K15811: Troubleshooting LDAP authentication for BIG-IP administrative users

Diagnostic

Original Publication Date: Jan 14, 2019
Update Date: Oct 23, 2019

Issue

You should consider using this procedure under the following conditions:

- Your BIG-IP system is configured to use the Lightweight Directory Access Protocol (LDAP) protocol for authenticating BIG-IP administrative users.
- Administrative user accounts defined on the remote LDAP server are unable to log in to the BIG-IP system.

Note: If the remote user accounts are unable to log in to the BIG-IP system, the locally defined user accounts, such as the default administrator account and the root command line account, are able to log in to the system.

Symptoms

As a result of LDAP authentication failures, you may encounter the following symptoms:

- The login process fails for BIG-IP administrative users.
- The BIG-IP system logs error messages related to LDAP login failures for administrative users.

Recommended Actions

The LDAP is a protocol used for accessing and maintaining distributed directory information over a network. LDAP is based on the X.500 standard, and described in a series of Request for Comment (RFC) publications, the latest as of this writing is Internet Engineering Task Force (RFC 4511).

In the context of LDAP authentication for BIG-IP administrative users, a typical session appears similar to the following:

- The BIG-IP administrative user attempts to log in to the BIG-IP system.
- The BIG-IP system establishes a TCP connection with the remote LDAP server over port 389.

  Note: If SSL is configured, the BIG-IP system attempts to establish a connection with the remote LDAP server over port 636.

- The BIG-IP system attempts to bind to the LDAP server using the DN and password for the LDAP administrator account.
- The BIG-IP system sends an LDAP search query for the BIG-IP administrative user account to the LDAP server.
• The LDAP server attempts to locate the administrative user account in the database and sends the response to the BIG-IP system.
• The BIG-IP system authenticates the administrative user account.

Procedures

When experiencing LDAP authentication issues, you can use the following troubleshooting steps to determine the root cause:

• Verifying the Remote-LDAP configuration on the BIG-IP system
• Verifying LDAP server availability
• Reviewing LDAP log messages
• Enabling debug logging for LDAP authentication
• Packet tracing LDAP traffic
• Debugging the LDAP server
• Debugging the LDAPS server

Verifying the Remote-LDAP configuration on the BIG-IP system

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

1. Log in to the Configuration utility using the administrator account.
2. Go to System > Users > Authentication.
3. Verify the LDAP server configuration settings:
   • **Host**: Specifies the IP address of the primary LDAP server that is hosting the LDAP database.
   • **Port**: Specifies the port for primary LDAP server communications. The default is 389.
   • **Remote Directory Tree**: The file location (tree) of the user authentication database on the LDAP server.

   For example, if the BIG-IP administrative user accounts are stored in the Users directory in the LDAP directory tree, the entry may appear as follows:

   ```
   ou=Users,dc=askf5,dc=pslab,dc=local
   ```

   • **Scope**: Specifies the level of the remote LDAP directory where the system should search for the user authentication. The default setting is **Sub**, which specifies that the system searches all subdirectories of the remote directory.
   • **Bind**: The **Bind DN** and password allow the BIG-IP system to bind to the LDAP server before authenticating user accounts.
     • **DN**: Specifies the distinguished name (DN) for the LDAP server user ID used to administer the LDAP database.

     For example:

     ```
     cn=admin,dc=askf5,dc=pslab,dc=local
     ```

   • **Password**: Specifies the password associated with the previously listed user ID.
• **User Template**: Specifies the distinguished name of the user who is logging on, and defines which part of the supplied login credentials is used to construct the distinguished name. You specify the template as a variable that the system replaces with user-specific information during the logon attempt.

For example, if using the following string, the system replaces `%s` with the name the user specified in the Basic Authentication dialog box, and passes that as the distinguished name for the bind operation:

```
%s@askf5.pslab.local
```

• **Check Member Attribute in Group**: Specifies whether to verify a user's group membership for remote-role determination purposes. The group information is given in those remote-role definitions, formatted as `*member*of=<group-dn>`.

• **SSL**: Specifies whether the system uses an SSL port to communicate with the LDAP server.

• **Login LDAP Attribute** (BIG-IP 11.4.1 and later): Specifies the LDAP directory attribute containing the username. This defaults to `uid`.

• **Fallback to Local** (BIG-IP 13.0.0 and later): The BIG-IP system will fallback to the local user database if it is unable to contact the LDAP server. The local admin user can always log in regardless of this setting.

4. Confirm that the previous settings match those configured on the LDAP servers.

**Verifying LDAP server availability**

When experiencing LDAP authentication issues, you should verify that the BIG-IP system can access the LDAP servers on the network. In most environments, the LDAP servers are configured to be reachable over the BIG-IP system's management network. However, it is possible that the servers are reachable over a Traffic Management Microkernel (TMM) network. To verify the LDAP server availability, perform the following procedure:

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

1. Log in to the TMOS Shell (**tmsh**) by entering the following command:

   `tmsh`

2. To determine the IP addresses of the defined LDAP servers, enter the following command:

   `list /auth ldap servers`

   For example:

   ```
   auth ldap system-auth {
   servers { 172.24.171.1 }
   }
   ```

3. Use a utility, such as **Ping** or **Traceroute**, to verify network availability of the remote LDAP server.

   For example:
4. If the LDAP server responds to the ICMP requests, you can verify that the server is listening on the expected LDAP port (normally port 389).

For example:

telnet <LDAP_server_ip> <port>

**Note:** Press **Control + ]** to return to the telnet prompt.

Reviewing LDAP log messages

If the LDAP servers are available on the network but fail to authenticate users, you may need to review the BIG-IP log files for relevant LDAP messages. To review the log messages related to LDAP authentication, perform the following procedure:

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

1. Log in to the BIG-IP command line using the root account.
2. Use a Linux text utility, such as `less` or `tail`, to review the `/var/log/secure` file.

   For example:

   `less /var/log/secure`

3. Review the log entries for error messages related to LDAP login failures.

When reviewing the log entries for LDAP login failures, you may view messages related to the following:

- **Error trying to bind (to the LDAP server):** The Bind DN / Password values specify the distinguished name and password used for binding to the LDAP server; these values usually represent the administrative username and password for the LDAP database. When binding to the LDAP server fails due to a bad username or password, the system logs error messages similar to the following example:

  `err httpd[25432]: pam_ldap: error trying to bind (Invalid credentials)
alert httpd[25432]: pam_unix(httpd:auth): check pass; user unknown
notice httpd[25432]: pam_unix(httpd:auth): authentication failure; logname= uid=48 euid=48 tty= ruser= rhost=192.168.58.58`

- **Error trying to bind as user:** When a BIG-IP administrative user attempts to log in using a bad username or password, the system logs messages similar to the following example:

  `notice httpd[25433]: 01070417:5: AUDIT - user devuser - RAW: httpd(mod_auth_pam): user=devuser (devuser) partition=[All] level=Administrator tty=/usr/bin/tmsh host=192.168.58.58 attempts=1 start="Thu Nov 13 09:10:00 2014" end="Thu Nov 13 09:10:10 2014".
err httpd[25427]: pam_ldap: error trying to bind as user "uid=devuser,ou=Users,dc=askf5,dc=pslab, dc=local" (Invalid credentials)
• The LDAP server fails to respond or refuses the connection: When the specified service port or IP address for the LDAP server is incorrect, or the LDAP server is configured to allow requests from only a certain address range, the system logs error messages similar to the following example:

   err httpd[28859]: pam_ldap: ldap_simple_bind "Can't contact LDAP server". A "Can't contact" error also happens when ssl handshakes go wrong.
   err httpd[28859]: pam_ldap: reconnecting to LDAP server...

• SSL handshake failure: When the BIG-IP system is configured to use SSL to communicate with the LDAP server and the handshake fails, the system logs error messages similar to the following example:

   err httpd[28858]: pam_ldap: ldap_set_option(LDAP_OPT_X_TLS_NEWCTX): Can't contact LDAP server
   err httpd[28858]: pam_ldap: _set_ssl_options failed
   err httpd[28858]: pam_ldap: ldap_simple_bind "Can't contact LDAP server". A "Can't contact" error also happens when ssl handshakes go wrong.
   err httpd[28858]: pam_ldap: reconnecting to LDAP server...

Enabling debug logging for LDAP authentication

You can enable debug logging for LDAP authentication, attempt to log in using remote user accounts, and then review the debug log files. To do so, perform the following procedure:

**Important:** Due to a known issue with enabling LDAP debug logging in BIG-IP 14.1.0 and later, performing the following procedure may not enable debug logging for LDAP authentication. Instead, you may need to enable debug logging using the workaround documented in Bug ID 805417.

**Impact of procedure:** F5 recommends that you return the log level to the default value after you complete the troubleshooting steps. Leaving debug logging enabled when the system is in normal production mode may generate excessive logging and cause poor performance.

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

   tmsh

2. To enable debug logging, enter the following command:

   modify /auth ldap all debug enabled

3. Test LDAP authentication by attempting to log in using remote user accounts.
4. After testing LDAP authentication, disable debug logging by entering the following command:

   modify /auth ldap all debug disabled
5. Review the `/var/log/secure` file for debug log messages.

Packet tracing LDAP traffic

You may need to run `tcpdump` packet captures to troubleshoot LDAP sessions. When reviewing LDAP `tcpdump` output, it is helpful to understand the sequence of an LDAP session in the context of authenticating BIG-IP administrative users.

To packet trace LDAP traffic, perform the following procedure:

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

1. Log in to the command line.
2. You can capture LDAP traffic by running one of the following `tcpdump` captures:
   - If the LDAP server is reachable on the management network, use the following syntax:
     ```
tcpdump -s0 -ni eth0 port 389 -vw /shared/tmp/ldap.pcap
     ```
   - If the LDAP server is reachable on a TMM network, use the following syntax:
     ```
tcpdump -s0 -ni <vlan> port 389 -vw /shared/tmp/ldap.pcap
     ```

   **Note:** The `-vw` switches write the output to `/shared/tmp/ldap.pcap` and it also starts a packet counter to show if any packets are being written to the file.

3. You can view the capture file in a packet analysis program for further debugging.

Debugging the LDAP server

You may need to debug the LDAP server. You can do this when logged into the LDAP server, or from the BIG-IP command line. To debug the LDAP server, perform the following steps:

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

1. Log in to the BIG-IP command line.
2. Use the following `ldapsearch` command to send LDAP queries to the server.

   ```
   ldapsearch [options] [filter [attributes...]]
   ```

   For example, the following command queries the LDAP server 172.24.171.1 for a BIG-IP administrative user account named `bigipwasa`:

   ```
   ldapsearch -x -h 172.24.171.1 -D "cn=admin,dc=askf5,dc=pslab,dc=local" -w askf5 -b 'uid=bigipwasa, ou=Users,dc=askf5,dc=pslab,dc=local' '(objectclass=*)'
   ```

   ```
   # extended LDIF
   #
   # LDAPv3
   # base <uid=bigipwasa,ou=Users,dc=askf5,dc=pslab,dc=local> with scope subtree
   ```
# filter: (objectclass=*)
# requesting: ALL
#

# bigipwasa, Users, askf5.pslab.local
dn: uid=bigipwasa,ou=Users,dc=askf5,dc=pslab,dc=local
ou: Users
uid: bigipwasa
sn: bigipwasa
cn: bigipwasa
userPassword:: YXNrZjUxMjM=
description: Test BIGIP Web Application Security Administrator User
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1

3. The command output will vary, depending on whether the command finds valid LDAP entries. Output options may include the following:
   • If one or more LDAP entries are found, the entries are written to standard output in LDAP Data Interchange Format.
   • If the command results in an error, a non-zero exit status and a diagnostic message are written to standard error.

Debugging the LDAPS server

You may need to debug the LDAPS server. Before doing so, you should verify that the default.crt and default.key files are in the correct locations on the BIG-IP system. To debug the LDAP server, perform the following procedure:

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

1. Log in to the BIG-IP command line.
2. To verify that the default.crt file is in the correct location, enter the following command:

```
tmsh list sys file ssl-cert default.crt | grep system-path
```

The output should appear similar to the following example:

```
system-path /config/ssl/ssl.crt/default.crt
```

If the path does not match the previous output, enter the following command:
export LDAPTLS_CERT=/config/ssl/ssl.crt/default.crt

3. To verify that the default.key file is in the correct location, enter the following command:

tmsh list sys file ssl-key default.key | grep system-path

The output should appear similar to the following example:

system-path /config/ssl/ssl.key/default.key

If the path does not match the previous output, enter the following command:

export LDAPTLS_KEY=/config/ssl/ssl.key/default.key

4. Use the following ldapsearch command syntax to send LDAPS queries to the server:

ldapsearch [options] [filter [attributes...]]

For example, the following command queries the LDAPS server 172.24.171.1 for a BIG-IP administrative user account named bigipwasa:

ldapsearch -LLL -h 172.24.171.1 -D "cn=admin,dc=askf5,dc=pslab,dc=local" -w askf5 -b 'uid=bigipwasa,ou=Users,dc=askf5,dc=pslab,dc=local' '(objectclass=*)' -d 255

5. The command output varies depending on whether the command finds valid LDAP entries.

6. (Optional) If you entered the export commands in steps 2 and 3, clear the variables by entering the following commands:

unset LDAPTLS_KEY
unset LDAPTLS_CERT

Supplemental Information

- K11072: Configuring LDAP remote authentication for Active Directory
- K13328: Troubleshooting LDAP authentication in BIG-IP APM access policies with tcpdump

Applies to:


Product: Legacy Products, BIG-IP Edge Gateway, BIG-IP PSM, BIG-IP WebAccelerator, BIG-IP WOM