Authentication Service and Privilege Elevation Service 5.6.1 (Release 19.9) Release Notes

Table of Contents

1. About This Release

```
Authentication Service and Privilege Elevation Service, part of the
product category Centrify Zero Trust Privilege Services (or previously
called Centrify Infrastructure Services), centralize authentication and
privileged user access across disparate systems and applications by
extending Active Directory-based authentication, enabling use of Windows
Group Policy and Single-Sign-On. With Centrify Zero Trust Privilege
Services, enterprises can easily migrate and manage complex UNIX, Linux
and Windows systems, rapidly consolidate identities into the directory,
organize granular access and simplify administration. Centrify
```

Authentication Service, through Centrify's patented Zone technology, allows organizations to easily establish global UNIX identities, centrally manage exceptions on Legacy systems, separate identity from access management and delegate administration. Centrify's non-intrusive and organized approach to identity and access management results in stronger security, improved compliance and reduced operational costs.

An upgrade application note (/Documentation/centrify-upgrade-guide.pdf) is provided with this release to guide customers who have installed multiple Centrify packages. The document describes the correct order to perform updates such that all packages continue to perform correctly once upgraded. This document is also available online.

The product related release notes and documents are available online at http://docs.centrify.com.

Centrify software is protected by U.S. Patents 7,591,005; 8,024,360; 8,321,523; 9,015,103; 9,112,846; 9,197,670; 9,378,391 and 9,442,962. (Ref: CS-44575)

2. Feature Changes

For a list of the supported platforms by this release, refer to the 'Supported Platforms' section in the Centrify Zero Trust Privilege Services release notes.

For a list of platforms that Centrify will remove support in upcoming releases, refer to the 'Notice of Termination Support' section in the Centrify Zero Trust Privilege Services release notes.

For a complete list of supported platforms in the latest releases, refer to the 'Centrify Zero Trust Privilege Services' section in the document available from www.centrify.com/platforms.

2.1. Feature Changes in Authentication Service and Privilege Elevation Service 5.6.1 (Release 19.9)

General

- Compatibility (Ref: CS-47393)

  This release of Centrify DirectControl Agent for *NIX will work with the following:

  - The latest released Centrify for DB2 and Centrify for Samba. (Ref: CS-44594)

  - Centrify DirectAudit Agent of Release 2017 or later, except

    - On AIX, Linux PowerPC platforms, DirectAudit Agent must be of Release 2017.3 or later. (Ref: CS-44597, CS-44601, CS-44749)

- On Solaris x86 and SPARC platforms, DirectAudit Agent must be of Release 2018 or later. (Ref: CS-44594)

- Centrify OpenSSH of Release 2017 or later, except

  - On Linux PowerPC platforms, all packages must be of Release 2017.3 or later. (Ref: CS-44749, CS-44753)

  - On Solaris x86 and SPARC platforms, Centrify OpenSSH must be of Release 2018 or later. (Ref: CS-44594)

Security Fix

- Fixed a security vulnerability in Access Manager that allowed an attacker to perform remote code execution - related to .NET framework vulnerability detailed in CVE-2012-0161. (Ref: CS-48368)

Centrify DirectControl Agent for *NIX

- Centrify DirectControl Agent's Microsoft Privilege Access Management (PAM) Privilege Escalation feature is enhanced to support single sign-on (SSO) scenario. Note: After the user has been granted elevation and added to the PAMGroup, the user is required to re-obtain a new ticket-granting ticket (TGT) for SSO login. (Ref: CS-45781)

Smart Card

- Centrify DirectControl Agent can now integrate with Citrix Linux Virtual Delivery Agent to support smart card login. (Ref: CS-47942)

Centrify Group Policy Management

- Added the GP mapper script to distribute CA Bundle for AIX and HPUX. (Ref: CS-48055)

Centrify Report Services

- Added the support of using PostgreSQL instead of MS SQL Server as the database for Centrify Report Services. The version of PostgreSQL must be 11 or above. Please note that Centrify reports cannot be used if the database engine is PostgreSQL. (Ref: CS-47790)

2.2. Feature Changes in Authentication Service and Privilege Elevation Service 5.6.0 (Release 19.6)

General

- Open Source component upgrade

  - Centrify cURL is upgraded based on cURL v7.65.0 instead of v7.61.1. (Ref: CS-47453, CS-47973)

- This includes several security fixes, e.g. CVE-2018-16890, CVE-2019-3822, and CVE-2019-3823, CVE-2019-5435, and CVE-2019-5436. For details, please refer to https://curl.haxx.se/docs/security.html.

- Centrify OpenLDAP is upgraded based on OpenLDAP v2.4.47 instead of v2.4.46. (Ref: CS-47385, CS-47614)

  - For changelog details, please refer to https://www.openldap.org/software/release/changes.html.

- Centrify OpenSSH is upgraded based on openssh v7.9p1 instead of v7.7p1. (Ref: CS-46985, CS-47038, CS-47710)

  - This includes several security fixes, e.g. CVE-2018-15473, CVE-2018-20685, CVE-2019-6109, CVE-2019-6110, and CVE-2019-6111. For changelog details, please refer to http://www.openssh.com/releasenotes.html.

- Centrify OpenSSL is upgraded based on OpenSSL v1.1.1b instead of v1.0.2p. (Ref: CS-45107, CS-47441, CS-47447, CS-47768, CS-47796)

  - This includes several security fixes for CVE-2018-0732, CVE-2018-0734, CVE-2018-0735, CVE-2018-0737, CVE-2019-1543. For changelog and vulnerability fix details, please refer to https://www.openssl.org/news/vulnerabilities.html and https://www.openssl.org/news/cl111.txt.

  - Note:

    - This is a major upgrade from v1.0.2 to v1.1.1 which means the internal openssl library and APIs are not backward compatible. Centrify OpenSSH is also upgraded based on openssh v7.9p1 because of this reason.

    - Several algorithms, EVP_sha, EVP_dss, EVP_dss1, EVP_ecdsa, are deprecated in OpenSSL v1.1.1 and hence no longer supported by our products, e.g. adcert, in this release.

    - There is no FIPS mode support in this version. That means, all affected Centrify products will not support FIPS mode in this release. For example, DirectControl agent will ignore the FIPS mode related group policy, 'Use FIPS compliant algorithms for encryption, hashing and signing', and the centrifydc.conf parameter, 'fips.mode.enable'. (Ref: CS-46785, CS-47979)

- Centrify PuTTY is upgraded based on PuTTY v0.71 instead of v0.70. (Ref: CS-47817)

  - This includes several security fixes, e.g. CVE-2019-9894, and CVE-2019-9895, CVE-2019-9896, CVE-2019-9897, and CVE-2019-9898. For details, please refer to https://www.chiark.greenend.org.uk/~sgtatham/putty/changes.html.

- Upgraded Microsoft SQL Server Compact (SQL CE) to v4.0 from v3.5 for Sudoers Import. (Ref: CS-47607)

  - For changelog details, please refer to https://www.microsoft.com/en-us/download/details.aspx?id=17876.

- Upgraded SQLite to v3.28.0 from v3.7.5. (Ref: CS-44014, CS-47996, CS-47967)

  - For changelog details, please refer to https://www.sqlite.org/chronology.html.

- Upgraded URI to v1.74 from v1.60. (Ref: CS-47560)

  - For changelog details, please refer to https://metacpan.org/release/URI.

- Compatibility (Ref: CS-47393)

  This release of Centrify DirectControl Agent for *NIX will work with the following:

  - The latest released Centrify for DB2 and Centrify for Samba. (Ref: CS-44594)

  - Centrify DirectAudit Agent of Release 2017 or later, except

    - On AIX, Linux PowerPC platforms, DirectAudit Agent must be of Release 2017.3 or later. (Ref: CS-44597, CS-44601, CS-44749)

    - On Solaris x86 and SPARC platforms, DirectAudit Agent must be of Release 2018 or later. (Ref: CS-44594)

  - Centrify OpenSSH of Release 19.6. (Ref: CS-45107)

  As Centrify Deployment Manager is already discontinued after Release 18.11, Deployment Manager cannot deploy this release of Centrify DirectControl Agent for *NIX. (Ref: CS-47626)

Security Fix

- N/A

Centrify DirectControl Agent for *NIX

- Added a feature on DirectControl Agent installer for Ubuntu to support the adapter library /lib/i386-Linux-gnu/ which hosts all 32-bit libraries on a 64-bit Ubuntu host. (Ref: CS-47593)

DirectControl Command Line Utilities

- Enhanced adcdiag command with the following:

    - Added the information on how much time a connector probe spent by logging the GMT timestamps when the probe starts and ends for each connector, the timestamp format is like 'Apr 18, 2019 08:28:12(GMT)'. (Ref: CS-47735)
    - Added the support for the parameter 'adclient.cloud.connector' to limit the probing to a specific connector. (Ref: CS-47759)
    - Added time-out to each connector probe attempt. (Ref: CS-47788)
    - Added the option "adcdiag -z" to display the Centrify Identity Platform configurations for the joined zone. (Ref: CS-48049)
    - Added the option "adcdiag -l connectors -I <tenantid>" to show the connectors for the specific tenant ID only. (Ref: CS-48049)
    - Added the qualifier "-d, --visible" for the "-l instances" or "-l connectors" option in adcdiag to show the instances or connectors only if they are visible to DirectControl agent. (Ref: CS-48057)

- Enhanced adcheck command to check for a running nscd and alert users if not. (Ref: CS-47518)

- Added the support for parallel execution of adjoin --precreate command to pre-create computers in a zone during provisioning. (Ref: CS-47237)

- Added the support in 'adjoin' and 'adleave' commands for automatic sasauth PAM configuration update. (Ref: CS-47756)

- Added an option --interactive to adkeytab --adopt command as an alternative to --newpasswd to prevent entering a password in clear text on the command line. (Ref: CS-47483)

    - Example of using option --newpasswd:
      $ adkeytab --adopt -K user1.keytab --local --newpasswd password1 user1
    - Example of using option --interactive:
      $ adkeytab --adopt -K user1.keytab --local --interactive user1
      user1@EXAMPLE.COM's password:

- Added two options to adleave command to remove role assignments from computer zone and computer zone itself when leaving a zone. (Ref: CS-35367, CS-40518)

- -o, --removecomputerzone, to remove computer zone from Active Directory
  - -O, --removemachinescope, to remove Direct Authorize scope from Active Directory

- Added an option -k, --removekeytab to adleave command to remove krb5.keytab file on successful leave. Without this option, adleave will only clean up keytab entries but not remove keytab file. (Ref: CS-29241)

- Added an option --case to adsyncignore command to do case-sensitive comparison to AD user/group names. By default, it will do case-insensitive comparison. (Ref: CS-47907)

- Added an option --dzcache to adsyncignore command for performance improvement. When this option is specified, the adsyncignore command will use the DZ cache from DirectControl agent instead of walking through the zone tree to check user visibility in the joined zone. This can usually improve the performance, especially when there is a lot of role assignments, and a lot of users who have complete Unix profiles but do not have role assigned. Also added two new properties for adsyncignore and similar commands: tool.minuid and tool.mingid. Please refer to the description in Configuration Parameters section below. (Ref: CS-47853)

- DirectControl command line utilities run by non-root users will now write kset files to /tmp instead of /var/centrifydc/user. The directory /var/centrifydc/user is now obsolete. (Ref: CS-31332)

Audit Trail Events

- N/A

Configuration Parameters

Added the following parameters in centrifydc.conf:
- adclient.cloud.connector.subnet.preference.enabled: This parameter specifies whether or not to enable the ability to select subnet preferences when the agent connects to a cloud connector. By default, this option is not enabled (false), which means that the agent selects the cloud connector based on the closest Active Directory site. If you enable this option, the agent selects the cloud connector located in the same subnet as the client within the current Active Directory site, then in different subnets within the current Active Directory site, and then in an Active Directory site that's different than the current one. (Ref: CS-47873)

- adclient.exit.on.incomplete.zone.hierarchy: This parameter specifies whether DirectControl agent should just exit if it fails to load the complete zone hierarchy successfully. The default is false. (Ref: CS-47962)

- adclient.legacyzone.mfa.tenantid: This parameter specifies the Centrify Identity Platform instance ID (tenant ID) for MFA in express, autozone, and classic zones, to locate Centrify connectors. The default is empty, which means DirectControl agent will use adclient.legacyzone.mfa.cloudurl to locate Centrify connectors. (Ref: CS-47807)

- adclient.local.forest.altupn.lookup: This parameter specifies whether or not to enable local forest altupn lookup. The default is true. (Ref: CS-47419)

- krb5.cache.renew.exclusion: This parameter specifies a list of users to be excluded from Kerberos cache renewal. The default is empty. If specified, DirectControl agent will not renew the specified users' Kerberos cache files. (Ref: CS-47690)

- tool.mingid: This parameter specifies the minimum gid number that an AD group will be assigned to. Tools, such as adsyncignore, will consider a group as local and hence will not process it if the corresponding gid is smaller than the specified value. The default is 1000. (Ref: CS-47853)

- tool.minuid: This parameter specifies the minimum uid number that an AD user will be assigned to. Tools, such as adsyncignore, will consider a user as local and hence will not process it if the corresponding uid is smaller than the specified value. The default is 1000. (Ref: CS-47853)

Modified the following parameters in centrifydc.conf:

- adclient.cloud.connector: This parameter specifies the ONLY cloud connector to be used between Centrify-managed *NIX systems and the cloud instance that provides authentication service. The default is not set which means the agent will do automatic discovery of connectors. (Ref: CS-47759)

- pam.mfa.program.ignore: This parameter specifies a list of programs that are not required to do MFA. The default is a list of known programs that do not support MFA. Now we have added wildcard '*' and exception '!' support to this parameter. E.g. '!sudo *' means except 'sudo', all other programs will not require MFA. (Ref: CS-48013)

Please refer to the manual, Configuration and Tuning Reference Guide, for details.

Centrify adedit

- Added an option '-notdelegateanyright' for adedit 'create_zone' command. By default, the switch is false, which means same behavior as before. If the switch is on, 'create_zone' will not set any security descriptor to the newly created zone object. (Ref: CS-47738)

- Added the support of a new zone field 'tenantid' for hierarchical zones in adedit 'get_zone_field' and 'set_zone_field' commands. (Ref: CS-48040)

Centrify OpenSSH

- Added a feature to allow remote root execution of commands without allowing remote login by root. Note: Please contact Centrify Support if you want to use it. (Ref: CS-46647)

- Added a new option GSSAPIKexAlgorithms in ssh_config and sshd_config to specify the list of key exchange algorithms that are accepted by GSSAPI key exchange. Possible values are gss-gex-sha1-, gss-group1-sha1-, gss-group14-sha1-. The default is 'gss-gex-sha1-, gss-group1-sha1-, gss-group14-sha1-'. This option only applies to protocol version 2 connections using GSSAPI. (Ref: CS-47748)

Centrify OpenLDAP Proxy

- N/A

Centrify Access Manager

- Added the console support to manage AIX extended attributes of users, groups, local users, and local groups. (Ref: CS-33865)

- Added the console support for the alternate nisNetGroup from RFC2307 schema. Access Manager now shows one more node named 'NIS NetGroups (RFC2307)' under each zone's 'UNIX Data' node. User could use RFC2307 schema nisNetGroup Active Directory object to manage NIS net groups under this new node for larger groups without worrying about 1024 characters limitation. Sample C# programs and PowerShell scripts are also provided in Centrify Access SDK to show how to manage this feature. Note: The usage of this nisNetGroup is controlled by the parameter 'ldapproxy.netgroup.use.rfc2307nisnetgroup' in the slapd.conf of Centrify OpenLDAP Proxy. (Ref: CS-47449)

- Added the console support in the Platform tab of the Zone Properties page to manage both the Centrify Identity Platform instance (tenant) ID and URL. (Ref: CS-48038)

Centrify Access Module for PowerShell

- Added a switch 'SkipPermissionSetting' in the cmdlet 'New-CdmZone' to not set the security descriptor when creating a zone. Note: This switch does not work on SFU zones yet. (Ref: CS-47737)

- Added a parameter 'Computer' in the cmdlet 'Get-CdmComputerRole' to get a list of computer roles for a specified computer from the zone hierarchy. (Ref: CS-47757)

- Added in the cmdlet 'Set-CdmRoleAssignment' the ability to update the description of a role assignment, and, similarly, in another cmdlet 'Get-CdmRoleAssignment' the ability to get the description of a role assignment. (Ref: CS-47890)

- Added a switch 'OverrideZPA' in the cmdlets 'Remove-CdmUserProfile' and 'Remove-CdmGroupProfile' to allow users to remove user and group profiles when auto-provisioning for profiles is enabled. (Ref: CS-47681)

- Added a parameter 'TenantId' to the cmdlets 'New-CdmZone', 'Set-CdmZone' for users to set the 'TenantId' property for a zone and added a property 'TenantId' to the 'CdmZone' object. (Ref: CS-48039)

Centrify Licensing Service

- N/A

Centrify Group Policy Management

- Added a selection of the populating location in the GPs 'Specify user names to ignore (lookup)' and 'Specify group names to ignore (lookup)' to select whether to populate the user/group names directly into the Centrify DirectControl configuration file or into the user/group ignore files. The default is Centrify Directcontrol configuration file. (Ref: CS-32016)

- On Solaris, added a Group Policy to install AD certificates to standard system certificate store. (Ref: CS-46901)

- On CoreOS, Group Policy is now supported. (Ref: CS-47675)

Centrify Report Services

- N/A

Centrify Zone Provisioning Agent

- Added an event log message to show the summary of a provisioning process. The summary information includes the start time, end time and elapsed time of the provisioning process, the count of objects provisioned and the count of objects deprovisioned. (Ref: CS-47965)

3. Bugs Fixed

3.1. Bugs Fixed in Authentication Service and Privilege Elevation Service 5.6.1 (Release 19.9)

General

- N/A

Centrify DirectControl Agent for *NIX

- Fixed a bug that sometimes automount share returned permission denied using Kerberos ticket generated by Centrify kinit but worked with native kinit, or users got access denied error after migration from Classic to Hierarchical zone. Centrify DirectControl Agent will always generate key entries of all encryption types in krb5.keytab, regardless of the adclient.krb5.tkt.encryption.types setting from centrifydc.conf. Note: There is no FIPS mode support in this version. In future versions that support FIPS mode, there will still be no key entries of non-FIPS-approved encryption types if FIPS mode is enabled. (Ref: CS-47884)

- Fixed a bug that role assignments to groups from a cross-forest one-way trusted domain failed to apply to its members. (Ref: CS-48078)

- Fixed a bug that sometimes DirectControl agent would return incomplete result to queries for a user's unix groups. (Ref: CS-48297)

- Fixed a bug that sometimes DirectControl agent would unnecessarily refresh all zone groups from Active Directory in the background. (Ref: CS-48322)

- Fixed a bug in the command line utility adcert not able to correctly verify the local certificate resulting that DirectControl agent would request a new certificate from Active Directory whenever updating group policies. (Ref: CS-48360)

3.2. Bugs Fixed in Authentication Service and Privilege Elevation Service 5.6.0 (Release 19.6)

General

- N/A

Centrify DirectControl Agent for *NIX

- Fixed a bug where DirectControl agent 'adclient' (or DirectAudit agent 'dad') process running in docker container is stopped when DirectControl (or DirectAudit) is upgraded on docker host. (Ref: CS-47406)

- Fixed a bug where DirectControl agent crashes while resolving group membership for a disabled or locked Active Directory user that has been migrated between domains. (Ref: CS-48164)

- Fixed a bug where DirectControl agent fails to lookup the UNIX group using overriding name in AD name format. (Ref: CS-48424)

- Fixed a bug where MFA fails to perform properly when adclient.cloud.connector parameter is set. (Ref: CS-47876)

- Fixed a bug where users with 'always permit login' role cannot login when DirectControl agent is down in a docker environment. Note: As part of the fix, the location of the file apu.lst has been changed from /etc/centrifydc/apu.lst to /etc/centrifydc/share/apu.lst. (Ref: CS-46600)

- Fixed a bug where some UNIX members of a zone group are missing after those members were moved on AD. (Ref: CS-47781)

- Fixed a bug where the password is shown when entering user password to run a scp command if NSS module is disabled but auditing command for "ssh" is enabled. (Ref: CS-47527)

- Fixed a bug where DirectControl agent during start-up fails to update its data cache related to zone hierarchy changes. (Ref: CS-46307, CS-48021)

DirectControl Command Line Utilities

- Fix a bug in 'adsyncignore' command where it incorrectly uses case-sensitive mode as default when doing comparison with AD user/group names. (Ref: CS-47907)

- Fixed a bug in 'dzinfo' command where it dumps out unnecessary INFO messages. (Ref: CS-35714)

Centrify adedit

- N/A

Centrify OpenSSH

- Fixed a bug where Centrify OpenSSH host-based authentication may fail on some machines. (Ref: CS-47508)

- Fixed a bug where Centrify OpenSSH cannot start up after system reboot. (Ref: CS-48425)

- On Solaris, fixed a bug where /usr/bin/ssh* unexpectedly point back to stock OpenSSH after OS upgrade. (Ref: CS-46934)
  - Now when Solaris SMF starter starts/restarts centrify-sshd, the startup script will update /usr/bin/ssh* symlinks to centrify-openssh client and backup the previous one to /usr/bin/ssh*.pre_cdc.XXXXXX.

Centrify OpenLDAP Proxy

- Fixed a bug where ldapproxy dumps out incorrect ERROR messages in the log like this: '... Attribute has multiple values (31) ...' even when the attribute to search does not have a value. (Ref: CS-46759)

- Fixed a bug where ldapsearch sometimes fails to return all the matches due to an error in the memory cache. (Ref: CS-47522)

- Fixed a bug where ldapsearch -l option sometimes not working. (Ref: CS-47990)

- Fixed a bug where restarting centrify.service sometimes wrongly overwrites the customer settings in /etc/centrifydc/openldap/slapd.conf. (Ref: CS-47652)

Centrify Access Manager

- Fixed a bug where an unexpected exception is thrown if a user refreshes the Computer Roles node when a filter is set on the 2nd/3rd column. (Ref: CS-33961)

- Fixed a bug where Import from UNIX wizard will incorrectly set the GECOS field if the source passwd file has ':' embedded in the GECOS field, e.g. %{u:displayName}. (Ref: CS-34649)

Centrify Access API for Windows

- Fixed a bug with SDK for Windows in creating user profiles via parallel processes where it may lead to duplicated users found in the same zone. (Ref: CS-48011)

Centrify Licensing Service

- Fixed a bug such that creating Directory Control license container in any domain within the entire forest is allowed through the Licensing Service Control Panel. (Ref: CS-47777)

Centrify Group Policy Management

- Fixed a bug where GP is killed for timeout due to the slow download of individual certificate revocation list (crl) files. Now the default timeout parameter 'adsec.crl_getter.timeout' is reduced from 30 seconds to 10 seconds such that individual file download is timeout and can return control back to the GP instead of having the GP killed for timeout. (Ref: CS-46902)

Centrify Report Services

- Fixed a bug in computation where it fails to finish due to data type overflow error. (Ref: CS-47989)

Centrify Zone Provisioning Agent

- Fixed a bug where ZPA will incorrectly use '__u_uid_' as login name during provisioning when the referenced AD attribute is not set. (Ref: CS-42103)

4. Known Issues

The following sections describe common limitations or known issues associated with this Authentication Service and Privilege Elevation Service release.

For the most up to date list of known issues, please login to the Customer Support Portal at http://www.centrify.com/support and refer to Knowledge Base articles for any known issues with the release.

Centrify DirectControl Agent for *NIX

- Known issues with Multi-Factor Authentication (MFA)

  If MFA is enabled but the parameter "adclient.legacyzone.mfa.required.groups" is set to a non-existent group, all AD users will be required for MFA. The workaround is to remove any non-existent groups from the parameter. (Ref: CS-39591b)

- Known issues with AIX

  On AIX, upgrading DirectControl agent from 5.0.2 or older versions in disconnected mode may cause unexpected behavior. The centrifydc service may be down after upgrade. It's recommended not to upgrade DirectControl agent in disconnected mode. (Ref: CS-30494a)

  Some versions of AIX cannot handle user name longer than eight characters. As a preventive measure, we have added a new test case in the adcheck command to check if the parameter LOGIN_NAME_MAX is set to 9. If yes, adcheck will show a warning so that users can be aware of it. (Ref: CS-30789a)

- Known issues with Fedora 19 and above (Ref: CS-31549a, CS-31730a)

  There are several potential issues on Fedora 19 and above:
  1) The adcheck command will fail if the machine does not have Perl installed.
  2) Group Policy will not be fully functional unless Text/ParseWords.pm is installed.

- Known issues with RedHat

  When logging into a RedHat system using an Active Directory user that has the same name as a local user, the system will not warn the user of the conflict, which will result in unpredictable login behavior. The workaround is to remove the conflict or login with a different AD user. (Ref: CS-28940a, CS-28941a)

- Known issues with rsh / rlogin (Ref: IN-90001)

  - When using rsh or rlogin to access a computer that has DirectControl agent installed, and where the user is required to

change their password, users are prompted to change their password twice. Users may use the same password each time they are prompted and the password is successfully changed.

- Known issues with compatibility

  Using DirectControl 4.x agents with Access Manager 5.x (Ref: IN-90001)

  - DirectControl 4.x agents can join classic zones created by Access Manager 5.x. It will ostensibly be able to join a DirectControl 4.x agent to a hierarchical zone as well, but this causes failure later as such behavior is undefined.

  Default zone not used in DirectControl 5.x (Ref: IN-90001)

  - In DirectControl 4.x, and earlier, there was a concept of the default zone. When Access Manager was installed, a special zone could be created as the default zone. If no zone was specified when joining a domain with adjoin, the default zone would be used.

  - This concept has been removed from DirectControl 5.0.0 and later as it is no longer relevant with hierarchical zones. In zoned mode, a zone must now always be specified.

  - A zone called "default" may be created, and default zones created in earlier versions of Access Manager may be used, but the name must be explicitly used.

Smart Card

- Smart Card is not supported on RHEL 8 yet due to the underlying OS infrastructure changes. (Ref: CS-48087)

- Release 18.8 includes an update to Coolkey to support Giesecke & Devrient 144k, Gemalto DLGX4-A 144, and HID Crescendo 144K FIPS cards. However, this has caused known issues that may cause CAC cards to only work sporadically. A workaround for CAC cards is to wait for it to prompt for PIN and Welcome, without removing the card, and then try again. (Ref: CC-58013)

- There is a Red Hat Linux desktop selection issue found in RHEL 7 with smart card login. When login with smart card, if both GNOME and KDE desktops are installed, user can only log into GNOME desktop even though "KDE Plasma Workspace" option is selected. (Ref: CS-35125a)

- On RHEL 5.10 and 5.11, if "Smart Card Support" is enabled and a smartcard is inserted on the login screen, a PIN prompt may not show up until you hit the "Enter" key. The workaround is to replace

libsoftokn3.so with the old one on RHEL 5.9, which is a shared object file in NSS package. (Ref: CS-35038a)

- On RHEL 5.10 and 5.11, if "Smart Card Support" is enabled and "Card Removal Action" is configured as "Lock", the screen will be locked several seconds after login with smart card. The workaround is to replace libsoftokn3.so with the old one on RHEL 5.9, which is a shared object file in NSS package. (Ref: CS-33871a)

- When a SmartCard user attempts to login on Red Hat 6.0 with a password that has expired, the authentication error message may not mention that authentication has failed due to an expired password. (Ref: CS-28305a)

- On RedHat, any SmartCard user will get a PIN prompt even if he's not zoned, even though the login attempt will ultimately fail. This is a divergence from Mac behavior - On Mac, if a SmartCard user is not zoned, Mac doesn't even prompt the user for PIN. (Ref: CS-33175c)

- If a SmartCard user's Active Directory password expires while in disconnected mode, the user may still be able to log into their machine using their expired password. This is not a usual case, as secure SmartCard AD environments usually do not allow both PIN and Password logins while using a Smart Card. (Ref: CS-28926a)

- To login successfully in disconnected mode (Ref: CS-29111a):
    - For a password user:
        - A password user must log in successfully once in connected mode prior to logging in using disconnected mode. (This is consistent with other DirectControl agent for *NIX behavior)
    - For a SmartCard user:
        - The above is not true of SmartCard login. Given a properly configured RedHat system with valid certificate trust chain and CRL set up, a SmartCard user may successfully login using disconnected mode even without prior successful logins in connected mode.
        - If certificate trust chain is not configured properly on the RedHat system, the SmartCard user's login attempt will fail.
        - If the SmartCard user's login certificate has been revoked, and the RedHat system has a valid CRL that includes this certificate, then the system will reject the user.

- After upgrading from DirectControl version 5.0.4 to version 5.1, a Smartcard user may not be able to login successfully. The workaround is to run the following CLI commands:

  ```
  sudo rm /etc/pam_pkcs11/cacerts/*
  sudo rm /etc/pam_pkcs11/crls/*
  sudo rm /var/centrify/net/certs/*
  ```

then run adgpupdate. (Ref: CS-30025c)

- When CRL check is set via Group Policy and attempting to
  authenticate via Smartcard, authentication may fail. The workaround
  is to wait until the Group Policy Update interval has occurred and
  try again or to force an immediate Group Policy update by running
  the CLI command adgpupdate. (Ref: CS-30090c)

- After upgrading from DirectControl agent Version 5.0.4 to version
  5.1.1, a SmartCard user may not be able to authenticate
  successfully. The workaround is to perform the following CLI command
  sequence:

      sctool -d
      sctool -e
      sudo rm /etc/pam_pkcs11/cacerts/*
      sudo rm /etc/pam_pkcs11/crls/*
      sudo rm /var/centrify/net/certs/*"
      adgpupdate

      and then re-login using the SmartCard and PIN. (Ref: CS-30353c)

- A name-mapping user can unlock screen with password even though the
  previous login was with PIN. (Ref: CS-31364b)

- Need to input PIN twice to login using CAC card with PIN on RedHat.
  It will fail on the first input but succeed on the second one. (Ref:
  CS-30551c)

- Running "sctool –D" with normal user will provide wrong CRL check
  result. The work-around is to run it as root. (Ref: CS-31357b)

- Screen saver shows password not PIN prompt (Ref: CS-31559a)

  Most smart card users can log on with a smart card and PIN only and
  cannot authenticate with a user name and password. However, it is
  possible to configure users for both smart card/PIN and user
  name/password authentication. Generally, this set up works
  seamlessly: the user either enters a user name and password at the
  log on prompt, or inserts a smart card and enters a PIN at the
  prompt.

  However, for multi-user cards, it can be problematic when the screen
  locks and the card is in the reader. When a user attempts to unlock
  the screen, the system prompts for a password, not for a PIN,
  although the PIN is required because the card is in the reader. If
  the user is not aware that the card is still in the reader and
  enters his password multiple times, the card will lock once the
  limit for incorrect entries is reached.

  On RHEL 7, an authenticated Active Directory user via smart card
  cannot login again if the smart card is removed.   This is due to a

bug in RHEL 7, https://bugzilla.redhat.com/show_bug.cgi?id=1238342. This problem does not happen on RHEL6. (Ref: CSSSUP-6914c)

Centrify Report Services

- The SQL Server Availability Group feature in SQL Server 2012 is not supported. (Ref: CS-39674a)

5. Additional Information and Support

In addition to the documentation provided with this package and on the web, you can find the answers to common questions and information about any general or platform-specific known limitations as well as tips and suggestions from the Centrify Knowledge Base.

The Centrify Resources web site provides access to a wide range of information including analyst report, best practice brief, case study, datasheet, ebook, white papers, etc., that may help you optimize your use of Centrify products. For more information, see the Centrify Resources web site:

www.centrify.com/resources

You can also contact Centrify Support directly with your questions through the Centrify Web site, by email, or by telephone. To contact Centrify Support or to get help with installing or using this software, send email to support@centrify.com or call 1-669-444-5200, option 2. For information about purchasing or evaluating Centrify products, send email to info@centrify.com.