Questions from PWG IDS participants on Microsoft NAP Architecture and Implementation
---

Q1: The NAP architecture document states that "A NAP client is a computer running Windows Vista, Windows Server 2008, or Windows XP with Service Pack 3..."

Does this mean that Microsoft will not support non-Windows-based NAP clients?

[MS-NAP] No – it means that those operating systems have native, out-of-the-box support for NAP. There are 3rd party NAP clients for Linux, Mac, etc.

Q2: When a NAP client is asked to send it's health information to the NAP servers for assessment, can the NAP client "lie" about this information? If clients cannot "lie" about it's health, how can the servers tell that clients aren't telling the truth about their health info?

[MS-NAP] A client can lie about its health state, but it is not a trivial matter to achieve this for a locked-down machine and will be increasingly difficult to do in the future.

Q3: I didn't see a specific document section that describes how a 3rd party (non-Microsoft) might code a System Health Validator plugin for NAP. In detail, I would like to know how a 3rd party SHV gets "triggered". Meaning, when a NAP server receives a statement of health from a NON-windows device, how does it know to pass the statement of health off to a plugin SHV? I would like to know the algorithm that NAP uses to examine a statement of health to determine whether or not to handle it with Microsoft standard SHVs, or pass it off to a particular SHV plugin.

[MS-NAP] There are many details relating to these subjects on MSDN, Technet, etc.

A SHV is triggered on NPS by the NAP Server. Specifically, the NAP Server knows the identity of the destination SHV based a GUID that is present in the SOH (the SOH was generated by the client SHA). Normally, SHAs and SHVs are matching, but it is possible for a given SHV to terminate MS-SOH protocol from multiple SHAs that produce the same SOH.

Q4: It's my understanding that there is a new security model for the "Device Profile for Web Services" (DPWS) and that this service supports digitally signing web service messages.

There are also certificates used in NAP.

There are also machine certificates, and user certificates, managed by a Windows Server certificate authority.

Do each of these subsystems all use the WIndows Server 2008 PKI? Or are there separate CAs for each application domain (NAP, DPWS, and WS-2008 CA)?

[MS-NAP] I'm not familiar with DPWS, but NAP optionally uses certificates in various scenarios. For example, when IPSec-NAP is deployed, the NAP HRA issues an x.509 certificate (a "NAP Health Certificate") that represents proof that a client has passed a NAP health evaluation. IPSec optionally consumes the NAP health certificate as a means of isolating non-NAP-policy-compliant machines from compliant machines.

NAP can also use x.509 certificates for authentication. For example, PEAP uses a certificate with TLS to secure EAP between a network client and the NAP server and EAP-TLS uses x.509 certificates on both client and server sides for authentication.

CA selection depends entirely on the scenario. If, for example, a customer is concerned about NAP health compliance and reporting, but *not* enforcement – an entirely separate PKI can be used (the value is in the *possession* of the health cert and what that means, not with the use of the cert).

However, if enforcement (or authentication) is desired, most customers will opt to use a shared PKI infrastructure.

Most customers will use a Windows CA.

Q5:
Which of the defined transport(s) are required to be supported in order to guarantee a device can attach to the network? MS defines DHCP, 802.1x, IPSec, and VPN and has extended each to add SOH information. So, in an environment where we are attaching wirelessly via 802.1x and receive our IP address from DHCP, what happens if we only support SOH over DHCP (or 802.1x)? Will we attach or fail?

I think the answer is that unless we are enrolled in their health certificate solution (MS-HCEP), we'll need to re-assess. However, this is something we need to clarify with MS.

[MS-NAP] The answer to this question _entirely_ depends on the needs of the customer and the deployment they choose.

Note that customers can choose to deploy one, a subset or all of the different transport mechanisms (we call the "enforcement clients", though enforcement may not be required or desired by the customer).

For example: a customer could choose to do the following:

Deploy

802.1x NAP (L2 access control)

+

DHCP NAP (upper L2/lower L3 access control)

+

IPSec NAP (L3 access control)

+

VPN and TSG NAP (remote access control)

etc. etc

The different layers can do enforcement, deferred enforcement or simply reporting, they can do auto-remediation (or no remediation), etc, etc.

Q6
Is the remediation step required to use NAP or can it be outside NAP?

[MS-NAP] Remediation is entirely a function of SHA/SHVs or the agents they represent. The NAP infrastructure directs the SHA/SHVs to remediate (and when), given that remediation is desired by the customer.

An example:

Support there's an AV SHA/SHV. The SHA reports that the AV signatures are X. The SHV evaluates X against current required AV signature and finds the current signature version is X+1. The SHV informs the client that is quarantined and optionally instructs the access gear/server to isolate the client. The SHA interprets the quarantine response from the SHV (called an SOHR) and "fixes" the deficiencies. For example, the AV SHA might "kick" the AV client that is installed on the client and cause it to download the latest AV signature file. Once the AV signature file is updated, the SHA will "kick" the NAP agent on the client to trigger another health check. This time, the AV signature will be up-to-date and the SHV will evaluate the client as "healthy"/"Compliant" and grant access.

Another example: the compliance issue might be that "firewall is turned off". The SHA remediation activity might be "turn AV on".

Q7
Would MS be willing to provide a class plug-in to assess imaging devices if the manufacturers committed to supporting NAP?

[MS-NAP] Microsoft would be interested in having a discussion on this subject.

Q8
Would MS be willing to host a "NAP Plugfest" for imaging (and other) devices?

[MS-NAP] Possibly - We can certainly discuss the subject.

Q9
The attributes being assessed consists of configuration settings and code levels. It seems the remediation steps would involve updating code levels and configuration settings. Both remedies could be standardized to use some corporate policy statement. How might this be handled?

[MS-NAP] The model expressed in this doc suggests multiple SHA implementations (one per device or maybe manufacturer) and a single server-side SHV. For this to work, there would need to be an agreement as to the semantics of the checks being discussed in the SOH/SOHR.

We would need to discuss the logistics of sharing those semantics – whether as a formal standard, "market" standard or some other mechanism.

Q10
Is a remediation plug-in allowed to operate in a "pass-thru" mode where it initiates remediation via some external mechanism?

[MS-NAP] Sure – But there are some constraints to this that impact usability of the scenario.

Q11
The MS-Machine-Inventory Packet only defines Microsoft OSes and x86 architecture. We need additional platform definitions. How should we proceed?

[MS-NAP] Need to look into this.

Q12
The MS-Quarantine-State Packet, that is required for SSoH, contains a URL. What is the purpose of the URL?

[MS-NAP] The URL is used to direct users to more information about the quarantine state. For example, users in quarantine can click a link in the Windows UX that takes them to a customer website that explains more about the reason for quarantine and how to address the issue.

Q13
It seems like the purpose of the MS-Packet-Info Packet is to differentiate between version 1 and 2. Is this correct?

[MS-NAP] Need to follow up on these.

Q14
The MS-SystemGenerated-Ids Packet is optional. However, it looks like if the SOH contains vendor extensions that this becomes a required packet. Is this attribute used to route the SOH to various assessment applications?

[MS-NAP] Need to follow up on these.

Q15
The MS-Machine-Inventory-Ex Packet defines client, server, and domain controller. Are there plans to expand this list? What should a print service use?

[MS-NAP] Need to follow up on these.

Q16 Section 2.2.8 SSoH specifies *MS-Machine-Inventory-Ex as optional. However, section 2.2.4.8 MS-Machine-Inventory-Ex Packet states the attribute MUST be present in the SSoH and MAY be present in the SSoHR. So, is it optional or required?

[MS-NAP] Need to follow up on these.