Centrify Infrastructure Services

Installation and Configuration Guide for High Availability On-Site Deployment

April 2018

Centrify Corporation

Legal notice

Contents

Chapter 2 Administering and Troubleshooting the Infrastructure Service

About this guide

Centrify Infrastructure Services include services that can be accessed securely through connections to Centrify cloud instances, or deployed as an on-site solution with passwords managed using your infrastructure of choice, whether the infrastructure is an internal protected network, a private cloud, or provided by a public cloud instance.

The *Installation and Configuration Guide for High Availability On-Site Deployment* describes how to install, upgrade, and configure the infrastructure service as an on-site solution in high availability (HA) environments containing multiple, clustered servers managed by Microsoft Windows Server Failover Clustering (WSFC).

Note For details about installing and configuring the infrastructure service as a standalone solution in non-HA environments, see the *Installation and Configuration Guide for Standalone On-Site Deployment*, located in the documentation folder of the standalone infrastructure service software installation package.

Intended audience

The *Installation and Configuration Guide for High Availability On-Site Deployment* is intended for administrators who are responsible for installing, upgrading, diagnosing, configuring, and uninstalling on-site Centrify Infrastructure Services. This guide focuses on using the infrastructure service installation utility, and on using the Admin Portal to initially configure the on-site infrastructure service.

You should note that this guide does not provide usage details of the on-site infrastructure service after you perform an installation, nor does it provide information about cloud-based infrastructure service. For information about those topics, see the Admin Portal online help, and the Centrify Infrastructure Services *Administrator's Guide*.

Conventions used in this guide

The following conventions are used in this guide:

- `Fixed-width` font is used for sample code, program names, program output, file names, and commands that you type at the command line. When *`italicized`*, the fixed-width font is used to indicate variables. In addition, in command line reference information, square brackets (`[ ]`) indicate optional arguments.
- **Bold** text is used to emphasize commands, buttons, or user interface text, and to introduce new terms.
- *Italics* are used for book titles and to emphasize specific words or terms.
- For simplicity, UNIX is used generally in this guide to refer to all supported versions of the UNIX and Linux operating systems unless otherwise noted.

Finding information about Centrify products

Centrify includes extensive documentation targeted for specific audiences, functional roles, or topics of interest. However, most of the information in the documentation set is intended for administrators, application developers, or security architects after you have purchased the software or licensed specific features. If you want to learn more about Centrify and Centrify products and features, start by visiting the Centrify website. From the Centrify website, you can download data sheets and evaluation software, view video demonstrations and technical presentations about Centrify products, and get the latest news about upcoming events and webinars.

Contacting Centrify

You can contact Centrify by visiting our website, www.centrify.com. On the website, you can find information about Centrify office locations worldwide, email and phone numbers for contacting Centrify sales, and links for following Centrify on social media. If you have questions or comments, we look forward to hearing from you.

Getting additional support

If you have a Centrify account, click Support on the Centrify website to log on and access the Centrify Customer Support Portal. From the support portal, you can to search knowledge base articles, open and view support cases, connect with other Centrify users on customer forums, and access additional resources—such as online training, how-to videos, and diagnostic tools.

Installing the Infrastructure Service

As an on-site solution that you manage without access to the Centrify cloud, the infrastructure service replicates the infrastructure provided by the Centrify Identity Platform using computers on your network. After you install the infrastructure service, you use the Admin Portal to add, manage, and access the resources, domains, and databases and the corresponding accounts you add to the infrastructure service.

Note Because the infrastructure service replicates the infrastructure provided by Centrify Identity Platform, some dialog boxes, tools, and other features of the infrastructure service are labeled "Centrify Identity Platform."

The the rest of this chapter describes how to configure a typical high availability (HA) environment to host the infrastructure service, and instructions for installing, upgrading, backing up, and uninstalling the infrastructure service in an HA environment.

Note For details about installing and configuring the infrastructure service as a standalone solution in non-HA environments, see the *Installation and Configuration Guide for Standalone On-Site Deployment*, located in the documentation folder of the standalone infrastructure service software installation package.

Overview of high availability installation

When you deploy the infrastructure service in high availability (HA) environments inside of the firewall for your organization, you will install and configure the infrastructure service on two or more clustered server nodes to provide uninterrupted service in the event of a system failure. The cluster is managed by Microsoft Windows Server Failover Clustering (WSFC).

Additionally, Centrify connectors reside on servers outside of the cluster, and a disk containing the Centrify Identity Service database (CisDB) is shared by the node computers in the cluster.

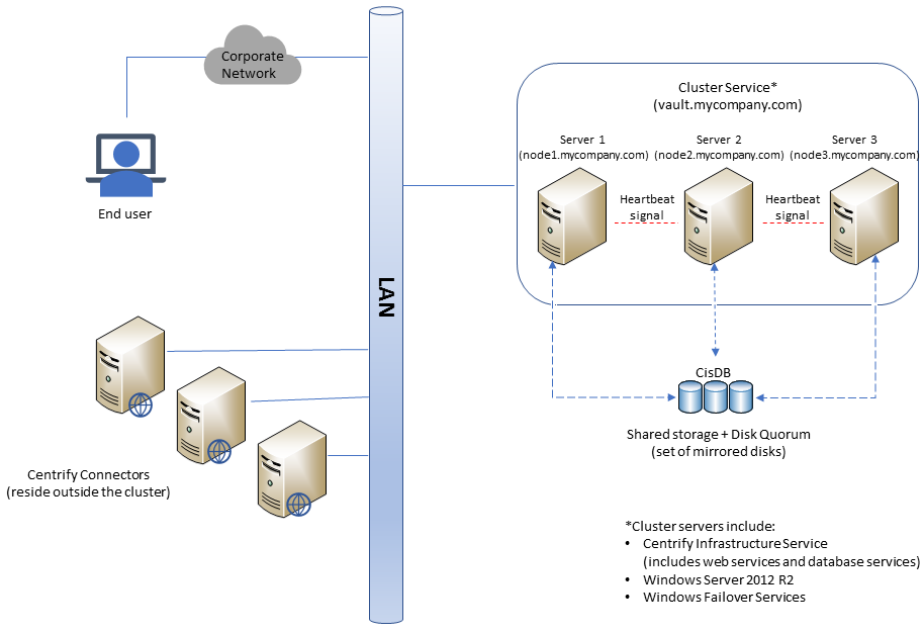


Figure 1. Example Centrify Privilege Service HA environment

In the infrastructure service HA environment, one server acts as the active server node while any additional nodes act as the passive server nodes. All infrastructure service activity is routed through whichever server node is active at the time. The cluster service continuously monitors the servers in the cluster. If the cluster service detects a problem, it attempts to restart failed components and services. If necessary, the cluster service promotes a secondary, passive server to be the active server, and all infrastructure service activity is then performed on that node.

Each server node has an identical configuration and includes the following:

- Centrify Infrastructure Services (including web services and database services)
- Windows Failover Clustering services.

Additionally, Windows Failover Cluster Manager must be installed on at least one node in the cluster.

In addition to configuring the server node cluster, you also need to add shared storage to the cluster. The shared disk hosts the active CisDB database and should be a set of mirrored disks on a SAN or equivalent storage system that the cluster servers can access. The cluster servers can use iSCSI, Fiber Channel or equivalent enterprise storage connectivity that is compatible with Windows Server 2012 R2. The shared storage must be mounted to the cluster using a dedicated storage network, such as iSCSI or Fiber Channel. They cannot be mounted as standard network share volumes.

Guidelines for environment configuration and data recovery

The exact configuration of your HA environment depends on your business needs, and is beyond the scope of this document. However, the following guidelines might be helpful as you plan and implement your environment:

- While your HA cluster configuration must include at least two servers, including three or more servers provides a more optimal failover/data recovery solution. Three or more clustered servers also provides uninterrupted service in the event that one of the servers in the cluster needs to be taken offline for a software upgrade or other maintenance.
- You can set up additional servers as nodes of the HA cluster in a remote data center location. You must ensure that the remote nodes have continuous access to the shared storage that hosts the CisDB database, and to all other nodes in the cluster.
- You can set up a separate, remotely located infrastructure service environment outside of the cluster, and use the infrastructure

service backup and restore scripts to manually restore service if the cluster fails. In this environment, you must ensure that the shared storage hosting the live CisDB database is *not* logically connected to the remote server. This ensures that only one infrastructure service server (the primary server in the cluster) is writing to the CisDB database at any given time.

Installation sequence

Installing the infrastructure service in an HA environment involves the following main steps:

1 Install the infrastructure service on the computer that will be the primary server in the cluster, as described in "Install on the primary server" on page 18.

When you install the infrastructure service on the primary server, you are prompted to provide details about the infrastructure service license key, file location, administrator credentials, CisDB disk location, certificate, FQDN, and cluster configuration file.

2 Install the infrastructure service on computers that will be secondary servers in the cluster, as described in "Install on secondary servers" on page 21.

When you install the infrastructure service on secondary server computers, you are prompted to provide details about the infrastructure service license key, file location, and the cluster configuration file that was created during primary server installation.

3 Configure Windows Server Failover Clustering (WSFC) to create the cluster and manage all node computers in the cluster, as described in "Create and configure a cluster" on page 23.

You use Failover Cluster Manager to configure failover clustering. Configuration can be performed from any cluster node where Failover Cluster Manager is installed. Configuration is typically performed from the primary server, but if necessary you can configure the cluster from any secondary server where Failover Cluster Manager is installed.

4 Install the connector on one or more computers outside of the cluster, as described in "Install the connector" on page 29.

Guidelines for storing sensitive information

When you install the infrastructure service on the primary server, you are prompted to specify a location for the cluster configuration file (also referred to as the *service setup/recovery* file) that is created during installation.

The cluster configuration file contains the following sensitive information:

- Non-recoverable encryption keys
- Information that is used to configure secondary servers in the cluster
- Information that is used to restore backup copies of CisDB on new servers

The location that you specify for the cluster configuration file must be secure, and any copies that you make of the cluster configuration file must also be stored in a secure location.

Note The database backup tools that are provided with the infrastructure service do not back up the cluster configuration file. If the cluster configuration file is lost for any reason, it will be impossible to restore the infrastructure service from backup files.

Prerequisites

The following summarizes what you need to do and the information you should have on hand for a successful installation of the infrastructure service in a high availability environment.

Cluster computers

- Ensure that each node computer (at least two but three or more is preferable) in the cluster where you are installing the infrastructure service meets the following hardware requirements:
  - At least two CPUs.
  - At least 16GB of memory.
  - At least 20GB of free disk space.
- Ensure that each node computer in the cluster where you are installing the infrastructure service meets the following software requirements:
  - The operating system is Windows 2012 R2.
  - The computer has access to the internet, or—if the computer is not connected to the internet—access to installation media for required software. For example, IIS, PowerShell, and other features are required to support the infrastructure service. If the supporting software is not already installed on the computer, it is installed automatically as part of the infrastructure service installation. If you are using local media to install required software, connect the media to the computer before you begin the infrastructure service installation.
  - If external access to installed services over https is necessary, port 443 must be available for TCP/IP.
  - One fixed IP address per computer.
  - The computer clock is set to synchronize with a known accurate time source.
- (Optional) All cluster node computers are joined to the domain.

Centrify Connector computers

- Ensure that at least one computer, and preferably multiple computers, are available outside of the cluster for Centrify connector installation.
- Ensure that all connector computers are joined to the domain.

IP addresses and DNS

- Reserve an unused IP address on your network, and assign the DNS name for your infrastructure service web site (for example, *vault.mycompany.com*).

  This is the cluster URL that will be used by end users to access the infrastructure service in a web browser (for example, *https://vault.mycompany.com/*).
- Reserve an unused IP address on your network and assign the DNS name for your Centrify WSFC Cluster administration service (for example, c*lusteradmin.mycompany.com).*

  This address will be used when WSFC accesses the clustered hosts.

You will be prompted to specify the infrastructure service URL/FQDN (for example, *vault.mycompany.com*) when you install the infrastructure service on the primary server in the node.

Note You cannot change the infrastructure service URL name after the infrastructure service is installed and the cluster is configured.

You will be prompted to specify the Cluster Administration name and address when configuring the WSFC cluster.

Certificates and License Keys

- Ensure that a trusted host certificate from a public certificate authority (CA) is available on the primary server in the cluster where you are installing the infrastructure service. The certificate must be for the URI of the infrastructure service web site (for example, *vault.mycompany.com*).

In a production environment, it is likely that you already have a trusted certificate that you can use. Before installing the infrastructure service, you should create or identify the certificate you want to use, verify that you know the location of the certificate file, and ensure that the file is available to each node computer. The certificate file must be a `PKCS #12` file with both private and public keys.

For more information about host certificates used with the infrastructure service, see "Certificates for infrastructure service authentication" on page 16.

- Obtain an infrastructure service license key that is specific to your company. During installation, you will be prompted for your company name and the license key that is bound to the company name. Contact a Centrify representative if you do not have an infrastructure service license key.

Shared Storage

- Ensure that the shared storage containing the CIS database (CisDB) is mounted and connected as follows:
  - The storage is connected and mounted to the primary server in the cluster.
  - The storage is connected to all secondary servers, but is not yet mounted to the secondary servers. After the cluster is configured, the failover clustering service will automatically configure and manage connections between the secondary servers and the shared storage.
- Ensure that a disk for the quorum with disk witness is available.

Additional requirements

- Obtain credentials (such as API keys, account names and passwords, and so on) for services and features that you want to enable after the infrastructure service is installed. While it is not essential that you have these credentials prior to the installation (that is, the installation will complete without them), having them

on hand and available will allow you to enable services and features immediately after the installation finishes.

Features that require manual enablement after you install the infrastructure service are:

- An SMTP server for email support.
- A Twilio account for SMS support.
- A Google account for Google Maps support.
- 42Matters credentials for mobile application search support.
- A trusted certificate for mobile device enrollment. The host certificate (described in Certificates and License Keys) must be trusted by mobile devices for device enrollment to succeed.

For details about configuring these services and features after you have installed the infrastructure service, see "Enable services and features after installation" on page 38.

- Decide whether to save a log file of the installation session. By default, the portion of the installation session that uses the installation wizard is not logged. To turn on installation logging for the installation wizard prior to performing the installation, see "Create an installation log file" on page 36.

Certificates for infrastructure service authentication

The primary infrastructure service server in the cluster must contain a certificate that is used for authentication between the infrastructure service and all endpoints that use the infrastructure service (such as enrolled devices, clients, browsers, connector computers, and so on).

The certificate must be for the infrastructure service URI (for example, *vault.mycompany.com*). This is necessary because all endpoints will use the infrastructure service URL host name to access the infrastructure service. All endpoints must trust the certificate authority that issues the host certificate.

When you install the infrastructure service on the primary server in the cluster, you can choose to specify an existing trusted host certificate,

or create a new, self-signed certificate. In a production environment, it is recommended that you specify an existing trusted host certificate. The option to create a self-signed certificate during installation is provided mostly for demonstration purposes, and is not intended for use in production environments.

To ensure that endpoints trust the infrastructure service host certificate, the certificate that you specify during installation should be from a known third-party certificate authority (for example, GoDaddy, Verisign, and so on).

During infrastructure service installation on the primary server, you will see the following certificate prompt (as described in Step 14 on page 20):

```
Would you like to provide a custom host certificate, if not,
one will be generated for you?
```

Respond to this prompt in one of these ways:

- To use an existing host certificate from a trusted third-party certificate authority, enter **Y** (yes). You will then be prompted for the location and file name of the certificate.
- To create a new self-signed certificate for demonstration purposes, select **N** (no). A new certificate will be created as part of the installation process.

  Note If you choose **N** (no), you will not be able to install the Centrify Connector on a separate computer unless the self-signed certificate and root are trusted on the domain.

During infrastructure service installation on secondary servers, you are not prompted for a certificate because certificate information is obtained from a cluster configuration file that is created during primary server installation.

Note After installation, you can change to a different certificate by executing the `update_host_cert.ps1` script as described in "Update or replace a host certificate" on page 42.

Install the infrastructure service

The procedures described in the following sections describe how to install the infrastructure service in a high availability environment.

Install on the primary server

Installing the infrastructure service on the computer that will be the primary server is performed in two stages.

The first stage uses an installation wizard to guide you through choices for the license agreement, feature selection, installation location, and installation of the software.

In the second stage, a PowerShell script launches automatically, and prompts you for additional information to set up the infrastructure service.

To install the infrastructure service on the primary server:

1. On the computer that will be the primary server, log in as a user with local administrator privileges.
2. Edit the machine hosts file on the primary server (located in C:\Windows\System32\drivers\etc\hosts), adding an entry similar to the following so that the DNS name of the infrastructure service URL (described earlier in "IP addresses and DNS" on page 14) resolves to the primary server in the cluster:

   ```
   127.0.0.1 localhost vault.mycompany.com
   ```

3. Download the infrastructure service installation file (the file is in `.exe` format).

   For backup and restoration purposes, it is recommended that you archive the infrastructure service installation file so that—if necessary—you can restore the version and build number that you originally installed. See "Back up and restore the infrastructure service" on page 43 for more information.

4. Double-click the installation file to start the installation.

5 When the Centrify Identity Platform installation wizard launches, follow the prompts to accept the license agreement, and provide a license key that is specific to your company name.

6 In the Feature Selection screen, select **Clustered: Primary** and click **Next**.

7 In the Destination Folder screen, select an installation folder and click **Next**.

8 In the Ready to Install Centrify Identity Platform screen, click **Install** to install components.

9 After all components are installed, click **Finish** to complete the installation of the infrastructure service software.

Immediately after you complete the installation, a Windows PowerShell console opens, prompting you for additional information to set up the service. You must provide the information described in the following steps before you can use the infrastructure service.

10 At the first PowerShell prompt, specify a name for a new Centrify Infrastructure Services user who will have infrastructure service administrative privileges, then press **Enter** to continue.

The user will be created as a Centrify Infrastructure Services user, and will be the initial system administrator for the infrastructure service. For example:

```
CISadmin@cps_demo.com
```

Note The user name that you specify must not match an existing Active Directory user name. If you specify an existing Active Directory user name, login conflicts will occur if the Active Directory user attempts to log in to the infrastructure service.

11 At the next PowerShell prompt, specify an email address for the administrative account, then press **Enter** to continue.

12 At the next PowerShell prompt, create a password for the administrative account, then press **Enter** to continue.

13 At the next PowerShell prompt, specify the URL (that is, a known, resolvable FQDN such as *https://vault.mycompany.com/*) for the

infrastructure service web site. This is the web site URL that was described earlier in "IP addresses and DNS" on page 14.

The host certificate that you will specify in the next step must be for this URL. The URL that you specify here is the URL that users will specify in their web browsers or clients to connect to the infrastructure service. After the installation finishes, you cannot change this URL name.

14 At the next PowerShell prompt, specify to use an existing certificate from a trusted certificate authority. See "Certificates for infrastructure service authentication" on page 16 for more information about how to respond to this prompt.

Note If you use a self-signed certificate, you must have configured your domain (or this computer) to trust the self-signed certificate root.

The certificate file must be a `PKCS #12` file with both private and public keys, and it must be issued for the infrastructure service URL that you specified in Step 13.

If necessary, you can change to a different certificate later as described in "Update or replace a host certificate" on page 42.

15 Next, you are prompted to select a folder for the service database (CisDB). Navigate to the CisDB shared disk, select a folder there, and click **Select Folder**.

16 Next, you are prompted to select a location for the service setup/recovery file (also referred to as the *cluster configuration file*). See "Guidelines for storing sensitive information" on page 12 for information about the contents of the file. Specify a secure location for the file, and click **Select Folder**.

The PowerShell script continues to run, displaying messages about the operations it performs. When the script finishes, you can access the infrastructure service by opening a browser to the URL *(https://vault.mycompany.com/)* that you specified in Step 13.

17 A Centrify login screen displays. Log in using the administrator user credentials that you specified in Step 10 and Step 12.

The infrastructure service launches, with the Admin Portal displayed by default. The infrastructure service is now usable, but

does not yet have any backup (secondary) servers. Also note that it does not yet reside in a cluster, and no connector has been installed yet.

18 Remove the edits you made to the machine hosts file on the primary server (located in C:\Windows\System32\drivers\etc\hosts).

19 Go to Install on secondary servers and continue from there to install backup servers.

Install on secondary servers

Installing the infrastructure service on computers that will be secondary servers is performed in two stages.

The first stage uses an installation wizard to guide you through choices for the license agreement, feature selection, installation location, and installation of the software.

In the second stage, a PowerShell script launches automatically, prompting you for the location of the cluster configuration file that was created when you installed on the primary server. Information from the cluster configuration file is then used by the PowerShell script for the rest of the installation.

To install the infrastructure service on secondary servers:

1 On a computer that will be a secondary server, log in as a user with local administrator privileges.

2 Download the infrastructure service installation file (the file is in `.exe` format).

3 Start the installation by double-clicking the installation file.

4 When the Centrify Identity Platform installation wizard launches, follow the prompts displayed to accept the license agreement, and provide a license key that is specific to your company name.

5 In the Feature Selection screen, select **Clustered: Secondary** and click **Next**.

6 In the Destination Folder screen, select an installation folder and click **Next**.

7 In the Ready to Install Centrify Identity Platform screen, click **Install** to install components.

8 After all components are installed, click **Finish** to complete the installation of the infrastructure service software.

Immediately after you complete the installation, a Windows PowerShell console opens, prompting you for additional information to set up the service.

9 At the PowerShell prompt, specify the location of the cluster configuration file that was created when you installed on the primary server.

If you saved the cluster configuration file on the primary server, enter the following at the prompt to go to the primary server, and then navigate to the file:

```
\\primary.server.name\c$
```

If you saved the cluster configuration file in the default location on the primary server, it is located here:

```
\program files\centrify\centrify
identity\platform\config\clconf.zip
```

The PowerShell script continues to run, displaying messages about the operations it performs. When the script finishes, you cannot yet access the secondary server. The secondary server must still be added to the cluster, and it must be able to access the shared CisDB disk (currently, only the primary server can access the shared CisDB disk).

10 Go to Create and configure a cluster and continue from there to create a cluster and add the primary and secondary servers to it.

Create and configure a cluster

To create and configure a cluster, you need to make sure that all servers you want to add to the cluster:

- Can access the shared storage (CisDB disk) and quorum with disk witness.
- Have the same version of Windows Server 2012 R2 installed.
- Have the Windows Failover Clustering service installed.
- Are joined to the same Active Directory domain.

Verify that the shared disk and quorum disk are available

Before you configure the server cluster, you must have the shared disks for CisDB and a disk for the quorum with disk witness available. Servers designated for the cluster must be connected to the shared disks and to the quorum disk. However, the shared disks should only be mounted to the server designated as the primary in the cluster. That is, shared disks should be connected, but not mounted, to the computers that will be secondary servers in the cluster. You can use the Windows Disk Management Tool to verify that the shared disk and a quorum disk are available; you should see at least one disk for data (CisDB) and one for the quorum with disk witness.

When you configure the cluster, the failover clustering service automatically configures a Disk witness as long as the disk is available (connected) during configuration.

Install the Windows Failover Cluster Manager

Before you create clusters, you must install the Windows Failover Cluster Manager onto all servers that you want to add to the cluster.

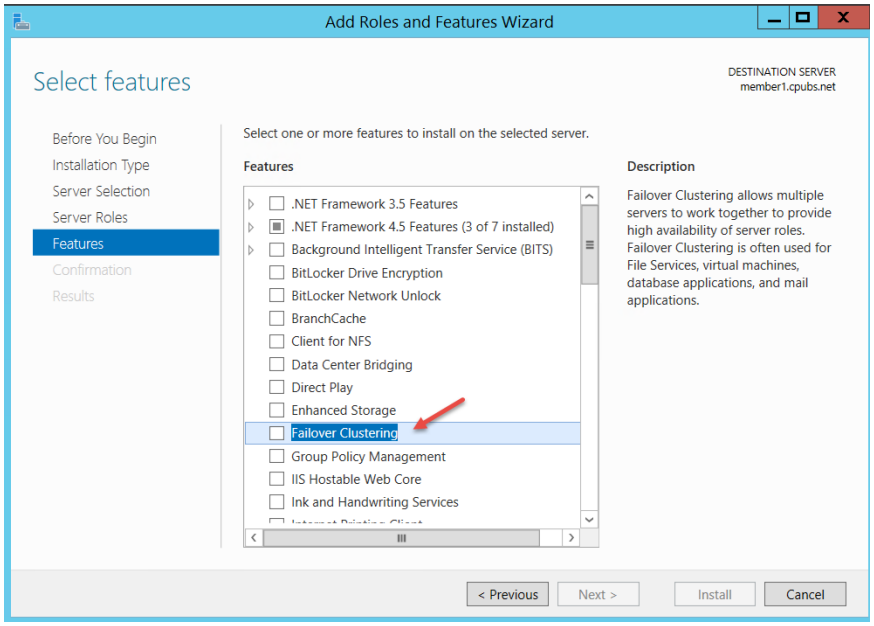
To install the Windows Failover Cluster Manager:

1. Log in to the server as a user with local administrator privileges.
2. Access the Windows Server Manager.

3 Click the **Manage** menu and then click **Add Roles and Features**.

4 In the Add Roles and Features wizard, click **Features**.

5 In Select features, check **Failover Clustering.**



6 Click **Next > Add feature > Next** and then **Install**.

The management tools are automatically installed.

7 Click **Close** to complete.

Create a cluster

Make sure the servers to be added to the cluster meet the prerequisites outlined in Prerequisites. Centrify recommends that you have at least two servers, although three is better, available to create the cluster. In order to create a cluster, you need to:

- Add servers and storage to the cluster.
- Create cluster roles to connect the cluster to the infrastructure service.

After you configure the cluster, you can test it to make sure it is operating properly, as described in Test the cluster.

To add servers and storage to the cluster:

1 Log in to the primary server as a user with local administrator privileges.

2 Access the Windows Server Manager.

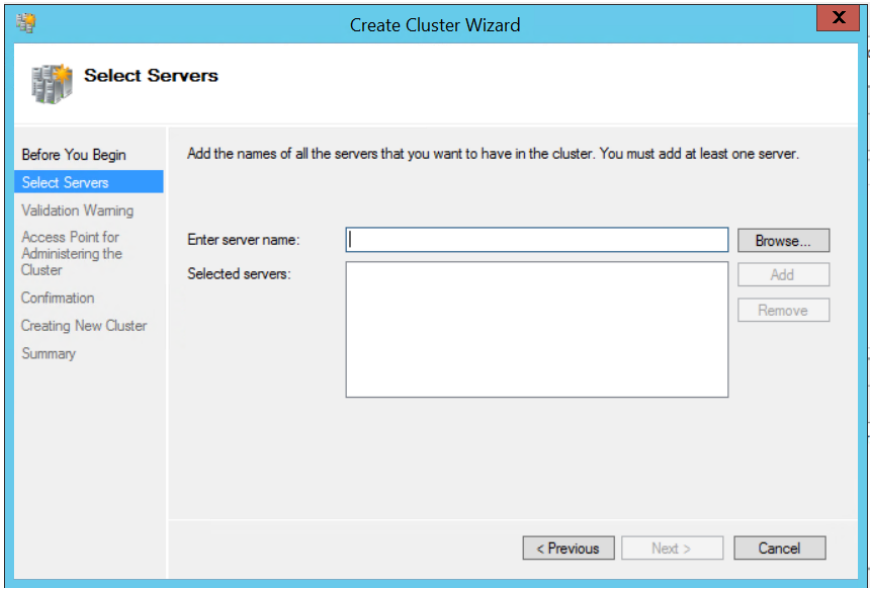
3 Click the **Tools** menu and then click **Failover Cluster Manager**.

4 In the Failover Cluster Manager, click **Action > Create Cluster**.

5 In the Create Cluster Wizard, click **Next** at Before You Begin.

6 In Select Servers, click **Browse** and select the servers you want to add to the cluster, then click **Ok > Next**.

Alternatively, you can enter the name of the server in the Enter server name field.



7 In Validation Warning, click **Yes** and then **Next** to run validation tests.

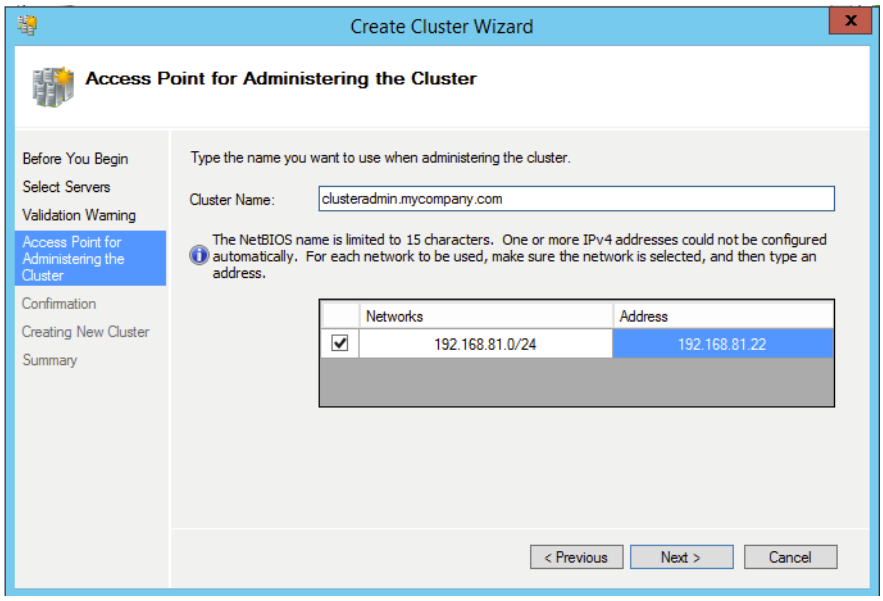
Run the validation tests to verify that the server hardware is compatible with the clustering service.

8 In the Summary screen, review the report and then click **Finish**.

9 In the Access Point for Administering the Cluster, type in a name for the cluster and enter its IP address (this is not the IP address of the web service).

This is the IP address and name that you use to manage the cluster and for communication between the nodes in the cluster (for example, *clusteradmin.mycompany.com)*. The name must not already exist in DNS or AD.

All nodes in the cluster are assigned the same IP address but only the active node responds to incoming network traffic.



10 At the Confirmation screen, make sure the **Add all eligible storage to the cluster** is selected.

Checking this option automatically joins the data and quorum with disk witness to the cluster. The Validation tests confirm which disks are eligible for storage.

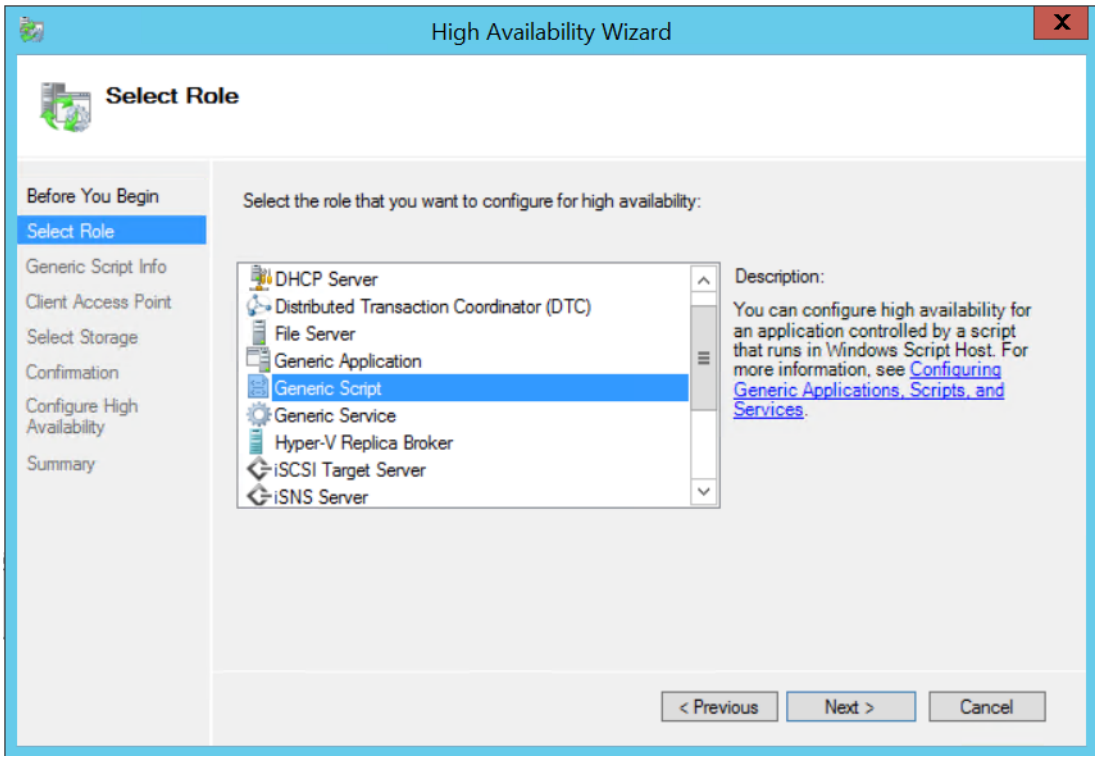
11 Click **Finish**.

To create clustered roles:

1 In the console tree, expand the cluster name and then right-click **Roles** and then click **Configure Role**.

2 Click **Next** at Before You Begin.

3 Select **Generic Script** and then click **Next**.



4 In the Script file path enter the following:

```
C:\program files\centrify\centrify identity
platform\scripts\iis_pgsql_cluster.vbs
```

The script, `iis_pgsql_cluster.vbs`, is available as part of the infrastructure service installation package.

5 In Client Access Point, type in a name for the Role and enter an IP address for the service.

This is the HA service name. The service name must not already exist in DNS or AD.

6 In Select Storage, select the CisDB disk and then click **Next**.

7 Click through the remaining screens to complete the High Availability Wizard and click **Finish** at the Summary screen to accept the installation.

8 Log in to the Centrify Admin Portal and click **About**.

You should see the server currently designated as the primary (for example, *node1.cps.com*) listed next to Host.

Manually configure a quorum with disk witness

In most situations, the failover clustering service automatically configures a quorum with disk witness when you perform the procedures described in the preceding sections. The following procedure describes how to manually configure a quorum with disk witness in the event that one was not configured automatically.

To manually configure a quorum with disk witness:

1. Open Failover Cluster Manager.
2. In Failover Cluster Manager, connect to the cluster.
3. Right-click the cluster, and select **More Actions > Configure Cluster Quorum Settings**.

   The Configure Cluster Quorum Wizard launches.
4. Click **Next** to proceed to the Select Quorum Configuration Option page in the wizard.
5. Click the **Select the quorum witness** button, and click **Next** to proceed to the Select Quorum Witness page in the wizard.
6. Click the **Configure a disk witness** button, and click **Next** to proceed to the Configure Storage Witness page in the wizard.
7. Select the storage volume (the disk) to use as the disk witness, and click **Next** to proceed to the Confirmation page in the wizard.
8. Review the information in the Confirmation page, and click **Next** to proceed to the Summary page in the wizard.
9. Click **Finish**.

   The quorum with disk witness is now configured.

Test the cluster

To test the cluster, you can move the role to each node in the cluster to make sure the cluster is operating correctly. Moving the role means that the shared CisDB disk is mounted to the server designated as the primary in the cluster. It may take extra time the first time you move the role, so it is good idea to perform the test at least once after you configure the cluster to initialize the database service.

To move the role to a secondary server:

1. Log in to the primary server (for example, *node1.cps.com*) as a user with local administrator privileges.
2. Access the Windows Server Manager.
3. Click the **Tools** menu and then click **Failover Cluster Manager**.
4. In the Failover Cluster Manager, expand the cluster name and then click **Roles.**
5. Right-click the role and then click **Move > Select Node**.
6. In Move Clustered Role, select one of the servers currently designated as a secondary and then click **OK**.

   The role and disks switch over to the selected server. The first time you switch the role you are required to log in to the server again.
7. Log in to the Centrify Admin Portal (for example URL *https://vault.mycompany.com/*) and click **About**.

   You should see the server you selected designated as the primary (for example, *node2.cps.com*) listed next to Host.

You can perform this test on each secondary node in the cluster.

Install the connector

After you have installed the infrastructure service on node computers and set up the cluster, install the Centrify Connector on at least one computer outside of the cluster, and configure the connector to use the cluster URL *(https://vault.mycompany.com/)*.

To avoid a single point of failure, it is highly recommended that you install the connector on more than one computer. Each computer that hosts a connector must reside outside of the cluster.

Note For additional information about installing the connector, including prerequisites and permission requirements, see the Centrify Identity Platform *Admin Portal User's Guide*.

To install the connector, you must first get the Centrify Identity Platform Management Suite package, and then run the installation wizard.

To install a connector on a host computer:

1. Log in to the host computer located outside of the cluster, using an account that has sufficient permissions to install the connector.
2. Open Admin Portal (for example, *https://vault.mycompany.com*).
3. Click **Settings > Network** > **Centrify Connectors** > **Add Centrify Connector**.
4. Click **64-bit** in the Download pane.

   The download begins.
5. Extract the files.
6. Double-click the installation program: `Cloud-Mgmt-Suite-rr.r-winaa.exe`

   In the file name, rr.r indicates the release version and aa indicates the processor architecture (64-bit).
7. Click **Yes** to continue if the User Account Control warning displays.
8. Click **Next** on the Welcome page.
9. Review the End User Software License and Services Agreement, accept the terms of agreement, then click **Next**.
10. Select the components to install, then click **Next**.

    The default is to install all components. Use the description on the installation UI determine what you want to install.
11. Click **Install** > **Finish** to open a second installation wizard.

This second installation wizard initiates the connection between Active Directory and your Centrify Identity Platform tenant.

12 Click **Next** on the Welcome page.

13 Type the administrative user name and password for your Centrify Identity Platform account, then click **Next**.

14 Click the **Advanced** button to change the default URL—*https://cloud.centrify.com/*— to the infrastructure service URL that you specified during infrastructure service installation (*https://vault.mycompany.com/*) on the primary server (Step 13 in the section Install on the primary server).

15 Click **Next** unless you are using a web proxy server to connect to Centrify Identity Platform.

If you are using a web proxy service, select the associated check box and specify the IP address, port, user name, and password to use.

16 Specify the monitored domains and relevant credentials to synchronize deleted objects in Active Directory/LDAP with Centrify Identity Platform, then click **Next**.

When you delete users in Active Directory and want this deletion synchronized with Centrify Identity Platform, you have two options:

- You must be the domain administrator of the Active Directory domain for the relevant deleted objects container. If you are deleting users in multiple domains, make sure that you are the domain administrator for all those domains.
- Delegate read permissions to the service account for the deleted objects container in the corresponding domain.

If you do not take one of the preceding actions, users deleted in Active Directory will be listed on the Users page in Admin Portal until you manually delete them. However, they will not have access to infrastructure service features.

The configuration wizard performs several tests to ensure connectivity.

17 Click **Next** if all of the tests are successful.

As the final step, the connector registers your customer identifier with your tenant, then runs in the background as a Windows service.

18 Click **Finish** to complete the configuration and open the connector configuration panel, which displays the status of the connection and your customer ID.

19 Click **Centrify Connector** to view or change any of the default settings.

20 Click **Close**.

After you have installed and configured at least one connector, you can use either Admin Portal or your default browser to log on to Centrify Identity Platform. The next time you log on and see the welcome page, select **Don't show this to me again**, then click **Close**.

Upgrade to a new infrastructure service release

This section describes how to upgrade to a new infrastructure service release in an HA environment where the infrastructure service is already installed and running.

Note This section does not describe how to upgrade from a standalone infrastructure service release to an HA infrastructure service release.

Upgrading in an HA environment involves the following main tasks:

- Install the infrastructure service on a secondary server in the cluster.
- Make the secondary server containing the new infrastructure service release the primary server. When you perform this task, the former primary server becomes a secondary server.
- Install the infrastructure service on the remaining secondary servers in the cluster.

To upgrade to a new infrastructure service release:

1 Ensure that the network used by the cluster allows WMI, and that all node computers in the cluster have port 5432 available for TCP communication between nodes.

2 On a secondary server in the cluster, log in as a user with domain administrator privileges.

3 Download the infrastructure service installation file (the file is in `.exe` format).

4 Start the installation by double-clicking the installation file.

The Centrify Identity Platform installation wizard launches, and detects the existing infrastructure service installation.

5 In the **Ready to Update Centrify Identity Platform** wizard screen, click **Update**.

System messages display as the new release is installed.

6 When the installation wizard finishes, click **Finish** at the prompt.

A Windows PowerShell console opens, prompting you for additional information to set up the service.

7 When the PowerShell script asks whether this is the final node to be updated, answer **N** and press **Return**.

When the script finishes, it instructs you to make this node the primary server if this node is the first to be upgraded.

8 In Failover Cluster Manager, make the upgraded node the primary server by performing the procedure described in "Test the cluster" on page 29.

When you perform this step, the former primary server becomes a secondary server.

9 Repeat Step 2 through Step 7 on the remaining secondary servers in the cluster. When you install on the final secondary server, answer **Y** at the prompt in Step 7.

The infrastructure service upgrade is now complete.

10 Optional: If your environment requires that the original primary server be the primary server again following the upgrade, use Failover Cluster Manager to manually make that change as described in "Test the cluster" on page 29.

Uninstall the infrastructure service

To uninstall the infrastructure service from node computers in the cluster:

1. On a computer where the infrastructure service is installed, log in as a user with local administrator privileges.
2. If the computer is a node in the cluster, remove the computer from the cluster. In Failover Cluster Manager, select **Nodes**, right click the node that you want to remove from the cluster, and select **More Actions > Evict**.
3. If you previously backed up configuration data and the Centrify Identity Service database, and if you plan to reinstall the infrastructure service and restore data from backup, ensure that your backup files reside in a location other than the Centrify folders that will be deleted. For example, backup files should not reside in `C:\Program Files\Centrify` or in any subfolders rooted there.
4. Launch the installation wizard by double-clicking the installation file.

   Or, if you do not have access to the infrastructure service installation file, you can use the **Uninstall** feature in the Windows **Programs and Features** control panel to launch the infrastructure service installation wizard and uninstall the infrastructure service.
5. Follow the prompts displayed until you reach the prompt giving you the choice to change, repair, or remove the infrastructure service. Select **Remove**.
6. After the installation wizard finishes removing files, click **Finish**.
7. Reboot the computer to complete the removal of the infrastructure service software.

Perform post-installation tasks

After you have installed the infrastructure service, perform the post-installation tasks described in this section to initially configure the installation for users.

To perform post-installation tasks:

1 In the Admin Portal, manually configure services and features as described in "Enable services and features after installation" on page 38.

2 In the Admin Portal, set up additional infrastructure service accounts and resources as described in the Admin Portal online help, and the *Getting Started Guide*.

3 In the Admin Portal, enroll devices as described in the following Admin Portal help topics:

- In the Admin Portal Dashboards page, select **Getting Started** from the dashboard drop-down list. In the left-hand pane, select **Enrolling mobile devices**.
- In any Admin Portal page, click the Help icon to open the online help system. In the table of contents in the left-hand pane, select either **Commonly used How To scenarios > How to enroll devices** or **Managing devices > Enrolling a device**.

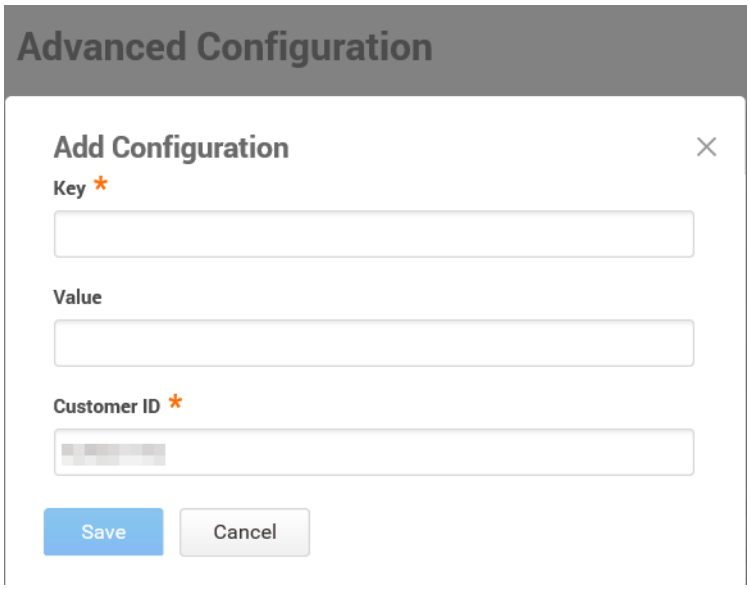
Note The issuer of host certificate (described in "Certificates for infrastructure service authentication" on page 16 must be trusted by mobile devices for device enrollment to succeed. The certificate is trusted by a device if it is issued by a public certificate authority. Also note that for device enrollment to succeed, you need disable certificate pinning (see To disable certificate pinning in the Admin Portal:).

To disable certificate pinning in the Admin Portal:

1 In the Admin Portal, click **Settings > Customization > Advanced Configuration** and then click **Add.**

2 At the Add Configuration screen, enter the following values:

- Key field—`HostCertificatePinningDisabled`
- Value field—`True`



3 Click **Save**.

Note If the `HostCertificatePinningDisabled` key is not configured as `true`, you must disable Cert Pinning in Settings > Server Authentication > Enable Cert Pinning when enrolling devices.

Create an installation log file

You can optionally use the native Windows installation logging facility to save information about your infrastructure service installation session.

To save installation session information using the Windows installation logger:

1 In a command prompt window, launch the installation with logging enabled.

For example, you would issue the following command to perform an installation using the `Centrify_Infrastructure_Service-17.7.exe` file, and save the log information in a file named `cis.log`:

```
Centrify_Infrastructure_Service-17.7.exe /l
cis.log
```

You can also use the `-log`, `/log`, or `-l` option to specify a log file.

If you do specify a file, log information is saved in the file `Centrify Identity Platform` *`version_timestamp`*`.log` in your computer's temporary file folder. For example:

```
C:\Users\Administrator\AppData\Local\Temp\Centrify Identity
Platform 17.4.125_20171205022113.log
```

2 Install the infrastructure service as described in Install the infrastructure service or Upgrade to a new infrastructure service release.

3 When the installation finishes, review the log file to verify that it saved the log events from the installation session.

Administering and Troubleshooting the Infrastructure Service

This chapter describes how to perform basic infrastructure service administration and troubleshooting tasks. It is assumed that you have already installed and logged in to the infrastructure service as described in "Upgrade to a new Centrify Infrastructure Services release" on page 7

The following topics are covered in this chapter:

- Enable services and features after installation
- Execute scripts provided with the infrastructure service
- Log diagnostic information
- Update or replace a host certificate
- Restore administrator access
- Back up and restore the infrastructure service
- Enable certificate authentication by smart card and tenant CAs

Enable services and features after installation

The following services and features are available by default in the cloud-based version of the infrastructure service, but are not available by default in the on-site version of the infrastructure service:

- SMTP server for email support.
- Twilio account for SMS.
- Google Maps.
- 42Matters.

To make these services and features available, you must enable them manually as described in the following sections after installing the infrastructure service.

Enable an SMTP server for email support

You must configure an SMTP server for email features to be available. If you do not configure an SMTP server, the following capabilities that require email support are not available in the infrastructure service:

- Invite new users to log on.
- Use email as an authentication option in multi-factor authentication.
- Request and approve access to applications through workflows.
- Request and approve password checkout and login access requests through workflows.
- Receive email notification about the results of password migration jobs.
- Receive email notification about the results of provisioning jobs.
- Receive directory synchronization reports.

To enable an SMTP server for email support:

1. In the Admin Portal, open **Customization > System Configuration** in the **Settings** tab.
2. In System Configuration, select the check box for **Use custom SMTP server settings**.
3. Provide an SMTP user name and password, the name or address of the SMTP server, and the server port number.
4. Click **Save** when you are finished.

Enable a Twilio account for SMS support

You must configure a Twilio account for SMS features to be available. If you do not configure a Twilio account, features that require SMS support are not available in the Admin Portal.

To enable a Twilio account for SMS support:

1 In the Admin Portal, open **Customization > System Configuration** in the **Settings** tab.

2 In System Configuration, select the check box for **Use custom Twilio account settings**.

3 Specify an account SID, an authentication token, and a From Number or sender ID.

Enable Google Maps

You must configure Google Maps for maps to be available. If you do not configure Google Maps, the map widget in the Admin Portal will indicate that maps are not available.

To enable Google Maps:

1 In the Admin Portal, open **Customization > System Configuration** in the **Settings** tab.

2 In System Configuration, select the check box for **Use custom Google API settings**.

3 Specify a Google client ID or API key (such as an ID or key from a Google or gmail account).

Enable 42Matters

You must configure 42Matters to enable searching for mobile applications. If you do not configure 42Matters, the mobile application UI is hidden in the Admin Portal.

To enable 42Matters to support mobile application searching:

1 In the Admin Portal, open **Customization > System Configuration** in the **Settings** tab.

2 In System Configuration, select the check box for **Use custom 42Matters.com settings**.

3 Specify a 42Matters API key.

Execute scripts provided with the infrastructure service

The infrastructure service provides several scripts, some of which you can execute manually to perform various configuration and administration tasks after the infrastructure service is installed. If the infrastructure service is installed in the default location, the scripts reside in this folder:

```
C:\Program Files\Centrify\Centrify Identity
Service\scripts
```

Log diagnostic information

A PowerShell script (`capture_diagnostics.ps1`) is provided with the infrastructure service to record information about the following areas:

- The product registry hive from `HKLM\Software\Centrify`.
- The `cisdb` database.
- Centrify log files for the connector, lrnode, web, and installation log4net.

To save infrastructure service diagnostic information using the capture_diagnostics.ps1 script:

1. Open a PowerShell console window as Administrator.
2. In the PowerShell console, change to the infrastructure service `scripts` folder. The `scripts` folder is located in the installation folder that was specified during the infrastructure service installation. If the default installation location was selected, the scripts folder is in `C:\Program Files\Centrify\Centrify Identity Service`.
3. Run the `capture_diagnostics.ps1` script:

   ```
   .\capture_diagnostics.ps1
   ```

   When the script finishes, output is saved in a file named `diag-`*`gid`*`-`*`date`*`.zip`.

Update or replace a host certificate

This section describes how to use the `update_host_cert.ps1` script to update an expired host certificate or change to a different host certificate.

Note The procedure described here applies only to standalone infrastructure service installations (that is, installations in which the database host and web host are installed on the same computer). If you have installed additional web hosts or a backup database host in a distributed (HA) environment, you cannot update or replace the host certificate.

To update or replace a host certificate:

1. On the computer where the infrastructure service is running and the host certificate resides, open a PowerShell console window as Windows administrator.
2. In the PowerShell console, change to the infrastructure service `scripts` folder. The `scripts` folder is located in the installation folder that was specified during the infrastructure service installation. If the default installation location was selected, the scripts folder is in `C:\Program Files\Centrify\Centrify Identity Service`.
3. Execute the `update_host_certificate.ps1` script:

   ```
   .\update_host_cert.ps1
   ```
4. When the script runs, you are prompted for the following information:
   - The location of the host certificate.
   - Whether a host certificate password is required.
   - The password for the host certificate, if a password is required.

Restore administrator access

This section describes how to use the `rescueuser.ps1` script to restore administrator access to the infrastructure service in the event that the administrator account becomes locked out.

While it is possible to reset the password for any user that is listed as a cloud user in the Admin Portal, the `rescueuser.ps1` script is intended to be used specifically to restore the infrastructure service administrator account (such as the administrator account that was created when the infrastructure service was originally installed). To see which users can have their password reset, switch to the Admin Portal, open the **Users** tab, and select **Cloud Users** in the **Search** field.

To reset a user password:

1. On the computer where the infrastructure service is running, open a PowerShell console window as Windows administrator.
2. In the PowerShell console, change to the infrastructure service `scripts` folder. The `scripts` folder is located in the installation folder that was specified during the infrastructure service installation. If the default installation location was selected, the scripts folder is in `C:\Program Files\Centrify\Centrify Identity Service`.
3. From the `scripts` folder, run the `rescueuser.ps1` script. When the script runs, it prompts you for the name of the user whose access you are restoring, and a new password for that user.

   For example, to reset the password for an infrastructure service user named `CISadmin@cps_demo.com`, you would issue the `rescueuser.ps1` command and respond to prompts as follows:

```
.\rescueuser.ps1
username: CISadmin@cps_demo.com
New password for CISadmin@cps_demo.com: **********
Verify new password: **********
User reset OK
```

Back up and restore the infrastructure service

For standalone infrastructure service, the `backup.ps1` and `restore.ps1` scripts are provided to back up and restore the infrastructure service database and configuration information.

For HA infrastructure service, the `pg_backup.ps1` and `pg_restore.ps1` scripts are provided to back up the infrastructure service database.

Use the scripts as described in this section to save data regularly to a secure location, and to recover data that was lost unexpectedly.

Data that is backed up and restored includes the Centrify Identity Service database, and additional configuration information such as application templates, the `config` folder (which retains the certificates necessary to configure the system, as well as encryption keys), and so on.

The information that you back up is specific to the infrastructure service release and build in which the data was created. You cannot use backup data from one release to restore data in another release, nor can you use backup data from one build to restore data in a different build of the same release. For example, if you back up data in infrastructure service release 17.7, you cannot restore that data in any release other than 17.7. Also, for example, if you back up data in infrastructure service build 17.7-190, you cannot restore that data in any build other than 17.7-190. Because of these restrictions, it is recommended that you save the infrastructure service installation file so that you can restore the version and build number that you originally installed.

To back up standalone infrastructure service:

Note The infrastructure service must be stopped (and is therefore unavailable) during standalone backup and restore operations.

1. On the computer where standalone infrastructure service is running, open a PowerShell console window as Windows administrator.
2. In the PowerShell console, change to the infrastructure service `scripts` folder. The `scripts` folder is located in the installation folder that was specified during infrastructure service installation. If the default installation location was selected, the scripts folder is in `C:\Program Files\Centrify\Centrify Identity Platform`.
3. From the `scripts` folder, run the `backup.ps1` script, using the `-backupDir` option to specify the folder where the backup file is saved.

   Note Do not specify the folder where the database resides as the location for the backup file. The folder containing the database is not a supported backup file location.

For example, to back up infrastructure service data and save the backup file in the `D:\Backups` folder, you would issue the following command:

```
.\backup.ps1 -backupDir D:\Backups
```

4 In the folder that you specified, verify that the backup file was created by executing the PowerShell `ls` command. You should see a file named `backup-`*`id_number`*`-`*`date`*`-zip`. For example:

```
backup-08958f1d-9301-4725-9468-afceedd0e43-2016-06-12.zip
```

To restore standalone infrastructure service:

Note The infrastructure service must be stopped (and is therefore unavailable) during standalone backup and restore operations.

1 On the computer where standalone infrastructure service is running, open a PowerShell console window as Windows administrator.

2 In the PowerShell console, change to the infrastructure service `scripts` folder. The scripts folder is located in the installation folder that was specified during infrastructure service installation. If the default installation location was selected, the `scripts` folder is in `C:\Program Files\Centrify\Centrify Identity Platform`.

3 From the `scripts` folder, run the `restore.ps1` script, using the `-backupFile` option to specify the absolute path name of a backup file that you created earlier using the `backup.ps1` script.

For example, to restore infrastructure service data from the backup file `D:\Backups\backup-08958f1d-9301-4725-9468-afceedd0e43-2016-06-12.zip`, you would issue the following command:

```
.\restore.ps1 -backupFile D:\Backups\backup-08958f1d-9301-
4725-9468-afceedd0e43-2016-06-12.zip
```

4 After `restore.ps1` finishes, a Centrify login screen displays in a browser.

To back up HA infrastructure service:

Note The infrastructure service does not need to be stopped during database back up in an HA environment.

1. On the primary server in the cluster, open a PowerShell console window as Windows administrator.
2. In the PowerShell console, change to the infrastructure service `scripts` folder. The scripts folder is located in the installation folder that was specified during infrastructure service installation. If the default installation location was selected, the `scripts` folder is in `C:\Program Files\Centrify\Centrify Identity Platform`.
3. From the `scripts` folder, run the `pg_backup.ps1` script, using the `-DestDir` option to specify the folder where the backup file is saved.

   Note Do not specify the folder where the database resides as the location for the backup file. The folder containing the database is not a supported backup file location.

   For example, to back up infrastructure service data and save the backup files in the `D:\Backups` folder, and do so in verbose mode, you would issue the following command:

   ```
   .\pg_backup.ps1 -DestDir D:\Backups -Verbose
   ```

To restore HA infrastructure service:

Note The infrastructure service database service and IIS must be stopped during restore operations in an HA environment.

1. On the cluster computer where you will perform the restore operation, ensure that the same drive letter that was used for the backup is available (for example, `D:`).
2. If the cluster computer where you will perform the restore operation already has a folder with the same name as the backup folder (for example, `D:\Backups`), ensure that the folder is empty.
3. Copy the backup files from the backup directory on the original (primary) computer to the same drive and folder on the computer where you are performing the restore operation (for example, `D:\Backups`).
4. On the computer where you are performing the restore operation, change to the infrastructure service `scripts` folder.

5 From the `scripts` folder, run the `pg_restore.ps1` script, using the `-SourceDir` option to specify the folder where the backup file resides.

   For example, to restore the infrastructure service from the backup files that you copied in Step 3, and to optionally initialize the database, and do so in verbose mode, you would issue the following command:

   ```
   .\pg_restore.ps1 -SourceDir D:\Backups -InitDB -Verbose
   ```

6 Restart IIS services on the computer where you performed the restore operation.

Enable certificate authentication by smart card and tenant CAs

The `setup_certauth.ps1` script is provided with the infrastructure service to enable certificate authentication when client certificates are issued by Centrify or by your own certificate authority.

After you execute `setup_certauth.ps1`, the Certificate Authorities feature located in the Admin Portal **Customization > Settings > Authentication** page is enabled. In the Certificate Authorities page, you can configure authentication by smart card, and by certificates issued by your PKI infrastructure. If you do not execute `setup_certauth.ps1`, the Certificate Authorities feature located in the Admin Portal **Customization > Settings > Authentication** page remains disabled, and is not visible.

Before you can execute `setup_certauth.ps1`, you must ensure that the following prerequisites are met:

- A CNAME record that points the DNS host to the infrastructure service host has been created within your DNS infrastructure. After the CNAME record is created, it can take up to 15 minutes for the CNAME to resolve the IP addresses of the DNS host and the infrastructure service host.
- A certificate from a trusted certificate authority has been issued for the DNS host. When the `setup_certauth.ps1` script runs, you will be prompted to specify the path to this certificate.

The `setup_certauth.ps1` script validates these prerequisites during runtime. If either prerequisite is not met, `setupcertauth.ps1` aborts.

To enable authentication by smart card and tenant CAs:

1. On the computer where the infrastructure service is running, open a PowerShell console window as Windows administrator.
2. In the PowerShell console, change to the infrastructure service `scripts` folder. The scripts folder is located in the installation folder that was specified during infrastructure service installation. If the default installation location was selected, the `scripts` folder is in `C:\Program Files\Centrify\Centrify Identity Service`.
3. From the `scripts` folder, run the `setup_certauth.ps1` script:

   ```
   .\setup_certauth.ps1
   ```
4. When the script prompts you to verify that the prerequisites are satisfied, type **`Y`** and press **Enter**.
5. The script validates prerequisites, and prompts you for the path to the DNS host certificate. Type the path to the certificate and press **Enter**.

   When the script finishes, the Certificate Authorities feature located in the Admin Portal **Customization > Settings > Authentication** page is enabled.