

Change the IP Address and HostName on a VMS Server

Document ID: 64074

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Changes Based on the Running Application

- Common Services
- PIX MC
- AutoUpdate Server
- Router MC
- Monitor Center for Performances
- IDS MC
- Security Monitor
- CSA MC
- Change the Hostname on Windows 2000
- Change the IP address on Windows 2000

Verify

Troubleshoot

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document explains how to change the IP address and, if needed, the hostname on a server running CiscoWorks VPN/Security Management Solution (VMS). This document is combined with a zip files containing a script and other utilities that help the execution and the modification of the files that you need to change.

Note: This was not tested with Common Services 2.3.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- PIX MC
- AUS
- Router MC
- Monitor Center for Performances
- IDS MC

- Security Monitor
- CSA MC

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Changes Based on the Running Application

Common Services

The files installed with Common Services are not tied to the name or IP address of the server. Extra changes are not required for changing the IP address and hostname on a Windows machine for a server running only Common Services.

PIX MC

The files installed with Common Services are not tied to the name or IP address of the server. Extra changes are not required for changing the IP address and hostname on a Windows machine for a server running only Common Services.

If you want to perform this operation and keep managing the same PIX firewalls, remember to rebootstrap the devices. Update the IP addresses that they have to allow for HTTP connection; this includes adding the new IP address and removing the old address.

You can change the device by adding the PIX configuration:

```
#http new_ip_address [netmask] [if_name]
#no http old_ip_address [netmask] [if_name]
#write memory
```

AutoUpdate Server

The files installed with Common Services are not tied to the name or IP address of the server. Extra changes are not required for changing the IP address and hostname on a Windows machine for a server running only Common Services.

If the AUS server has changed the IP address, remember to update the address in the PIX MC. You can update the address using the PIX MC and deploying direct to the device, or via command line. In both cases, if the device has already been deployed to AUS, remember to also redeploy the new configuration to the AUSs server; otherwise, after the first time the device calls home, the old IP address for the server remains in the configuration.

Router MC

The files installed with Common Services are not tied to the name or IP address of the server. Extra changes are not required for changing the IP address and hostname on a Windows machine for a server running only Common Services.

You do not need to update or re-bootstrap the devices.

Monitor Center for Performances

The files installed with Common Services are not tied to the name or IP address of the server. Extra changes are not required for changing the IP address and hostname on a Windows machine for a server running only Common Services.

the devices should be rebootstrapped accordingly for these reasons:

- devices are configured to send messages to the server, or
- devices are configured to allow the server to poll information connecting to the device

IDS MC

After performing the change for Windows (before the server can be functional again), there are few files that need to be changed. Complete these steps to change the files:

1. Stop the daemon manager.
2. Modify the `CSCOPx\MDC\etc\ids\xml\SystemConfig.xml` file.
3. Change value to the new value (if the change of IP address is needed).
4. Change value to the new value (if the change of hostname is needed). Note, there are two fields with hostname in the file; change only that one that has the IP address, and not the field that contains the localhost string.
5. Copy this file to
`CSCOPx\MDC\Tomcat\vms\ids-config\web-inf\classes\con\Cisco\nm\mdc\ids\com`
6. Restart the daemon manager

If there are sensors in the system, you need to modify each one.

From the GUI, choose **Configuration > Settings > Communications > remote hosts page**. Edit the IP address to change the old with the new one.

Security Monitor

After performing the change for Windows (before the server can be functional again), there are few files that need to be changed. Complete these steps to change the files:

1. Stop the daemon manager.
2. Modify the `CSCOPx\MDC\etc\ids\xml\SystemConfig.xml` file.
3. Change value to the new value (if the change of IP address is needed).
4. Change value to the new value (if the change of hostname is needed).
5. Copy this file to
`CSCOPx\MDC\Tomcat\vms\ids-monitor\web-inf\classes\con\Cisco\nm\mdc\ids\com`
6. Change the IP address for the hostname given in input.
7. If needed, change the hostname in the routing table.
8. Restart the daemon manager

From the GUI, choose **Configuration > Settings > Communications > remote hosts page**. Edit the IP address to change the old with the new one.

CSA MC

For CSA MC, the main problem is the certificate that is used for the communication between the CSA MC and the CSA agent. If you change only the IP address on the server, there is no problem. If you change the name of the server, then you have to regenerate the certificate on the server, and also update the certificate on all the agents. Complete these steps to regenerate the certificate on the server:

To stop the CSA services, issue these commands from a command prompt:

```
net stop csagent
net stop crmdmgt
```

1. Delete these files:

- ◆ In the CSCOPx\CSAMC\cfg directory, delete sslca.crt and sslhost.crt.
- ◆ In the CSCOPx\lib\web\conf directory, delete root.crt, server.key, and server.crt.
- ◆ In the CSCOPx\MDC\Apache\conf\ssl directory, delete chain.cer, root.crt, server.key, and server.cert.

2. Open the CMD window.

3. Enter these commands:

```
cd CSCOPx\CSAMC\Bin
..\..\bin\perl.exe installcert.pl -forceinstall
```

This generates a new certificate in the X:\Program Files\CSCOPx\CSAMC\cfg directory and copies them in the appropriate files in the CMF and core apache.

4. Run the script from the CMD.

```
Run:
net start crmdmgt
net start csagent
To refresh kits, got to CSAMC bin directory and type "webmgr makekits_refresh"
```

You can see the new location of the files.

After generating the new certificate on the CSAMC server, you need to change the certificate on the agent machines. On each server, you need to edit the sysvars.cf file on each agent machine to reflect the new name of the CSA MC. You also need to download the new certificate that is generated into each agent's CFG directory.

Change the Hostname on Windows 2000

Complete these steps:

1. Right-click **My Computer**.
2. Choose **Properties**.
3. Choose the **Network Identification** tab.
4. Click **Properties**.
5. Edit the computer name in the text field.
6. Reboot the computer.

Change the IP address on Windows 2000

Complete these steps:

1. Right-click **My Network Places**.
2. Choose **Properties**.
3. Right-click the LAN connection on which you want to change the IP address.
4. Choose **Properties**.
5. Choose **IP/TCP protocols**.
6. Click **Properties**.
7. Define your network properties, such as IP address, network mask, and gateway.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

Related Information

- [CiscoWorks VPN/Security Management Solution Support Resources](#)
- [Technical Support – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Oct 17, 2008

Document ID: 64074
