Health Enforcement and Remediation

Updated: February 29, 2012

Applies To: Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Vista

All NAP enforcement methods enable you to monitor and report the health status of NAP client computers and choose the level of network access that will be granted to them. Depending on the type of health policies that you have deployed on your network, you can also automatically update noncompliant computers so that they meet requirements.

For more information about when the health of NAP client computers will be evaluated, how the access of client computers might be restricted, and how the health state of client computers can be remediated, see the following sections in this topic:

Note

When you restrict the network access of noncompliant computers you are not denying access to the network; rather, you are granting a level of access that is different from that the access given to compliant computers. The degree of access restriction applied to noncompliant computers is up to you.

Health checks

One of the benefits of NAP is that the health of client computers is continuously monitored. Each SHA installed on a NAP client computer is responsible for providing the current health status of the software or settings that it is monitoring. If the status of the client computer does not change, then no update is required unless the computer's access has expired or unless a device on the network specifically requests the computer to provide its current health status. The following circumstances can prompt a NAP client computer to report its current health state:

- **Service start**: The client computer will provide its health status when the NAP Agent service is started or restarted.
- **Access renewal**: All network access technologies used by NAP can require that the client computer periodically renews its access to the network.
    - With IPsec enforcement, a NAP client will attempt to renew its health certificate 15 minutes before the expiration of the current certificate.
    - With 802.1X enforcement, networks that are configured for periodic 802.1X reauthentication will cause NAP clients to provide updated health status and renew their access.
    - With VPN enforcement, a NAP client will provide its health status when it initiates a VPN session.

    - With DHCP enforcement, NAP clients will provide their health status during DHCP lease renewal. The client will attempt to renew its DHCP lease when half of the time in the current lease has elapsed.

- **SoH expiration**: Some SHVs also allow you to configure a validity period for the client SoH. If the client does not provide an updated health status prior to the expiration of the SoH, it will be considered noncompliant. The client will undergo a health check in the process of renewing its SoH.

- **Configuration change**: When its configuration changes, a NAP client computer might attempt to renew its access to the network. It will always attempt to renew access if the configuration that changed is monitored by NAP client components. If a NAP client computer is using the IPsec enforcement method, it will also attempt to renew access if it receives a Group Policy update.

Access restriction

The following three NAP enforcement settings are used in a network policy to specify the access level of NAP client computers:

- **Allow full network access**. NAP client computers that match a policy with this enforcement setting do not have their network access restricted. Use this setting for compliant NAP clients. Noncompliant computers also use this setting when you deploy NAP in reporting mode. When you use this NAP enforcement setting, users will not receive NAP notifications.

- **Allow full network access for a limited time**. NAP client computers that match a policy with this enforcement setting will be granted full network access until the specified date and time. Their access will then be restricted. Use this setting for noncompliant computers when you deploy NAP in deferred enforcement mode. When you use this enforcement setting, users will receive NAP notifications.

- **Allow limited access**. NAP client computers that match a policy with this enforcement setting will be granted a restricted level of network access. Use this setting for noncompliant computers when you deploy NAP in full enforcement mode. When you use this enforcement setting, users will receive NAP notifications.

The way in which access is granted or restricted depends on the enforcement method that is used and the way that network polices are configured. Some enforcement methods apply default settings to NAP client computers when they are granted a restricted level of access. Other enforcement methods require that you specify the type of access that is granted to noncompliant computers.

Access restriction with IPsec enforcement

NAP with IPsec enforcement does not grant or deny access at the network access level. Instead, access is controlled on a peer-to-peer basis. IPsec negotiation occurs when a NAP client that has IPsec policies applied attempts to communicate with other computers. In order for the communication to be successful, both computers must be able to communicate using IPsec and meet the authentication requirements of the IPsec policies. For NAP, IPsec policies are configured to require that computers have a health certificate before they are allowed to initiate communication with other computers on the IPsec secure logical network.

The acquisition and deletion of health certificates is managed by the IPsec enforcement client on a NAP client computer. When a client is noncompliant, its health certificate will be deleted and it will be unable to initiate communication with compliant client computers. Noncompliant computers can still initiate communication with computers on the IPsec logical boundary network because the IPsec policy on boundary computers requests, but does not require, a health certificate for incoming communications.

Certificate requirements can differ slightly based on the operating system of the NAP client, the type of IPsec rules applied, and the way in which policies and other settings are configured. In all cases, communication is allowed to proceed if computers meet the requirements of the IPsec policies. The following two interfaces are available to configure IPsec policies:

- **IP Security Policy Management**. Use the IP Security Policy Management snap-in to create IPsec policies for computers running Windows XP or Windows Server 2003. These policies can also be applied to computers running Windows Vista, Windows 7, Windows Server 2008, or Windows Server 2008 R2. However, to take advantage of new security algorithms and other new features in Windows Vista, Windows 7, Windows Server 2008, and Windows Server 2008 R2, use the Windows Firewall with Advanced Security snap-in. Rules that you create using the IP Security Policy Management snap-in are called IP security policies.

- **Windows Firewall with Advanced Security**. Use the Windows Firewall with Advanced Security snap-in to create IPsec policies for computers running Windows Vista, Windows 7, Windows Server 2008, and Windows Server 2008 R2. These policies cannot be applied to computers running earlier versions of the Windows operating system. Rules that you create using the Windows Firewall with Advanced Security snap-in are called connection security rules.

When you deploy both types of IPsec policy settings on a network, you must configure each with the same protocol and authentication requirements to ensure that communication is enabled between computers with different policies applied. For NAP, settings are used to require client computers to authenticate with a certificate. When you configure certificate-based authentication, connection security rules have the option to accept health certificates only. This **Accept only health certificates** option is not available with IP security policies. You can use the following registry setting on computers running Windows XP SP3 or Windows Server 2003 to cause health certificates to be preferred when multiple certificates are available for IPsec certificate-based authentication.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PolicyAgent\Oakley\IKEFlags

This IKEFlags registry entry is a REG_DWORD type. You must manually create this entry if it does not already exist. To enable NAP functionality, set the value to 0x1c. To use this setting on a computer running Windows Server 2003 or Windows XP SP2 that has been issued a NAP exemption certificate, you must also install an update to IPsec. For more information, see article 914841 (http://go.microsoft.com/fwlink/?LinkID=69286). This update is included in Windows XP SP3.

Note

Computers running Windows Server 2003 or Windows XP SP2 are not NAP-capable. In order for these computers to communicate on an IPsec NAP-enabled network, they must be issued NAP exemption certificates and have IPsec policies applied.

When the IKEFlags registry setting is configured to 0x1c, computers will prefer health certificates, but can also use a computer certificate with the client authentication enhanced key usage (EKU) if no other certificate is available. The certificate must still meet root CA requirements specified in the IP security policy.

The following table provides a summary of communication results between NAP client computers, with exceptions noted for different operating systems. It is assumed that connection security rules are applied to computers running nextref_vista and IP security policies are applied to computers running Windows XP SP3. The Accept only health certificates option has been selected in the connection security rules and computers running Windows XP SP3 have the IKEFlags registry entry set to 0x1c. Behavior is displayed for source and destination computers that have a health certificate, a computer certificate, no certificate, or both types of certificates.

Source	Destination	Result
Health	Health	Allowed
Computer	Health	Denied[A]
None	Health	Denied
Both	Health	Allowed
Health	Computer	Allowed[B]
Computer	Computer	Denied[C]
None	Computer	Denied
Both	Computer	Allowed[B]
Health	None	Denied
Computer	None	Denied
None	None	Denied
Both	None	Denied
Health	Both	Allowed
Computer	Both	Denied
None	Both	Denied
Both	Both	Allowed

A Allowed if both source and destination are running Windows XP SP3.

B Denied if source is running Windows Vista with no service packs installed or Windows XP SP3.

C Allowed if destination is running Windows XP SP3.

Health certificates must have a system health authentication EKU and a client authentication EKU. Computer certificates must have a client authentication EKU and might have other EKUs, such as server authentication. To prevent the use of computer certificates for authentication in some cases, use a different root CA for your health certificate PKI and deny enroll permissions for other types of certificates.

Known issue with clients running Windows XP SP3

The behavior of IPsec NAP clients running Windows XP SP3 is currently under investigation. Links to configuration instructions and updates, if necessary, will be provided in a future release of this guide.

Access restriction with 802.1X enforcement

When you deploy NAP with 802.1X enforcement, network restriction occurs at the point of network access. This is typically an 802.1X authenticating switch or wireless access point. Network access of compliant and noncompliant computers is specified by configuring network policies with RADIUS attributes that are passed to the access device and applied to the client connection. These attributes can tell the device to place the client on a specified VLAN, to enforce an ACL, or both. When a NAP client computer matches a network policy, it will have the RADIUS attributes present in that policy applied to the connection. If you specify, computers that meet health requirements will be placed on a VLAN different from the VLAN used for computers that do not meet requirements. Because the 802.1X enforcement method uses RADIUS attributes from network policy to determine properties of the client connection, access is restricted only if these attributes provide the client with an access profile that does not allow full access to the network. NAP settings for 802.1X enforcement do not automatically provide a restricted access profile.

Note

To use the 802.1X enforcement method with reporting mode, use the same RADIUS attributes in compliant and noncompliant network policies. To deploy deferred enforcement mode, include the policy expiration condition in noncompliant network policy and create a second noncompliant network policy with no expiration that will be used when the first policy expires.

Access restriction with VPN enforcement

NAP with VPN enforcement restricts client access at the point of access, in this case, the VPN server. Access is restricted if the client is determined to be noncompliant when it initiates a VPN session or if it becomes noncompliant during a session. If the computer is able to remediate its health and meet requirements, full access is restored without the user having to initiate another VPN session.

Access restriction for NAP clients using the VPN enforcement method occurs through the application of IP filters to the VPN connection. These filters are created automatically to allow access to all addresses configured in remediation servers groups. You can also specify access for both compliant and noncompliant VPN clients by configuring IP filters in your compliant and noncompliant network policies, respectively. You must configure a remediation server group with at least one member or configure IP filters in order for noncompliant NAP clients to have restricted access.

Access restriction with DHCP enforcement

NAP with DHCP enforcement restricts client access by controlling the IPv4 address configuration and routing table entries of the client computer. When a DHCP NAP client is compliant, it is granted an IPv4 address configuration using scope options configured in the default user class. If a client becomes noncompliant, it will renew its IP address lease and obtain a restricted configuration using options configured in the default NAP class.

If you have configured the 003 router option in the default NAP class, this will not be provided to the client computer except as a next hop address for the DHCP server or remediation servers if they are located on a different subnet. A noncompliant client will also be issued a classless subnet mask (255.255.255.255) that restricts access to only those addresses found in the routing table. If you have configured remediation servers, the noncompliant client will be provided

with static host routes to these IP addresses. After a noncompliant client has successfully remediated its health state, it will renew its DHCP address and be provided with an IPv4 address configuration that grants full network access.

Remediation

When a NAP client computer is not compliant with health requirements, it can be remediated. The way in which it is remediated depends on the following:

- The type of health credential that is noncompliant with health requirements. If the client computer is noncompliant because of a setting that can be changed without user intervention, or because it does not have a software update that can be downloaded and installed automatically, then the computer might be updated without user intervention. Health requirements that cannot be automatically remediated require manual remediation by the user. If you configure a troubleshooting URL, the NAP notification will contain instructions the user can follow to remediate the health of the computer.
- The remediation services available. In order for remediation to be successful, a noncompliant NAP client computer must have access to services that are allowed to update the computer. For example, you might want to provide a noncompliant NAP client with access to AD DS, DNS, DHCP, and Windows Update or WSUS.
- Whether automatic remediation is enabled. If you do not enable automatic remediation in noncompliant network policy, noncompliant NAP client computers will require manual remediation.

When a NAP client computer has successfully remediated its health state either automatically or through user intervention, it will send a new access request to a NAP enforcement point. If the computer is compliant with current policy conditions, it will be granted full network access.

Community Additions