AD Bridge

Error Codes Reference Guide

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

TC:2/28/2024

Table of Contents

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

AD Bridge Error Codes Reference Guide

This guide shows system administrators and security administrators how to handle errors that could arise while using BeyondTrust AD Bridge. An example, cause, and resolution are provided for each error.

This document is not an inclusive list of all possible AD Bridge errors. Additionally, there may be resolutions for these issues other than those detailed in this document.

If you encounter an error not covered in this guide, or if a recommended resolution does not resolve your issue, please contact BeyondTrust Technical Support.

For more information, see "Contact BeyondTrust Technical Support" on page 34.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

Failed to Validate GPO Security Descriptor

Error

When AD Bridge fails to validate Active Directory and GPO Security Descriptor, the following is returned:

```
Error: Failed to validate the discretionary access control list
Error: Failed to validate GPO Security Descriptor
```

Cause

This typically occurs when there is a failure to validate the system access control list and discretionary access control list.

Resolution

We have created a Security Descriptor tool usage: **/opt/pbis/libexec/verify-sd <hex-string>**. This tool displays relative security descriptor validation error information. It accepts hex string representations of security descriptors and performs the same validation checks as gpagent.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

Decrypt Integrity Check Failed

Error

When AD Bridge users attempt to log in, they receive a standard password mismatch error preceded by a Kerberos error:

```
Nov 21 23:52:50 linux-hostname lsass: [LwKrb5InitializeUserLoginCredentials /builder/src-
git/Platform/src/linux/lwadvapi/threaded/lwkrb5.c:1492] KRB5 Error code: -1765328353 (Message:
Decrypt integrity check failed)

Nov 21 23:52:50 linux-hostname lsass: [lsass] Failed to authenticate user (name =
'domain\username') -> error = 40022, symbol = LW_ERROR_PASSWORD_MISMATCH, client pid = 8057
```

Cause

This error will prevent all domain users from logging into this host, but attempts made on working hosts will verify the password is not actually incorrect.

Resolution

Search for duplicate computer objects of the same name in Active Directory and remove any duplicates. Once the duplicate computer object is located, remove it and rejoin the affected computer to the domain.

To easily find duplicate SPN names, run the following command on a Windows domain controller:

- **Single Domain Environment**:

  ```
  setspn -x
  ```

- **Environments with Multiple Trusted Domains**:

  ```
  setspn -t * -t home -x
  ```

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

DNS_ERROR_BAD_PACKET

Error

```
DNS_ERROR_BAD_PACKET
```

Cause

These errors typically occur if there are DNS issues or all of the ports AD Bridge requires are not open.

Resolution

Verify:

1. You can resolve the domain you are joining.
2. The domain controllers returned can be resolved and connected to.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

ERROR_BAD_FORMAT

Error

When attempting to join a domain, the following is returned:

```
ERROR_BAD_FORMAT
```

Cause

This issue typically occurs when there is a character that is unexpected in the **krb5.conf**. It could also be an issue with a special character in the OU or domain.

Resolution

Check the **/etc/krb5.conf** for any special characters or formatting issues.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

ERROR_GEN_FAILURE

Error

When attempting to join a domain, the following is returned:

```
ERROR_GEN_FAILURE
```

Cause

Possible causes:

- One possible cause can be observed on Solaris 10. Administrators must verify they have added DNS or the join will fail.
- The Administrator account does not have correct permissions to join a domain.

Resolution

- On Solaris 10, ensure **/etc/nsswitch** has the **host: files dns** line.
- Review permissions on the Administrator account.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

NO_SUCH_CELL

Error

When attempting to join a domain, the following is returned:

```
Error: NO_SUCH_CELL on domain join.
```

Cause

This error typically occurs if there is no cell in Active Directory (AD) for AD Bridge to join. AD Bridge runs in three modes: **Directory Integrated** mode, **Unprovisioned** mode, or **ID Range**. Directory Integrated mode is the preferred method.

> ***Note:*** *Directory Integrated mode can use **Default** or **Named Cell**, while Unprovisioned mode is Named Cell only. ID Range mode is mutually exclusive from having cells defined. ID Range mode and either Default Cells or Named Cells may not be defined at the same time.*

If IDRange was in use then it is possible that the --IDRange flag

A Default Cell is an AD object that sits at the root of the domain and allows all users and groups enabled in that cell to access any Linux or Unix machine joined to AD. Access can be restricted by using security groups and enabling **require membership of** in the group policy applied to the servers. Once enabled, select the appropriate security groups for access.

A Named Cell is similar in concept. However, a Named Cell can exist in any OU and users enabled in this cell only have access to servers within the same OU the cell exists in or below, but nowhere else. With Default Cell, there is only one, but with Named Cell, multiple cells are allowed.

> ***Tip:*** *We recommend a maximum of four Named Cells for ease of administration purposes. There is no limit to the number of cells that AD Bridge supports. A mix of Default and Named Cells can coexist in the same environment.*

A cell must be created for AD Bridge to work. Prepare AD first to allow AD Bridge to function, then install the agent on a Linux or Unix machine.

> *For more information, see the AD Bridge Installation Guide at www.beyondtrust.com/docs/ad-bridge/getting-started/installation.*

Resolution

Join to a location that has either a Default or Named Cell. If that does not exist, create a Default or Named Cell.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

ERROR_KRB5KDC_ERR_C_PRINCIPAL_UNKNOWN

Error

When attempting to join a domain, the following is returned:

```
LW_ERROR_KRB5KDC_ERR_C_PRINCIPAL_UNKNOWN
```

Cause

This issue typically occurs because the user specified to join the computer to the Active Directory (AD) domain does not exist in AD. In the following example, **user2** is not a valid AD user.

```
[user1@host1 bin]$ ./domainjoin-cli --loglevel debug --logfile /tmp/join.log join --ou 'My OU'
example.com user2

Joining to AD Domain: example.com

With Computer DNS Name: host1.example.com

User2@EXAMPLE.COM's password:

Error: LW_ERROR_KRB5KDC_ERR_C_PRINCIPAL_UNKNOWN [code 0x0000a309]

Client not found in Kerberos database
```

Resolution

To correct this issue, verify a valid AD user is specified during the join process.

GSSAPI Error: The Referenced Context has Expired (Unknown Error)

Error

Occasionally, you may see multiple errors in the logs.

```
Mar 4 07:34:59 linuxhost lsass: GSSAPI Error: The referenced context has expired (Unknown error)
```

This may or may not be associated with slow logins.

Cause

If a user does not enter their password for 8 hours after they initially logged in, the Kerberos ticket will expire and may not be renewed. This is the default Kerberos expiration time. There may be issues with user load or concurrency, which could prevent the ticket from being refreshed.

Other reasons you must renew a user's Kerberos ticket include when the user is using:

- Single sign-on (SSO)
- Another SSH client
- An SMB client. For example, using Nautilus from a workstation desktop.
- NFSv4 mounts

Resolution

If you don't need SSO, you can turn off the following configuration setting (enabled by default), which may improve performance:

```
Name: RefreshUserCredentials
Description: Whether to refresh user credentials against AD domain controller
Type: boolean
Current Value: true
Accepted Values: true, false
```

> ***Note: Current Value** is determined by local policy.*

You may also use a group policy to manage this centrally. Typically located under the **Authorization and Identification** group, configure the **Lsassd: Enable user credential refreshing** setting.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

LSASS Error Code [code 0x00009da2]

Error

When attempting to join a domain, the following is returned:

```
LSASS Error Code [code 0x00009da2]
```

Cause

A failed attempt to join the domain has left a computer object behind in Active Directory.

Resolution

Delete the account from Active Directory and try to join again.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

LSASS Error [code 0x0000000b] The OU format is invalid

Error

The OU format is invalidError

```
Lsass Error [code 0x0000000b] The OU format is invalid
```

Cause

The issue appears when an **INVALID_PARAMETER** error occurs and the domain join translates that to an OU error. This could be a license related issue as it uses the same **INVALID_PARAMETER** error.

Resolution

Check the lsass logs for the following error:

```
20210304081807:INFO:lsass:LsaCheckLicense():/builder/src-git/Enterprise/src/linux/lsass-enterprise/server/auth-providers/ad-enterprise-provider/provider-main.c:7713: License check complete, status code: 87, Bits: 0x00000000
```

If found then try the following:

- Check the computer object has rights to read the license from the container.
- Try recreating the license container and importing the license file.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

LW_ERROR_ACCESS_DENIED

Error

```
[user1@host1 bin]$ ./domainjoin-cli –loglevel debug --logfile /tmp/join.log join --ou 'My OU'
example.com Administrator

Joining to AD Domain: example.com
With Computer DNS Name: host1.example.com
Administrator@EXAMPLE.COM's password:

LW_ERROR_ACCESS_DENIED [code 0x00009cde]
Incorrect access attempt
```

Cause

This issue typically occurs because the user who is running the **domainjoin-cli** command does not have sufficient privileges. In the above example, the domain join is being run by **user1**.

Resolution

To correct this issue, either re-run the **domainjoin-cli** command as root or by using **sudo**.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

LW_ERROR_CLOCK_SKEW [code 0x00009c97]

Error

When attempting to join a domain, the following is returned:

```
LW_ERROR_CLOCK_SKEW [code 0x00009c97]
```

Cause

This message indicates that the system time on the Linux or Unix host you are trying to join to your domain is different from that of the domain controller by greater than 5 minutes (300 seconds). AD Bridge cannot operate with a clock skew greater than 300 seconds, so the domain join is halted.

Resolution

To resolve the error, update the time on the client host and then run **domainjoin-cli** again.

```
/opt/pbis/bin/domainjoin-cli join <arguments>
```

Example:

```
/opt/pbis/bin/domainjoin-cli join mydomain.com MyAdminUser
```

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

LW_ERROR_DOMAIN_IS_OFFLINE

On Domain Join

Error

```
LW_ERROR_DOMAIN_IS_OFFLINE [code 0x00009cb9] the domain is offline.
```

Cause

This issue typically occurs because network ports required by Kerberos are blocked.

```
[root@host1 bin]$ ./domainjoin-cli --loglevel debug --logfile /tmp/join.log join --ou 'My OU'
example.com Administrator
Joining to AD Domain: example.com
With Computer DNS Name: host1.example.com
Administrator@EXAMPLE.COM's password:
Error: LW_ERROR_DOMAIN_IS_OFFLINE [code 0x00009cb9] The domain is offline
```

Resolution

To correct this issue, verify all ports required by Kerberos are open or modify firewall rules to allow Kerberos traffic on the following ports.

- **Kerberos**: 88 UDP/TCP
- **Machine password changes (typically after 30 days)**: 464 UDP/TCP

In the gpagent Logs

Error

```
LW_ERROR_DOMAIN_OFFLINE error while primary domain is online in gpagent.
```

Cause

The **gpagent** service consistently throws **LW_ERROR_DOMAIN_OFFLINE** errors while primary domain is online. Group policies may also correctly appear in the **/var/lib/pbis/grouppolicy** directory.

```
gpagent: [gpagent] Error processing group policies while processing list of group policy objects
for computer, error: [0x 9CB9] (LW_ERROR_DOMAIN_IS_OFFLINE)
```

In this situation, there may be no discernible impact, but the above errors continue to appear in **/var/log/messages** (or equivalent).

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

You may see this error without any visible impact if one of the trusted domains in the customer's environment is unreachable. To verify this, run **/opt/pbis/bin/get-status** and look in the list of trusted domains for:

```
Domain flags: [0x0002]
[0x0002 - Offline]
```

The **gpagent** service will attempt to download any group policies it has access to, even if they aren't intended to be applied to the target computer. To resolve the errors, investigate network or DNS issues that may be preventing communication with the trusted domain that is unavailable.

Resolution

If the domain is unavailable by design, you can exclude it from being enumerated by setting the **Lsass:Domain trust enumeration exclude list** group policy setting and specifying the domains you would like to exclude.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

LW_ERROR_ERRNO_EISDIR

Error

When attempting to join a domain, the following is returned:

```
{color:#455464}Error: LW_ERROR_ERRNO_EISDIR [code 0x00009cef]{color}
```

Cause

This message indicates that a system file AD Bridge is trying to write to is actually a directory. While rarely seen, the event has occurred on the **domainjoin-cli.log** file.

Resolution

To resolve the error, remove the directory that is causing the conflict, and then run **domainjoin-cli** again.

To remove the **domainjoin-cli.log** file:

```
rm -r /var/log/domainjoin-cli.log
```

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

LW_ERROR_GSS_CALL_FAILED

Error

gpagent generates User policy errors. You see repeated errors in the log similar to the following:

```
Jan 1 12:00:00 pbishost gpagent: [gpagent] Error in User policy applicator (Error while
contacting domain controller for user domain), error: [0x 9C70](LW_ERROR_GSS_CALL_FAILED)
Jan 1 12:00:00 pbishost gpagent: [gpagent] Failed to apply policy for user [uid:12345678]
```

Cause

User group policy is enabled and the user:

- Has not logged into the system
- Has previously logged into the system, but the Kerberos ticket has expired
- Does not exist

Resolution

If you do not use User group policy processing, you can disable this through a group policy setting.

For more information, see the AD Bridge Group Policy Reference Guide at www.beyondtrust.com/docs/ad-bridge/how-to/group-policy.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

LW_ERROR_INTERNAL

Error

When attempting to join a domain, the following is returned:

```
Error: LW_ERROR_INTERNAL [code 0x00009c50]
Internal Error
```

Cause

The system is out of memory and cannot continue.

Resolution

- Free up system resources.
- Reboot the impacted host to free up its memory.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

LW_ERROR_INVALID_MESSAGE

Error

When attempting to join a domain, the following is returned:

```
LW_ERROR_INVALID_MESSAGE
```

Cause

This error occurs if you do not enter a password during a domain join. This could be an issue with Kerberos.

Resolution

Uninstall using **purge** and reinstall AD Bridge.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

LW_ERROR_INVALID_MESSAGE (The Inter Process message is invalid)

Error

After a host level outage or host outage work, there's a rare case where older versions of AD Bridge cause the cache file **/var/lib/pbis/db/lsass-adcache.filedb.*** to become 0 bytes. The file also cannot be written to, so it causes an error when attempting to perform a domain join similar to the following:

```
root@host /opt/pbis/bin > pbis-status
LSA Server Status:
Compiled daemon version: 8.5.3.293
Packaged product version: 8.5.289.0
Uptime: 0 days 0 hours 0 minutes 47 seconds

[Authentication provider: lsa-activedirectory-provider]
Status: Unknown
Mode: Unknown
root@pl000680 /opt/pbis/bin > domainjoin-cli join DOMAIN.LOCAL join-user
Joining to AD Domain: domain.local
With Computer DNS Name: computername

join-user@DOMAIN.LOCAL's password:
Error: LW_ERROR_INVALID_MESSAGE [code 0x00009c46]
The Inter Process message is invalid
```

Cause

This was identified as an issue in older versions of AD Bridge.

Resolution

Note: *This issue has been resolved in AD Bridge versions 8.6.0 and later.*

To resolve the issue in older versions of AD Bridge, follow the below steps.

1. **rm /var/lib/pbis/db/lsass-adcache.filedb.***
2. **service lwsmd restart**
3. Rejoin domain.

If you remove this file and restart **lwsmd**, the issue will be resolved.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

LW_ERROR_KRB5_CC_NOMEM

Error

The following error is returned during a login attempt. The user cannot authenticate.

```
LW_ERROR_KRB5_CC_NOMEM
```

Cause

This issue typically occurs because there is an issue with the user's Kerberos cache file. There will be events like the following in the **lsass** debug log file.

```
6.1/src/linux/lsass/server/api/auth.c:174] Failed to authenticate user (name = 'username') ->
error = 41931, symbol = LW_ERROR_KRB5_CC_NOMEM, client pid = -1
6.1/src/linux/lwadvapi/threaded/lwkrb5.c:613] KRB5 Error code: -1765328186 (Message: No more
memory to allocate (in credentials cache code))
```

In this particular case, there was an old **/tmp/krb5cc_<uid>** Kerberos cache file for the user. Once the file was deleted, the user could authenticate and a new Kerberos cache file was created with the new UID.

Resolution

Delete the **/tmp/krb5cc_<uid>** file. Attempt to authenticate and the user should be allowed in.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

LW_ERROR_LDAP_ALREADY_EXISTS

Error

When using AD Bridge and running **/opt/pbis/bin/domainjoin-cli join <arguments>** to join a Linux or Unix system to the domain, the following error is returned:

```
/opt/pbis/bin/domainjoin-cli join --ou "MyOU/OU" mydomain.com myadminuser
Joining to AD Domain: mydomain.com
With Computer DNS Name: mycomputer.mydomain.com
myadminuser@mydomain.COM's password:
Error: LW_ERROR_LDAP_ALREADY_EXISTS
```

Cause

This error is typically encountered while attempting to re-join an existing computer to the domain.

The computer object for this computer still exists in Active Directory (AD) and the admin account you are using to run the domain join command does not have permission to modify computer objects in the domain.

Resolution

This can be resolved either by removing the existing computer object from AD, using Active Directory Users and Computers with an account which has permissions to delete computer objects, or by giving the account modify permissions in the domain.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

LW_ERROR_LDAP_CONSTRAINT_VIOLATION

Error

When attempting to join a domain, the following is returned:

```
LW_ERROR_LDAP_CONSTRAINT_VIOLATION [code 0x00009d7b]
```

In the following example, **user2** does not have the correct permissions in Active Directory (AD).

```
[root@host1 bin]$ ./domainjoin-cli --loglevel debug --logfile /tmp/join.log join --ou 'My OU'
example.com user2
Joining to AD Domain: example.com
With Computer DNS Name: host1.example.com
User2@EXAMPLE.COM's password:
Error: LW_ERROR_LDAP_CONSTRAINT_VIOLATION [code 0x00009d7b]
```

Cause

The error typically occurs when the user account in the **domainjoin** command does not have the permissions required to add and modify computer objects.

Resolution

To correct this issue, verify the user has the correct permissions to add and modify computer objects, or use an account such as **Administrator**.

Even if an object for the computer pre-exists in AD, the administrator account used to join to the domain must have access to modify objects as certain attributes must be modified on join.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

LW_ERROR_LDAP_INSUFFICIENT_ACCESS [code 0x00009d8b]

Error

When using AD Bridge and running **/opt/pbis/bin/domainjoin-cli join <arguments>** to join a Linux or Unix system to the domain, the following error is returned:

```
/opt/pbis/bin/domainjoin-cli join --ou "MyOU/OU" mydomain.com myadminuser
Joining to AD Domain: mydomain.com
With Computer DNS Name: mycomputer.mydomain.com
myadminuser@mydomain.COM's password:
Error: LW_ERROR_LDAP_INSUFFICIENT_ACCESS [code 0x00009d8b]
LW_ERROR_LDAP_INSUFFICIENT_ACCESS [code 0x00009d8b]
```

Cause

This error is typically encountered while attempting to re-join an existing computer to the domain. The computer object for this computer still exists in Active Directory (AD) and the admin account you are using to run the domain join command does not have modify permissions for objects in the OU you are trying to join.

Resolution

This can be solved either by removing the existing computer object from AD using Active Directory Users and Computers, or by giving the account modify permissions in the target OU.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

LW_ERROR_LDAP_NO_SUCH_OBJECT

Error

```
Jan 30 13:48:25 pbishost gpagent: [gpagent] Error at
/builder/src-buildserver/Enterprise-7.0/src/linux/grouppolicy/server/ldap/
gpadirectory.c:371. Error code [0x 9d7e] (LW_ERROR_LDAP_NO_SUCH_OBJECT)
```

This error message is generated by the **gpagentd** daemon when it checks for new group policy objects online, either for users at logon, or for the computer. This error message can be ignored.

Cause

There are certain pieces of data that exist in LDAP to tell a computer (AD Bridge or Windows) what the structure of a Group Policy object is.

When pulling down GPO, the computer must inspect and verify those pieces of data. For example, if a policy is not set in a GPO, that data doesn't exist in the particular GPO. This causes the **LW_ERROR_LDAP_NO_SUCH_OBJECT** message in AD Bridge.

> ***Note:*** *This error is an "ignore and continue" error. This should be emitted only at **VERBOSE** logging level in newer versions of AD Bridge.*

Resolution

This error message can be ignored.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

LW_ERROR_NOT_HANDLED

Error

```
LW_ERROR_NOT_HANDLED [code 0x00009c51]
```

Cause

This error could occur during an install where the library paths may be set in the environment, which results in a botched install when importing the registry.

Resolution

If you were to run **env | grep -i lib** or **env | grep ld** and see any library paths, these should be unset before installing or purging the software.

Additionally, a purge sometimes does not cleanly remove everything. After the purge uninstall, you should verify no Likewise or AD Bridge packages are still installed and delete everything under **/opt/likewise***, **/opt/pbis***, **/var/lib/likewise***, and **/var/lib/pbis***.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

LW_ERROR_PASSWORD_EXPIRED

Error

When attempting to join a domain, the following is returned:

```
LW_ERROR_PASSWORD_EXPIRED
```

Cause

This issue typically occurs because the user account used to join the domain has an expired password in Active Directory. In the following example, the password for **Administrator** has expired:

```
[root@host1 bin]$ ./domainjoin-cli --loglevel debug --logfile /tmp/join.log join --ou 'My OU'
example.com Administrator
Joining to AD Domain: example.com
With Computer DNS Name: host1.example.com
Administrator@EXAMPLE.COM's password:
Error: LW_ERROR_PASSWORD_EXPIRED [code 0x00009c58]
Password expired
```

Resolution

To correct this issue, reset the password for the **Administrator** account (or whichever join account is specified) in Active Directory.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

LW_ERROR_PASSWORD_MISMATCH

Error

When querying domainjoin status, the following is returned:

```
/opt/pbis/bin/domainjoin-cli query
Error: LW_ERROR_PASSWORD_MISMATCH [code 0x00009c56]
"The password is incorrect for the given account"
```

Cause

If you see this error specifically when querying domain join status, this indicates the machine account password has expired or does not match the password stored in Active Directory.

Resolution

To correct this, run the following command:

```
/opt/pbis/bin/domainjoin-cli join <join arguments>
```

Example:

```
/opt/pbis/bin/lsa authenticate-user --user username --domain example.com
```

This will refresh the locally cached machine account password with what is stored in Active Directory.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

LW_ERROR_UNKNOWN

Error

When attempting to join a domain, the following is returned:

```
LW_ERROR_UNKNOWN
```

Cause

This issue typically occurs when there is a character that is unexpected in the domain join function.

Resolution

Check the syntax of the **domainjoin** command.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

NERR_DCNotFound

Error

When attempting to join a domain, the following is returned:

```
NERR_DCNotFound
```

Resolution

In any event, SRV records cannot be added to **resolv.conf** files (or hosts files). They can only be served out by DNS servers.

There are three options:

1. Point all to Active Directory (AD) DNS.
2. Forward the AD zones from whatever DNS server they are using (possibly best for their environment).
3. Configure new (bind) DNS servers (possibly even on the boxes themselves) that either forward the zones or host the AD data directly using an export from AD. This is not recommended as it takes a lot of maintenance to keep current.

All products which bridge AD will have similar requirements.

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

Undocumented Exception

Error

When attempting to join a domain, the following is returned:

```
Error: Undocumented exception [code 0x00009efc] An undocumented exception has occurred. Please
contact BeyondTrust technical support and use the error code to identify this exception.
```

Cause

This error typically occurs if there are host name or DNS issues with the computer object and the account used does not have the right to set the required attributes.

Resolution

Confirm that the host name is correct and matches the DNS entry.

Confirm that the account used with the **domainjoin** command has the right to update the **servicePrincipalName** and **dNSHostName** attributes of the computer object.

Contact BeyondTrust Technical Support

BeyondTrust provides an online knowledge base, as well as telephone and web-based support.

> *For BeyondTrust Technical Support contact information, please visit www.beyondtrust.com/support.*

Before Contacting BeyondTrust Technical Support

To expedite support, collect the following information to provide to BeyondTrust Technical Support:

- AD Bridge version: available in the AD Bridge Console by clicking **Help > About** on the menu bar
- AD Bridge Agent version and build number
- Linux or Unix version
- Windows or Windows Server version

If you are contacting BeyondTrust Technical Support about one of the following issues, also provide the diagnostic information specified.

Segmentation Faults

Provide the following information when contacting BeyondTrust Technical Support:

- Core dump of the AD Bridge application:

  ```
  ulimit - c unlimited
  ```

- Exact patch level or exact versions of all installed packages

Program Freezes

Provide the following information when contacting BeyondTrust Technical Support:

- Debug logs
- tcpdump
- An **strace** of the program

Domain-Join Errors

Provide the following information when contacting BeyondTrust Technical Support:

- Debug logs: copy the log file from **/var/log/pbis-join.log**
- tcpdump

All Active Directory Users Are Missing

Provide the following information when contacting BeyondTrust Technical Support:

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

- Run **/opt/pbis/bin/get-status**
- Contents of **nsswitch.conf**

All Active Directory Users Cannot Log On

Provide the following information when contacting BeyondTrust Technical Support:

- Output of **id <user>**
- Output of **su -c 'su <user>' <user>**
- **lsass** debug logs

> ℹ *For more information, see Generate Debug Logs in the AD Bridge Troubleshooting Guide, at www.beyondtrust.com/docs/ad-bridge/how-to/troubleshoot.*

- Contents of **pam.d/pam.conf**
- The sshd and ssh debug logs and syslog

AD Users or Groups are Missing

Provide the following information when contacting BeyondTrust Technical Support:

- The debug logs for lsass
- Output for **getent passwd** or **getent group** for the missing object
- Output for **id <user>** if user
- tcpdump
- Copy of lsass cache file.

Poor Performance When Logging On or Looking Up Users

Provide the following information when contacting BeyondTrust Technical Support:

- Output of **id <user>**
- The lsass debug log
- Copy of lsass cache file.

> ℹ *For more information about the file name and location of the cache files, see the AD Bridge Linux Administration Guide, at www.beyondtrust.com/docs/ad-bridge/getting-started/linux-admin.*

- tcpdump

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

Generate a Support Pack

The AD Bridge support script copies system files that AD Bridge needs to function into an archive. This archive can then be sent to support to assist in the investigation.

Installed location:

/opt/pbis/libexec/pbis-support.pl

©2003-2024 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.