AD Bridge 23.2 Release Notes

October 5, 2023

Requirements:

For installation requirements, please see the following:

- *For the AD Bridge agent, Install Requirements for the AD Bridge Agent, at https://www.beyondtrust.com/docs/ad-bridge/getting-started/installation/install-agent/requirements-agent.htm.*
- *For the management console, Requirements to Use AD Bridge with Active Directory, at https://www.beyondtrust.com/docs/ad-bridge/getting-started/installation/install-console/index.htm.*
- *For a list of supported platforms for the latest version of AD Bridge, please see the Supported Platforms Guide, at https://www.beyondtrust.com/docs/ad-bridge/getting-started/supported-platforms/index.htm.*
- *Supported Platforms Guides for previous versions of AD Bridge can be found in the AD Bridge Documentation Archive, at https://www.beyondtrust.com/docs/archive/ad-bridge/index.htm.*

For the latest information on features included in this release, see the What's New in AD Bridge 23.2 document, at https://www.beyondtrust.com/docs/ad-bridge/documents/getting-started/adb-whats-new.pdf.

New Features and Enhancements:

Azure Integration for Pure Azure Accounts

With AD Bridge 23.2, you can use Azure AD identities to authenticate seamlessly to Unix and Linux endpoints, with no requirements for on-premises AD. This includes advanced functionality like MFA and other login requirements. This seamless support for Azure AD helps organizations remove the complexity of managing separate identity directories.

IMPORTANT!

Azure AD (now called Entra ID) requires the purchase of a separate SKU.

- AD Bridge can now authenticate against Azure AD with a Pure Azure account. This requires:
  - An application setup in the Azure tenant under **App registrations** that **Allow public client flows** and permits Microsoft Graph **application.read.all**, **user.read.all** and **group.read.all** rights.
  - Secret generated for the application and stored on the endpoint in a file.
  - Joining to Azure with the **/opt/pbis/bin/tenantjoin-cli** binary.
  - Pure Azure users can log in when joined to the tenant.
  - The Azure user must be a member of a group in order to log in. The first group assigned to them will be their Primary GID.

Azure-OAuth Provider

- Added the **AssumeDefaultTenant** option to the config tool, to add the ability to authenticate without providing the full User Principal Name (UPN).
- Added the **AzureRequiremembershipOf** option to config tool, to restrict logon access to a computer to specific users or group members.
- Added the ability to log in with Pure Azure user accounts.
- AD Cache adds Azure users and groups to the cache upon login and enumerates them.
- AD Cache works only when joined to a tenant.
- After a tenant join, Azure-OAuth is the only provider in the provider list.
- Azure cache is written to a file.
- Azure cache can be backed up and restored.
- Azure **nsswitch** has been modified to find the group ID.
- On provider shutdown/startup, the Azure cache is initialized.
- AD Cache has new **–tenant** flag to filter Azure user/group objects.
- Integrated UID/GID collision detection for Pure Azure users/groups.
- Modified PAM stack for pure Azure environments.
- **get-status** displays secret expiration date.
- Implemented Azure ID hashing for UID/GID.
- OAuth events are sent to ElasticSearch.

Azure Tenant Join

- **tenantjoin-cli** can query the tenant.
- Removed the **–tenant-name** option from **tenantjoin-cli**.
- **tenantjoin-cli** can update a secret with new **renew** option.
- A message is displayed when running **tenantjoin-cli** query and not joined to a tenant.

Azure Tenant License

- Added license version column to BMC License Management to display version.
- Integrated the tenant licensing.
- Added Azure license check to the Azure-OAuth provider.
- Added Azure license check to Azure provider.
- Applied license messaging about expiration, evaluation, or no license during user login.

Update BMC Utilities

- Update BMC utilities to connect to other domains. The **Status** page has been updated to show which domain the BMC is connected to. Duplicate Scanner and Orphaned Objects now launch to the connected domain.

Add Installer Option for ADB Scripts

- A new module has been added to the Windows installer that allows users to place ADB scripts on the system. The current script allows users to create a default cell at the root of the domain without installing the other ADB Windows modules.

Add Support for KRB5 Option

- Support for KRB5 option **KRB5_CONF_DNS_CANONICALIZE_HOSTNAME** has been added.

Update-DNS

- **update-dns** can delete address records from the DNS server.

Add Support for Stronger Encryption

- **preferred_enctypes** in the **/etc/krb5.conf** file have been updated to support stronger encryptions.

IMPORTANT!

*This version of AD Bridge includes an upgrade to our Kerberos libraries, which deprecates some legacy cipher suites. Customers who are concerned about support for legacy cipher suites should review the cipher suites listed in the **/etc/krb5.conf** file and perform compatibility testing as necessary.*

Issues Resolved:

- Resolved issue in which the incorrect exit codes were being returned for **setkey-cli**. The correct codes are now returned.
- Resolved issue in which group policy never completed while waiting for user policy to be applied.
- Resolved issue in which AD users were not appearing on the **Access Privileges by User** report.
- Resolved issue where the **pbis-support** pack was not reading **rsyslog** lines correctly.
- Resolved issue where **msiexec** wasn't installing **Group Policy Management**.
- Resolved issue where incorrect operating system versions were appearing in the **Target Platforms** group policy.
- Resolved issue in **automount** seg faults on Debian/rhel/sles.
- Resolved issue in **auto enroll** seg faults on ubuntu.
- Resolved issue in which the local provider reported status *unknown*.
- Resolved issue in **gpupdate —rsop** failed on Debian.
- Resolved issue where root logins events with ssh keys were not being captured.
- Resolved issue where the **reapsysl** service was dead after a reboot.
- Resolved issue where upgrading ADB breaks tenant joins.
- Resolved issue where the Windows installer certificates were expired.

Known Issues:

- None.

Notes:

- AD Bridge 23.2.0.447 supports upgrades from 21.1, 22.1, 22.2, and 22.3.
- RPM x86_64 is now built on RHEL 7.
- RPM PPC is no longer supplied.
- DEB x86_64 is now built on Debian 10.
- Solaris 10 - 11.3 x86/sparc is no longer supplied.
- Solaris 11.4 x86/sparc is the only version of Solaris supported.