Introduction to Network Access Protection (Part 1)

One aspect of network security that annoys many administrators is the inability to control the configuration of remote computers. Although a company's network may be working safely, there is nothing to prevent remote users from accessing the network through a computer that has been infected or not.

One aspect of network security that annoys many administrators is the inability to control the configuration of remote computers. Although a company's network may be working safely, there is nothing to prevent remote users from accessing the network via a computer that has been infected with a virus or has holes that have not been patched. timely. In this article, we will introduce you to network access protection in Longhorn Server and how it works.

As an administrator, one thing that really frustrates me is that there is too little control over remote users. The organization's business needs allow remote users to connect to the company's network from different locations outside the office. The problem arises here is that, although I have used many methods to check the network for the company, I still cannot control all the computers that connect remotely to the network.

The frustrating reason here is that I cannot know the status of the remote computers being accessed. In some cases, remote users use an infected computer to connect to the network or use an old version operating system. Although I have step by step protected the corporate network, I am afraid for remote users who do not have adequate security to harm other file systems on the network due to the virus, or may accidentally let reveal information because their computers are infected with Trojans.

A few years ago there was a glimmer of hope when Microsoft was about to release Windows Server 2003 R2, including a new feature called Network Access Protection. However, due to irrelevance, this network access protection feature was removed before launching R2 version.

Microsoft has also spent a lot of effort to study this feature after that time so that this protection feature will be one of the main security features in Longhorn Server. Although Longhorn's Network Access Protection version is easier to configure than in Windows Server 2003, it still has a bit of complexity. Therefore, the purpose of this article is mainly to give you a little introduction to Network Access Protection and how it works before Longhorn Server is released.

Before start

Before I start, there is one thing I want to make clear when I am interested in the Network Access Protection (NAP) feature. The purpose of this feature is to ensure that remote users' computers comply with the security requirements in your organization. NAP will do nothing to prevent unauthorized access to the network. If an intruder has a computer that meets the company's security policies, NAP will not perform inactivity to stop this person's access. Preventing this person's access is the work of other security techniques. NAP is simply designed to prevent users from logging on to the network when using unsecured computers.

Another thing to mention before starting another NAP with Network Access Quarantine Control is in Windows Server 2003. The functionality that is included with this Windows Server 2003 provides check. Control limited protection policies for remote computers but completely inferior to NAP.

Basic foundation of NAP

NAP is designed to increase corporate VPN. The design process begins when clients establish a VPN session with Longhorn Server using remote access and routing services. After the user establishes the connection, the server with the network policy will check the validity of the 'health' or the security of the remote system. This is done by comparing the configuration of the remote computer to the network access policy defined by the administrator. So what happens is entirely dependent on the policy that the administrator set up.

Administrators will have the option of configuring a policy for only checking or quarantining. If a test policy is in effect, any user with a valid set of necessary permissions can access network resources regardless of the computer that complies with the security policy. confidentiality of the company or not.

In my view, a test-only policy is best suited for creating transitions for the NAP environment. If you have some remote users who need access to resources in the network to do their jobs, you may not want to enable NAP initially in quarantine mode. If you do that, then no computer will be able to access the corporate network. Instead, you will initially configure NAP to use a check-only policy. This allows you to assess the impact of network access policies without having to prevent anyone from doing their job. When all the nodes have been checked well, you can switch the policy to isolation mode.

As expected, isolation mode works by locating remote computers that do not comply with the company's security policies and will be isolated from network resources. But eventually, the administrator must also control what this non-compliant computer can access. Typically, an administrator will give computers the right to access a quarantined network segment (this issue will be discussed later) and restrict access to certain important resources or prevent it. Access to all network resources.

Perhaps you are wondering what are the advantages to agreeing on computers that do not comply with this administrator's policy to access the quarantined network. When a non-compliant computer is attached to the network and NAP is operating in quarantine mode, the non-compliant computer will be isolated from the large network. Typically, this isolation is extended throughout the user's connection period. Simply isolating a non-compliant machine can help prevent intrusions caused by viruses or security holes on your network, but it is not entirely good for remote users because of those who This user cannot connect to network resources and is therefore unable to do their job.

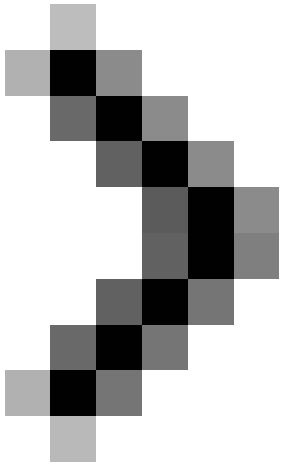
And when this problem occurs, the network segment becomes important. An administrator can safely put upgraded resources into quarantine sections. Safe upgrade resources are protected servers that make non-compliant remote access computers compliant. They can install security patches or virus software updates.

One thing to note here is that NAP does not have any techniques to verify the safety of the remote computer or apply updates to the remote computer. This problem is the work of System Health Agents and System Health Validators. There is information that these components will be integrated into the next version of SMS Server.

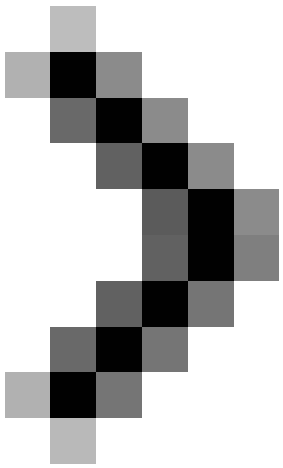
Conclude

In this article, I have introduced you to Longhorn Server's NAP feature. In Part 2 of this series, I will continue

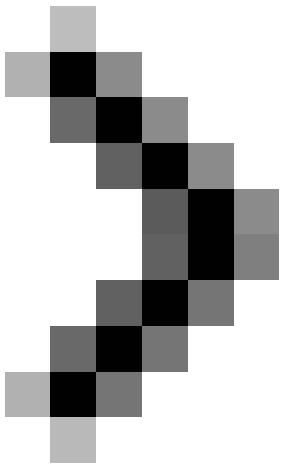
the discussion by showing you how to configure it.



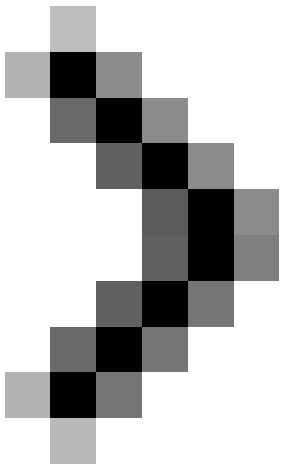
Introduction to Network Access Protection (Part 2)



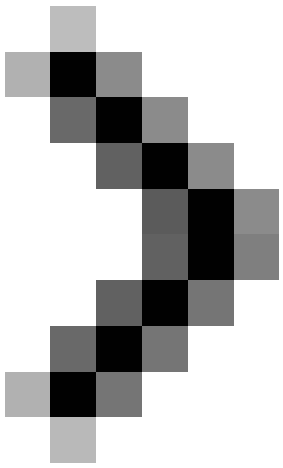
Introduction to Network Access Protection (Part 3)



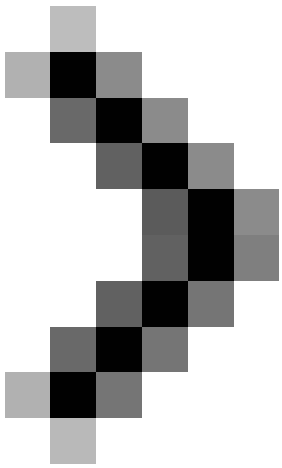
Introduction to Network Access Protection (Part 4)



Introduction to Network Access Protection (Part 5)



Introduction to Network Access Protection (Part 6)



Introduction to Network Access Protection (Part 7)

You finished reading the article "**Introduction to Network Access Protection (Part 1)**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.