

Replicate Reverse Proxies for IBM® Security Access Manager

Reagan Knowles
Identity & Access Management
Support Professional



Join IBM VIP Rewards

Engage. Earn points. Get Rewards.



IBM VIP Rewards is a way to engage with and recognize the ways that you, the client, add value to IBM. Complete fun challenges and get rewarded for interacting with IBM, learning new technologies and sharing your knowledge.

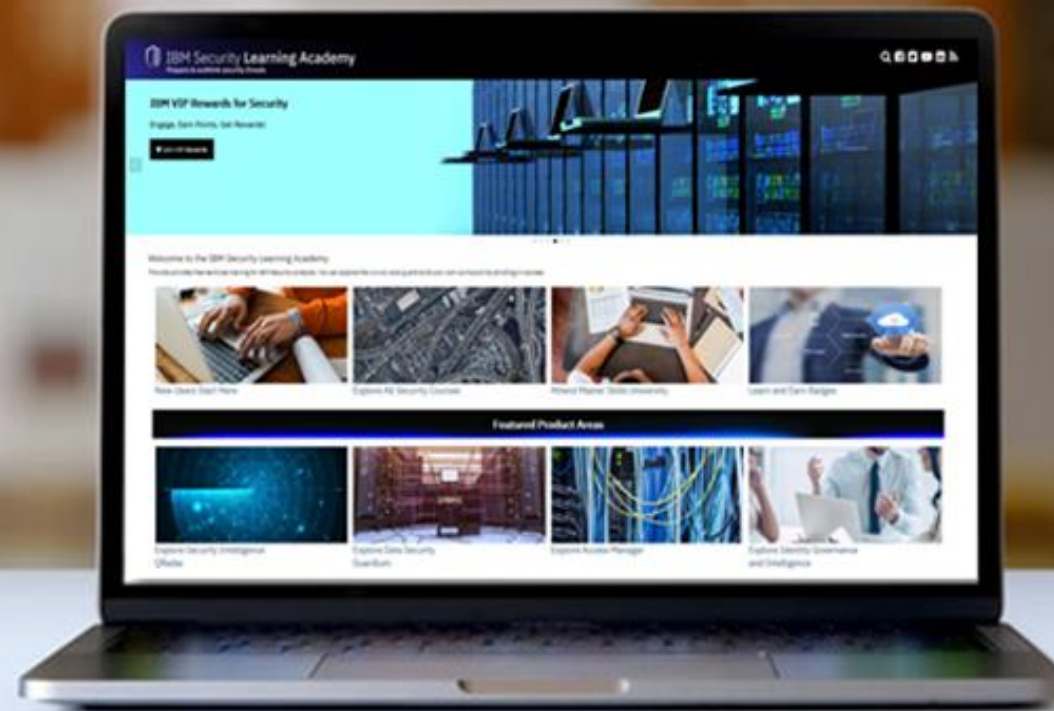
Learn more... ibm.biz/vip-rewards	Join IBM VIP Rewards for Security... ibm.biz/JoinIBMVIPRewards-Security
--	---



IBM VIP Rewards for **Security**

IBM Security Learning Academy

SecurityLearningAcademy.com



- Courses
- Videos
- Hands-on Labs
- Live Events
- Badges

Learning at no cost.

New content published daily.

Table of contents

- Benefits

- Three methods

Ansible playbook on github

Export/Import via LMI or REST API

pdadmin server sync command

- Troubleshooting

Benefits

- Save time
- Prevent mistakes
- Use with ease

Ansible playbook

- Visit Github for playbook samples for ISAM
- A bunch of content for the entire ISAM appliance!
- <https://github.com/IBM-Security/isam-ansible-playbook-sample>

Ansible playbook

- Example YAML files

IBM-Security / isam-ansible-playbook-sample		
Code Issues 5 Pull requests 0 Actions Projects 0 Wiki		
Branch: master isam-ansible-playbook-sample / web /		
svetterIO +1 playbook: import_certificate_mapping_files		
..		
configure_federated_directories.yml	+1 playbook: configure_federated_directories.yml	
configure_management_root.yml	Feature: gather_facts NO	
configure_policyserver.yml	Feature: gather_facts NO	
configure_reverseproxy_instances.yml	Feature: gather_facts NO	
configure_reverseproxy_junctions.yml	Feature: gather_facts NO	
configure_runtime_components.yml	+1 playbook: configure_runtime_components.yml	
create_reverseproxy_instances.yml	Feature: gather_facts NO	
create_sso_keys.yml	BugFix: Change role to corresponding st	
execute_pdadmin.yml	Feature: gather_facts NO	
export_sso_keys.yml	New Playbook: export sso keys	
import_certificate_mapping_files.yml	+1 playbook: import_certificate_mapping_files.yml	
import_keytab_files.yml	New playbooks: 9x	

IBM-Security / isam-ansible-playbook-sample		
Code Issues 5 Pull requests 0 Actions Projects 0 Wiki		
Branch: master isam-ansible-playbook-sample / aac /		
Sebastian-Vetter +1 playbook: configure_access_control_policy_resources		
..		
configure_access_control_attributes.yml	+1 playbook: configure_access_control_attributes.yml	
configure_access_control_policies.yml	+1 playbook: configure_access_control_policies.yml	
configure_access_control_policy_attachments.yml	+1 role: configure_access_control_policy_attachments	
configure_access_control_policy_resources.yml	+1 playbook: configure_access_control_policy_resources.yml	
configure_advanced_configurations.yml	New Playbook: configure advanced configurations	
configure_api_protection_clients.yml	Fix: description correction	
configure_api_protection_definitions.yml	Fix: description correction	
configure_authentication_mechanisms.yml	Typo: Whispaces, NewLines, gather_facts, exam	
configure_authentication_policies.yml	New playbooks: 9x	
configure_mapping_rules.yml	Typo: Whispaces, NewLines, gather_facts, exam	
configure_runtime_template_root.yml	CleanUp: gather_facts no for sub playbooks	
configure_scim.yml	+1 playbook: configure scim	

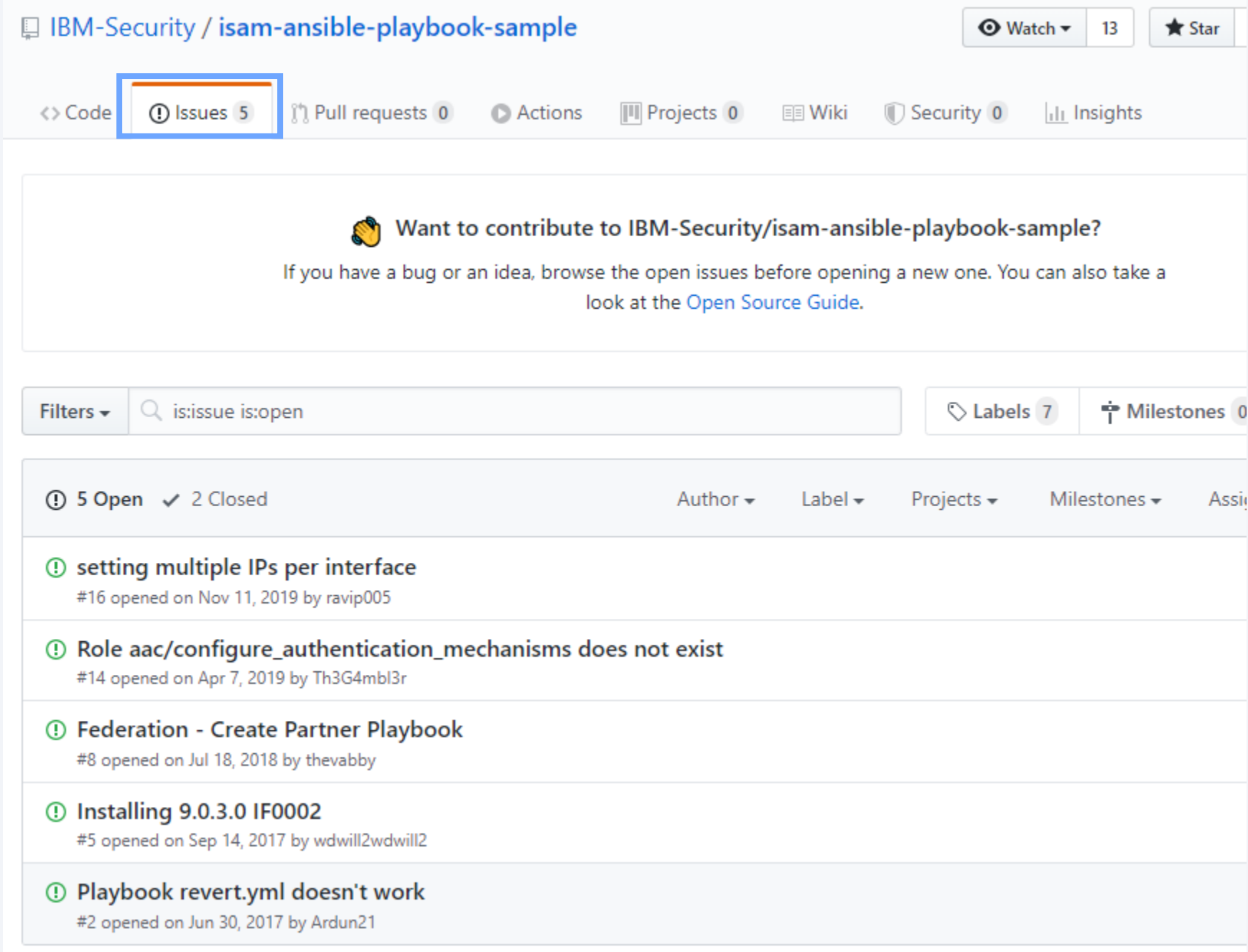
Ansible playbook

- Browse to [isam-ansible-playbook-sample/web/configure_reverseproxy_instances.yml](#)

```
---
# Configure
#   configure reverse proxy instances
#   Example:
#       instances:
#         - inst_name: default
#           entries:
#             - { method: set, stanza: server, entry_name: server-name,
value: default }
- hosts: "{{ hosts | default('all') }}"
  connection: local
  gather_facts: no
  roles:
    - role: web/configure_reverseproxy_instances
      tags: configure_reverseproxy_instances
```


Ansible playbook

- Post questions and comments to Github

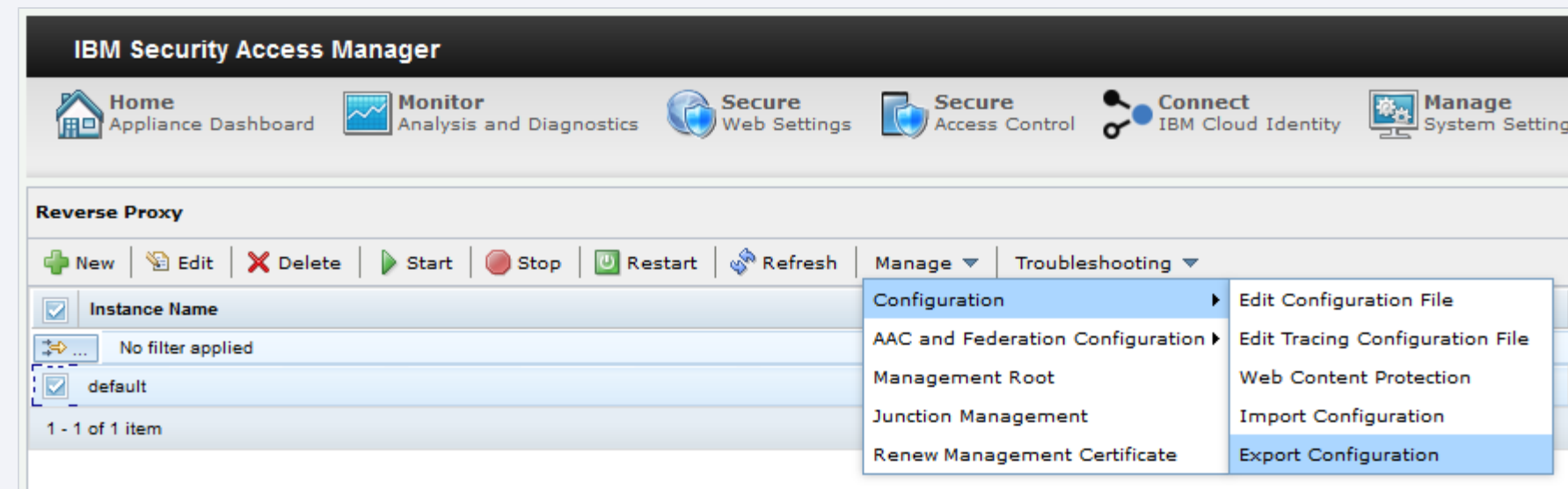


The screenshot shows the GitHub repository page for `IBM-Security / isam-ansible-playbook-sample`. The 'Issues' tab is selected and highlighted with a blue box. The repository has 13 stars and 5 issues. Below the repository header, there is a message encouraging contributions and a link to the Open Source Guide. The 'Issues' section shows 5 open issues and 2 closed issues. The list of open issues includes:

- setting multiple IPs per interface** (#16 opened on Nov 11, 2019 by ravip005)
- Role aac/configure_authentication_mechanisms does not exist** (#14 opened on Apr 7, 2019 by Th3G4mbl3r)
- Federation - Create Partner Playbook** (#8 opened on Jul 18, 2018 by thevabby)
- Installing 9.0.3.0 IF0002** (#5 opened on Sep 14, 2017 by wdwil2wdwil2)
- Playbook revert.yml doesn't work** (#2 opened on Jun 30, 2017 by Ardun21)

Export/Import via LMI

1. Select the reverse proxy
2. Manage drop-down
3. Configuration
4. Export Configuration (or Import)



Export via REST API

- GET <https://{hostname}/wga/reverseproxy/{id}?action=export>
- For curl, specify the output file

```
curl -k -H "Accept:application/json" -u "admin:admin" -X GET  
https://samapp2m1.tivlab.austin.ibm.com/wga/reverseproxy/default?action=export --output samapp2m1_default_config.zip
```

Import via REST API

- POST `https://{hostname}/wga/reverseproxy/{id}/migrate` -F file -F overwrite
- Specify the file name
- By default, files will not be overwritten (more later)

```
curl -k -H "Accept:application/json" -u "admin:admin" -X POST  
https://samapp1m1.tivlab.austin.ibm.com/wga/reverseproxy/default/migrate -F file=@samapp2_default_config.zip -F "overwrite=true"
```

Import via REST API

- POST `https://{hostname}/wga/reverseproxy/{id}/migrate -F file -F overwrite`

```
curl -k -H "Accept:application/json" -u "admin:admin" -X POST
https://samapp1m1.tivlab.austin.ibm.com/wga/reverseproxy/default/migrate -F file=@samapp2_default_config.zip -F "overwrite=false"

{"message":"Error: WGAWA0041E  The following files already exist:
\njmt/jmt.conf\nndynurl/dynurl.conf\nkeytab/pdsrv.sth\nkeytab/pdsrv.kdb"}
```

- If overwrite is false, then remove files from the zip to avoid the error

`/jmt/jmt.conf`

`/dynurl/dynurl.conf`

`/keytab/pdsrv.sth`

`/keytab/pdsrv.kdb`

(or just remove what you want and use `overwrite=true`)

Import via REST API

- Keep track of any manual changes you make to the zip. Some changes can prevent the zip from being imported.
- Incorrect directory structure results in error.

Good Path

Downloads > webseal_config.zip		
	Name ^	Type
✳	doc-root	File folder
✳	dynurl	File folder
✳	etc	File folder
✳	jmt	File folder
✳	junctions	File folder
✳	keytab	File folder

Bad Path

Downloads > samapp2m1_webseal_config.zip		
	Name ^	
✳	webseal_config	

A zip within a zip created this problem

After the Import – What stays the same?

- Not everything is exactly replicated
- Many parameters retain original values to maintain network settings

server-name

https-port

network-interface

bind-dn (LDAP)

master-host (Policy Server)

Be aware of Cluster Settings

- “Replicate with cluster” will always takes precedent

SSL Certificates

New

Delete

Refresh

Replicate with Cluster

☒

Manage ▼

No filter applied

Certificate Database Name ▲	Type
embedded_ldap_keys	Local
lmi_trust_store	Local
pdsrv	Local
rt_profile_keys	Local

Manage

Export/Import via LMI or REST API

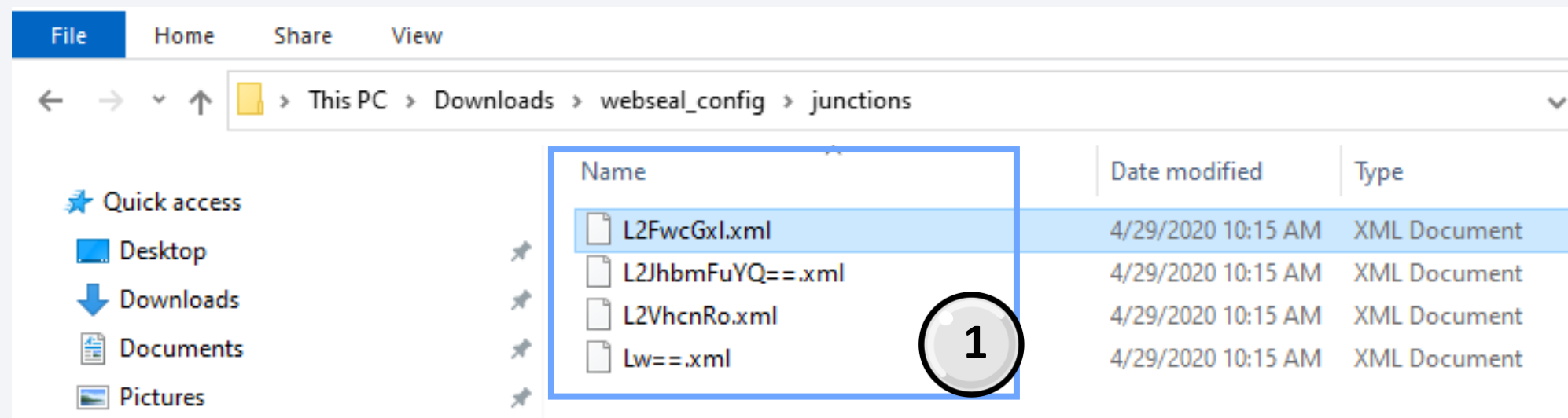
- If migration involves different back-end servers then create a script to programmatically change the back-end server IP addresses/hostnames
- Some junction properties might be different

HOST

PORT

VIRTHOSTNM

LOCALADDRESS



```
<JUNCTION>
  <VERSION>9.0.7.1</VERSION>
  <NAME>/earth</NAME>
  <JUCTYPE>tcp</JUCTYPE>
  <HARDLIMIT>0</HARDLIMIT>
  <SOFTLIMIT>0</SOFTLIMIT>
  <BASICAUTH>filter</BASICAUTH>
  <CLIENTID>do not insert</CLIENTID>
  <REQUESTENCODING>utf8_uri</REQUESTENCODING>
  <UUID>9ff11bf2-8a2b-11ea-81d2-00d0c9d884d8</UUID>
  <HOST>earth.tivlab.austin.ibm.com</HOST>
  <PORT>80</PORT>
  <VIRTHOSTNM>earth.tivlab.austin.ibm.com</VIRTHOSTNM>
  <SERVERDN></SERVERDN>
  <URLOC>/cgi-bin/query_content</URLOC>
  <LOCALADDRESS></LOCALADDRESS>
  <OPERATIONALMODE>online</OPERATIONALMODE>
  <WHENTHROTTLED>0</WHENTHROTTLED>
</JUNCTION>
```

Old Method

- `pdadmin server sync` command
- No longer recommended (still supported)

Troubleshooting

- Confirm all changes have been deployed before exporting/importing
- If you edit the zip file, then keep track of the changes.
Confirm the target zip has directories in correct order

Summary

- Pick a method and replicate away!

Ansible

Export/Import

pdadmin server sync command (don't pick this one)

Questions for the panel

Ask the panelists a question now

Enter your question in the Q&A area

Ask a question after this presentation

You are encouraged to ask follow-up questions in the Support forums:

<https://www.ibm.com/mysupport/s/forumshome>

IBM Security Access Manager Support forum:

<http://ibm.biz/ISAM-support-forum>

For more information

IBM Security Access Manager Forum:

<https://www.ibm.com/mysupport/s/forumsproduct?name=Access+Manager&id=OTO500000002601GAA>

Security Learning Academy: <https://www.securitylearningacademy.com/>

IBM Knowledge Center for IBM Security Access Manager:

https://www.ibm.com/support/knowledgecenter/SSPREK_9.0.7/com.ibm.isam.doc/welcome.html

IBM Security Access Manager Support: <https://www.ibm.com/mysupport/s/topic/OTO500000002601GAA/access-manager?productId=01t50000004XlxqAAG>

Useful links:

[Get started with IBM Security Support](#) [IBM Support](#)
[Sign up for My Notifications](#) [IBM Security Community](#)



Follow us:

Thank you

Follow us:

securitylearningacademy.com

ibm.biz/JoinIBMVIPRewards-Security

youtube/user/IBMSecuritySupport

[@AskIBMSecurity](https://twitter.com/AskIBMSecurity)

ibm.biz/IBMSecurityClientSuccess-LinkedIn

securityintelligence.com

xforce.ibmcloud.com

ibm.com/security/community

© Copyright IBM Corporation 2020. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and ibm.com are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at <http://www.ibm.com/legal/copytrade.shtml>.

All names and references for organizations and other business institutions used in this deliverable's scenarios are fictional. Any match with real organizations or institutions is coincidental. All names and associated information for people in this deliverable's scenarios are fictional. Any match with a real person is coincidental.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.