Self Service Password Reset

Performance and Sizing Guidelines

July 2023

Legal Notice

© Copyright 2023 Micro Focus or one of its affiliates.

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

For additional information, such as certification-related notices and trademarks, see http://www.microocus.com/about/legal/.

Contents

About this Book **5**

1 Self Service Password Reset Overview **7**

Self Service Password Reset Key Features. 7

2 Test Strategy **9**

3 Performance/Reliability/Stress Tools **11**

4 Test Environment Configuration **13**

SSPR Server 13
Active Directory Server. 13
MS SQL Database 14

5 Results **15**

Active Directory 15
New User Registration. 15
Change Password. 16
Forgotten Password. 16
External Database (MS-SQL) 18
New User Registration. 19
Change Password. 19
Forgotten Password. 20

About this Book

This guide provides the performance and sizing recommendations for Self Service Password Reset. This information helps you in deploying the correct configuration in your environment. The test results are simulated in a lab environment. On similar hardware, you may have different results. The test result may vary based on the applications used, type of data, user store, and a number of other dependent components operating in the environment. It is recommended to first verify the performance in your environment before deploying the product in a high-scale environment.

For information about the test strategy, hardware, and software used in the tests, See Test Strategy.

1 Self Service Password Reset Overview

Self Service Password Reset is a web-based password management solution. You can deploy SSPR to any web server or application server that supports a web archive. It eliminates users' dependency on administrators' assistance for changing passwords. It brings higher returns by reducing the cost and workload of the help desk. It allows you to ensure that all passwords in the organization comply with established best practice policies.

Self Service Password Reset also provides enhanced security. The user gets authenticated through a series of questions and answers known only to the user. During password reset, Self Service Password Reset uses a challenge-response authentication method to authenticate the user. You can store the challenge-response information in the back-end directory, external database, or local database. Users can change or reset their password and reset any forgotten password by using the configured challenge-response information.

Self Service Password Reset increases a user's productivity by synchronizing changed passwords, eliminating the need for users to wait for password resets and account unlocks. At the same time, the help desk can perform tasks more critical than password resets.

To learn more about the key features of Self Service Password Reset, see "Self Service Password Reset Key Features" on page 7

Self Service Password Reset Key Features

Self Service Password Reset provides the following key features and benefits:

- **Easily Change Passwords:** Users can change their password without the help of an administrator.
- **Reset Forgotten Passwords:** Users can reset their passwords by answering challenge questions configured by an administrator. Self Service Password Reset stores the challenge questions and the users' responses for when they forget their password.
- **Recover Forgotten Username:** Users can easily search for forgotten usernames by using the search filter that is configurable by administrators.
- **Configure Challenge-Response Authentication:** Administrators can configure a set of challenge questions for the users. The questions can include random and required questions. The first time users log into Self Service Password Reset, it prompts users to provide answers to these questions. Users can reset their password by answering the same questions they saved earlier.
- **Self-Registration for New Users:** New users can self-register, saving time and money.
- **Activate User Accounts:** Administrators create or provision LDAP accounts for the users, then the users claim these accounts for the first authentication and set a password through the Activation module.
- **Edit Profile:** Users can view and update their profiles.
- **Search for People:** Users can search for their information as well as search for information about colleagues. Users can perform interactive wildcard searches.

- **Simplify Help Desk Support:** The Help Desk Module simplifies administrative tasks, such as resetting passwords, clearing intruder lockout, unlocking user accounts, and debugging user information.
- **Create Password Policies:** Administrators can use password policies to enforce restrictions on the types of passwords that users can create.
- **Generate Usage and Lockout Reports:** Administrators can generate reports for intruder lockout, daily usage statistics, and online log information for debugging purposes.
- **Supports Localization:** Self Service Password Reset provides an easy way to add new languages. Self Service Password Reset provides default localization support for English, Canadian English, Canadian French, Catalan, Chinese Simplified, Chinese Traditional, Danish, Dutch, Hebrew, French, German, Italian, Japanese, Polish, Portuguese (Brazilian), Russian, Spanish, Swedish, and Norwegian.
- **Easily Customized:** Administrators can easily customize Self Service Password Reset to integrate with external web authentication methods as well as integrate with NetIQ Identity Manager to add automated workflows and account claiming support.
- **Supports of Web Services:** Self Service Password Reset supports web services.
- **Supports Google reCAPTCHA API:** Self Service Password Reset supports Google reCAPTCHA API to protects your site from spam and abuse by using the advanced risk analysis techniques to tell humans and bots apart .
- **SMS Gateway integration:** Self Service Password Reset supports SMS Gateway integration to manage the way to send specified, bulk text messages.
- **Mail Server Configuration and Notification Support:** Self Service Password Reset supports the mail server configuration and provides notification support.
- **Supports Single Sign-On (SSO):** Self Service Password Reset supports SSO that allows the users to log in to any of several related, yet independent, software systems with a single ID and password.

2 Test Strategy

The test is designed to represent a medium-sized business with heavy traffic to help predict performance for both smaller and larger implementations. The performance, reliability, and scalability tests cover the critical areas that customers need to know to design a system for their environment.

The tests cover major functional areas such as the following:

1. Set up challenge responses in Active Directory and External DB (MS-SQL) separately.
2. Changing user's password via **Private change password** module post login.
3. Change user's password when they forget their password via **Public forgotten password** module, after validating their LDAP attribute stored in Active Directory and the challenge-response stored in Active Directory / external database.

3 Performance/Reliability/Stress Tools

The Micro Focus LoadRunner tool is used for testing SSPR. This tool replicates larger number of concurrent user login transactions. It supports handling of server response parameters using different correlation techniques which helps in handling the session id's specific to each login request. The parameterization support provided by the tool helps in dynamic replacement of user credentials, LDAP specific attributes, and challenge response answers. The tools controller feature helps to generate test scenarios to replicate more closely with the real-world environments with real browser interactions.

Other Factors influencing Performance:

- **Network Bandwidth:** Gigabit copper networking is used throughout the testing process to meet the testing result. If you are running at a slow Internet connection, the product cannot solve this bottleneck. In this case, the connectivity between SSPR Server, LDAP Directory and external Database are all part of same subnet.
- **LDAP User Stores:** This critical component can be another major cause for the variance in the SSPR results.The variance depends upon configuration, hardware, and the layout of the directory. The user store is usually the most common problem with performance, so testing must be done with the LDAP user stores that are used in the environment. Expect adjustments if you are attempting to get the maximum speed in a cluster environment for different LDAP user stores.
- **Timeout:** If you run a performance test, you must consider sessions that are stored on the SSPR server. Make sure there is a timeout between the tests so that the tests do not overrun the number of user sessions on the system.

4 Test Environment Configuration

The following parameters were tuned during the test to optimize the system performance. Use the following information to configure LDAP directory profiles and settings for your environment.

- "SSPR Server" on page 13
- "Active Directory Server" on page 13
- "MS SQL Database" on page 14

SSPR Server

The following table describes the test environment configuration:

Operating System	SUSE Linux Enterprise Server 12 SP4 (x86_64)
System Type	(x86_64) VM
Processor	Intel(R) Xeon(R) Gold 6130 CPU @ 2.10GHz, 2095.078 Mhz, 8 Cores
Installed Physical Memory (RAM)	4.00 GB
Total Physical Memory	4.00 GB
Available Physical Memory	2.00 GB
Total Virtual Memory	1.00 GB
Available Virtual Memory	0.95 GB
Hard Disk	40.00 GB

Active Directory Server

The following table describes the test environment configuration:

Operating System	Windows Server 2019 Standard
System Type	64 bit, x64 based processor
Processor	Intel(R) Xeon(R) Gold 6130 CPU @ 2.10GHz, 2.10 GHz, 4 Cores
Installed Physical Memory (RAM)	16.00 GB
Total Physical Memory	16.00 GB
Available Physical Memory	12.00 GB
Total Virtual Memory	18.34 GB

Available Virtual Memory	14.4 GB
Hard Disk	160 GB
Total paging size	2.4 GB

MS SQL Database

The following table describes the test environment configuration:

Operating System	Windows Server 2016 Standard
Database Version	Microsoft SQL Server 2017 (RTM) - 14.0.1000.169 (X64)
System Type	64 bit, x64 based processor
Processor	Intel(R) Xeon(R) Gold 6130 CPU @ 2.10GHz, 2.10 GHz,1 Core
Total Physical Memory	4.00 GB
Available Physical Memory	2.43 GB
Total Virtual Memory	4.69 GB
Available Virtual Memory	3.04 GB
Hard Disk	40.00 GB
Total paging size	704 MB

5 Results

Tests are run on Self Service Password Reset 4.5.0.0. Later versions of Self Service Password Reset are expected to behave similarly. These tests include the performance of SSPR with the following Challenge-Response Storage Locations:

- "Active Directory" on page 15
- "External Database (MS-SQL)" on page 18

Active Directory

The following table describes the details of test environment.

Load	50,000 virtual users
Directory	Active Directory
Challenge-Response Storage Location	Active Directory

The tests cover the following functional areas:

- "New User Registration" on page 15
- "Change Password" on page 16
- "Forgotten Password" on page 16

New User Registration

This test is to measure the performance of Self Service Password Reset while registering a new user. Perform the following steps to check the performance:

1. Access SSPR login page (first time) and login with the credentials.
2. Answer the Challenge-Response
3. Save the responses and logout.

Scenario: Total of 50000 users performing submitting their challenge-response for the first time in which 200 are concurrent users performing transactions simultaneously.

The following table describes how the application performs.

Number of transactions	Number of concurrent users	Time interval between each concurrent user login	Constant wait Timer between each transactions	CPU and memory usage	Number of Failed Transaction
50000	200	2seconds	◆ 10 seconds to login ◆ 10 seconds to answer challenge-response	◆ CPU- 99% ◆ Memory- 24%	9

Change Password

This test is to measure the performance of Self Service Password Reset while changing the password of a existing user. Perform the following steps to check the performance:

1. Access SSPR login page and login.
2. Post authentication, click **Change password**.
3. Auto logout from the server after changing password.

Scenario: Total of 50000 users changing their password in which 180 are concurrent users performing transactions simultaneously.

The following table describes how the system performs.

Number of transactions	Number of concurrent users	Time interval between each concurrent user login	Constant wait Timer between each transactions	CPU and memory usage	Number of Failed Transaction
50000	180	1 second	◆ 20 seconds to login. ◆ 20 seconds to change password.	◆ CPU- 56% ◆ Memory- 23%	6

Forgotten Password

This test is to measure the performance of Self Service Password Reset while changing the password through forgotten password module. Perform the following steps to check the performance:

NOTE: Forgotten password operation requires high CPU utilization. So, necessary resources need to be allocated before performing a higher number of concurrent user transactions.

1. Access SSPR login page.
2. Click **Forgotten Password**.

3. Enter the last name for user validation.
4. Answer the challenge-response.
5. Change the password.
6. Auto log out from the server after changing password.

Scenario: Total of 50000 users changing their password in which 180 are concurrent users performing transactions simultaneously.

The following table describes how the application performs.

Number of transactions	Number of concurrent users	Time interval between each concurrent user login	Constant wait Timer between each transactions	CPU and memory usage	Number of Failed Transaction
50000	180	2 seconds	◆ 10 seconds to enter the last name. ◆ 4 seconds to answer challenge-response ◆ 10 seconds to change password.	◆ CPU- 99% ◆ Memory- 23%	6

Scenario: Total of 50000 users changing their password in which 450 are concurrent users performing transactions simultaneously.

Number of transactions	Number of concurrent users	Time interval between each concurrent user login	Constant wait Timer between each transactions	CPU and memory usage	Number of Failed Transaction
50000	450	2 seconds	◆ 10 seconds to enter the last name. ◆ 4 seconds to answer challenge-response. ◆ 10 seconds to change password.	◆ CPU- 99% ◆ Memory- 23%	24

Scenario: Total of 50000 users changing their password in which 850 are concurrent users performing transactions simultaneously.

Number of transactions	Number of concurrent users	Time interval between each concurrent user login	Constant wait Timer between each transactions	CPU and memory usage	Number of Failed Transaction
50000	850	2 seconds	◆ 10 seconds to enter the last name. ◆ 4 seconds to answer challenge-response ◆ 10 seconds to change password.	◆ CPU- 99% ◆ Memory- 23%	1383

Scenario: Total of 50000 users changing their password in which 1100 are concurrent users performing transactions simultaneously.

Number of transactions	Number of concurrent users	Time interval between each concurrent user login	Constant wait Timer between each transactions	CPU and memory usage	Number of Failed Transaction
50000	1100	2 seconds	◆ 10 seconds to enter the last name. ◆ 4 seconds to answer challenge-response ◆ 10 seconds to change password.	◆ CPU- 99% ◆ Memory- 23%	24834

External Database (MS-SQL)

The following table describes the details of test environment:

Load	50 ,000
Directory	Active Directory
Challenge-Response Storage	External Database (MS-SQL)

The tests cover the following functional areas:

- "New User Registration" on page 19
- "Change Password" on page 19
- "Forgotten Password" on page 20

New User Registration

This test is to measure the performance of Self Service Password Reset while registering a new user. Perform the following steps to check the performance.

1. Access SSPR login page and login with the credentials.
2. Answer Challenge-Response.
3. Save the responses and logout.

Scenario: Total of 50000 users performing submitting their challenge-response for the first time in which 200 are concurrent users performing transactions simultaneously.

The following table describes how the application performs.

Number of transactions	Number of concurrent users	Time interval between each concurrent user login	Constant wait Timer between each transactions	CPU and memory usage	Number of Failed Transaction
50000	200	2 seconds	• 10 seconds to login. • 10 seconds to answer challenge-response.	• CPU- 99% • Memory- 24%	1

Change Password

This test is to measure the performance of Self Service Password Reset while changing the password of an existing user. Perform the following steps to check the performance.

1. Access SSPR login page and login.
2. Post authentication, Click **Change password**.
3. Auto logout from the server after changing password.

Scenario: Total of 50000 users changing their password in which 200 are concurrent users performing transactions simultaneously.

The following table describes how the application performs.

Number of transactions	Number of concurrent users	Time interval between each concurrent user login	Constant wait Timer between each transactions	Max CPU and memory usage	Number of Failed Transaction
50000	200	1 seconds	◆ 20 seconds to login. ◆ 20 seconds to change password.	◆ CPU- 99% ◆ Memory- 24%	23

Forgotten Password

This test is to measure the performance of Self Service Password Reset while changing the password through forgotten password module. Perform the following steps to check the performance.

NOTE: Forgotten password operation requires high CPU utilization. So, necessary resources need to be allocated before performing higher number of concurrent user transactions.

1. Access SSPR login page.
2. Click **Forgotten Password**.
3. Enter the last name for user validation.
4. Answer the challenge-response.
5. Change the password.
6. Auto log out from the server after changing password.

Scenario: Total of 50000 users changing their password in which 200 are concurrent users performing transactions simultaneously.

The following table describes how the application performs.

Number of transactions	Number of concurrent users	Time interval between each concurrent user login	Constant wait Timer between each transactions	Max CPU and memory usage	Number of Failed Transaction
50000	200	2 seconds	◆ 10 seconds to enter the last name. ◆ 4 seconds to answer challenge-response ◆ 10 seconds to change password.	◆ CPU- 99% ◆ Memory- 24%	35