Dell™ One Identity Cloud Access Manager - How to Configure for High Availability

February 2015

- Cloning the database
- Cloning the STS host
- Cloning the proxy host

This guide describes how to extend a typical two host environment described in the Dell™ 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 STS host.

The diagram below 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 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.

![SQL Server Configuration Manager](image)

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 will 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 when changing the database connection settings as each STS host stores a copy of the connection details. If the connection details change, they must be updated on each STS host.

2 Navigate to the Advanced Settings by clicking on the gear icon, then click Show Advanced Settings.

3 Click Configure the Database.

4 The Data Source should contain the hostname or IP address to use 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.

NOTE: 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 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 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 Dell 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. 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 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 the Cloud Access Manager application portal has been accessed by users.
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 Dell 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 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 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 FQDN’s 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 the users always use the same proxy host unless in a failover situation.

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 on 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.
Legal notices

© 2015 Dell Inc.
ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser’s personal use without the written permission of Dell Inc.

The information in this document is provided in connection with Dell products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Dell products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, DELL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL DELL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF DELL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Dell makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Dell does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Dell Inc.
Attn: LEGAL Dept
5 Polaris Way
Aliso Viejo, CA 92656

Refer to our web site (software.dell.com) for regional and international office information.

Trademarks

Dell, the Dell logo and Dell™ One Identity Cloud Access Manager are trademarks of Dell Inc. and/or its affiliates. Microsoft, Windows, SQL Server and Microsoft .NET are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell disclaims any proprietary interest in the marks and names of others.

Legend

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

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

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