K15387: Overview of BIG-IP APM session cookies

Non-Diagnostic

Original Publication Date: May 13, 2015

Update Date: Oct 3, 2022

Topic

The BIG-IP APM system tracks user sessions of BIG-IP APM access profiles by using multiple HTTP session cookies.

Description

The following table lists session cookies that the BIG-IP APM system uses, and the purpose for each of these cookies.

Cookie Name	Purpose
F5_fullWT	Cookie is used to mark a full webtop.
F5_HT_shrinked	Cookie is used to mark a shrinked home tab in portal access.
F5_ST	Cookie is used exclusively to keep the client informed about session-timeout and inactivity timeout through use of specific BIG-IP APM browser-based JavaScript.
LastMRH_Session	Tracking the last 8 digits of the MRHSession session ID. For example: LastMRH_Session=41f45923; MRHSession=d896020385383db9ece7ac6d41f45923 You can use the value of LastMRH_Session in the Configuration utility to view the details of a particular BIG-IP APM session. For security purposes, when processed through the Access Policy evaluation, the first 24 digits of MRHSession is rotated, but the last 8 digits of LastMRH_Session is retained.
MRHSequence	Cookie is used to keep the version of a set of cookies changed by the BIG-IP server and JavaScript.
MRHSession	BIG-IP APM Session ID 32 random hex digits.
MRHSHint	Cookie is used for Microsoft SharePoint or for IBM Lotus Domino iNotes. MRHSHint cookie is used to carry information for SharePoint ActiveX controls.
TIN	Cookie is used to keep client informed about the remaining time in session inactivity timeout.
	Cookie is used to keep information about preferred method of

F5_VdiUserClientChoicecitrix	launching application in Citrix VDI deployment.
F5_VdiUserClientChoicevmware_view	Cookie is used to keep information about preferred method of launching application in Vmware View VDI deployment.

Session cookie design

The MRHSession cookie uses 32 randomly generated hex digits to generate the session ID. The MRHSession cookie is designed to ensure that only the BIG-IP APM controller and client can view the full session ID. The following safeguards ensure that a third party will not have access to any of the session IDs in use.

- The session ID value is generated securely using a proprietary algorithm. The algorithm creates session ID values that are not reversible or predictable and provide unique session IDs per client.
- Session cookies are set only after the SSL handshake between the BIG-IP APM system and the user has completed, ensuring that the MRHSession cookies are protected from interception with SSL encryption.
- To ensure that the client browser will not send session cookies unencrypted, the HTTP header that the BIG-IP APM uses when sending the session cookie is set with the secure option. For example:

  Set-Cookie: MRHSession=d896020385383db9ece7ac6d41f45923; path=/; secure

  Note: Vulnerability scanners may detect that the secure flag is not set on all of our cookies. When the cookie is deleted, the secure flag is not set. The value of the cookie is set to **deleted**, and the expiration date is set to **01/01/1970** so the browser will discard the cookie.

  For example:

  Set-Cookie: MRHSession=deleted;expires=Thu, 01-Jan-1970 00:00:01 GMT;path=/

- F5 has designed BIG-IP APM session cookies with inherent security properties.

  - Session cookies are stored in the client's device memory; accessing this data requires access to the client device memory of the account on the user's device.
  - Session cookies expire when the user's browser is closed.
    Note: Some browsers may include features that let you restore a session. This may keep you logged in to websites that you were logged in to before you closed the browser. For example, in Firefox, refer to Restore previous session - Configure when Firefox shows your most recent tabs and windows. You can configure your browser to disable this feature. For more information, refer to your browser's documentation.

- Each login to the BIG-IP APM system triggers new session cookies and a session ID to be generated.

- You can configure the following options for BIG-IP APM cookies in the Configuration utility:

  - **Access > Profiles / Policies > access profile name > SSO/Auth Domains** (BIG-IP APM 13.x and later)

- **Access Profiles > Access Profile Lists > access profile name > SSO/Auth Domains** (BIG-IP APM 12.x and earlier)

    - **Secure**: If the BIG-IP APM virtual server is configured with a Client SSL profile, select **Secure** (default setting) when configuring the BIG-IP APM SSO/Auth Domain cookie settings.
    - **Persistent**: Session cookie persistence functions only on BIG-IP LTM and APM deployments. For BIG-IP APM deployments with connectivity resources (such as Network Access, Portal Access, etc.), you cannot set BIG-IP APM cookies as **Persistent**. This is by design, as session cookie persistence can present a security risk. For some deployments of the BIG-IP APM system, as with Microsoft SharePoint, cookie persistence may be required. When you select cookie persistence, persistence is hard coded at 60 seconds.
    - **HTTP Only**: For BIG-IP APM deployments with connectivity resources (such as Network Access, Portal Access, etc.), do not set BIG-IP APM cookies with the **HTTP Only** flag.

- By default, F5 does not set the **Http Only** attribute for BIG-IP APM session cookies. BIG-IP APM session cookies and BIG-IP APM cookie handling is designed to ensure that resources other than the BIG-IP APM and required client side applications cannot access the cookie contents; the BIG-IP APM system does not pass the cookie to the destination resources. The BIG-IP APM rewrite/reverse proxy engine processes all content between users and the destination resources, ensuring that non-BIG-IP APM resources have no direct access to session cookies. You can configure BIG-IP APM 11.2.0 and later access profiles to use the **Http Only** attribute; you should consider the following factors when setting the attribute:

    - When the **Http Only** attribute option is enabled, only BIG-IP LTM and APM (a BIG-IP LTM virtual server with an access policy) is supported.
    - An access profile configured with the **Http Only** attribute will impede session traffic for Network Access and Network Access Tunnels, and the BIG-IP system will not run Access Policies with client side checks or actions.

      Note: Some vulnerability scanners may trigger a false positive based solely on session cookies not set with the **Http Only** attribute.

- In BIG-IP 11.2.0 and later, during the course of an access policy evaluation, the first 24 hex digits of the session ID are randomly rotated to prevent session hijacking and fixation attempts. This feature can cause issues with older clients or deployments using iRules if they assume a fixed session ID value. After Access Policy evaluation, the session ID remains static. This feature is controlled by the **apm.rotatesessionid** database variable and has a default value of **enable**.

Recommendations

None

Supplemental Information

- K15384: Overview of FirePass controller session cookies

Applies to:

Product: BIG-IP, BIG-IP APM
17.0.X, 16.1.X, 16.0.X, 15.1.X, 15.0.X, 14.1.X, 14.0.X, 13.1.X, 13.0.X, 12.1.X, 12.0.X, 11.6.X, 11.5.X, 11.4.X, 11.3.X, 11.2.X, 11.1.X, 11.0.X, 10.2.X, 10.1.X

Product: Legacy Products, BIG-IP Edge Gateway
17.0.X, 16.1.X, 16.0.X, 15.1.X, 15.0.X, 14.1.X, 14.0.X, 13.1.X, 13.0.X, 12.1.X, 12.0.X, 11.6.X, 11.5.X, 11.4.X, 11.3.X, 11.2.X, 11.1.X, 11.0.X, 10.2.X, 10.1.X