

IDS Error Message "Error when attempting to install: /usr/cids/idsRoot/var/updates/IDS-sig.."

Document ID: 64091

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Background Information

Step-by-Step Procedures

- Step 1: Verify the File Name

- Step 2: Verify the Package has been Downloaded

- Step 3: FTP Server Versus HTTP Upgrade

- Step 4: Manual Download using a Service Account

Verify

Troubleshoot

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

Use the procedure in this document if you cannot update the signature level from the network (if it fails). This procedure downloads the update to the Sensor and then upgrades from the local file system.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on the Intrusion Detection System (IDS) 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

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Background Information

An error is sometimes generated when one cannot update the signature level from the network (if it fails). The procedure this document describes in order to help you resolve the error downloads the update to the Sensor and then upgrades from the local file system. A sample of the error you receive can look like this output:

```
Error when attempting to install
/usr/cids/idsRoot/var/updates/IDS-sig-4.1-4-S146.rpm.pkg
```

```
Error when attempting to install
/usr/cids/idsRoot/var/updates/IDS-sig-4.1-4-S146.rpm.pkg
```

Note: Not all the steps in this document are required. However, follow them in the order listed.

Step-by-Step Procedures

Step 1: Verify the File Name

Important: It is important that you do not change the file name upon download.

Step 2: Verify the Package has been Downloaded

One quick way to identify whether the package you have downloaded is truly corrupted is to verify the MD5 hash of the file. This can be done two ways. If you download the file to a UNIX/Linux system, you can type:

```
md5sum <filename>
```

This outputs the hash that you can compare to the hash listed at the IDS signature download site. Since you are installing the updates using the IDS MC, you are probably downloading `IDS-sig-X.X-X-XXXX.zip` from the Cisco IDS Management Center – Version 4.x Signature Updates (registered customers only) software download site.

For example, when you click the filename **IDS-sig-4.1-4-S146.zip** to download, you see a field on the next page called 'MD5'. This is an example:

```
80cfe7f34eaedcd9f22518b30f4e2b3
```

Use a tool such as WinMD5Sum to verify the M5Sum on Windows. Compare the hash of the file you downloaded to the `80cfe7f34eaedcd9f22518b30f4e2b3` hash. If the hashes are different, then something has happened to the file.

Step 3: FTP Server Versus HTTP Upgrade

Use an alternate FTP server or HTTP to upgrade the IDS signatures if possible. If this is not possible, try a manual download of the file using a service account.

Step 4: Manual Download using a Service Account

Complete these steps in order to perform a manual download using a service account:

1. Create a service account.
2. Perform a manual FTP to IDS.
3. Issue a Secure Copy (SCP).

Step 1: Create a Service Account

You must first create a service account in order to proceed with a manual download. Complete these steps:

1. Log into the Sensor using the "cisco" account:

```
sensor#
```

2. Enter configure terminal mode:

```
sensor#configure terminal
```

3. Create the service account:

```
sensor(config)#username <service_account_user_name> privilege service password cisco
```

Note: You can only configure one service account.

Step 2: Manual FTP to IDS

Complete these steps:

1. Log in using the service account. This output shows an example of the prompt:

```
bash-2.05a$
```

2. Connect to the FTP server.

```
bash-2.05a$ftp <ftp_server_address>
```

3. Setup the FTP client to use a binary mode to get the file.

```
ftp>bi
```

4. Check that the file is in the FTP server.

```
ftp>ls
```

Sample output:

```
* 227 Entering Passive Mode .
```

```
* 125 Data connection already open; Transfer starting.
```

```
* -rwxrwxrwx 1 owner group 13280279 Aug 28 14:44 IDS-K9-min-4.1-1-S47.rpm.pkg
```

```
* -rwxrwxrwx 1 owner group 2061291 Aug 28 14:47 IDS-sig-4.0-2-S47.rpm.pkg
```

```
* -rwxrwxrwx 1 owner group 2120589 Oct 20 18:26 IDS-sig-4.1-1-S53.rpm.pkg
```

```
* -rwxrwxrwx 1 owner group 2124411 Oct 20 19:43 IDS-sig-4.1-1-S54.rpm.pkg
```

```
* -rwxrwxrwx 1 owner group 2125132 Oct 20 20:15 IDS-sig-4.1-1-S55.rpm.pkg
```

```
* -rwxrwxrwx 1 owner group 2127802 Oct 20 20:15 IDS-sig-4.1-1-S56.rpm.pkg
```

```
* -rwxrwxrwx 1 owner group 2143144 Oct 20 20:22 IDS-sig-4.1-1-S57.rpm.pkg
```

```
* 226 Transfer complete.
```

5. Retrieve the file (you can copy and paste the filename from the output in step 4).

```
ftp>get <upgrade_file>
```

6. Close the FTP connection and quit the FTP client.

```
# ftp>close
```

```
# ftp>quit
```

7. Check to see if you can see the file.

```
# bash-2.05a$ls
```

```
# <upgrade_file>
```

8. Log out of the service account.

```
bash-2.05a$exit
```

Step 3: Issue a Secure Copy (SCP)

Complete these steps:

1. Log into the Sensor using the cisco account. This output shows an example of the prompt:

```
sensor#  
2. Enter configure terminal mode.
```

```
sensor#configure terminal  
3. Create the key.
```

```
sensor(config)#ssh host-key <sensor_ip_address>  
4. Type yes to accept the key.  
5. Apply the upgrade.
```

```
# sensor(config)#upgrade scp://  
# User: <service_account_user_name>  
# Server's IP Address: <sensor_ip_address>  
# Port[22]:  
# File name: <upgrade_file>  
# Password: *****  
# Warning: Executing this command will apply a signature update  
to the application partition.  
# Continue with upgrade? : yes
```

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

- [Cisco Intrusion Prevention System](#)
- [Security Product Field Notices \(includes Cisco Secure Intrusion Detection\)](#)
- [Technical Support & Documentation – Cisco Systems](#)

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Jan 19, 2006

Document ID: 64091
