Authentication Service and Privilege Elevation Service 5.7.0 (Release 2020) 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 5.7.0 (Release 2020)

General

- Open Source component upgrade
    - Centrify cURL is upgraded based on cURL v7.70 from v7.65.0. (Ref: CS-48004)
        - This includes several security fixes. For details, please refer to https://curl.haxx.se/docs/security.html.

    - Centrify OpenLDAP is upgraded based on OpenLDAP v2.4.50 from v2.4.47. (Ref: CS-48161)

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

    - Centrify OpenSSH is upgraded based on openssh v8.2 from v7.9p1. (Ref: CS-47903)

        - This includes several security fixes and potentially incompatible changes, e.g. removal of 'ssh-rsa'(RSA/SHA1) algorithm from those accepted for certificate signatures (i.e. the client and server CASignatureAlgorithms option). For changelog details, please refer to http://www.openssh.com/releasenotes.html.

        - This also fixed the issue of running Centrify OpenSSH on Fedora 30 or above. (Ref: CS-47895)

        - This also fixed the compatibility issue with RHEL 8 crypto-policies package. (Ref: CS-48603)

        - Note that with this upgrade, Centrify OpenSSH does not support the use of 'Use PAM no' anymore. (Ref: CS-48603)

    - Centrify OpenSSL is upgraded based on OpenSSL v1.1.1g from v1.1.1b. (Ref: CS-47986)

        - For changelog and vulnerability fix details, please refer to https://www.openssl.org/news/vulnerabilities.html and https://www.openssl.org/news/cl111.txt.

    - Centrify PuTTY is upgraded based on PuTTY v0.73 from v0.71. (Ref: CS-48152)

        - This includes several security fixes. For details, please refer to https://www.chiark.greenend.org.uk/~sgtatham/putty/changes.html.

    - Upgraded SQLite to v3.31.1 from v3.28.0. (Ref: CS-48474)

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

    - Upgraded TCL to v8.6.10 from v8.5.x. (Ref: CS-27205)

        - For changelog details, please refer to http://www.tcl.tk/software/tcltk/8.6.html.

- Packaging change

    - On Solaris, the 64-bit executables are now placed in the appropriate directories. In x86 packages, it is "bin/amd64", while in sparc packages, it is "bin/sparcv9". Because of these changes, all Solaris packages have to be upgraded together. For example, you cannot install prior version of CentrifyDC package and install this version of CentrifyDC-openssh package. (Ref: CS-45176)

  - Added the support for IPS packaging format for Solaris 11. The new packages are centrify-infrastructure-services-2020-sol11-i386.tgz, and centrify-infrastructure-services-2020-sol11-sparc.tgz. (Ref: CS-48186, CS-48707)

- Compatibility (Ref: CS-48610)

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

  - 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)

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

  On Solaris, you need to upgrade all packages to Release 2020. E.g. this release of Centrify DirectControl Agent for *NIX will not work with old versions of adbindproxy package, DirectAudit Agent, Centrify OpenSSH, etc., as the location of 64-bit executables is changed (e.g. 'bin/amd64' for x86, and 'bin/sparcv9' for sparc). (Ref: CS-45176)

  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 in DirectControl agent a periodic update of the following information to 'postalAddress' attribute of the computer object in Active Directory, e.g. current domain controller, current connector, update timestamp, adclient process elapse time, computer up time, and connector up time. The adjoin command also adds 'join time' to the attribute. Users can use this information for quick cloud deployment. Note: the update interval is controlled by the configuration parameter 'adclient.deploy.report.update.interval'. (Ref: CS-42377, CS-48372)

- Also added in DirectControl agent a heartbeat (INFO) message to syslog in this format, 'WATCH HostName: <Local host name> DomainName: <Joined to domain> JoinAs: <joined as> PreWin2kName: <pre-win2k name> CurrentDC: <current dc> PreferredSite: <prefered site> Zone: <zone name> LastPasswordSet: <last password set> Mode: <CentrifyDC mode> LicensedFeature: <Licensed Features>'. The interval is configurable through Group Policy, with default to 0 to disable the message. This message is useful in Analytics, and SIEM software to monitor the healthiness of the agent. (Ref: CS-46731)

- Added a new feature to assist users to manage 'external' keytabs that contain SPN keys. After successful password change and krb.keytab update, DirectControl agent will launch an optional user process/command to do user-specified action, controlled by the configuration parameter, 'adclient.krb5.password.change.hook'. Also enhanced the adkeytab command with a new option '-o/--copy' to copy the specified keys from an input keytab file into an output keytab file based on specified SPN. This can be useful to users as base to create script to manage their keytab file in their own way. See adkeytab man page for details. (Ref: CS-48384)

- Added the capability of smart connector and domain controller selection by using the next_closest_site, controlled by a new configuration parameter 'adclient.next.closest.site.lookup.enabled'. Please refer to 'KB-14229 Methods used by the Centrify agent when selecting a connector' for details. (Ref: CS-48458, CS-33977)

- Added the capability in DirectControl watch dog to emit alert when adclient CPU consumption is too high. See below for the configuration parameters. (Ref: CS-48467)

- Added a new feature in Multi-Factor Authentication (MFA) policy for Linux, UNIX and Windows Servers to respect MFA profile pass-through duration. You may choose to apply this pass-through duration base on source and/or target. Once it is enabled, one will not be re-prompted for MFA credentials if one has successfully done MFA within a set duration. (Ref: CS-48711)

DirectControl Command Line Utilities

- Enhanced dzdo command with the following:

    - Added the support of dzdo on Fedora 30 or above. (Ref: CS-47892)

Audit Trail Events

- N/A

Configuration Parameters

Added the following parameters in centrifydc.conf:

- adclient.deploy.report.update.interval: This parameter specifies the interval in hours for DirectControl agent to update some useful statistics information to the computer object in Active Directory, such as current domain controller, current connector, adclient process elapse time, computer up time, DC update timestamp, and connector update timestamp. (Ref: CS-48372)

- adclient.gc.locator.shortcut: This parameter specifies whether or not to use a shortcut to Global Catalog. By default, this option is not enabled (false), which means that the agent connects to GC through normal channel. If you enable this option, the agent checks if the currently connected Domain Controller is also a GC and uses it if yes. (Ref: CS-47786)

- adclient.heartbeat.interval: This parameter specifies the interval in minutes for DirectControl agent to emit heartbeat INFO message to syslog. The default is 0, which means this feature is disabled. (Ref: CS-46731)

- adclient.krb5.password.change.hook: This parameter specifies the full path of the command that will be executed after DirectControl agent successfully changed the password and updated the krb5.keytab file. The default is empty string, which means no extra command will be executed. (Ref: CS-48384)

- adclient.next.closest.site.lookup.enabled: This parameter specifies whether to enable the 'Try Next Closest Site' feature. The default is true, which means DirectControl agent will try to use the domain controller from the next closest site if no domain controller available in the same site. (Ref: CS-33977)

- adclient.watch.cpu.utilization.info.threshold: This parameter specifies the threshold value that cdcwatch will write a INFO message when adclient's CPU usage is higher than this value. The default is -1, which means no threshold is set. (Ref: CS-48467)

- adclient.watch.cpu.utilization.warning.threshold: This parameter specifies the threshold value that cdcwatch will write a WARN message when adclient's CPU usage is higher than this value. The default is -1, which means no threshold is set. (Ref: CS-48467)

- dzdo.use_pty: This parameter specifies whether dzdo will run commands in a pseudo-tty or not. The default is false. (Ref: CS-47464)

Modified the following parameters in centrifydc.conf:

- N/A

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

Centrify adedit

- Added a new option '-notdelegateanyright' in 'precreate_computer' command. When this option is specified, the command will not set the security descriptor when creating a computer object. (Ref: CS-48687)

Centrify Access Manager

- Added a column 'Agent Version' in Access Manager. Users can now see the agent version without running a report. (Ref: CS-48554)

- Access Manager can now manage local Windows users and groups. PowerShell cmdlets, and audit trail events are also available for local Windows accounts management. For details, please refer to Administrator’s Guide for Windows. (Ref: CS-46257, CS-47714, CS-47715, CS-47716, CS-47717, CS-47724)

Centrify Access Module for PowerShell

- Added a new switch 'SkipPermissionSetting' in 'New-CdmManagedComputer' command to not set the security descriptor when creating a computer object. (Ref: CS-48670)

- Added the support of DN/SID/<samAccountName>@<domain>/ADComputer to the command 'Get-CdmComputerRole -Computer'. (Ref: CS-48086)

Centrify Windows SDK

- The following methods are added to the Centrify Access API. These methods are used to pre-create computers or computer zones without delegating permission. (Ref: CS-48966)
  1) IHierarchicalZoneComputer PrecreateComputerZone(string dnsName, DirectoryEntry trustee, bool skipPermissionSetting);
  2) IComputer PrecreateWindowsComputer(DirectoryEntry adComputerEntry, bool skipPermissionSetting);
  3) IComputer PrecreateComputer(DirectoryEntry adComputerEntry, string[] spn, DirectoryEntry trustee, bool skipPermissionSetting);
  4) IComputer PrecreateComputer(DirectoryEntry containerEntry, string cn, string dnsName, string[] spn, DirectoryEntry trustee, bool skipPermissionSetting);

Centrify Group Policy Management

- The group policy 'Computer Configuration' -> 'Windows Settings' -> 'Security Settings' -> 'Public Key Policies' -> 'Trusted Root Certification Authourities' (i.e. group policy script, certgp.pl) is enhanced to validate and not install expired CA certificates. (Ref: CS-48597)

Centrify Licensing Service

- Added a new 'Joined Time' field to Licensing Report to show when a computer has joined. (Ref: CS-42362, CS-42377, CS-42383)

- Added the zip feature to Licensing Report notification email. When the size of a Licensing Report is larger than the specified value of the registry key 'ReportNotificationCompressionThreshold' (Path: HKLM\SOFTWARE\Centrify\Licensing Service; Type: DWORD; default value: 10 MB), the report will be compressed into a zip file before sending out as the attachment in the notification email. (Ref: CS-48479)

Centrify OpenLDAP Proxy

- Added the support in systemd configuration to automatically restart Centrify OpenLDAP Proxy when it crashes. (Ref: CS-48355)

Centrify OpenSSH

- N/A

Centrify Report Services

- N/A

Centrify Smart Card

- Added the support of smart card login on RHEL 8. (Ref: CS-48087)

Centrify Zone Provisioning Agent

- Enhanced the logic to tolerate slow network. When accessing the Active Directory objects, the maximum tolerance before logging a performance warning in the Centrify logs is now configurable with a default value of 8 seconds. (Ref: CS-47172, CS-47173)

2.2. 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)

3. Bugs Fixed

3.1. Bugs Fixed in Authentication Service and Privilege Elevation Service 5.7.0 (Release 2020)

General

- Fixed an issue in the package description for some architectures on Linux platforms. (Ref: CS-48559)

- Added the required additional perl module check in rpm spec files so that if users install DirectControl via rpm and not via install.sh, it will also alert users about the missing modules too. (Ref: CS-48570)

Centrify DirectControl Agent for *NIX

- Fixed an issue that the group refresh background task cannot stop when adclient is shutting down causing intermittent missing cache information during reboot. (Ref: CS-48637)

- Fixed an issue that when DirectControl searches for available cloud connectors, it will try to extend the cloud connector computer object, and this may result in showing a warning message if no GC is connectable. The DirectControl now do not extend the computer object, thus no more warning message in that case. (Ref: CS-48023)

- Fixed an issue in large cache environment that may cause high CPU usage on various servers due to force refresh of group members. We now have an option to restore the old behavior. (Ref: CS-48675, CS-48526)

- Fixed an issue on MFA login failure due to intermittent SSL connection error caused by dead connector. (Ref: CS-47264)

- Fixed an issue of an unnecessary ERROR message complaining about no cloud connector in a domain where MFA is not even used. (Ref: CS-48694)

- Fixed an unnecessary warning message in the log '… WARN util.fbbuf FBBufCtrl - bAlloc failed: Insufficient space'. (Ref: CS-48314)

- Fixed an issue which caused failure to perform offline login due to cache flushed after adclient crashed. (Ref: CS-48373)

- Changed the default behavior in MFA such that experimental features are disabled. (Ref: CS-49018)

- Fixed an issue on AIX in configuration update script causing zoned user login failure after OS upgrade and DirectControl installation. (Ref: CS-48482)

- Fixed an issue on AIX in the logic in loading computer roles if custom attribute is used causing users not showing up. (Ref: CS-48183)

- Fixed an issue on AIX that 'lsuer ADUSER' command returns the primary group twice. (Ref: CS-48850)

- Added SELinux rules to bypass domain_can_mmap_files check on RHEL8. (Ref: CS-48545)

- Fixed an issue on HPUX not able to create Kerberos cache file causing user ssh login to fail. (Ref: CS-48221)

- Fixed an issue on RHEL7 such that the authentication will simply exit when hitting CTRL-C at password prompt even with MFA enabled. (Ref: CS-48118)

DirectControl Command Line Utilities

- Fixed an issue that adcert failed the 'verify certificate check' even there existed one good CA cert. (Ref: CS-33681)

- Fixed an issue that dzdo cannot get the correct status from dzcheck.sample if dzcheck.sample is interrupted by signal. (Ref: CS-48982)

Centrify adedit

- N/A

Centrify OpenSSH

- Fixed an issue that Single-Sign-On may fail in some cases. (Ref: CS-48547)

- Fixed an issue that Single-Sign-On fails when you map root to AD user using gssapi-keyex as preferred authentication. (Ref: CS-48738)

- Fixed the format of the parameter 'loginGraceTime' to be consistent with stock openssh. (Ref: CS-48583)

Centrify OpenLDAP Proxy

- Fixed an issue that caused the LDAP proxy to crash due to incorrect RootDSE search filter. (Ref: CS-48311)

Centrify Access Manager

- Fixed a display issue found in Access Manager console when the target system has Korean Windows 2016 Server installed that the option of 'Require multi-factor authentication' in the 'Run As' tab got hidden when creating new Windows Application in 'Applications' under 'Windows Right Definitions'. (Ref: CS-48631)

- Fixed an issue that the column 'Joined To Zone' shows 'Y' even though the computer is not yet joined to the zone after pre-creating the computer. (Ref: CS-34775)

- Fixed an issue in Export/Import Wizard that caused missing Unix command settings. (Ref: CS-48286)

Centrify Access Module for PowerShell

- The switch 'SkipPermissionSetting' in the cmdlet 'New-CdmZone' now also works on SFU zones. (Ref: CS-48028)

- Fixed an issue that 'Get-CdmEffectiveGroupProfile' returns all the UNIX group profiles with the same name or GID on a specified computer even though the profiles may be in conflict. A new switch parameter 'ExcludeConflictedGroup' is introduced to filter out those group profiles with the name or GID conflicting. (Ref: CS-48708)

Centrify Licensing Service

- N/A

Centrify Group Policy Management

- Fixed an issue on Solaris that the group policy script incorrectly copies a certificate into system cert store again even if it is already there. (Ref: CS-48359)

- Fixed an issue on group policy that the /etc/centrifydc/user.ignore and /etc/centrifydc/group.ignore files may be altered even if the user/group ignore GP is unconfigured. (Ref: CS-48851)

- Fixed an issue on SELinux setting that caused GNOME3 GPO settings not able to be applied. (Ref: CS-48522)

Centrify Report Services

- Fixed a validation error message to make it more user-friendly when the server name and port number format of the existing SQL database in user input URI in Report Services Configuration Wizard is invalid. (Ref: CS-48151)

Centrify Zone Provisioning Agent

- Fixed an issue that Zone Provisioning Agent cannot provision user profiles when the parameter 'GecosOption' is not set by Set-CdmZpaSetting. (Ref: CS-48799)

3.2. 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)

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

- 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-58013a)

- 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.