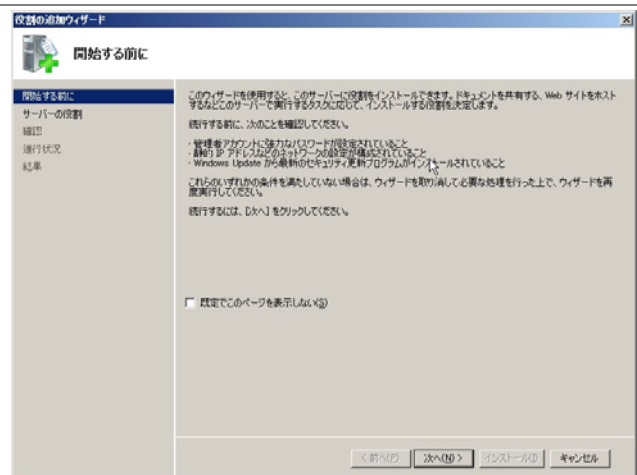
「Start」をクリックして「管理ツール」-「サーバーマネージャー」を起動します。



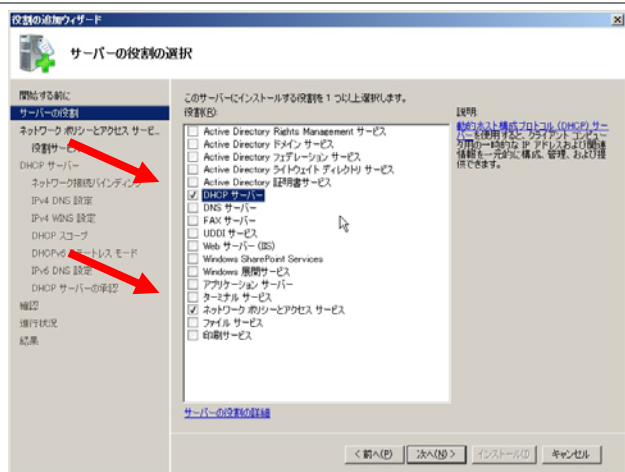
「役割の概要」を展開して「役割の追加」をクリックします。「次へ」をクリックします。



「役割の追加ウィザード」が起動するので「次へ」をクリックします

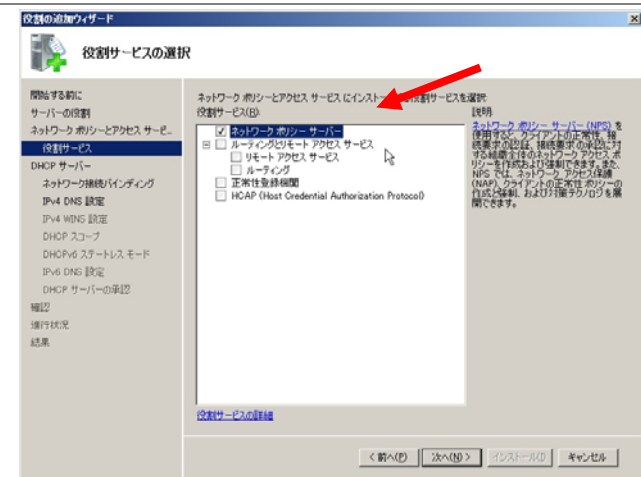


「サーバーの役割の選択」ページが開くので「DHCP サーバー」と「ネットワークポリシーとアクセスサービス」にチェックを入れて「次へ」をクリックします



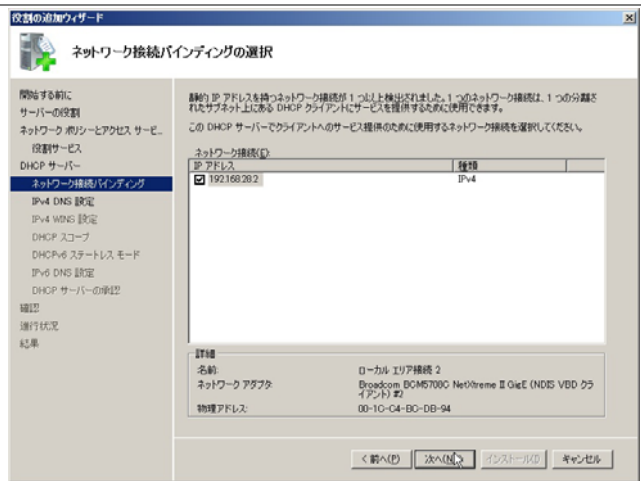
「ネットワークポリシーとアクセスサービス」に関する説明が表示されます。「次へ」をクリックします。

「役割サービスの選択」ページで「ネットワークポリシーサーバー」にチェックを入れます。「次へ」をクリックします。

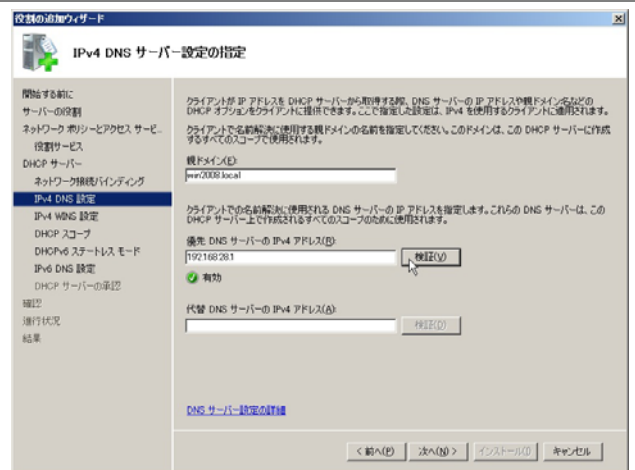


「DHCP サーバー」に関する説明が表示されます。「次へ」をクリックします。

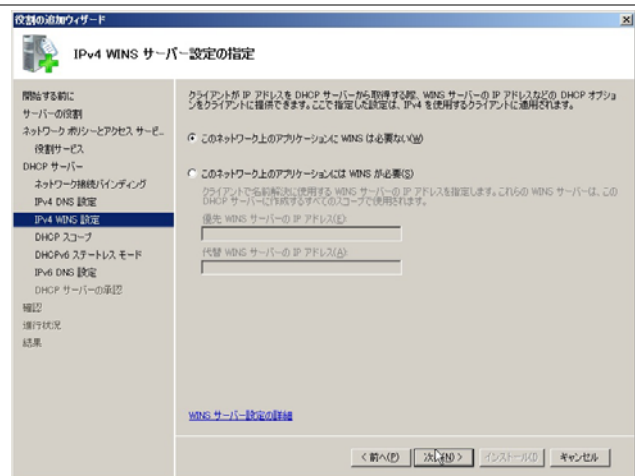
「ネットワーク接続バインディングの選択」ページで DHCP サービスのために使用するネットワーク接続を持つ「IP アドレス」を選択して「次へ」をクリックします。



「IPv4 DNS サーバー設定の指定」ページで親ドメインボックスに「win2008.local」、優先 DNS サーバーボックスに IP アドレスを入力して「次へ」をクリックします。入力が終わったら「検証」ボタンをクリックして「有効」と表示されたら「次へ」をクリックします。

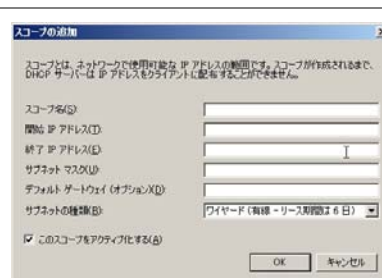


「IPv4 WINS サーバー設定の指定」ページで「このネットワーク上のアプリケーションに WINS は必要ない」が選択されているのを確認して、「次へ」をクリックします。

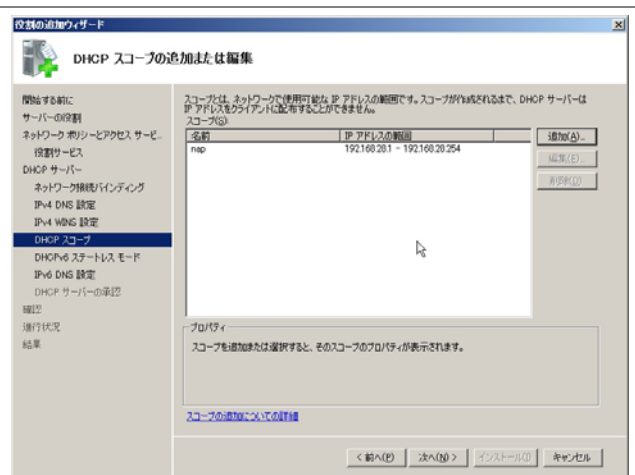


「DHCP スコープの追加または編集」ページが表示されるので「追加」をクリックします。

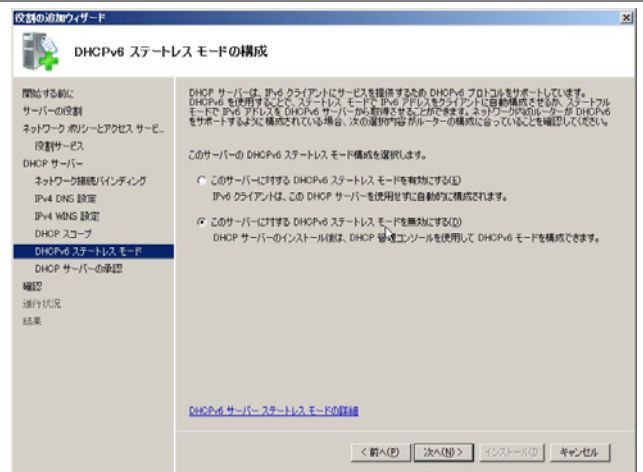
「スコープの追加」ダイアログが表示されるので、スコープ名、開始 IP アドレス、終了 IP アドレス、サブネットマスクを入力して（デフォルトゲートウェイはオプション）サブネットの種類を確認したら、「OK」をクリックします。



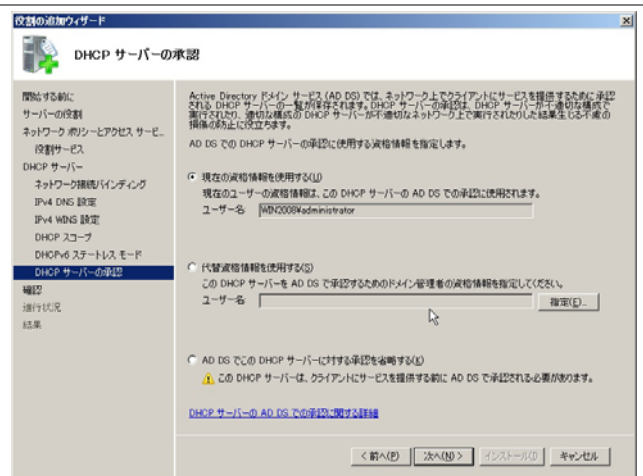
入力したスコープが反映されれば、「次へ」をクリックします。



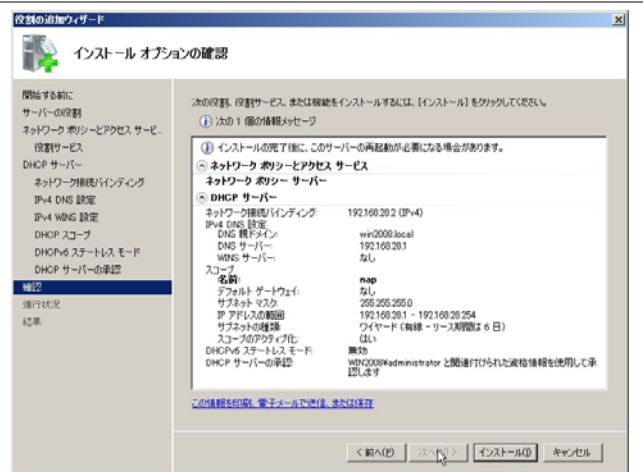
「DHCPv6 ステートレスモードの構成」ページが表示されます。「このサーバーに対する DHCPv6 ステートレスモードを無効にする」を選択して、「次へ」をクリックします。



「DHCP サーバーの承認」ページで「現在の資格情報を使用する」が選択されているのを確認して「次へ」をクリックします。



「インストールオプションの確認」ページで内容を確認して問題がなければ、「インストール」をクリックします。

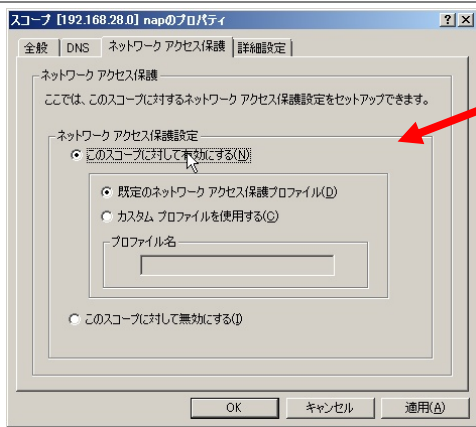
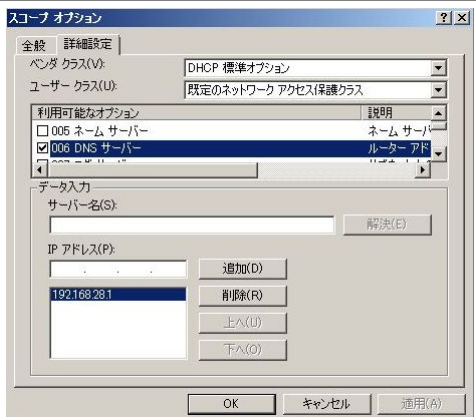
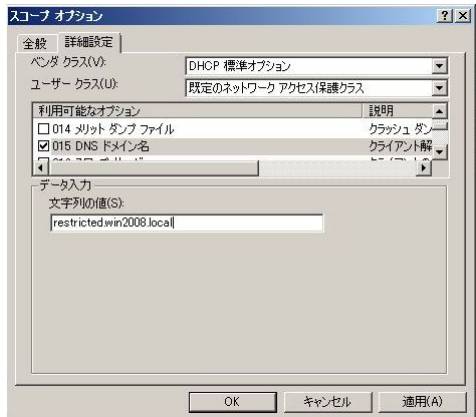


「インストールの結果」画面でインストールが正常に完了したことを確認したら、「閉じる」をクリックして、「役割の追加ウィザード」を終了します。続いて「サーバーマネージャー」も閉じます。

以上で NPS と DHCP がインストールされました。

DHCP サービスの構成

NAP を使用するため必要な設定を DHCP サービスに対して行います。

<p>スタートをクリックして「管理ツール」-「DHCP」をクリックします。</p> <p>「DHCP」コンソールが開いたら、「LH02.win2008.local」を展開して次に「IPv4」を展開します。スコープを右クリックして「プロパティ」をクリックします。「スコープのプロパティ」が表示されたら「ネットワークアクセス保護」タブを開いて、「ネットワークアクセス保護設定」の項目から「このスコープに対して有効にする」を選択し「既定のネットワークアクセス保護プロファイル」を選択して「OK」をクリックして画面を閉じます。</p>	
<p>スコープオプションに「既定のネットワークアクセス保護クラス」を追加します。「スコープオプション」を右クリックして「オプションの構成」をクリックします。</p> <p>「スコープオプション」の画面が表示されたら「詳細設定」タブを開いて「ユーザークラス」で「既定のネットワークアクセス保護クラス」を選択します。「006 DNS サーバー」にチェックを入れ、データ入力の欄にドメインコントローラ(DNS)の IP アドレスを入力します。</p>	
<p>「015 DNS ドメイン名」にチェックを入れて、データ入力の欄に文字列として「restricted.win2008.local」を入力します。</p>	
<p>入力が完了したら、「OK」をクリックして画面を閉じます。</p>	

これで、DHCP サーバーの設定は完了です。

ネットワークポリシーサーバーの設定

NAP を提供するためのポリシーサーバーを構成します。

まずはウィザードを利用して必要なポリシーを作成し、その後、セキュリティ正常性検証ツールを設定します。

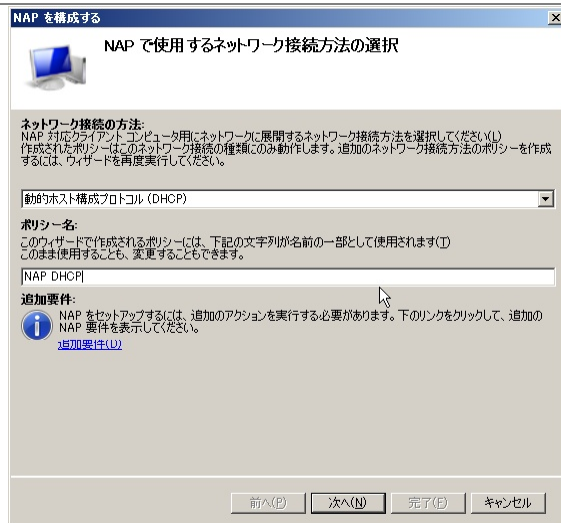
AD への登録

スタートをクリックして「管理ツール」-「ネットワークポリシーサーバー」をクリックします。「NPS(ローカル)」を右クリックし、「Active Directory にサーバーを登録」をクリックします。

NAP 構成ウィザード

スタートをクリックして「管理ツール」-「ネットワークポリシーサーバー」をクリックします。「ネットワークポリシーサーバー」のコンソールが開いたら「NAP(ローカル)」をクリックします。右ペインで「ネットワークアクセス保護(NAP)」を選択し、「NAP を構成する」をクリックしウィザードを起動します

「NAP で使用するネットワーク接続方法の選択」ページが開いたら、「ネットワーク接続の方法」でプルダウンから「動的ホスト構成プロトコル(DHCP)」を選択します。「ポリシー名」には自動的に「NAP DHCP」が入ります。「次へ」をクリックします。

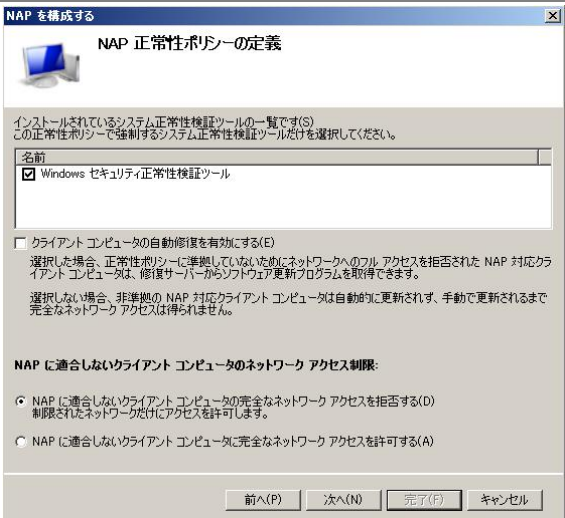



「DHCP サーバーサービスを実行する NAP 強制サーバーの指定」ページでは特に何も設定せず、「次へ」をクリックします。

「DHCP スコープの指定」ページでは、今回特に設定を行わないので、「次へ」をクリックします。

「ユーザーグループとコンピュータグループの構成」ページでも、今回特に設定を行わないので、「次へ」をクリックします。

「NAP 修復サーバーグループおよび URL の指定」ページでも今回特に設定を行わないので、「次へ」をクリックします。

<p>「NAP 正常性ポリシーの定義」ページではデフォルト設定を確認します。テストのために「クライアントコンピュータの自動修復を有効にする」のチェックをはずします。</p>	
<p>「NAP 強制ポリシーおよび RADIUS クライアント構成の完了」ページで「完了」をクリックして、ウィザードを終了します。</p>	

ウィザードが完了し、6 つのポリシーが作成されました。

正常性ポリシー

- NAP DHCP 準拠
- NAP DHCP 非準拠

接続要求ポリシー

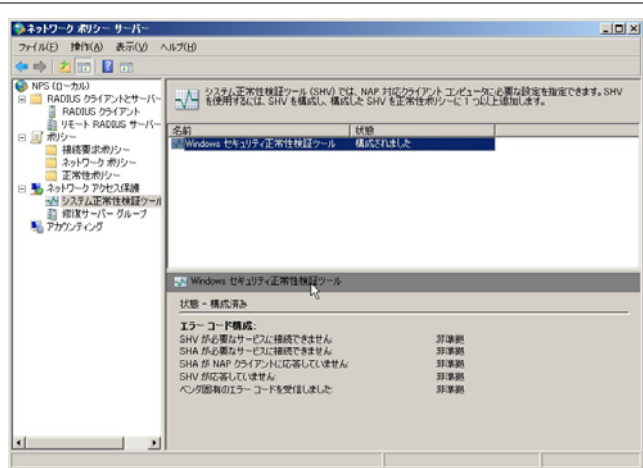
- NAP DHCP

ネットワークポリシー

- NAP DHCP 準拠
- NAP DHCP 非準拠
- NAP DHCP 未対応

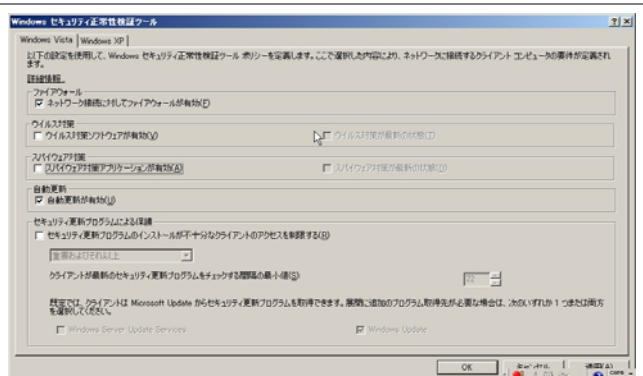
セキュリティ正常性検証ツールの設定

「ネットワークポリシーサーバー」のコンソールで「NAP(ローカル)」を展開し、「ネットワークアクセス保護」-「システム正常性検証ツール」をクリックします。右ペインで「Windows セキュリティ正常性検証ツール」をダブルクリックしてプロパティを表示させます。



「Windows セキュリティ正常性検証ツールのプロパティ」ダイアログが表示されるので「構成」をクリックします。

「Windows セキュリティ正常性検証ツール」ダイアログが表示されるので「Windows Vista」タブで「ファイアウォール」と「自動更新」だけチェックを入れた状態にして「OK」をクリックしてダイアログを閉じます。



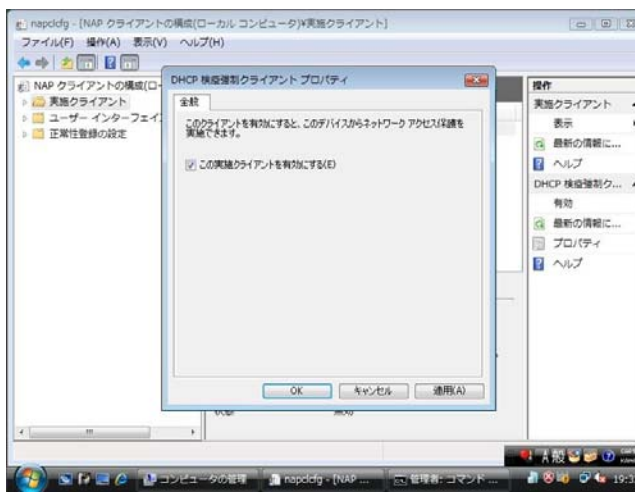
再び「Windows セキュリティ正常性検証ツールのプロパティ」のダイアログに戻るので、「OK」をクリックしてダイアログを閉じます。

「ネットワークポリシーサーバー」のコンソールを終了します。これで、ネットワークポリシーサーバーの設定は完了です。

クライアントの設定

最後にクライアントの設定を行います。

Windows Vista に管理権限のあるアカウントでログオンします。

<p>「スタート」-「すべてのプログラム」-「アクセサリ」-「ファイル名を指定して実行」をクリックします。 「NAPCLCFG.MSC」と入力して「OK」をクリックします。</p>	
<p>「NAPCLCFG – NAP クライアントの構成 (ローカルコンピュータ)」コンソールが開きます。「実施クライアント」をクリックし、右ペインに表示される項目のうち「DHCP 検疫強制クライアント」を選択して「プロパティ」を表示します。 「DHCP 検疫強制クライアントプロパティ」ダイアログが表示されたら「この実施クライアントを有効にする」にチェックを入れて、「OK」をクリックしてダイアログを閉じます。</p>	
<p>コンソールを終了します。</p>	

「コンピュータの管理」-「サービス」から「Network Access Protection Agent」のプロパティを表示して「全般」タブで「スタートアップの種類」を「自動」にし、「開始」ボタンをクリックしてサービスを開始させます。

これで一通りの設定が完了しました。

動作確認

本書の手順では、正常性検証ツールの設定として Windows ファイアウォールと自動更新を選択しています。また、自動修復のオプションも有効になっています。

よって、Windows ファイアウォールや自動更新が無効に設定されていると検疫ネットワークとして隔離され、自動修復された後に通常のネットワークに接続されます。

正常な状態では ipconfig の結果は以下のとおりです。

```

C:\Users\Administrator> ipconfig

Windows IP 構成

イーサネット アダプタ ローカル エリア接続:

   接続固有の DNS サフィックス . . . . : win2008.local
   IPv4 アドレス . . . . . : 192.168.28.100
   サブネット マスク . . . . . : 255.255.255.0
   デフォルト ゲートウェイ . . . . . :

Tunnel adapter ローカル エリア接続* 6:

   接続固有の DNS サフィックス . . . . : win2008.local
   リンクローカル IPv6 アドレス . . . . : fe80::5efe:192.168.28.100%10
   デフォルト ゲートウェイ . . . . . :

C:\Users\Administrator>
  
```

Windows ファイアウォールを無効にした場合、ポリシーに合致しないと判断され、検疫ネットワークに隔離されます。

その状態で ipconfig を実行すると、以下のようになります。

```

Microsoft Windows [Version 6.0.6000]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\Administrator> ipconfig

Windows IP 構成

イーサネット アダプタ ローカル エリア接続:

   接続固有の DNS サフィックス . . . . : restricted.win2008.local
   IPv4 アドレス . . . . . : 192.168.28.100
   サブネット マスク . . . . . : 255.255.255.255
   デフォルト ゲートウェイ . . . . . :

Tunnel adapter ローカル エリア接続* 9:

   接続固有の DNS サフィックス . . . . : restricted.win2008.local
   リンクローカル IPv6 アドレス . . . . : fe80::5efe:192.168.28.100%18
   デフォルト ゲートウェイ . . . . . :

C:\Users\Administrator>
  
```

サブネットマスクが 255.255.255.255 となっています。

これにより、自分以外のマシンとはそのままでは通信できない状態です。

この状態では修復サーバーへの静的ルートのみが設定されており、必要に応じてウィルスのパ

ターンファイルを更新したり、Windows Update でパッチを最新にすることができます。

自動修復が有効な状態では、Windows ファイアウォールを無効にただけでは、即時に有効に変更されます。

おわりに

ここまで見てきたように、Network Access Protection(NAP)を利用すると、セキュリティレベルの低いマシンを社内 LAN から分離し、全社的なレベルを維持することができます。

NAP には様々な構成方法がありますが、本書で取り上げた DHCP 構成が最も導入が容易で、入門編とも言える構成です。

ただ、DHCP 構成には限界があるのも事実ですので、他の方式への移行も検討する必要があります。

NAP の場合は他の方式への移行もスムーズに行えるため、「とりあえずは DHCP で、順次 802.1X に」という段階導入も可能です。

そのあたりも実環境への展開時には考慮、検討してください。

平成 20 年 1 月 作成

平成 20 年 2 月 改訂

伊藤忠テクノソリューションズ株式会社

IT エンジニアリング室

プラットフォーム技術部

Windows 技術課

付録 NPS と DHCP の分離構成

ここでは NPS と DHCP を別筐体で運用するための手順を示します。

分離構成と言っても完全には分離できません。認証を行う NPS と DHCP は分離できるのですが、DHCP だけでは NPS に認証要求を渡せません。そこで、DHCP サーバーに NPS をインストールし、RADIUS Proxy として NPS に要求を転送するように設定します。

インストール手順

LH02 が NPS、LH03 が DHCP という環境の場合の手順は以下の通りです。

- LH02 に NPS をインストール
- NAP 構成ウィザードでポリシーを作成
- LH03 に NPS と DHCP をインストール
- DHCP を設定
- LH03 の NPS で転送用の接続要求ポリシーを作成

インストールそのものは同居構成の時と同じです。ただ、LH02 では NPS のみを選択し、LH03 で NPS と DHCP の 2 つを選択するという点だけ注意してください。

NAP 構成ウィザード

ウィザードの中の「DHCP サーバーサービスを実行する NAP 強制サーバーの指定」ページで RADIUS クライアントとして LH03 を定義します。



DHCP サーバーの IP アドレスと共有シークレットを入力します。

作成された RADIUS クライアントのプロパティを開き、「RADIUS クライアントが NAP に対応している」をチェックします。

DHCP サーバーの設定

DHCP サーバーの設定は同居構成と全く同じです。

RADIUS Proxy の設定

LH03 の NPS の設定で LH02 へ要求を転送するための設定を行います。

「リモート RADIUS サーバグループ」を新規に作成します。

IP アドレスを適切に入力します。

RADIUS サーバーの追加

アドレス | 認証/アカウント | 負荷分散 |

追加する RADIUS サーバーの名前または IP アドレスを入力してください。

サーバー(S):
192.168.28.2

確認(V)...

OK キャンセル 適用(A)

「認証/アカウント」タブにて NAP 構成ウィザードを実行した際に入力したのと同じ共有シークレットを入力します。

RADIUS サーバーの追加

アドレス | 認証/アカウント | 負荷分散 |

認証ポート(U): 1812

共有シークレット(S): *****

共有シークレットの確認入力(C): *****

要求はメッセージ認証機能を含んでいる必要がある(R)

アカウント

アカウントポート(T): 1813

認証とアカウントが同じ共有シークレットを使用する(E)

共有シークレット(H):

共有シークレットの確認入力(O):

ネットワーク アクセス サーバーの開始と停止の通知をこのサーバーに転送する(F)

OK キャンセル 適用(A)

「接続要求ポリシー」を新規に作成します。

新しい接続要求ポリシー

接続要求ポリシー名と接続の種類を指定

接続要求ポリシーの名前およびポリシーに適用する接続の種類を指定できます。

ポリシー名(A):
Prod

ネットワーク接続の方法
NPS に接続要求を送信するネットワーク アクセス サーバーの種類を選択してください。ネットワーク アクセス サーバーの種類を選択するか、[ベンド固有]を指定することができます。

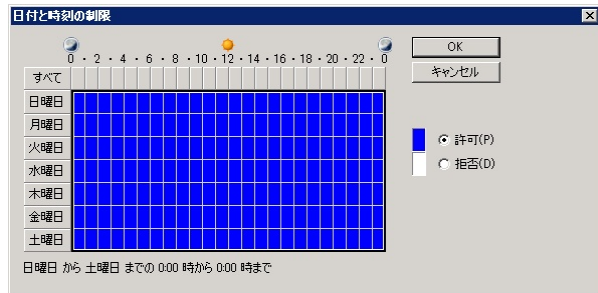
ネットワーク アクセス サーバーの種類(S):
Unspecified

ベンド固有(V):

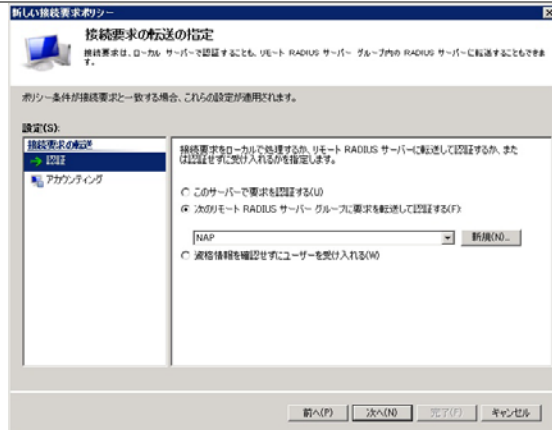
前へ(B) 次へ(N) 完了(F) キャンセル

すべての要求を転送するだけなので、ネットワークアクセスサーバーの種類は指定する必要がありません。

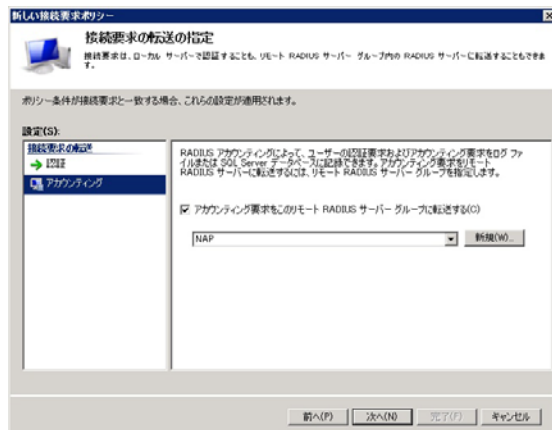
条件としてすべての時間に接続を許可するように設定します。



「認証」の設定画面で、「次のリモート RADIUS サーバグループに要求を転送して認証する」を選択し、先ほど作成したグループが自動的に選択されていることを確認します。



必要に応じて、アカウントिंग要求に関しても転送するならば同様に設定します。



これで分離構成での設定は完了です。
同居構成と同様の動作確認を行ってください。

CTC

Challenging Tomorrow's Changes