K8217: Managing BIG-IP ASM attack signatures (11.5.x - 14.0.x)

Non-Diagnostic

Original Publication Date: Dec 11, 2018

Update Date: May 4, 2022

Topic

This article applies to BIG-IP ASM 11.5.x through 14.0.x. For information about other versions, refer to the following article:

- K82512024: Managing BIG-IP ASM Live Updates (14.1.x and later)

Description

Contents

Overview

Attack signatures are rules or patterns that identify attack sequences or classes of attacks on a web application and its components. You can apply attack signatures to both requests and responses.

F5 releases a new attack signature update for the BIG-IP ASM system on a regular basis. The attack signature update includes new attack signatures as well as enhancements to existing attack signatures.

Attack signature updates are released only for supported versions of software, as detailed in K5903: BIG-IP software support policy.

Attack signature updates are available from the F5 Downloads site under the version of the BIG-IP system that you are currently running.

Because new web application attacks and threats are constantly being developed, you should update the system-supplied attack signatures on a regular basis to ensure that your applications are protected against new attacks. You can configure automatic updates, or you can manually update the signatures.

The attack signature updates are cumulative; when you update the system-supplied attack signatures, the update provides the latest signatures and all signatures from the previous updates. Updating the attack signatures also provides any revisions to existing attack signatures.

Attack signatures are also saved in user configuration set (UCS) archives. When a UCS archive is created, the current cumulative signature set is saved in the archive. When a UCS archive is restored, the attack signatures in the archive fully replace existing signatures. If the UCS archive is old, the attack signatures may be out-of-date and need to be updated separately.

Note: When signatures are updated in BIG-IP ASM 11.0.0 and later, new signatures are placed in a staging (non-blocking) update and unchanged signatures remain in the configured mode (blocking).

Understanding attack signature updates and BIG-IP device groups

When the **Attack Signatures Update Mode** is set to **Scheduled**, the system automatically updates attack signatures when it detects an update. This action ensures that the attack signature sets are always current with the latest security updates. When you configure the BIG-IP ASM system as part of a BIG-IP device group, you can synchronize the attack signature update settings to the peer device when you enable application security synchronization on the same device group. However, each BIG-IP ASM device in the device group updates independently, based on the configured attack signature scheduled update interval.

When the BIG-IP ASM system is configured with the **Manual Attack Signature Update** option and **Delivery Mode** is set to **Automatic**, you must manually execute the attack signatures update when new updates become available.

When the BIG-IP ASM system is configured with **Update Mode** and **Delivery Mode** both set to **Manual**, to update attack signatures you must download the attack signature update file manually from the F5 Downloads site and then manually upload the attack signature update file to the BIG-IP ASM system to manually update the device.

When a BIG-IP ASM system is configured with **Update Mode** set to **Manual** and the device attack signatures are manually updated, the updated signature sets synchronize to the peer BIG-IP ASM device when synchronizing to the device group.

Note: After you synchronize the attack signature update, the peer device's Configuration utility may still report a signature update is available until the next daily signature check occurs.

To configure **Attack Signatures Update** settings for the BIG-IP ASM device using the Configuration utility, perform the **Configuring automatic updates for system-supplied attack signatures** procedure or the **Configuring manual updates for system-supplied attack signatures** procedure.

Note: The BIG-IP ASM system records details about the most recent update activity, including a Readme file pertaining to the latest update. This information is displayed in the Configuration utility when accessing the **Application Security** page for security updates.

Licensing requirements

For the system to initiate the attack signature update for both **Manual** and **Automatic**, the **Service Check Date** in the BIG-IP ASM system's license must be within 18 months of the system date.

Note: From the TMOS Shell (**tmsh**), you can view the **Service Check Date** by using the **show /sys license detail | grep -i 'Service Check Date'** command.

If the **Service Check Date** is recent enough, the system allows the signature update.

If the **Service Check Date** is too old, the BIG-IP ASM system attempts to contact the license server and downloads a new license.

Note: The following is not applicable to **VMCP** guest instances.

- If the system can reach the license server and the support contract for the system is current:
    - The system downloads a new license and verifies the **Service Check Date**.

      Note: The system does not install the new license, but only examines it for the required date.

    - If the **Service Check Date** is within seven days of the system date (accounting for time zone differences and system clock variance), the system initiates the signature update.
- If the license server cannot be reached or the support contract for the system is not current:
    - The Configuration utility reports an error message that appears similar to the following example and the system logs the message to the **/var/log/asm** file:

      Service contract cannot be verified (500 read timeout at /ts/packages//iControl.pm line 1005). Please re-license your installation of the BIG-IP system manually.

    - You must manually reactivate the system license and re-initiate the attack signature update.

      Important: Log in to the system with the administrator user account to perform the manual licensing procedure. For more information, refer to K9965: The admin user account must be used to license the system.

      Note: If the error persists when you attempt to manually reactivate the license, contact F5 Support for questions about the status of the support contract for the affected system.

Configuring automatic updates for system-supplied attack signatures

The BIG-IP ASM system consults the Traffic Management Microkernel (TMM) and Linux routing tables when requesting attack signature updates using the Automatic Method. The source IP address of the resulting traffic uses either a non-floating self IP address or the management IP address, depending on the matching route. If Internet access is not available for automatic updates, the Configuration utility reports error messages similar to the following examples and the system logs the messages to the **/var/log/asm** file:

Configuration utility

Signature file server cannot be reached (No response from update server). Please download the Attack Signatures file and install manually.

The /var/log/asm file

```
01310027:2: ASM subsystem error (asm_config_server.pl,F5::ASMConfig::Handler::
log_error_and_rollback): Signature file server cannot be reached (No response from update server). Please
download the Attack Signatures file and install manually.
```

To configure the BIG-IP ASM system to download the attack signature update files over the internet, you can choose to update the signature files using a scheduled or manual update mode. To do so, perform one of the following procedures:

Impact of procedures: Performing the following procedures should not have a negative impact on your system.

- Configuring the BIG-IP ASM system to download the attack signature update files using a scheduled update mode
- Configuring the BIG-IP ASM system to download the attack signature update files using a manual update mode

Configuring the BIG-IP ASM system to download the attack signature update files using a scheduled update mode

1. Log in to the Configuration utility.
2. Go to the **Attack Signature Update** page, depending on your version:

   BIG-IP 12.0.0 through 14.0.x

   - **Security** > **Security Updates** > **Application Security**

   Versions prior to BIG-IP 12.0.0

   - **Security** > **Options** > **Application Security** > **Attack Signatures** > **Attack Signatures Update**
3. For **Update Mode**, select **Scheduled**.

   Note: When choosing **Weekly**, the BIG-IP system begins checking for updates a week from the day you configure the setting. When choosing **Monthly**, the BIG-IP system begins checking for updates a month from the day you configure the setting. You can perform a manual initial check before the automatic checks begin by clicking **Check for Updates**.

4. For **Update Interval**, select an update interval.
5. Select **Save Settings**.

Configuring the BIG-IP ASM system to download the attack signature update files using a manual update mode

When you choose **Manual** for **Update Mode**, you update the attack signatures on your own schedule by clicking **Update Signatures**. To configure manual update mode, perform the following procedure:

1. Log in to the Configuration utility.
2. Go to the **Attack Signature Update** page, depending on your version:

BIG-IP 12.0.0 through 14.0.x

- **Security** > **Security Updates** > **Application Security**

Versions prior to BIG-IP 12.0.0

- **Security** > **Options** > **Application Security** > **Attack Signatures** > **Attack Signatures Update**

3. For **Update Mode**, select **Manual**.
4. For **Delivery Mode**, select **Automatic**.
5. Select **Save Settings**.
6. When you are ready to update the attack signatures, select **Check for Updates**, and, if an update is available, install the signatures using one of the following methods, depending on your version:

   BIG-IP 14.0.x:

   - Select **Update Attack Signatures**.

   BIG-IP 12.x through 13.x

   - Select **Update Security**.

   Versions prior to BIG-IP 12.0.0

   - Select **Update Signatures**.

Configuring manual updates for system-supplied attack signatures

You can configure the BIG-IP ASM system to use attack signatures from an update file that was manually downloaded from an F5 server. For example, you can use this option if your BIG-IP ASM system does not have direct Internet access. To use attack signatures from an update file that was manually downloaded from an F5 server, perform the following procedure:

Impact of procedure: Performing the following procedure should not have a negative impact on your system.

1. Browse to the F5 Downloads site.
2. Manually download the latest signature file to your local workstation.
3. Log in to the Configuration utility.
4. Go to the **Attack Signature Update** page, depending on your version:

   BIG-IP 12.0.0 through 14.0.x

   - **Security** > **Security Updates** > **Application Security**

   Versions prior to BIG-IP 12.0.0

   - **Security** > **Options** > **Application Security** > **Attack Signatures** > **Attack Signatures Update**

5. For **Update Mode**, select **Manual**.
6. For **Delivery Mode**, select **Manual**.
7. Select **Save Settings**.

8. Select **Choose File** and then locate the previously saved signature file.
9. Install the signatures using one of the following methods, depending on your version:

   BIG-IP 12.0.0 to 14.0.x

   - Select **Install Updates**.

   Versions prior to BIG-IP 12.0.0

   - Select **Update Signatures**.

Allowing signature updates through a firewall

If your BIG-IP ASM system is behind a firewall, you should allow access for the following host servers, DNS servers, and ports so that the BIG-IP ASM system can obtain the attack signature updates:

DNS servers

- The firewall should allow port 53 access for the DNS nameservers configured for use by the BIG-IP ASM system.
- If you have not configured the BIG-IP ASM system with a reachable DNS nameserver, the system attempts to query the public DNS IANA root nameservers. The firewall should allow port 53 access for the DNS root nameservers. For a list of DNS root nameservers, refer to the IANA Root Servers page.

  Note: The IANA Root Servers link takes you to a resource outside of AskF5. The third party could remove the document without our knowledge.

  F5 recommends that you configure the BIG-IP ASM system to use one or more DNS servers of your choosing. For more information about configuring DNS, refer to the K13205: Configuring the BIG-IP system to resolve DNS hostnames (11.x and later).

  Note: For information about how to locate F5 product manuals, refer to K98133564: Tips for searching AskF5 and finding product documentation.

Note: To obtain the IP addresses for the previously listed F5 hosts, refer to K15202: IP addresses for F5 hosted services.

Configuring signature file updates through an HTTPS proxy

You can configure the system to use an HTTPS proxy, which allows an administrator to configure the BIG-IP ASM system to update attack signatures securely and automatically. To do so, perform one of the following procedures:

Impact of procedures: Performing the following procedures should not have a negative impact on your system.

- Configuring signature file updates through an HTTPS proxy in BIG-IP ASM 12.0.0 and later
- Configuring signature file updates through an HTTPS proxy in BIG-IP ASM versions prior to 12.0.0

Note: The BIG-IP system does not use the configured proxy address when attempting to contact the licensing server to download a new license. If the Service Check Date is not within 18 months of the system date and the BIG-IP system is unable to contact the licensing server, you must manually reactivate the license and then update the attack signatures.

Configuring signature file updates through and HTTPS proxy in BIG-IP ASM 12.0.0 and later

Beginning in BIG-IP ASM 12.0.0, you can configure the system to use an HTTPS proxy by using **BigDB** database keys. Configuring the proxy settings by manually modifying the **services.ini** file is no longer used. To do so, perform the following procedure:

1. Log in to **tmsh** by entering the following command:

   ```
   tmsh
   ```

2. Set the destination proxy server by using the following command syntax :

   ```
   modify /sys db proxy.host value <hostname>
   ```

   Note: In this command syntax, **<hostname>** is the destination proxy host name.

   Note: To revert this change use the command **modify /sys db proxy.host reset-to-default**

3. Set the destination proxy server port by using the following command syntax:

   ```
   modify /sys db proxy.port value <port>
   ```

   Note: In this command syntax, **<port>** is the numeric port value of your proxy host.

   Note: To revert this change use the command **modify /sys db proxy.port reset-to-default**

4. Set the destination proxy server protocol by using the following command syntax:

   ```
   modify /sys db proxy.protocol value <protocol>
   ```

   Note: In this command syntax, **<protocol>** is **http** or **https**.

   Note: To revert this change use the command **modify /sys db proxy.protocol reset-to-default**.

5. To set the destination proxy server username, use the following command syntax:

   ```
   modify /sys db proxy.username value <username>
   ```

   Note: In this command syntax, **<username>** is the username for authentication to the proxy server.

   Note: To revert this change use the command **modify /sys db proxy.username reset-to-default**

6. To set the destination proxy server username password, use the following command syntax:

   ```
   modify /sys db proxy.password value <password>
   ```

   Note: In this command syntax, **<password>** is the username password when authenticating to the proxy server.

   Note: To revert this change use the command **modify /sys db proxy.password reset-to-default**.

7. Exit **tmsh** by entering the following command:

   ```
   quit
   ```

Configuring signature file updates through a proxy in BIG-IP ASM versions prior through 12.0.0

For BIG-IP ASM versions prior to 12.0.0, you can configure the system to use an HTTPS proxy by editing the **services.ini** file. To do so, perform the following procedure:

1. Log in to the BIG-IP ASM command line.
2. Change directories to the **/ts/etc/** directory by entering the following command:

   ```
   cd /ts/etc/
   ```

3. Create a backup of the **services.ini** file by entering the following command:

   ```
   cp services.ini /var/tmp/services.ini.bak
   ```

4. Use a text editor to edit the **services.ini** file.
5. Use the following syntax to add a section to the end of the file:

   ```
   [proxy]
   https_proxy=https://<IP address of your HTTPS proxy server>:<HTTPS proxy server port>
   ```

   For example:

   ```
   [proxy]
   https_proxy=https://172.16.10.100:33750
   ```

   Note: Configuration of the **https_proxy** is sensitive to whitespace. Before saving any configuration changes, ensure that there are no whitespace characters around the equals symbol (**=**) and no trailing whitespace characters after the **IP:Port** definition.

6. Save the changes made to the **services.ini** file.

   Note: You must manually make this change on both systems in redundant pair configurations. The system does not copy the **services.ini** file to the peer system during configuration synchronization (ConfigSync) operations.

Rolling back BIG-IP ASM attack signatures to a previous version

F5 recommends keeping BIG-IP ASM attack signatures up-to-date; however, in a troubleshooting event such as false positive signature investigation, you can configure the BIG-IP ASM system to roll back to a previous attack signature. To do so, perform the following procedure:

Impact of procedure: The impact of running outdated attack signatures depends on the specific environment. F5 recommends testing any such changes during a maintenance window with consideration to the possible impact on your specific environment.

1. Browse to the F5 Downloads site.
2. Go to the BIG-IP ASM version that you are running and select **ASM-PastSignatureFiles**.
3. Download the past ASM signature file that you want to install.
4. Log in to the Configuration utility.
5. Go to the **Attack Signature Update** page, depending on your version:

   BIG-IP 12.0.0 through 14.0.x

   - **Security** > **Security Updates** > **Application Security**

   Versions prior to BIG-IP 12.0.0

   - **Security** > **Options** > **Application Security** > **Attack Signatures** > **Attack Signatures Update**
6. For **Update Mode**, select **Manual**.
7. For **Delivery Mode**, select **Manual**.
8. Select **Save Settings**.
9. Select **Choose File** and then locate the previously saved signature file.
10. Install the signatures using one of the following methods, depending on your version:

    BIG-IP 12.0.0 through 14.0.x

    - Select **Install Updates**.

    Versions prior to BIG-IP 12.0.0

    - Select **Update Signatures**.
11. Select **continue** when the system displays a message similar to the following example:

    The attack signature update file you want to use is older than the attack signature file currently installed in your system.
    Do you want to install this file anyway?

Supplemental Information

- K62525205: Searching for attack signature updates using the Cloud Docs attack signatures table
- K15000: Overview of the Automatic Update Check and Automatic Phone Home features
- K80272033: Older BIG-IP ASM versions may not receive the latest attack signatures
- K13284: Overview of management interface routing (11.x and later)

Applies to:

Product: BIG-IP, BIG-IP ASM
14.0.X, 13.1.X, 13.0.X, 12.1.X, 12.0.X, 11.6.X, 11.5.X

Product: F5 App Protect, F5 DDoS Hybrid Defender
14.0.X, 13.1.X, 13.0.X, 12.1.X