Authlogics Authentication Server

High availability, Load balancing and Redundancy

Product Version: 4.2

Publication date: February 2023

Call us on: +44 1344 568 900 (UK/EMEA)
+1 408 706 2866 (US)

Email us: sales@authlogics.com

The information contained in this document represents the current view of Authlogics on the issues discussed as of the date of publication. Because Authlogics must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Authlogics, and Authlogics cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. AUTHLOGICS MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS Document.

Table of Contents

Introduction

This document has been created to show how Authlogics Multi-factor Authentication can be made to highly available, load-balanced and redundant based on the various agents authenticating to the Authlogics servers.

For Enterprise environments, Authlogics recommends that at least 2 Authlogics Servers are deployed within an environment however, more than 2 servers can be deployed as required.

Furthermore, when the enterprise is spread over numerous geographic locations, we recommend that each location has its own Authlogics Authentication Server deployments so that authentication requests are sent over potentially slow WAN links and processed locally

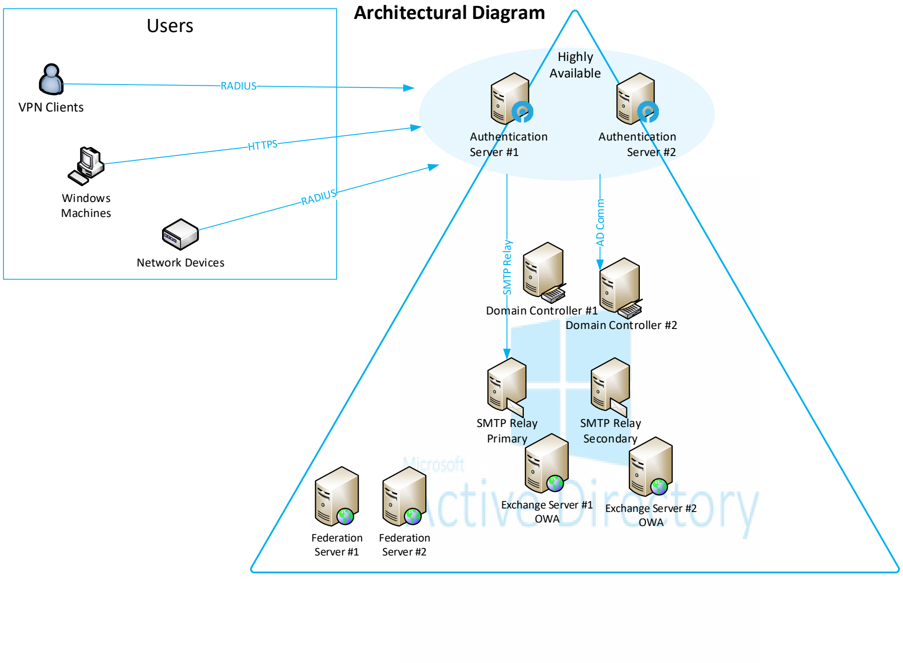
The Authlogics Database is Active Directory

Authlogics utilises the existing Active Directory database as the underlying user account database; with no schema extensions. As such, in environments where there are multiple Domain Controllers, the Authlogics settings and user information is automatically replicated to the multiple deployed Domain Controllers.

For recovery purposes, an install of a new Authlogics server, with the private key of the original certificate, will be able to access the user and settings from the Active Directory with no loss of data.

Architecture

The following higher-level architecture diagram depicts a typical Authlogics deployment showing the various clients attaching to the Authlogics servers.



Agents

Authlogics Windows Desktop Agent

The Authlogics Windows Desktop Agent (WDA) is designed for high availability as soon as more than one Authlogics Authentication Server is installed within the AD forest. When attempting an authentication request, WDA will query Active Directory to determine the names of all deployed Authlogics servers. Once WDA knows what Authlogics servers are registered within AD, WDA will then poll the Authlogics servers to determine which server has the fastest response time.

As soon as the first Authlogics server responds, the authentication request will be sent to the that Authlogics Authentication Server. If one of the registered Authlogics Server is not available, the other registered serves will respond and authentication requests will only be passed to these servers. If no servers are available then WDA will work offline.

With this functionality, WDA is natively Active-Active highly available and network load-balancing is not required. WDA determines which servers are accessible and the server which responds the quickest will be used to process the authentication request. This is also useful if PC's move between different offices to ensure the local Authentication Server is used.

Authlogics Exchange Agent

As with the Windows Desktop Agent, the Authlogics Exchange Agent is also designed to be automatically highly available as soon as more than one Authlogics Authentication Server is deployed within the AD forest. When attempting an authentication request, the Exchange Agent will query Active Directory and request the server names of all deployed Authlogics servers. Authlogics Exchange Agent will poll the registered Authlogics Authentication Server and will determine each server's availability.

Authlogics Exchange Server agent will then send the authentication requests to the first responding server thus satisfying both high-availability, redundancy and load-balancing natively in an Active-Active manner.

Authlogics ADFS Agent

The Authlogics ADFS Agent is also designed to be automatically highly available as soon as more than one Authlogics Authentication Server is deployed within the AD forest. When attempting an authentication request, Authlogics ADFS Agent will query Active Directory and request the server names of all deployed Authlogics servers. Authlogics ADFS Agent will poll the registered Authlogics Authentication Server and will determine each server's availability.

Authlogics ADFS Agent will then send the authentication requests to the first responding server thus satisfying both high-availability, redundancy and load-balancing natively in an Active-Active manner.

Authlogics RADIUS Server

Every deployed Authlogics Authentication Server deployed within the environment is a RADIUS Server. They are available to be accept RADIUS authentication requests from RADIUS clients, e.g. from VPN solutions like Palo Alto, Cisco Server , F5, Citrix and Linux Servers. Authlogics leverages the Microsoft Network Policy Server role for processing RADIUS server authentication.

> ***Note***
> *Ensure that all the Authlogics RADIUS Servers have the appropriate RADIUS clients configured within the Network Policy Server. Please refer to the Authlogics Authentication Server for more information.*

High availability, load-balancing and redundancy can be achieved in multiple ways. Below is a description of these mechanisms.

Active-Passive

This is the most common deployment method where configuration of the RADIUS client defines the load-balancing / high-availability by specifying the Primary and Secondary RADIUS servers at the client end.

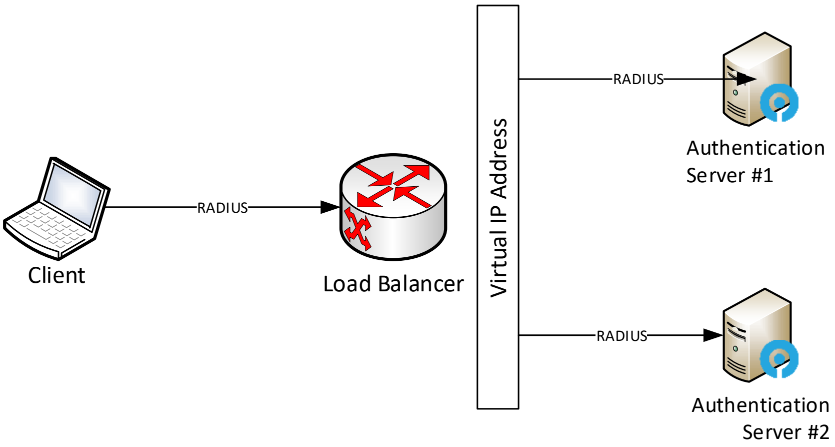
In this scenario, Authlogics Server #1 will be configured as the Primary RADIUS Server and Authlogics Server #2 as the Secondary RADIUS Server. When configured in this manner, the RADIUS client will send authentication requests to the Primary RADIUS Server. Should this server not be available, then the client will fall-over to the Secondary Server for authentication request processing.

Active-Active

To make Authlogics RADIUS Server highly available in an Active-Active manner, multiple Authlogics Authentication Servers must be published behind a Hardware or Software Load Balancer such as Windows Network Load Balancing (NLB).

The load balancer will create a Virtual IP Address and forward the RADIUS protocols UDP ports1645 and 1812. RADIUS clients will pass RADIUS authentication requests to this virtual IP address. The load-balancer will then determine the Authlogics Server availability and pass the authentication request to the appropriate server for processing.

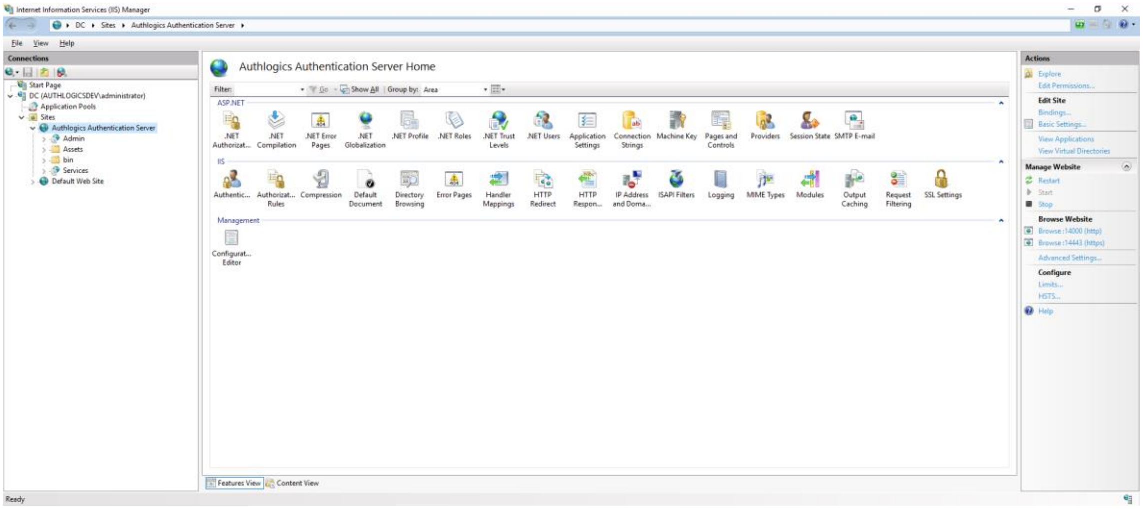
The following diagram depicts this scenario.



Authlogics Authentication Server Services

Authlogics Authentication Servers are also deployed with specific services, namely the Self-Service Portal, Web Operator Console and Web Service APIs. These services are web sites and services published on the Authentication Server's Internet Information Services (IIS) instance under the site **Authlogics Authentication Server.**

By default, these sites are running on the HTTPs protocol bound to port 14443.

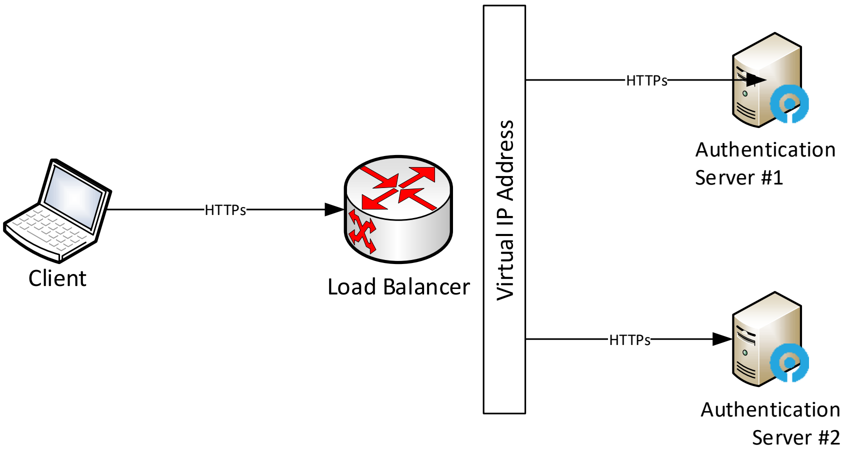


In order to load balance these services and make them highly available and redundant, a hardware or software load-balancer will need to be implemented and reverse proxy these protocols.

The following services are published on Authlogics Authentication Servers:

- Self-Service Portal - https://{Authlogics Servername}:14443/login.aspx
- Web operator console - https://{Authlogics Servername}:14443/admin
- Web Service APIs -https://{Authlogics Servername}:14443/services/wsapi.asmx

The following diagram shows the infrastructure:


Client
HTTPs
Load Balancer
Virtual IP Address
HTTPs
Authentication Server #1
HTTPs
Authentication Server #2