Centrify Isolation & Encryption Service 5.4.3 (2017.3) Release Notes

Table of Contents

1.   About This Release

Centrify Isolation & Encryption Service is Centrify's implementation of IPsec enablement for Linux and UNIX machines through Centrify DirectSecure Agent for *NIX and Microsoft Active Directory. It brings the same "It Just Works" mode of operation for IPsec deployment to non-Windows platforms that Windows users enjoy in a pure Windows environment.

The software comes in the form of platform-specific bundles. Each bundle contains the following:

- This release notes, i.e. DirectSecure-Release-Notes.html.

- The platform-specific software package in the form of centrifyds-<ds version number>-<os platform><os version>-<os architecture>.<package> format.

The documentation, Centrify Isolation & Encryption Service Administrator's Guide (centrify-directsecure-guide.pdf), which provides information for installing, configuring, and troubleshooting Centrify Isolation & Encryption Service, is available for download.

The latest copies of this release notes as well as the above-mentioned documentation 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. Supported Platforms

For the list of supported platforms for a Centrify Isolation & Encryption Service version, please refer to the corresponding Feature Changes section below.

For the list of supported platforms in all Centrify Isolation & Encryption Service releases, please refer to the document in www.centrify.com/platforms.

3. Feature Changes

3.1. Feature Changes in DirectSecure Agent for *NIX 5.4.3

- Support for DirectControl Agent for *NIX 5.4.3 in Release 2017.3

  This version of DirectSecure Agent for *NIX works with DirectControl Agent for *NIX 5.4.3 but not earlier releases.

- Support is provided for the following operating systems:

  - Red Hat Enterprise Linux 5, 6 and 7.0-7.2 (x86_64)
  - Linux Ubuntu Server 14.04 LTS, 16.04 LTS (x86_64)
  - Oracle Solaris 10, 11 (x86, x86_64, SPARC)
  - SUSE Linux Enterprise Server 11 SP2 (x86_64)

3.2. Feature Changes in DirectSecure Agent for *NIX 5.4.2

- Support for DirectControl Agent for *NIX 5.4.2 in Release 2017.2

  This version of DirectSecure Agent for *NIX works with DirectControl Agent for *NIX 5.4.2 but not earlier releases.

- It is integrated with OpenSSL 1.0.2k.

- Support is provided for the following operating systems:

  - Red Hat Enterprise Linux 5, 6 and 7.0-7.2 (x86_64)
  - Linux Ubuntu Server 14.04 LTS, 16.04 LTS (x86_64)
  - Oracle Solaris 10, 11 (x86, x86_64, SPARC)
  - SUSE Linux Enterprise Server 11 SP2 (x86_64)

- Support is removed for the following operating systems:

  - All 32-bit Linux
  - Linux Ubuntu Server 12.04 LTS
  - Red Hat Enterprise Linux 4

4. Bugs Fixed

4.1. Bugs fixed in DirectSecure Agent for *NIX 5.4.3

- There are no major bug fixes in this release.

4.2. Bugs fixed in DirectSecure Agent for *NIX 5.4.2

- There are no major bug fixes in this release.

5. Known Issues

The following sections describe common known issues or limitations associated with Centrify DirectSecure Agent for *NIX.

- Fails to connect due to time out

  When trying to connect, say with ssh, from a Solaris machine to another UNIX machine after applying IPsec group policy, the connection may fail with time-out. The reason is that Solaris does not work properly with 'non-mirror' or 'any protocol' settings in the IPsec policy (Ref: DS-521, DS-438).

- Restarting centrify-racbridge and centrify-racoon services on Solaris (Ref: DS-449)

"svcadm restart centrify-racbridge" does not start the centrify-racbridge and centrify-racoon services in proper order. Use "adsec -r" instead.

- DirectSecure Agent for *NIX does not works with Windows 10. (Ref: DS-524).

- CertGP takes a long time and can get aborted on Solaris (Ref: IN-90001)

  PKI certificate handling is implemented in DirectSecure Agent for *NIX as a group policy and is run by the DirectControl Group Policy mapper. On Solaris, the CertGP group policy takes longer to run than on other platforms and can run longer than the default timeout value associated with group policies on DirectControl, resulting in CertGP being aborted.

  To avoid this, you should increase the default timeout in /etc/centrifydc/centrifydc.conf. Locate the value

      # gp.mappers.timeout: 30

  and remove the "# " at the beginning to uncomment the value. Now change the value to 60 and save the file.

  Restart DirectControl Agent for *NIX with:

      /usr/share/centrifydc/bin/centrifydc restart

- Computers on which IPsec policy allows only ICMP traffic are not always able to ping

  Where the effective IPsec policy allows ICMP traffic but not UDP or TCP traffic, Windows computers will be able to ping UNIX computers, but UNIX computers will not be able to ping Windows. The problem is caused by the Linux implementation of ping; it does a UDP bind to the remote machine and this causes IPsec to establish SAs even though they are not needed.

  To avoid this problem, you can use the following:

  ping -I <my ip address> <remote ip address>

- Certificate principal mapping is not supported

  Certificate principal mapping ensures that the computer is known to Active Directory before accepting certificates. This feature is not supported.

- Certificate-based IPsec to the CA is not supported

  This is not a usual configuration (it is usual to allow unrestricted access to a CA), however it is possible to create

this configuration by specifying, for example, a subnet-wide policy with no exclusions. This configuration is also unsupported in pure Microsoft Windows environments.

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

6. Getting Started

Read through the Centrify Isolation & Encryption Service Administrator's Guide, centrify-directsecure-guide.pdf, that is everything about this package.

Before installing the Centrify DirectSecure Agent for *NIX package, you should make sure you have the matching DirectControl Agent for *NIX version installed.

You must be able to log on to the console of the system where you are installing the Centrify DirectSecure Agent for *NIX package.

You must log on as root to install on any operating system.

You should ensure that there are no other IPsec implementations running on the machine.

6.1. Installation

If you need to install Centrify DirectSecure Agent for *NIX, follow these steps:

  a. Download the Centrify DirectSecure Agent for *NIX package to your computer.
  b. Install Centrify DirectSecure Agent for *NIX package:
  • On SUSE, RHEL
      o rpm -Uvh <centrify-directsecure-package>.rpm
  • On Solaris
      o gzip -d <centrify-directsecure-package>.tgz
      o tar -xvf <centrify-directsecure-package>.tar
      o pkgadd -d CentrifyDS
  • On Debian
      o dpkg -i <centrify-directsecure-package>.deb
  c. Ensure the package is installed:
  • On SUSE, RHEL
      o rpm -qa CentrifyDS
      o you should see something like this "CentrifyDS-<release>"
  • On Solaris
      o pkginfo -l CentrifyDS
      o pkginfo should show status of "completely installed"

- On Debian
    - dpkg -l | grep centrifyds
    - You should see something like this "centrifyds-<release>"
  d. Special instruction on Solaris
    - Installing on Solaris computers with zones
        - Zones with their own physical network interface cards may have DirectSecure Agent for *NIX installed in them following the directions in steps a…c above. Each zone is effectively treated as a separate (virtual) computer.
        - Zones with virtual network interface cards (i.e. where the Global Zone provides the network interface) should not have DirectSecure Agent for *NIX installed in them, but instead DirectSecure Agent for *NIX should be installed in the Global Zone (using pkgadd with the -G option) and will provide isolation & encryption services for all zones for which it provides a network interface.

6.2. Uninstallation

If you need to uninstall Centrify DirectSecure Agent for *NIX, run the following command:

- On SUSE, RHEL
    - rpm -e CentrifyDS
- On Solaris
    - pkgrm CentrifyDS
- On Debian
    - dpkg -P centrifyds

7. Additional Information and Support

In addition to the documentation provided for this package, the Centrify Knowledge Base gives answers to common questions and information about general or platform-specific known limitations as well as tips and suggestions.

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 website, 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.

If a problem occurs, please send a problem description to
support@centrify.com. To improve the speed of resolution, please include
information about the system and version of software you are using.
One way of doing it is to run the following commands and paste the
output into the report:

1. hostname ; uname -a; nslookup `hostname`; rpm -qa | grep
   Centrify*; adsec –support (on SUSE or RHEL)

2. hostname ; uname -a; nslookup `hostname`; pkginfo -l CentrifyDS;
   adsec –support (on Solaris)

3. hostname ; uname -a; nslookup `hostname`; dpkg -l | grep
   centrify*; adsec –support (on Debian)

For information about purchasing or evaluating Centrify products,
send email to info@centrify.com.