Cluster installation - SSO

ⓘ Last reviewed: 2017-08-30

Overview

This page specifies the requirements, and steps for clustered deployment of Ubisecure SSO. The scope of the document includes the overall deployment architecture, installation of reverse proxy, Installation of Ubisecure applications and LDAP.

Goals

The pursued goals affect the choice of clustering algorithms and deployment architecture. The possible goals, and recommended solutions for clustering each component of the Ubisecure SSO are the following:

- **High Availability**
  The system remains available despite a failing node. Improved availability is achieved using supported active/passive, High Availability clustering.

- **Scalability and High Availability**
  The system remains available despite a failing node, and can be scaled to serve more clients in a time unit. Improved performance is achieved using active/active clustering for SSO Server and Redis Cluster in-memory database cluster for storing session data.

Prerequisites

Competence in the following technologies is required for deploying a Ubisecure SSO cluster:

- Application server clustering (included Tomcat Server)
- Directory server clustering and replication (OpenLDAP for Linux / ADLDS for Windows)
- Reverse proxy (Environment specific, not provided by Ubisecure)
- Redis, in-memory data structure store (Not provided by Ubisecure)

High Level Architecture Overview, Recommended Clustering Setups

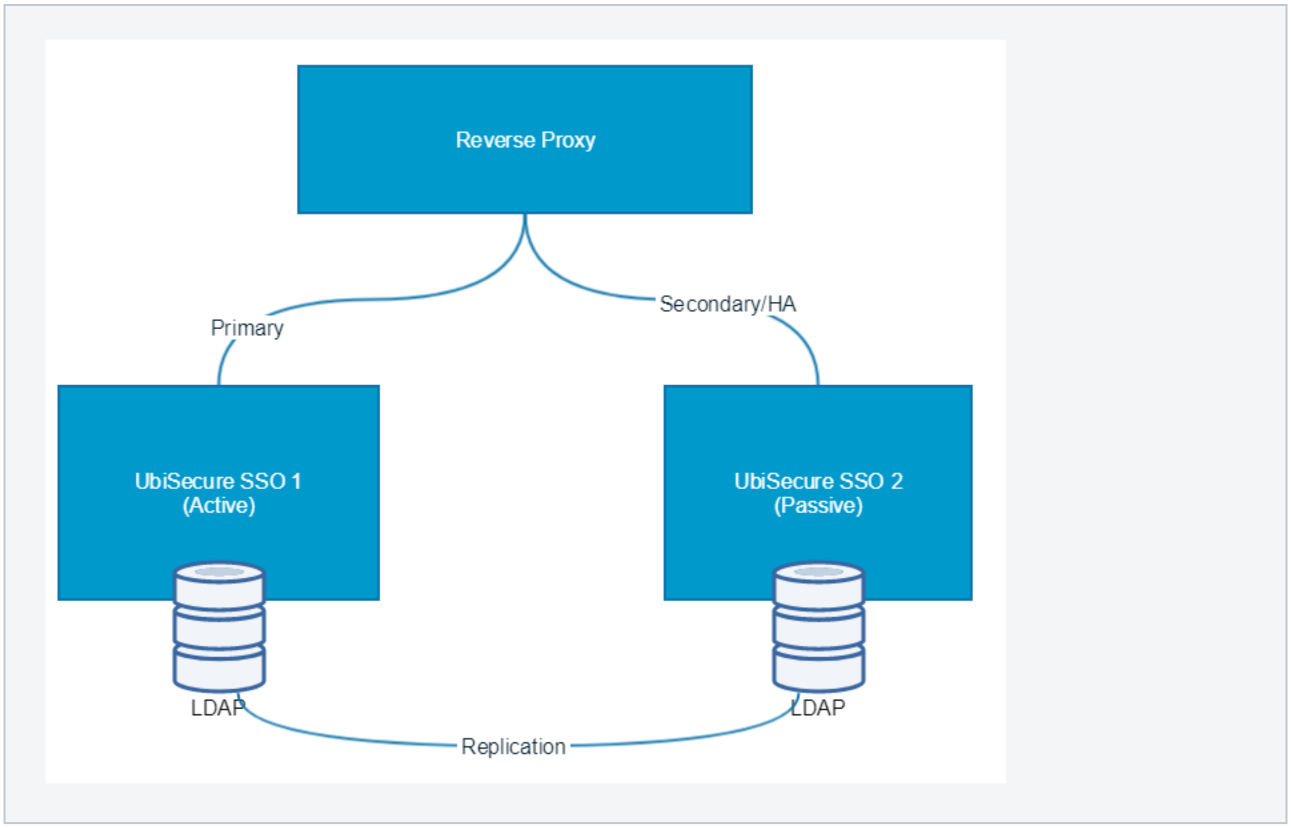
SSO High availability cluster

Diagram below describes the basic SSO high avalability cluster.

High availability is achieved by installing two SSO instances in active/passive cluster, so that there is one active SSO node, and another passive SSO node.

Note that Ubilogin Directory is replicated between two LDAP instances, but both SSO's use their own Ubilogin Directory. Optionally Ubilogin Directory services can be installed also into their own nodes.

Reverse proxy is configured to use primarily SSO1, and SSO2 only when SSO1 is not available.

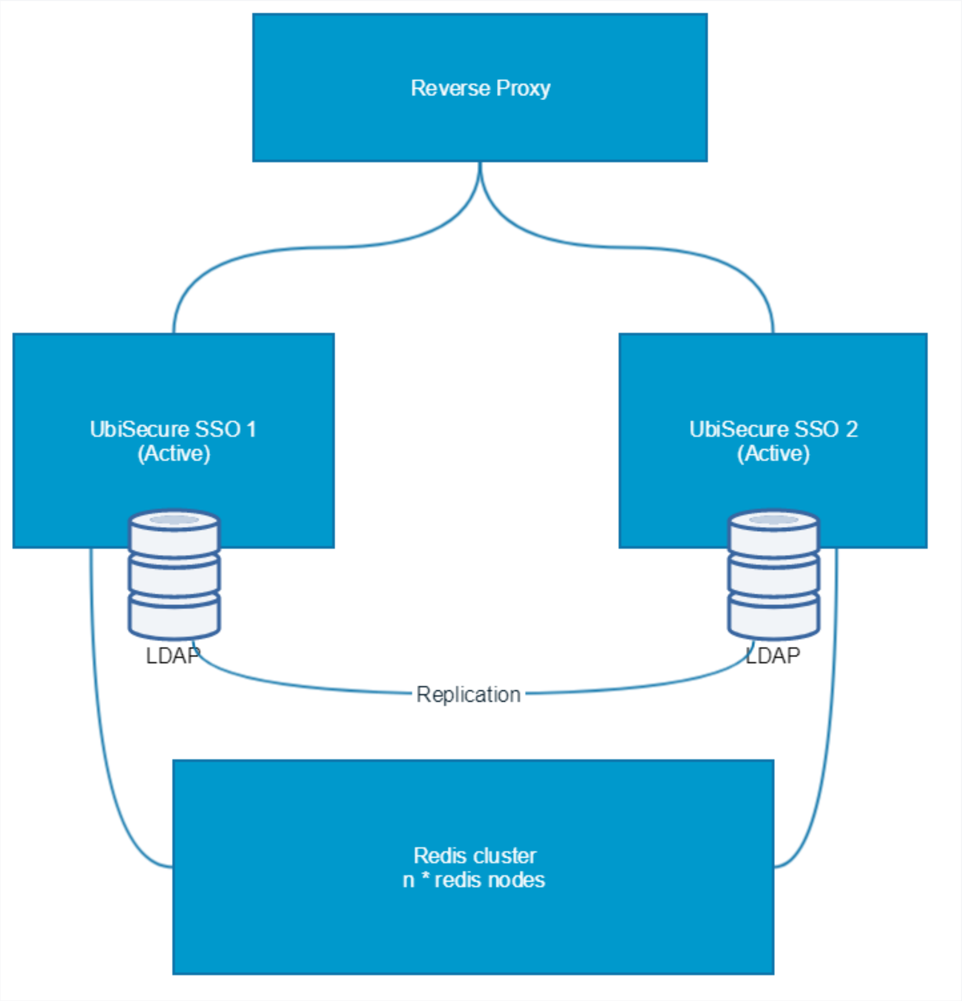


SSO Scalability and High availability cluster

Diagram below describes the basic SSO scalability and high availability setup.

Scalability and high availability is achieved by installing two or more SSO instances, a Ubilogin Directory instances, and a Redis cluster that is used to store session related data. Reverse proxy is configured to even the load on the SSO instances.

If only two SSO instances are installed, the Ubilogin Directory instances can be installed in SSO nodes. If more than two SSO instances are installed, it's recommended to install a separate Ubilogin Directory cluster with two nodes.



Components

Reverse Proxy

Reverse proxy is used to take care of high availability and load balancing (in scalability setup only). Installed into a separate server node.

Ubisecure SSO server

SSO server instance running on Tomcat.

Ubilogin Directory

Stores the configurations, user and session data (SSO can be configured to use Redis backed session storage to improve performance.

Redis

Redis is a open source in-memory database project. https://redis.io/

SSO can be configured to use Redis backed session storage to improve performance.

Cluster Installation

Overview

An overview of deploying Ubisecure SSO cluster is described in the following steps:

1. Install Ubilogin Directory (ADLDS or OpenLDAP) in both nodes
2. Configure Ubilogin Directory replication

3. Configure all the Ubisecure SSO applications on the first node.
    a. Install everything as instructed in the single node installation instructions, but do not run the last step (do not start SSO/Tomcat)
4. Copy the Ubisecure SSO configurations from the first node to the other node.
5. Install and configure the reverse proxy
6. Only on *scalability* setup: Install and configure Redis cluster, configure SSO to use Redis backed session storage
7. Start SSO in both nodes
8. Start reverse proxy

Cluster can be installed into windows or linux platforms

Installation steps

- Linux high availability setup - SSO
    - Linux scalability and high availability setup - SSO
    - OpenLDAP clustering - SSO
        - Install node 1 - SSO
        - Install node 2 - SSO
        - Firewall considerations - SSO
        - Troubleshooting for OpenLDAP clustering - SSO
- Windows high availability setup - SSO
    - AD LDS installation - SSO
        - AD LDS installation requirements - SSO
        - AD LDS installation steps (nodes 1 and 2) - SSO
        - AD LDS clustering setup (node 1) - SSO
        - AD LDS clustering setup (node 2) - SSO
    - Windows reverse proxy installation - SSO
    - Windows scalability and high availability setup - SSO
- Redis configuration - SSO