Cloud Access Manager 8.1.3

How to Configure for High Availability

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Cloud Access Manager How to Configure for High Availability
Updated - October 2017
Version - 8.1.3

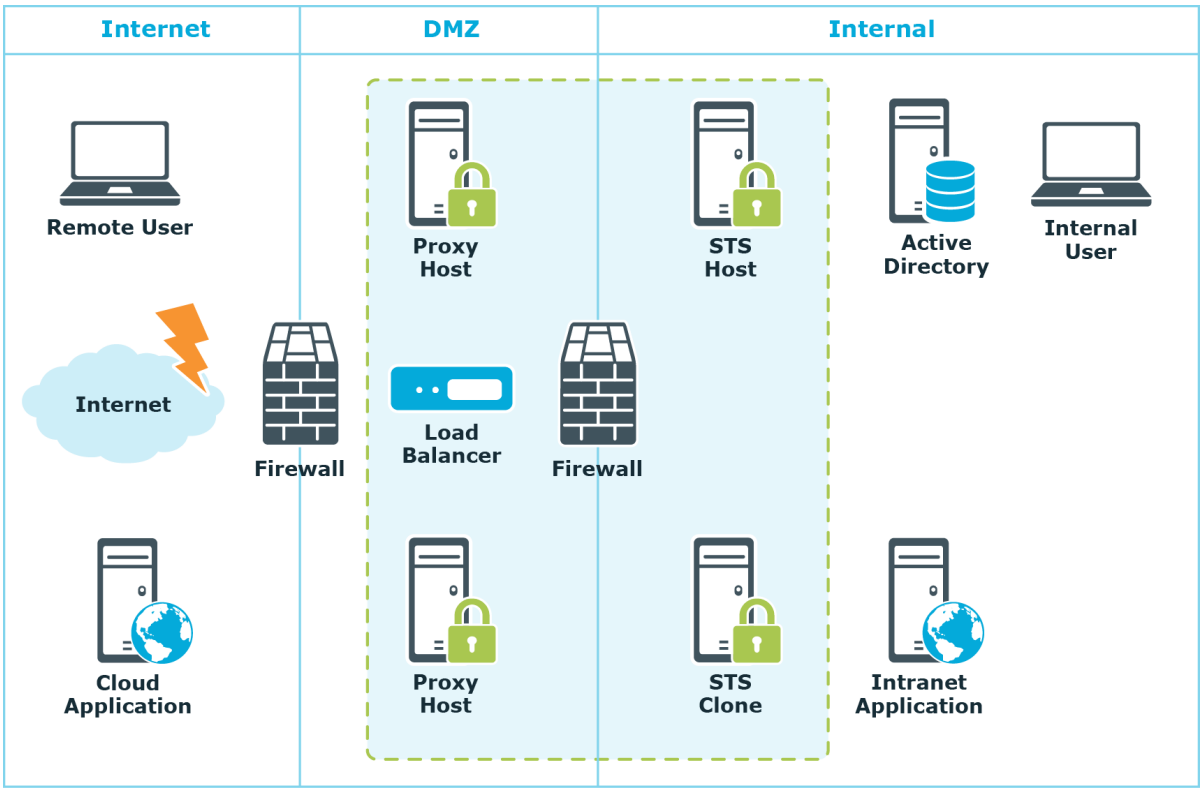
Contents

Introduction

This guide describes how to extend a typical two host environment described in the *One Identity Cloud Access Manager Installation Guide* to include two additional hosts to provide both redundancy and additional capacity. One host will be deployed in the DMZ to become a clone of the Cloud Access Manager Proxy host and the other will be deployed on the internal network to become a clone of the Cloud Access Manager Security Token Service (STS) host.

Figure 1 represents a typical high availability deployment using four Cloud Access Manager hosts.

Figure 1: Cloud Access Manager high availability deployment



Cloning the database

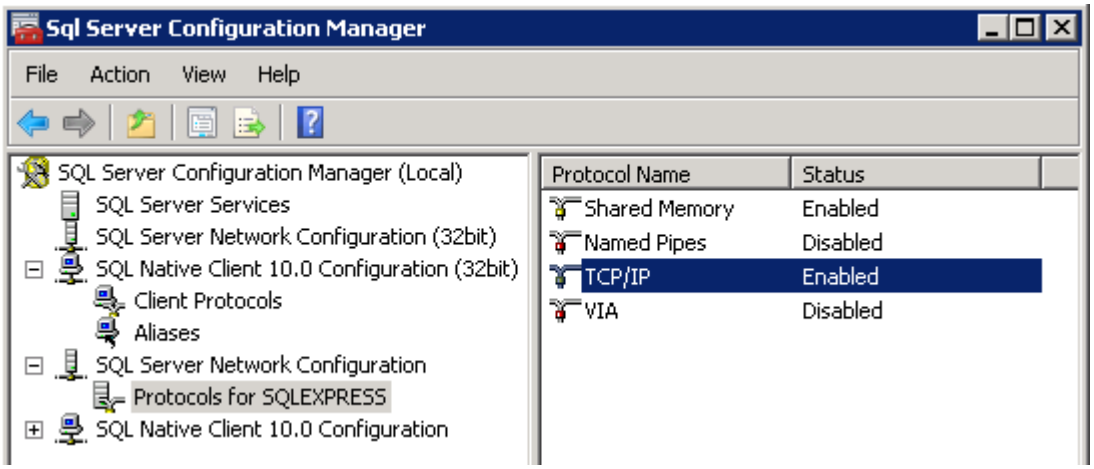
Cloud Access Manager requires an instance of Microsoft SQL Server Edition 2012, 2008R2 or 2008 to store its configuration, audit and session data. In a high availability Cloud Access Manager environment the database should also be configured for high availability, for example using SQL Server AlwaysOn Availability Groups.

The Security Token Service (STS) hosts need to access the database using a single hostname/IP address for the database cluster. The nodes in the database cluster can be deployed either on dedicated hosts or on the STS hosts. Please refer to the Microsoft SQL Server documentation that describes how to deploy SQL Server for high availability.

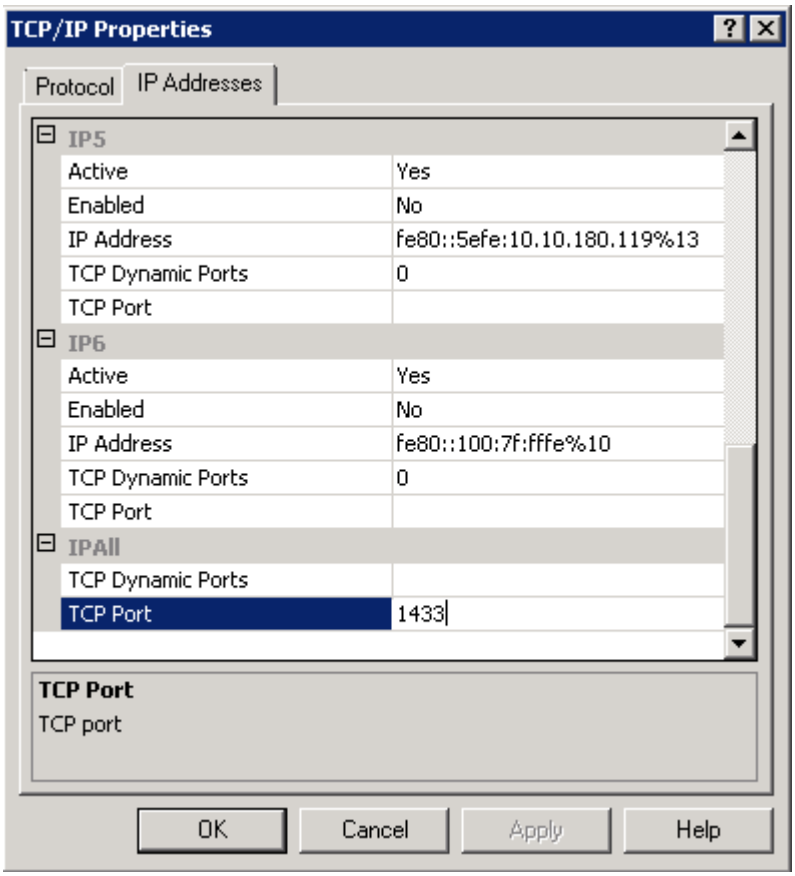
The database can be configured for high availability either before or after cloning the STS host. Whichever option you choose, before you clone an STS host, you need to make sure the database can be remotely accessed by TCP/IP and that Cloud Access Manager is using this connection method rather than the default shared memory connection method which will only allow local access.

To verify that SQL Server is configured to allow access using TCP/IP

1. In **SQL Server Configuration Manager**, in the console pane, expand **SQL Server Network Configuration**.
2. In the console pane, click **Protocols for <*Instance Name*>** for the database instance used by Cloud Access Manager.
3. In the details pane, ensure that the **TCP/IP protocol** is **Enabled**. If it is not enabled, right-click and select **Enable**.



4. Next, verify that the database is configured to allow access using a fixed port. To do this, double-click **TCP/IP** to display the **TCP/IP Properties** page.
5. From the **IP Addresses** tab, check that the **TCP Dynamic Ports** field is not populated in the **IPAll** section. If it is populated, clear the port range to ensure a fixed port is used to access the database.
6. In the **TCP Port** field, verify a port is specified to access the database. For example, the default SQL Server port 1433.



7. If you have made changes to the TCP/IP configuration, you now need to restart the SQL Server service.
8. In the console pane, click **SQL Server Services**.
9. In the details pane, right-click **SQL Server instance name**, and then click **Restart** to stop and restart the SQL Server service.

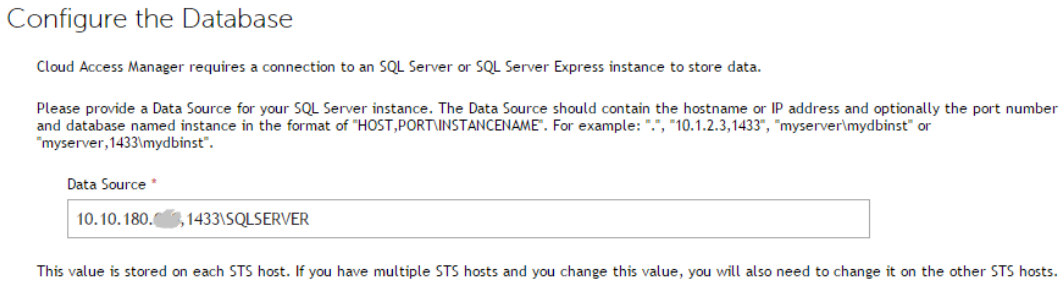
To verify that Cloud Access Manager is configured to access the database using TCP/IP

1. Login to the STS host and access the Cloud Access Manager Administration UI using the **Cloud Access Manager Administration (fallback login)** shortcut on the desktop. Using the fallback shortcut allows you to access the instance of the STS running on the host you are logged into. This is important if you change the database connection settings as each STS host stores a copy of the connection details. If you change the connection details, you must update them on each STS host.

   NOTE: If you plan to configure your database for high availability after configuring Cloud Access Manager for high availability, you need to repeat this section for each STS host. This is true if the database hostname/IP address or port changes as a result of changing the database configuration for high availability. For example, if the database now needs to be accessed using the virtual IP address of the cluster.

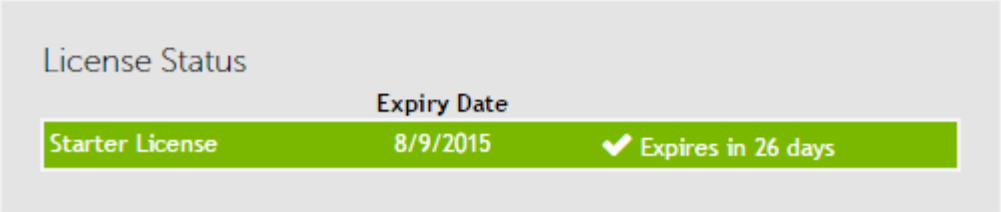
2. Click the gear icon to navigate to **Settings**, and then click **Show Advanced Settings**.
3. Click **Configure the Database**.
4. The **Data Source** should contain the hostname or IP address to connect to the database and optionally the port number and database instance. If the hostname/IP is not present or has changed since configuring the database for high availability, update the database and click **Save**.

   NOTE: The port number is required when using a port number other than the standard SQL Server port 1433. A comma is used to append a port number to the hostname/IP address. In addition the instance name is required when using a named instance rather than a default instance. A backslash is used to append the instance name.



5. Click the **Configuration Status** icon in the top-right corner, verify that you can see each host and that the status of the components on each host is running and configured.

   NOTE: If you do not see your hosts, revisit the database settings and verify that the connection details are correct. You may also need to check that any firewalls between the two hosts are configured to allow access to the database.



Cloning the STS host

To clone the STS host

1. Provision a new host alongside the existing Cloud Access Manager Security Token Service (STS) host on the internal network. For simplicity, we recommend that the host is of the same hardware and operating system type as the existing host, however no technical limitation applies.
2. On the new STS host, either mount the Cloud Access Manager software ISO or extract the Cloud Access Manager software .ZIP file to a temporary location.
3. Start the Autorun and navigate to the **Install** section.
4. Click **Install** on the **Cloud Access Manager IIS Components**.
5. Accept the License Agreement. Click **Next**.
6. Click **Production Installation**.
7. Enter the same user account used during the installation of the first STS host. Click **Next**.
8. Click **Install** to deploy the components required for the new STS host.

NOTE: The STS host requires the Microsoft .NET framework version 4.5. If this is not already installed on the host, the installer will download and install the Microsoft .NET framework from the internet.

9. When the installation is complete, click **Launch** to start the configuration wizard. The configuration wizard will guide you through the steps to connect your new STS host to your existing environment.
10. When prompted for the database connection details, select the **My database server is not an SQL Express instance installed on the same machine as Cloud Access Manager** check box and enter the same data source used in the previous section, for example, the same data source used by the first STS host.
11. On the **Proxy Settings** page confirm the settings are the same as those on the initial STS host, and then click **Next**.
12. When all items are complete on the **Configuring Cloud Access Manager** page, click **Finish**.
13. When the configuration wizard has finished, click the **Configuration Status** icon in the top-right corner and verify that:
    - You can see the new STS host.
    - The status of the components on the host is running and configured.
14. Restart the Cloud Access Manager proxy service on the existing proxy host.

Verifying the new STS host

To verify that the new STS host is working correctly

1. Verify that users can log in to the Cloud Access Manager portal as normal using the hostname configured on the **Proxy Settings configuration** page:

   https://<*proxy host FQDN*>/CloudAccessManager
2. Stop the **World Wide Web Publishing** service on the existing Security Token Service (STS) host so that only the new STS host is running.
3. Verify that users can still log in to the Cloud Access Manager portal as normal.
4. Restart the **World Wide Web Publishing** service on the existing host and stop the **World Wide Web Publishing** service on the new STS host.
5. Verify that users can still log in to the Cloud Access Manager portal as normal.
6. Restart the **World Wide Web Publishing** service on the new host.
7. From within the Cloud Access Manager Administration UI, click the **Configuration Status** icon in the top-right corner. Verify that you can see each Cloud Access Manager host and that the status of the components on each host is running and configured.

   NOTE: Some components may not show as running until users have accessed the Cloud Access Manager application portal.

Cloning the proxy host

To clone the proxy host

1. Provision a new host alongside the existing Cloud Access Manager proxy host in the DMZ. For simplicity, we recommend that the host is of the same hardware and operating system type as the existing host, however no technical limitation applies. If you are using hosts with different hardware, the load balancer in front of the proxy hosts may require additional configuration to weight the number of requests in favor of the more powerful host.
2. On the new proxy host either:
   - Mount the Cloud Access Manager software ISO

     or
   - Extract the Cloud Access Manager software ZIP file to a temporary location.
3. Start the Autorun and navigate to the **Install** section.
4. Click **Install** on the Cloud Access Manager Proxy.
5. Accept the License Agreement and then click **Next**.
6. Enter the hostname of the first Security Token Service (STS) host you installed, for example the primary STS host.
7. Enter the shared secret for your Cloud Access Manager environment and click **Install**. The shared secret is defined during the configuration of the first STS host. To find the shared secret click **Fallback Password and Shared Secret** in the **Settings** section of the Cloud Access Manager Administration UI.
8. The proxy installation will now start, when the installation is complete, click **Close**.
9. Deploy a load balancer in front of the two Cloud Access Manager proxy hosts to distribute the traffic between the two hosts. This should be a layer 4 load balancer to allow Cloud Access Manager to handle the Secure Sockets Layer (SSL) connections from the users. Using a layer 7 load balancer, for example, would require the SSL connections to be terminated on the load balancer itself rather than on the Cloud Access Manager proxy hosts.

   Update the network configuration to route traffic destined for the external fully qualified domain names used by the Cloud Access Manager proxy hosts to the VIP address of the load balancer, rather than the primary proxy host as before.

   NOTE: The load balancer must have sticky IP enabled to ensure users always use the same proxy host unless in a failover situation.

NOTE: If you use a reverse proxy server or load balancer in front of One Identity Cloud Access Manager, you must ensure that all headers required by Cloud Access Manager are maintained at all times. For instance, Cloud Access Manager injects JavaScript into app pages to manage session idle timeout and at the same time sets no cache headers on the response. It is essential to maintain the no cache headers at all times for Cloud Access Manager to function as designed. Removing or changing the no cache headers may cause session management issues, for example when a user uses the **Back** button on their browser.

10. From within the Cloud Access Manager Administration UI, click the **Configuration Status** icon in the top-right corner. Verify that you can see each Cloud Access Manager host and that the status of the components on each host is running and configured.

Verifying the new proxy host

To verify that the new proxy host is working correctly

1. Verify that users can log in to the Cloud Access Manager portal as normal.
2. Stop the Cloud Access Manager proxy service on the existing proxy host, so that only the new proxy host is running.
3. Verify that users can still log in to the Cloud Access Manager portal as normal.
4. Open the Cloud Access Manager proxy log on the new proxy host, **CloudAccessManagerProxy.log** Search the log for entries containing the userid used to verify access to the portal. This will confirm the user was using the new proxy host. Also verify that the log entry contains the user's IP address, typically their public IP address. If the IP address is that of the load balancer, the load balancer configuration may need to be updated to preserve the original client IP address rather than using its own.

   NOTE: The private IP address for internal users is only visible if you have configured your internal DNS to resolve the proxy's hostname to the private IP address of the proxy load balancer.

5. Restart the Cloud Access Manager proxy service and stop the Cloud Access Manager proxy service on the new proxy host.
6. Verify that users can still log in to the Cloud Access Manager portal as normal.
7. Open the Cloud Access Manager proxy log on the existing proxy host, **CloudAccessManagerProxy.log**. Search the log for entries containing the userid used to verify access to the portal. This will confirm the user was using the existing proxy host rather than the new host. Verify that the log entry contains the user's IP address, typically their public IP address.
8. Restart the Cloud Access Manager proxy service.

9. From within the Cloud Access Manager Administration UI, click the **Configuration Status** icon in the top-right corner. Verify you can see each Cloud Access Manager host and the status of the components on each host is running and configured.

About us

Contacting us

For sales or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product