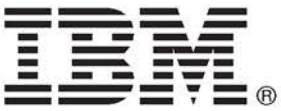
IBM PureData System for Analytics

Configuring LDAP Authentication for Operating System User Accounts



Rev. 2.0 7-May-2015

Table of Contents

1. About this document 1
1.1. About the NPS user accounts 1
1.2. Prerequisites 1
2. Obtain the Hardware Support Tools software 2
3. Configure LDAP authentication 2
4. Important information for Red Hat OS upgrades 3
5. Troubleshooting tips 3
5.1. Search for a user name 3
5.2. Retrieve user information 4
5.3. Avoid authentication changes 5
5.4. Review the log files 5
6. Disable LDAP OS authentication 5

1. About this document

This document describes how to configure the IBM PureData System for Analytics appliances to support operating system logins by users who are authenticated through an LDAP server within your environment.

This procedure can be used with IBM PureData System for Analytics appliances that are running Red Hat Enterprise Linux 5.7 or later 5.x releases, as well as Red Hat 6.4 or later 6.x releases.

IMPORTANT: The Netezza user documentation includes numerous references that LDAP authentication is supported *only* for Netezza database user accounts. With this procedure, you can configure LDAP authentication for operating system user access.

1.1. About the NPS user accounts

The IBM PureData System for Analytics appliances define three key Linux operating system users, root, nz, and nzibmsupport13. These users can log in to the NPS hosts using command shells or through the KVM supplied with the appliance.

- The root user (the Linux superuser) is typically used to perform Linux and hardware-level administrative tasks on the appliance.
- The nz user is the NPS administrator who can run nz* commands to perform tasks such as stopping and starting the NPS software, obtaining NPS status or appliance hardware information, or to perform NPS software upgrades.
- The nzibmsupport13 user is a special account for the optional restricted environment and is used for support operations such as disk replacements. With this account, IBM Support engineers and field personal can perform replacement tasks without requiring nz or root passwords.

The Netezza Platform Software (NPS) and its related applications create a number of Linux user accounts that are typically not used by any users. For example, there is a default hacluster user which is used internally by the Heartbeat application for the high availability software on the Netezza hosts. There are a number of service user accounts defined in /etc/passwd.

CAUTION: **Do not change** the root and nz users or any default accounts like hacluster or the service accounts defined in the /etc/passwd file to use LDAP authentication. These users must remain locally authenticated to ensure that services and processes continue to run as expected on the appliance.

You could use the Linux commands to create new Linux user accounts, which would be authenticated on the Netezza host by the Linux operating system. With the LDAP authentication support, you can allow users who are defined at and authenticated by your LDAP environment to connect to the NPS host as operating system users.

IMPORTANT: Operating system/Linux users **are not the same** as Netezza database user accounts. That is, operating system users can log in to access the local host and file systems, but they do not have NPS database user privileges and cannot access the Netezza databases or tables. Only Netezza database user accounts can open database connections and run queries on the NPS databases.

1.2. Prerequisites

The process to configure the LDAP authentication for operating system accounts on the NPS host requires IBM Netezza Hardware Support Tools version 8.3.0.3 software and root access to the NPS hosts.

Requirement	Notes
User Access	You must have permission to log in as the **root** user on the Netezza host to configure the OS LDAP support.
Netezza System State	As a best practice, ensure that the IBM PureData System for Analytics appliance is operating normally and that there are no hardware issues. Before you begin, log in to the NPS system as nz and use the **nzstate** command to ensure that the system is online, and use the **nzhw -issues** and **nzds -issues** commands to confirm that there are no hardware issues or conditions such as regenerations taking place. The system can remain online and available for database connections during this procedure.
LDAP environment	Make sure that you have the required information from your LDAP administrator for your site. You need information for the domain component name, LDAP host name, LDAP server

information	IP address, binding name for LDAP server, and the binding password from LDAP server administrator. You also need an LDAP user account and password to validate the configuration by logging in to the NPS host as an LDAP user.
Information and Commands	You should be familiar with Linux commands such as **cp** and running scripts from a command prompt. You should also be familiar with the user and group accounts on the system, which are documented in the *IBM Netezza System Administrator's Guide*.

2. Obtain the Hardware Support Tools software

To configure the LDAP OS login support, download and install the IBM Netezza Hardware Support Tools version 8.3.0.3 software from IBM Fix Central.

1. Log in to NPS host 1 (also referred to as HA 1 or the active NPS host) as the root user.
2. Run the following command to make sure that you have version 8.3.0.3 or later of the Hardware Support Tools. (The build date and build number could vary based on the kit that you downloaded.)

```
[root@nzhost1 ~]# more /opt/nz-hwsupport/version.txt
nz-hwsupport-tools 8.3.0.3
Build Number: 20150429, Date: 20150429-0844
```

If the version is less than 8.3.0.3, download the 8.3.0.3 or later kit from Fix Central. To install the Hardware Support Tools:

1. Log in to NPS host 1 as the root user.
2. Copy the nz-hwsupport-version.date.tar.gz file to a directory on or accessible to the NPS host 1.
3. Uncompress the software kit:

```
[root@nzhost1 mydir]# gunzip nz-hwsupport-V8.3.0.3-build.tar.gz
```

4. Uncompress the TAR file:

```
[root@nzhost1 mydir]# tar -xvf nz-hwsupport-V8.3.0.3-build.tar
```

5. Install the hardware tools:

```
[root@nzhost1 mydir]# ./hw-install.pl
```

The hardware support tools are installed in the /opt/nz-hwsupport directory.

3. Configure LDAP authentication

Use the steps in this procedure to configure the OS level LDAP authentication on your NPS appliance. This procedure updates both hosts (HA1 and HA2) of the appliance with the LDAP changes. If for any reason the scripts cannot update both hosts, the scripts display error messages and "undo" the changes to retain the local Linux OS authentication on the hosts.

1. Log in to NPS host 1 (also referred to as HA 1 or the active NPS host) as the root user.
2. Change to the /opt/nz-hwsupport/pts directory:
3. Make sure that you have the LDAP information required for your NPS appliance. In this example, the command uses the following information:

Domain Component Name:	mycomp.com
LDAP Host Name:	sqaldap.mycomp.com
LDAP Server IP Address:	1.2.3.4
Binding Name for LDAP server:	mycompname
Binding password from LDAP Server Administrator:	mypassword

4. Using the LDAP information, run the rhel_ldap_support.sh script to configure the OS account authentication:

```
[root@nzhost1 ~]# sh rhel_ldap_support.sh -withSSL no
-dcName dc=mycomp,dc=com -ldapIP 1.2.3.4
-ldapHostName sqaldap.mycomp.com  -bindDn mycompname
-bindPasswd mypassword
The configuration steps are completed. To test the authentication, log in as
an LDAP user account to the NPS host 1 and/or host 2 to confirm that you can
successfully log in. Make sure that you use an LDAP account and that you
specify the password in the LDIF file for that user.
You could test using an ssh connection as follows:

ssh ldapUser@nzhost1.company.com
ldapUser@nzhost1.company.com's password: <enter LDIF password>
```

5. If you are using SSL and enabled the support using the **-withSSL yes** option of the command, you must copy the SSL certificate from the LDAP server to the /etc/openldap/cacerts/ directory on each NPS host. The certificate file must be named `cacert.pem`. If the /etc/openldap/cacerts/ directory does not exist on the NPS host, you can create it using the **mkdir /etc/openldap/cacerts** command.

4. Important information for Red Hat OS upgrades

If the Red Hat Enterprise Linux release on your NPS hosts is upgraded to a later release, you must reapply the changes described in this document to use LDAP authentication for your OS user accounts. Typically, IBM Support or IBM field personnel perform the Red Hat upgrades. Make sure that you inform the IBM Support or field engineer if your system is configured for LDAP OS authentication, and plan for the time to reconfigure the LDAP support after the OS upgrade is finished.

5. Troubleshooting tips

The following sections describe some common troubleshooting steps for checking the LDAP configuration.

5.1. Search for a user name

You can use the **ldapsearch** command to determine whether the LDAP configuration is set up correctly. You must log in to the NPS active host as root to run the command.

NOTE: Contact IBM Support if the **ldapsearch** command is not present on your Netezza host. The command is not yet a default part of the NPS Red Hat distribution.

Suppose there is a user with username abhi and domain components netezza and com. The following example shows how to run the **ldapsearch** command and the expected results when searching for user abhi. For the value myldap, use the hostname or IP address of the server where the Directory Server is installed.

```
[root@nzhost1 ~]# ldapsearch -x -b "cn=abhi,dc=netezza,dc=com" -H ldap://myldap
# extended LDIF
#
```

```
# LDAPv3
# base <cn=abhi,dc=netezza,dc=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# abhi, netezza.com
dn: cn=abhi,dc=netezza,dc=com
objectClass: top
objectClass: person
objectClass: posixAccount
objectClass: shadowAccount
uid: abhi
uidNumber: 100
gidNumber: 104
cn: abhi
sn: abhi
description: This is user abhi, with password Netezza
loginShell: /bin/bash
homeDirectory: /home/abhi
shadowExpire: -1

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

If the user encounters any problems with the LDAP login, the administrator can review the uidNumber and gidNumber arguments that are provided in the ldif file from the output of the **ldapsearch** command. There should be a unique pair of the UID and GID values for each LDAP user.

5.2. Retrieve user information

After nslcd is set up on a RHEL 6 NPS system, you can use the Linux **getent** and **id** commands to check the LDAP configuration. You must log in to the NPS active host as root to run the command.

You can use the **getent passwd** command to show the LDAP and local users after LDAP is configured on the NPS active host.

```
[root@nzhost1 ~]# getent passwd
```

Sample output follows:

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
...
ldap_usr1:x:507:507::/home/ldap_usr1:/bin/bash
user2:x:508:508::/home/user2:/bin/bash
```

You can use the **id** ***user_name*** command to confirm that LDAP lookups are working. For example:

```
[root@nzhost1 ~]#  id user2
uid=508(user2) gid=508(user2) groups=508(user2)
```

If either the **getent** or **id** commands fail, the problem might be that the LDAP configuration information is incorrect, or a firewall could be blocking the port.

5.3. Avoid authentication changes

After making changes to the NPS hosts to enable host-level LDAP authentication, use caution when performing other configuration operations such as the **authconfig** command. Your configuration changes could undo or corrupt the LDAP configuration changes.

5.4. Review the log files

Use the /var/log/secure log file to obtain more information when you are debugging LDAP authentication problems. For example, the following sample log message shows a successful user login using LDAP authentication:

```
Dec 10 05:23:23 nzhost1 sshd[16898]: Accepted password for nz from 1.2.3.4 port
38291 ssh2
Dec 10 05:23:23 nzhost1 sshd[16898]: pam_unix(sshd:session): session opened for user
user1 by (uid=0)
```

The following sample message shows the error from a failed LDAP authentication attempt for a user without a password who specified the wrong password:

```
Jul 25 01:40:32 nzhost1 su: pam_unix(su:session): session opened for user root by
nz(uid=500)
Jul 25 01:42:18 nzhost1  sshd[23220]: pam_unix(sshd:auth): authentication failure;
logname= uid=0 euid=0 tty=ssh ruser= rhost=host.company.com  user=user_withoutpasswd
Jul 25 01:42:20 nzhost1  sshd[23220]: Failed password for user_withoutpasswd from
9.74.12.213 port 43126 ssh2
Jul 25 01:42:25 nzhost1  sshd[23220]: Failed password for user_withoutpasswd from
9.74.12.213 port 43126 ssh2
Jul 25 01:42:30 nzhost1  sshd[23220]: Failed password for user_withoutpasswd from
9.74.12.213 port 43126 ssh2
Jul 25 01:42:30 nzhost1  sshd[23221]: Connection closed by 1.2.3.4
Jul 25 01:42:30 nzhost1  sshd[23220]: PAM 2 more authentication failures; logname=
uid=0 euid=0 tty=ssh ruser= rhost=host.company.com  user=user_withoutpasswd
```

6. Disable LDAP OS authentication

Use the steps in this procedure to disable the LDAP authentication for OS user accounts on your NPS appliance. This procedure updates both hosts (HA1 and HA2) of the appliance to disable the LDAP changes. If for any reason the scripts cannot update both hosts, the scripts display error messages and "undo" the changes to retain the current LDAP authentication on the hosts.

1. Log in to NPS host 1 (also referred to as HA 1 or the active NPS host) as the root user.
2. Change to the /opt/nz-hwsupport/pts directory:
3. Make sure that you have the LDAP information required for your NPS appliance. In this example, the command uses the following information:

Domain Component Name:	mycomp.com
LDAP Host Name:	sqaldap.mycomp.com
LDAP Server IP Address:	1.2.3.4
Binding Name for LDAP server:	mycompname

Binding password from LDAP Server Administrator: mypassword

4. Using the LDAP information, run the rhel_ldap_removal.sh script to disable the LDAP OS account authentication:

```
[root@nzhost1 ~]# sh rhel_ldap_removal.sh -withSSL no
-dcName dc=mycomp,dc=com -ldapIP 1.2.3.4
-ldapHostName sqaldap.mycomp.com  -bindDn mycompname
-bindPasswd mypassword
LDAP authentication for system logins has been disabled  for host nzhost1.
Login credentials will now be authenticated via the local operating system.
IBM recommends that you confirm that this capability is working properly now
by attempting to log in to the host from a remote system using a valid local
username and password.
```

5. If you were using SSL for your OS user authentication, remove the /etc/openldap/cacerts/cacert.pem file from each NPS host.

From another system in the network, you could test using an ssh connection as follows:

```
ssh nz@nzhost1.company.com
nz@nzhost1.company.com's password: <enter local account password>
```