Business Process Monitor

Software Version: 9.51

Script Segregation - Internal Guide for SaaS

Document Release Date: November 2018

Software Release Date: November 2018

Legal notices

Warranty

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.

Restricted rights legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright notice

Trademark notices

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

AMD, the AMD Arrow symbol and ATI are trademarks of Advanced Micro Devices, Inc.

Citrix® and XenDesktop® are registered trademarks of Citrix Systems, Inc. and/or one more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries.

Google™ and Google Maps™ are trademarks of Google Inc.

Intel®, Itanium®, Pentium®, and Intel® Xeon® are trademarks of Intel Corporation in the U.S. and other countries.

iPad® and iPhone® are trademarks of Apple Inc.

Java is a registered trademark of Oracle and/or its affiliates.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Microsoft®, Windows®, Lync®, Windows NT®, Windows® XP, Windows Vista® and Windows Server® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

NVIDIA® is a trademark and/or registered trademark of NVIDIA Corporation in the U.S. and other countries.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates.

Red Hat® is a registered trademark of Red Hat, Inc. in the United States and other countries.

SAP® is the trademark or registered trademark of SAP SE in Germany and in several other countries.

UNIX® is a registered trademark of The Open Group.

Documentation updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To verify you are using the most recent edition of a document, go to https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result?doctype=manuals?keyword=.

To check for recent software patches, go to https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result?doctype=patches?keyword=.

This site requires that you register for a Passport and sign in. To register for a Passport ID, go to https://cf.passport.softwaregrp.com/hppcf/login.do.

Or click the **Register** link at the top of the Software Support page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your sales representative for details.

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To verify you are using the most recent edition of a document, go to https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result?doctype=online help.

This site requires that you register for a Passport and sign in. To register for a Passport ID, go to https://cf.passport.softwaregrp.com/hppcf/login.do.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your sales representative for details.

For information and details about the products, services, and support that offers, contact your Client Director.

Support

Visit the Software Support Online web site at https://softwaresupport.softwaregrp.com/.

This web site provides contact information and details about the products, services, and support that offers.

online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Manage software licenses
- Download new versions of software or software patches
- Access product documentation
- Manage support contracts
- Look up support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require you to register as a Passport user and sign in. Many also require a support contract.

To register for a Passport ID, go to https://cf.passport.softwaregrp.com/hppcf/login.do.

Visit the Software Support Online web site at https://softwaresupport.softwaregrp.com/.

This web site provides contact information and details about the products, services, and support that offers.

online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Manage software licenses
- Download software
- Access product documentation
- Manage support contracts
- Look up support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require you to register as a Passport user and sign in. Many also require a support contract.

To register for a Passport ID, go to https://softwaresupport.softwaregrp.com/.

To check for recent updates or to verify that you are using the most recent edition of a document, contact your Client Director.

Contents

Chapter 1: About Script Segregation

The BPM Segregation feature was developed at the request of AppPulse Active team as well as other customers.

The main objective is to allow APM to assign script jobs from multiple customers to a single BPM instance, while a running script does not have any permission on any other location on the disk except for the script itself (read, write or execute). The same requirement exists for assigning script jobs for several instances.

All current BPM functionality has been preserved.

Chapter 2: Requirements

Platforms

- Script segregation is support only on Windows
- All machines must have the same operating system, the following operating systems are currently supported:
  - Microsoft Windows Server 2008 SP2 (32/64 bit) Standard and Enterprise Editions
  - Microsoft Windows Server 2008 R2 SP1 (64 bit) Standard and Enterprise Editions
- At least 5GB of free space is required on the C: drive in each implemented machine.

BSM Connector/APM Versions

- APM 9.50
- BPM 9.51

Functionality

The actions of **Set BPM as user** of **Set BPM Instance as user** are not allowed when this feature is activated as it is prohibited to assign multiple permissions on the MDRV process which runs the script.

Configuration

- The BPM workspace must be set as the **default workspace location** for all BPMs. This is required to remove permissions for Users group.
- A special BPM tool should be run by the implementer. This tool creates users and encrypts the passwords configuration file. The configuration file should be located in BPM configuration folder.
- You need to turn on a flag to enable the BPM segregation feature in the **topaz_agent_ctrl.cfg** file, located in the **<BPM Home>/tools** folder.

  To turn on this flag, in the **General** section add the following parameter:

  ```
  SegregationMode=1
  ```

- The number of created users is located at the top of the **script_segregation_users.cfg** file which is created in the **config** folder.

Chapter 3: Functional Specifications

Installation

To perform a bulk operation for several dozens BPMs, you need to automate the SaaS process.

> **NOTE:**
> All operations must be done as the machine administrator.

SaaS automation to configure Server Automation (SA) requires the following actions:

- Verify that there are no open folders in the machine.
- Stop BPM
- Install the required version of BPM
- Run **BPM Users Creator Tool** on the BPM machine. This tool must be run from a constant place on the disk and does the following:
    - Get as an input:
        - **<N>** - the number of created users
        - BPM workspace folder path
        - Configuration folder path to locate the output file
    - Generate **N** random passwords for the users before their creation. Each password will be 16 bytes length.
    - Create N users with the created N passwords in the **Users** group by Windows API with simple permissions. Consider creating a new group for the created users.
    - For each user, create a user profile. This profile should include the user Temp folder.
    - Encrypt the passwords created by AES256 encryption algorithm. For further information, see Encryption, on page 10.
    - Create a **BPM Users Configuration File** which will contain the following.
        - User name
        - User encrypted password
        - User Temp folder path

      This is the actual output of this tool. For further information, see BPM Users Configuration File, on page 13.
    - **Optional:** Create another configuration file with the user and unencrypted password for maintenance. This file must be cut from the machine.
    - Remove permissions (special permissions as well as any other permission such as read-only) from the BPM workspace for the **Users** groups. This is needed, as BPM installation may give permissions for Users group for the workspace folder.
    - Log every action in a log file with an ERROR tag for any error. System administrators should validate that there are no errors in the log. If there are any errors, stop the process.
    - Copy the **BPM Users Configuration File** to the Configuration folder given as an input.
- Add an entry in the **BPM config\topaz_agent_ctrl.cfg** file:

  In the **[General]** section, add **SegregationMode=1**
- Restart BPM

NOTE:
Automatic Password expiration is not supported by BPM. Therefore, a SaaS operator should run the **BPM Users Creator Tool** on a regular basis (for example once a month) and rerun the steps described above.

Chapter 4: Encryption

During Installation, BPM creates an encryption key unique for the installation machine. The encryption key is created by the **AES/ECB/NoPadding** algorithm.

The **BPM Users Creator Tool** will use the same algorithm for password encryption.

Before running a script by MDRV, note the following:

- You need to decrypt the password. This is done by the current API in use by **BPM HP_CRYPT_DECRYPT** which is compatible with the password encryption.
- You need to set the command line for a segregated running.

Chapter 5: Security Considerations

The following requirements are needed to comply with the new security layer we are providing with the script segregation feature:

- Make sure that the BPM machine does not contain any important web applications other than the BPM itself.
- Block unnecessary access of BPM machines to private network IPs. The BPM machines require access only to APM machines.
- Enable Tomcat authentication to prevent attacks against the BPM admin application.

These steps will prevent malicious BPM scripts meant to run on the BPM hosting server from harming the server.

Chapter 6: Limitations

QTP scripts are not supported.

The actions **set BPM as user** and **Set BPM Instance as user** are not allowed when this feature is activated as you cannot assign multiple double permissions to the MDRV process which runs the script.

Password expiration is not supported by BPM. Therefore, the SaaS operator should run **BPM Users Creator Tool** on a regular basis, for example once a month.

If BPM tries to execute additional MDRVs and there are no available users, the current run of the script will be skipped. The status of the run will be shown as **Skipped by segregation** in the BPM console. In general, we recommend to have at least the same number of users created as the number of scripts running.

Chapter 7: BPM Users Configuration File

Example of the Users Configuration file:

```
[General]
UserNum=100
[User1]
UserName=
UserPassword=
UserTempPath=
[User2]
UserName=
UserPassword=
UserTempPath=
```

Send documentation feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Script Segregation - Internal Guide for SaaS (Micro Focus Business Process Monitor 9.51)

Add your feedback to the email and click **Send**.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to docs.feedback@microfocus.com.

We appreciate your feedback!