

Centrify Authentication Service and Centrify Privilege Elevation Service 5.5.2 (Release 18.11) Release Notes

© 2004-2018 Centrify Corporation.
This software is protected by international copyright laws.
All Rights Reserved.

Table of Contents

1. About This Release.....	3
2. Feature Changes.....	3
2.1. Feature Changes in Centrify Authentication Service and Centrify Privilege Elevation Service 5.5.2 (Release 18.11)	4
General.....	4
Security Fix.....	5
Centrify DirectControl Agent for *NIX	5
Centrify adedit	7
Centrify OpenSSH	7
Centrify OpenLDAP Proxy	7
Centrify Access Manager.....	7
Centrify Access Module for PowerShell	8
Centrify Licensing Service	8
Centrify Group Policy Management.....	8
Centrify Report Services.....	8
Centrify Zone Provisioning Agent.....	8
2.2. Feature Changes in Centrify Authentication Service and Centrify Privilege Elevation Service 5.5.1 (Release 18.8)	9
General.....	9
Security Fix.....	10

Centrify DirectControl Agent for *NIX	10
Centrify OpenSSH	14
Centrify OpenLDAP Proxy	14
Centrify Access Manager.....	14
Centrify Licensing Service	14
Centrify Group Policy Management.....	14
Centrify Report Services.....	14
Centrify Zone Provisioning Agent.....	14
3. Bugs Fixed	15
3.1. Bugs Fixed in Centrify Authentication Service and Centrify Privilege Elevation Service 5.5.2 (Release 18.11)	15
General.....	15
Centrify DirectControl Agent for *NIX	15
Centrify adedit	16
Centrify OpenSSH	16
Centrify OpenLDAP Proxy	16
Centrify Access Manager.....	16
Centrify Access API for Windows	16
Centrify Licensing Service	16
Centrify Group Policy Management.....	16
Centrify Report Services.....	16
Centrify Zone Provisioning Agent.....	17
3.2. Bugs Fixed in Centrify Authentication Service and Centrify Privilege Elevation Service 5.5.1 (Release 18.8)	17
General.....	17
Centrify DirectControl Agent for *NIX	17
Centrify OpenSSH	18
Centrify OpenLDAP Proxy	18
Centrify Access Manager.....	18
Centrify Access API for Windows	18
Centrify Licensing Service	18
Centrify Group Policy Management.....	19

Centrify Report Services.....	19
Centrify Zone Provisioning Agent.....	20
Centrify adedit	20
4. Known Issues.....	20
Centrify DirectControl Agent for *NIX	20
Smart Card	21
Centrify Report Services.....	24
5. Additional Information and Support.....	24

1. About This Release

Centrify Authentication Service and Centrify Privilege Elevation Service (part of the product category 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 Infrastructure 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 Centrify Infrastructure Services 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 Infrastructure 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 Infrastructure Services release notes.

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

2.1. Feature Changes in Centrify Authentication Service and Centrify Privilege Elevation Service 5.5.2 (Release 18.11)

General

- Open Source component upgrade
 - Centrify curl is upgraded based on curl 7.61.1 instead of 7.61.0. (Ref: CS-47114)
 - This includes security fixes for CVE-2018-14618. For details, please refer to <https://curl.haxx.se/docs/security.html>.
 - Centrify OpenSSL is upgraded based on OpenSSL 1.0.2p instead of 1.0.2o. (Ref: CS-46958, CS-45793)
 - This includes security fixes for CVE-2018-0732, and CVE-2018-0737. For details, please refer to <https://www.openssl.org/news/vulnerabilities-1.0.2.html> and <https://www.openssl.org/news/cl1102.txt>.
- 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

- N/A

Centrify DirectControl Agent for *NIX

- Added support of SMB3 in Centrify SMB stack. This enables the agent to retrieve group policies or files from SMB shares on Windows 8, Windows 2012 or above that requires data encryption. (Ref: CS-30935)
- Implemented mechanisms to prevent forged host ticket (aka. "silver ticket" attack). To prevent PAC spoofing, a new setting, `krb5.pac.validation`, is added to configure whether Agent should validate PAC in the user ticket with KDC before using the information such as user's group membership in the PAC. By default, PAC validation is disabled. (Ref: CS-39827)
- Extended the NSS support for mail aliases on zone enabled AD users. (Ref: CS-45499)
- Enhanced the Multi-Factor Authentication performance to prefer connectors in the same subnet and then in the same Active Directory site. This enhancement does not apply to AIX platforms. (Ref: CS-45588)
- Added an option to ignore 'gid override' of the primary group when checking for primary group members. (Ref: CS-46835)
- Added a provision to support alternate password hash for Solaris disabled users. (Ref: CS-47275)
- Added the support for MIT Kerberos commands or programs linked with MIT Kerberos library (release 1.13 or above) to inter-operate with Centrify KCM service on Solaris platforms. (Ref: CS-46466)

DirectControl Command Line Utilities

- Added the support of the command "`adinfo -y domain`" to print out the domain prefix IDs by which DirectControl algorithm uses to generate unique UNIX user (UID) and group (GID) IDs. This new feature is to allow users to better control how the UIDs/GIDs are generated in relation to a domain (SID) and it is only for hierarchical zones. (Ref: CS-46478)
- Added a new option "`-I, --noprompt`" to "`adjoin`" and "`adleave`" commands. If there are no credentials found, when this option is

specified, the command will not prompt for password and just fails.
(Ref: CS-46695)

Audit Trail Events

- Added new "dzdo" audit trail events for dzdo command execution starts/ends. With these new audit trail events, users can determine how long an elevated privilege command has run. (Ref: CS-45228)
- Added new "Kerberos" audit trail events for KCM Kerberos credential access. (Ref: CS-44042)
- Added new "PAM" audit trail events for user logins to the system in rescue mode. (Ref: CS-45603)

Configuration Parameters

Added the following parameters in centrifydc.conf:

- `adclient.krb5.conf.domain_realm.any_site`: The `krb5.conf [realm]` section is updated with information of KDC's from the preferred site. Setting this parameter to true will extend this to include all reachable KDC's regardless of site. The default is false. (Ref: CS-47422)
- `audittrail.<product>.<component>.overrides`: Please refer to the description for `audittrail.<product>.<component>.targets` below. (Ref: CS-46740)
- `audittrail.<product>.<component>.targets`: This parameter and `audittrail.<product>.<component>.overrides` together allow users to enable/disable audit trail events per product/component. Note: Please refer to documentation for the complete list of product and component (also called category). Please also replace any space in product/component name with '_' when specifying the parameters. The value for product/component overrides or targets setting is a bit mask same usage as in `audittrail.targets`. There is no default value for product/component targets setting, and the default value for product/component overrides is '0', meaning that this product/component observes the global setting. (Ref: CS-46740)
- `krb5.pac.validation`: When performing credential verification, a service ticket is fetched for the local system. After the credential is verified, the PAC information in the service ticket will be used by the local system. Before using the user's PAC, user can select to verify if the PAC is from a trusted KDC to prevent a well-known "silver ticket" attack. This setting takes effect when `krb5.verify.credentials` is true or when DirectControl is using user's PAC from a service ticket. However, this setting does not apply to PAC retrieved using S4U2Self protocol. There are 3 possible values:
 1. disabled (default) - No PAC Validation will be done at all.
 2. enabled - If PAC Validation fails, PAC is still used, and user login is allowed.

3. enforced - If PAC Validation fails, PAC is discarded, and user login is denied.

Note: Setting this to enabled/enforced will have significant impact on user login and user's group fetch performance. (Ref: CS-39827, CS-46564)

- `nss.alias.source`: This parameter specifies the source to look up aliases. There are three possible values: `nismaps`, `mail`, and `proxyaddress`. The default is `nismaps` which means the logic will look up alias from NisMaps. If you want to look up alias from zone enabled AD user objects, you have the option of either by the attribute `"mail"` or `"proxyaddresses"`. Note: AD users with empty `"mail"/"proxyAddresses"` are considered as invalid alias entries even if users exist and are zone enabled. To use the attribute `"proxyaddresses"`, you need to include it in the `adclient.custom.attributes.user` parameter since it is a custom attribute; otherwise it will fall back to `"nismaps"`. (Ref: CS-45499)

There is no parameter changed in, or removed from, `centrifydc.conf` in this release.

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

Centrify adedit

- Added a new command `"forest_from_domain"` in the command utility `"adedit"`. It can be used to get the forest name given a domain name. (Ref: CS-46628)
- Added the support of `"sid2iddomainmap"` field in the commands `"set_zone_field"` and `"get_zone_field"` for the domain prefix IDs by which DirectControl algorithm uses to generate unique UNIX user (UID) and group (GID) IDs. Also added a new option `"-domainidmap"` in the commands `"sid_to_uid"` and `"sid_to_id"` to support the generation of UID/GID with the new algorithm. This new feature is to allow users to better control how the UIDs/GIDs are generated in relation to a domain (SID) and it is only for hierarchical zones. (Ref: CS-46213)

Centrify OpenSSH

- N/A

Centrify OpenLDAP Proxy

- Added the support of the critical search extension flag `('!')` with `pagedResults` control (e.g. `-E '!pr=50'`) on LDAP search results. (Ref: CS-46512)

Centrify Access Manager

- Added the support in zone property pages to allow users to specify the domain prefix IDs by which DirectControl algorithm uses to generate unique UNIX user (UID) and group (GID) IDs. This new feature is to allow users to better control how the UIDs/GIDs are generated in relation to a domain (SID) and it is only for hierarchical zones. (Ref: CS-46192)

Centrify Access Module for PowerShell

- Added a new parameter, "SidToIdDomainMap", in the cmdlets, "New-CdmZone" and "Set-CdmZone", to allow users to specify the domain prefix IDs by which DirectControl algorithm uses to generate unique UNIX user (UID) and group (GID) IDs. This new feature is to allow users to better control how the UIDs/GIDs are generated in relation to a domain (SID) and it is only for hierarchical zones. (Ref: CS-46174)

Centrify Licensing Service

- N/A

Centrify Group Policy Management

- N/A

Centrify Report Services

- Added the capability in Centrify Report Services Configuration Wizard to deploy Centrify reports onto any accessible SQL Service Reporting Services. (Ref: CS-46219)
- Packaged Microsoft SQL Server 2016 Express with Advanced Services SP2 for Centrify Report Services in Centrify Infrastructure Services ISO. (Ref: CS-40928)
- Improved the performance of resolving computer roles applicable to the joined computer. (Ref: CS-46559)

Centrify Zone Provisioning Agent

- Added in provisioning profiles the support of the domain prefix IDs by which DirectControl algorithm uses to generate unique UNIX user (UID) and group (GID) IDs. This new feature is to allow users to better control how the UIDs/GIDs are generated in relation to a domain (SID) and it is only for hierarchical zones. (Ref: CS-46173)

2.2. Feature Changes in Centrify Authentication Service and Centrify Privilege Elevation Service 5.5.1 (Release 18.8)

General

- Open Source component upgrade
 - Centrify curl is upgraded based on curl 7.61.0 instead of 7.58.0. (Ref: CS-45501, CS-45495, CS-45496, CS-45497, CS-46015, CS-46016)
 - This includes security fixes for CVE-2018-0500, CVE-2018-1000120, CVE-2018-1000121, CVE-2018-1000122, CVE-2018-1000300, CVE-2018-1000301. For details, please refer to <https://curl.haxx.se/docs/security.html>.
 - Centrify OpenSSH is upgraded based on OpenSSH 7.7p1 instead of 7.6p1. (Ref: CS-45683)
 - This is primarily a bug fix release. This release also removes the compatibility support for some very old SSH implementations, including ssh.com <=2.* and OpenSSH <= 3.*. For details, please refer to <http://www.openssh.com/releasesnotes.html>.
 - Centrify OpenSSL is upgraded based on OpenSSL 1.0.2o instead of 1.0.2n. (Ref: CS-45643)
 - This includes security fixes for CVE-2018-0739. For details, please refer to <https://www.openssl.org/news/vulnerabilities-1.0.2.html> and <https://www.openssl.org/news/cl102.txt>.
- Product packaging changes
 - Starting this release, Centrify Infrastructure Services product structure has changed: (Ref: CS-46233)
 - The product previously called Centrify Identity Broker Service is now called Centrify Authentication Service, to align with other product offerings.
 - The release numbering scheme now aligns with other Centrify products. This release is now called 18.8.
 - The bundle filename convention is also changed to Centrify-Infrastructure-Services-18.8-<product>.iso/zip for Windows bundles and centrify-infrastructure-services-18.8-<platform>.tgz for *nix bundles.
 - The DirectControl agent package (CentrifyDC) for CoreOS is now split into 4 packages: CentrifyDC-openssl, CentrifyDC-openldap,

CentrifyDC-curl, and CentrifyDC, just like the DirectControl agent packages on all other platforms. Note: if you are doing upgrade from Release 2018, you should use the umbrella installer, install.sh, and it will take care of the dependent packages. (Ref: CS-44417, CS-46752)

- Added a new plug-in package, CentrifyDC-cifsidmap, for Linux platforms to support the cifs-utils utility which provides the mapping of Active Directory User/Group to the corresponding zone enabled UIDs/GIDs in Common Internet File System (CIFS) support. (Ref: CS-44864)
- Compatibility

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 DirectSecure Agent of Release 2017.2 or later, except
 - On Solaris x86 and SPARC platforms, DirectSecure Agent must be of Release 2018 or later. (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

- N/A

Centrify DirectControl Agent for *NIX

- Sample docker files for installing and setting up Centrify DirectControl inside a docker container are published in github. The docker files can be found in Github repository under centrify/container-security/docker-files/Centrify-Active-Directory-Agent-for-Linux (<https://github.com/centrify/container->

[security/tree/master/docker-files/Centrify-Active-Directory-Agent-For-Linux](#)) (Ref: CS-34433)

Note: Both Docker host and containers must have the same version of DirectControl agent for proper operation. (Ref: CS-46754)

- Microsoft Privilege Access Management for Active Directory is now supported. The support of this feature is by default disabled. To enable the support in agent, set "microsoft.pam.privilege.escalation.enabled" setting to true in centrifydc.conf, or use the corresponding Group Policy "Enable Active Directory PAM Privilege Escalation Feature" to do so. Please refer to user documentation for details. (Ref: CS-45092)
- A single non-existing user or group can now be ignored by adding the corresponding UID or GID into /etc/centrifydc/uid.ignore or /etc/centrifydc/gid.ignore files using the input format, such as, uid1-uid1, or gid2-gid2. (Ref: CS-45822)
- On Linux or AIX platforms, MIT Kerberos commands or programs linked with MIT Kerberos library (release 1.13 or above) can now inter-operate with Centrify KCM service. (Ref: CS-44043)
- A new field "assignee" for "get_role_assignment_field" is added in the command "adedit". It can be used to get a role assignment's assignee DN. (Ref: CS-45452)
- The command "adinfo" now has the following new options
 - "-i, --cipinfo" to show information about the Centrify Identity Platform and the HTTP proxy server used by DirectControl. (Ref: CS-45940)
 - "--product-version" to display the Centrify Infrastructure Services version information. The previous option "--suite-version" is still valid and displays the same information. (Ref: CS-45985, CS-46233)
- The command "adjoin" now has the following new options
 - "-o, --createComputerZone" to create computer zone for the machine at join time. (Ref: CS-32700)
 - "-O, --forceDeleteExistingComputerZone", effective only with "-o --createComputerZone", to remove the existing computer zone in Active Directory and to force a new computer zone creation at join time. (Ref: CS-32700)
 - "-E, --prestage <dir>" to specify <dir> as the directory where the pre-stage cache is located. This option is useful for improving performance of adjoin, especially in large deployment scenario. Please refer to user documentation for details. (Ref: CS-40351)

- The command "dzdo", and the corresponding Access Manager User Interface and sudoers import feature, now support sudo's "command digests". Now dzdo supports specifying multiple SHA-2 digests in privileged command right by setting its new 'digest' field. The supported hash types are 'sha224', 'sha256', 'sha384', and 'sha512'. Please check the manual for its format details. Note: This is supported only if the explicit path matches the command right, and only if it is in a hierarchical zone. Also, to avoid the security issue CVE-2015-8239 of sudo, dzdo will deny the execution of a dzdo command allowed by a privileged command right, if the right has digest check required and passed, but the command file is writable to the run user. In addition, the SHA-2 algorithms used by the command digest check in dzdo and dzsh are all FIPS-compliant. (Ref: CS-45542, CS-45933, CS-38738, CS-45393, CS-46005)
- Audit Trail events
 1. The command "adwebproxyconf" used by Multi-Factor Authentication (MFA) now also generates audit trail events under the category "Centrify Commands" for web proxy configuration changes. (Ref: CS-45604)
 2. The commands "sftp" and "scp" in Centrify OpenSSH now also generate audit trail events under the category "Centrify sshd". (Ref: CS-44236)

Configuration Parameters

The following parameters are added in centrifydc.conf:

- adclient.dns.cachingserver: This parameter enables DirectControl to work in an environment where caching-only DNS server (such as dnscache) is deployed. The default is false. Set this parameter to true if adjoin fails to join domain and caching-only DNS server is deployed in your environment. (Ref: CS-45017, CS-45987)

Note:

- o The command adcheck now has a new option '-r' to do the checking - adcheck will fail on a caching-only DNS server without this option but pass with the option.
 - o You can also instruct install.sh to run adcheck with the option '-r' by applying the option '--dns_cache' on install.sh.
- adclient.krb5.permitted.encryption.types.strict: This parameter specifies if DirectControl should add or replace the encryption types in the setting permitted_ectypes in krb5.conf with the ones specified in adclient.krb5.permitted.encryption.types in centrifydc.conf. The default is false which means just add. When this is set to true, DirectControl will replace the setting permitted_ectypes in krb5.conf to match exactly with the setting in adclient.krb5.permitted.encryption.types in centrifydc.conf. (Ref: CS-45047)

- `adclient.krb5.tkt.encryption.types.strict`: This parameter specifies if DirectControl should add or replace the encryption types in the setting `default_tgs_etypes`, and `default_tkt_etypes` in `krb5.conf` with the ones specified in `adclient.krb5.tkt.encryption.types` in `centrifydc.conf`. The default is false which means just add. When this is set to true, DirectControl will replace the setting `default_tgs_etypes`, and `default_tkt_etypes` in `krb5.conf` to match exactly with the setting in `adclient.krb5.tkt.encryption.types` in `centrifydc.conf`. (Ref: CS-45047)
- `adclient.krb5.ccache.dir`: This parameter specifies the directory where Kerberos ccache files are stored when `krb5.cache.type` is FILE. The default is empty and the ccache files are stored in `/tmp`. (Ref: CS-44846)
- `adclient.krb5.ccache.dir.secure.usable.check`: This parameter specifies whether to do secure and usability check on the CONFIGURED Kerberos ccache directory. The default is false. Do not enable until you know the exact requirements. (Ref: CS-44846)
- `adclient.one-way.x-forest.trust.force`: This parameter specifies a list of root domains, not accessible due to some reasons, e.g. behind a firewall, in two-way trusted forests that DirectControl Agent needs to treat them as one-way trusted domains. The default is an empty list. (Ref: CS-44419)
- `dzdo.requiretty`: This parameter specifies whether dzdo will run only when the user is logged in to a real tty. The default is false. When set to true, dzdo can only run from a login session but not via other means, such as, `cron(8)`, or `cgi-bin` scripts. (Ref: CS-45064)
- `krb5.conf.kcm.socket.path`: This parameter specifies the alternate socket path for KCM server. The default is empty string meaning that the default path in `/etc/krb5.conf`, `/var/run/.centrify-kcm-socket`, is used. If this parameter is set to a valid alternate path, the `kcm_socket` setting in `/etc/krb5.conf` will be updated and will take effect after `adreload`. (Ref: CS-44845)
- `krb5.conf.kcm.socket.path.secure.usable.check`: This parameter specifies whether to do secure and usability check on the alternate socket path for KCM server. The default is false. Do not enable until you know the exact requirements. (Ref: CS-46584)
- `microsoft.pam.privilege.escalation.enabled`: This parameter specifies if Centrify DirectControl agent uses Microsoft PAM Privilege Escalation feature in the machine. The default is false. When this is set to true, DirectControl will support dzdo privilege escalation. (Ref: CS-45092)

The following parameters are updated in `centrifydc.conf`:

- `krb5.sso.block.local_user`: This parameter specifies whether to allow Kerberos library to block a local user to do Single-Sign-On (SSO) with `.k5login` or not. If the parameter is set to true, the

user UNIX name is checked against the nss.ignore.user list. If the UNIX name is in the list, the user is considered a local user, and SSO is not allowed. To log in the user must enter the local user password. The default is changed from false to true. (Ref: CS-45906)

There is no parameter removed from centrifysdc.conf in this release. Please refer to the manual, Configuration and Tuning Reference Guide, for details.

Centrify OpenSSH

- N/A

Centrify OpenLDAP Proxy

- N/A

Centrify Access Manager

- The attribute page of command right properties now has a new dialog to support input/display of command digests. (Ref: CS-45393)

Centrify Licensing Service

- N/A

Centrify Group Policy Management

- N/A

Centrify Report Services

- There is a change in the User Interface of all zone-based reports (Ref: CS-45348):
 - The display format of zone selection is changed to '<parent zone>/<child zone>' to show the zone hierarchy as well.
 - The default selected zone is changed from '--All--' to just the first zone in the list to improve the initial report display time.

Centrify Zone Provisioning Agent

- N/A

3. Bugs Fixed

3.1. Bugs Fixed in Centrify Authentication Service and Centrify Privilege Elevation Service 5.5.2 (Release 18.11)

General

- Packaging
 - Fixed the packaging scripts on CentrifyDC/CentrifyDA packages to remove confusing and useless "Provides" from CentrifyDA and CentrifyDC-openssh RPMs. (Ref: CS-47226)

Centrify DirectControl Agent for *NIX

- Fixed a bug so that User Principal Name (UPN) should be used, if exists, for user name in audit trail events. (Ref: CS-45475)
- Fixed a bug in the handling of cached objects with unknown origin where it shows a repeating warning message in the log like this "... adclient[...]: WARN <... NSSGetCurrentGroupData > daemon.ipcclient2 Unable to retrieve current group information: ADAttribute '_server' is empty". (Ref: CS-47239)
- Fixed a bug in the sorting of internal group member list where pam.allow.groups is not working after upgrading. (Ref: CS-47279)
- Fixed a bug in the installer where it fails to upgrade openssl, openldap, curl packages using individual installer commands with "-u" option. (Ref: CS-46863, CS-46856)
- Fixed a bug in in the nis service where niswatch daemon is not able to restart the service if the firewall is set to block access to the local host by allowing alternate configuration using interface address instead of local host loop-back address. (Ref: CS-45302)

DirectControl Command Line Utilities

- Fixed a bug in the command "adcheck" on AIX where it fails to check disk space requirement. (Ref: CS-47029)
- Fixed a bug in services, like SMB and NTP, that DirectControl agent does not bind to the Domain Controller in the preferred or closest site as other services do. (Ref: CS-45936)
- Changed the behavior of the command 'adwebproxyconf -D' to not only delete http proxy credential from local machine, but also reset http proxy server, http authentication type and http authentication required configurations to default value in centrifydc.conf. This makes the behavior consistent between 'adwebproxyconf -D' and 'adwebproxyconf -S'. (Ref: CS-46769)

- Renamed the option '-y cloud' to '-y cip' in command "adinfo" to correctly reflect that the output is related to Centrify Identity Platform. The old option '-y cloud' is still supported for compatibility purpose but it will soon be deprecated. (Ref: CS-46560)
- Removed a misleading line showing an incorrect value for "Domain controller type" in verbose mode print-out of the command "adcheck". Please instead use the field "domainControllerFunctionality" for the same purpose. (Ref: CS-46861)

Centrify adedit

- N/A

Centrify OpenSSH

- N/A

Centrify OpenLDAP Proxy

- N/A

Centrify Access Manager

- Fixed a bug in "Orphan zone data objects and invalid data links" of forest analysis where the one-way trusted cross forest AD user will be marked as orphan if the local domain admin does not have enough right to access it. (Ref: CS-46004)
- Fixed a bug in "Sudoers Import" where it fails to identify sudoers file with Digest_Spec under any commands defined in Cmnd_Alias definition. (Ref: CS-45945)
- Fixed a bug in "list role assignments" and "add member" operations of a newly created computer role where it fails sometimes in a multiple domain controller environment. (Ref: CS-47241)

Centrify Access API for Windows

- N/A

Centrify Licensing Service

- N/A

Centrify Group Policy Management

- N/A

Centrify Report Services

- Fixed a bug in zone mode where it fails to synchronize some Active Directory objects such as user, group and computer. (Ref: CS-46923)
- Fixed a bug in permission validation where it incorrectly flags "insufficient permission" to access report database. (Ref: CS-47379)

Centrify Zone Provisioning Agent

- N/A

3.2. Bugs Fixed in Centrify Authentication Service and Centrify Privilege Elevation Service 5.5.1 (Release 18.8)

General

- Filenames of DEB and RPM types (i.e for Debian, RHEL, and SuSE packages) now have both version and build numbers. Filenames with just version numbers are also available as symlinks to the real files. (Ref: CS-45909)
- Fixed various errors reported by rpmlint.

Note:

- Fixed all the manpage-not-compressed errors. (Ref: CS-43284)
- Customer can safely ignore the rpath errors (i.e. rpath-in-buildconfig and binary-or-shlib-defines-rpath) from rpmlint as the RPATHs are either required or safe to use. (Ref: CS-43281)
- Customer can safely ignore the setuid-binary, setgid-binary, and non-standard-executable-perm errors from rpmlint as these permissions are required and it's safe to use the corresponding RPM packages. (Ref: CS-43280)

Centrify DirectControl Agent for *NIX

- When a user is removed from an AD group, the corresponding batch renewal keytab file is not removed. This is fixed by having a background task to do the clean-up. (Ref: CS-45238)
- Fixed an issue where user specified Web Proxy Server does not work properly if 'negotiate' authentication type is used and proxy user's password/machine's password is configured to be cached in an RODC. (Ref: CS-44177)
- On SLES systems, dzdo PAM configuration is now properly set for AppArmor. i.e. If the pam_apparmor.so library is not present on a SLES system, the pam_apparmor.so line will be removed from the dzdo pam configuration files during the DirectControl Agent installation. (Ref: CS-45478)

- The command wrapper for running "ssh" command is now using fully qualified command path when invoked. (Ref: CS-46140)
- Fixed an issue where the command "adjoin" will mess up nsswitch.conf if passwd_compat or group_compat are enabled on Solaris 11. (Ref: CS-44843)
- Fixed the following "adquery group" issues
 - The command fails to show a user whose sysrights are updated through a computer role assignment. (Ref: CS-46259)
 - The command may not properly expand the list of group members if the group contains multiple nested groups and some of which contain the same member group. Note: Even the command "adflush -f" cannot help in this case. (Ref: CS-46064)

Centrify OpenSSH

- Added a new Group Policy "Enable Rlogin Control Ssh" to control the option 'RloginControlSsh' in sshd_config. (Ref: CS-45592)
- Fixed a rekeying failure with GSSAPI key exchange. (Ref: CS-46409)

Centrify OpenLDAP Proxy

- Fixed the following resource leakage issues
 - a memory leak issue when the ldap search scope is base. (Ref: CS-45744)
 - socket and file descriptor leak issues which may appear as error message saying, "Failed to communicate with adclient due to broken session handle". (Ref: CS-46218)

Centrify Access Manager

- Fixed an issue where the principle name field incorrectly uses user's display name instead of logon name in the creation/update/removal of "Role assignment" audit trail events. (Ref: CS-45137)

Centrify Access API for Windows

- N/A

Centrify Licensing Service

- Licensing Report is now correctly showing the entries of CoreOS/Atomic host and containers.

When you join both CoreOS/Atomic host and containers to zones individually, each of them will be counted in the license usage.

i.e. the host counts one license and each individual container also counts one license. (Ref: CS-45768)

Centrify Group Policy Management

- If the group policy "Force Sudo Re-authentication when rlogin" is enabled/disabled, group policy migration will be performed and will enable/disable the corresponding group policy "Sudo Rights". This behavior is not desirable in most cases. This is now fixed by controlling whether to do group policy migration with a new registry key. By default, no policy migration will be performed in new installation. You can manually add a key "migration.enabled" (REG_DWORD type) in key path "HKEY_LOCAL_MACHINE\Software\Centrify\GPOE\" and set the value to 1 if you prefer to have group policy migration perform when loading the Group Policy Object Editor. If the key value set as 0, no policy migration will be performed (same as the default). (Ref: CS-45247)
- When the GPO setting "Specify network login message settings" is set to be "Not configured", we now properly keep the /etc/issue.net link as it is without removing nor creating it. (Ref: CS-45279)

Centrify Report Services

- Fixed an issue where Report Services do not work under Zone mode if Global Catalog (GC) is not operational. (Ref: CS-43506)
- Fixed an issue where Delegation Report and Effective Delegation Report fail to show delegation tasks for Managed Service Account (MSA) or group Managed Service Account (gMSA). (Ref: CS-44414)
- The column name 'SubGroup_NTLogoName' is changed to 'SubGroup_NTLogonName' in the Report Services DB view ReportView.ADGroupSubGroups. (Ref: CS-45584)
- Fixed an issue where the exception 'The item already exists' will be thrown during computation if there exists a role which is assigned to a local UNIX user and another local UNIX group having the same account name. (Ref: CS-45948)
- Fixed an issue where the following 7 reports show duplicate data if one role is assigned to same account with different start time and end time on same zone, computer or computer role (Ref: CS-45957):
 - 1) Hierarchical Zone - Computer Role Assignments Report
 - 2) Hierarchical Zone - Computer Role Effective Assignments Report (UNIX)
 - 3) Hierarchical Zone - Computer Role Effective Assignments Report (Windows)
 - 4) Hierarchical Zone - Effective Rights Report
 - 5) Hierarchical Zone - Effective Role Report
 - 6) Hierarchical Zone - Zone Effective Assignments Report (UNIX)
 - 7) Hierarchical Zone - Zone Effective Assignments Report (Windows)

Centrify Zone Provisioning Agent

- N/A

Centrify adedit

- Added a new option named 'enctype' to the 'precreate_computer' command to specify which encryption types are permitted in the pre-created computer. (Ref: CS-45782)

4. Known Issues

The following sections describe common known issues or limitations associated with this Centrify Infrastructure Services 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-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.