SANGFOR

IAM

AD Domain Association Group Policy and User Configuration Guide

Version 12.0.18

Change Log

Date	Change Description
Dec 16, 2019	Version 12.0.18 document release.

CONTENT

Chapter 1 Content requirements 1
1 Product Introduction 1
2 Application Scenario 1
3 Requirement Condition 1
4 Configuration Idea 1
5 Configuration Guide with Screenshot 1
5.1 Configuration of AD domain Server. 1
5.2 Testing Result 3
6 Precaution 4

Chapter 1 Content requirements

1 Product Introduction

This document mainly focus on configuring AD domain service in Windows Server, the configuration does not related with the IAM12.0.18 device, it mainly provide the testing guide of the Single Sign-On for everyone.

2 Application Scenario

1. Client network has used AD domain server to manage the internal PC, when the user login to the AD domain at the same time our device will perform AD SSO authentication to allowed internet access immediately. This login method high stability and high successful rate.
2. We need to configure group policy in the AD domain server, assign to related user after complete the authentication configuration at IAM12.0.18 is completed. This document provide the guide that you able to configure group policy by yourself if the client server administrator is not around.

3 Requirement Condition

A server with AD Domain service, as well as a PC that able to join AD domain.

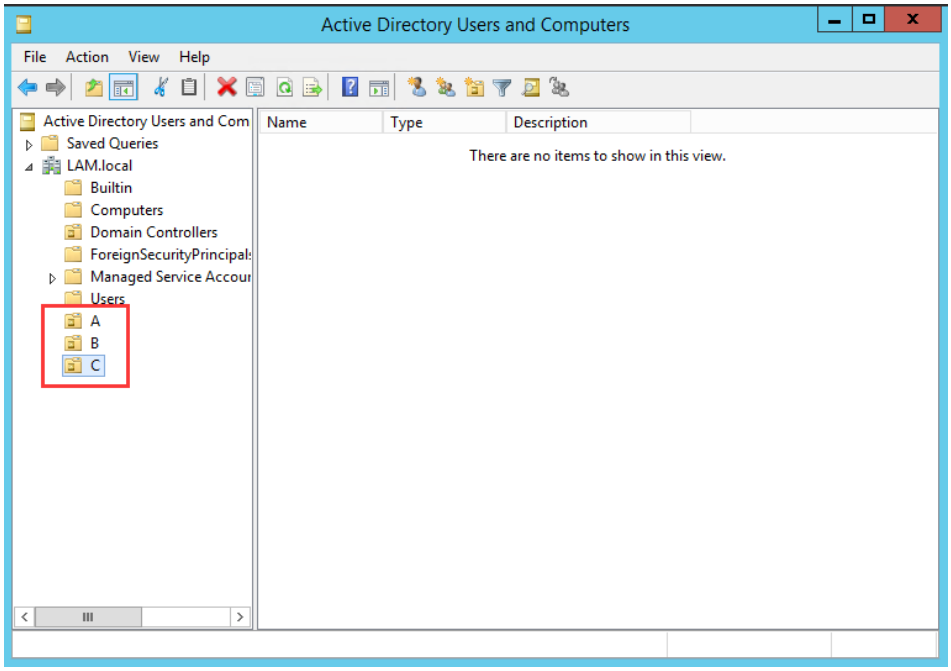
4 Configuration Idea

1. Create a group policy in the AD Domain server and assign to user.
2. Test and observe the policy distributed result.

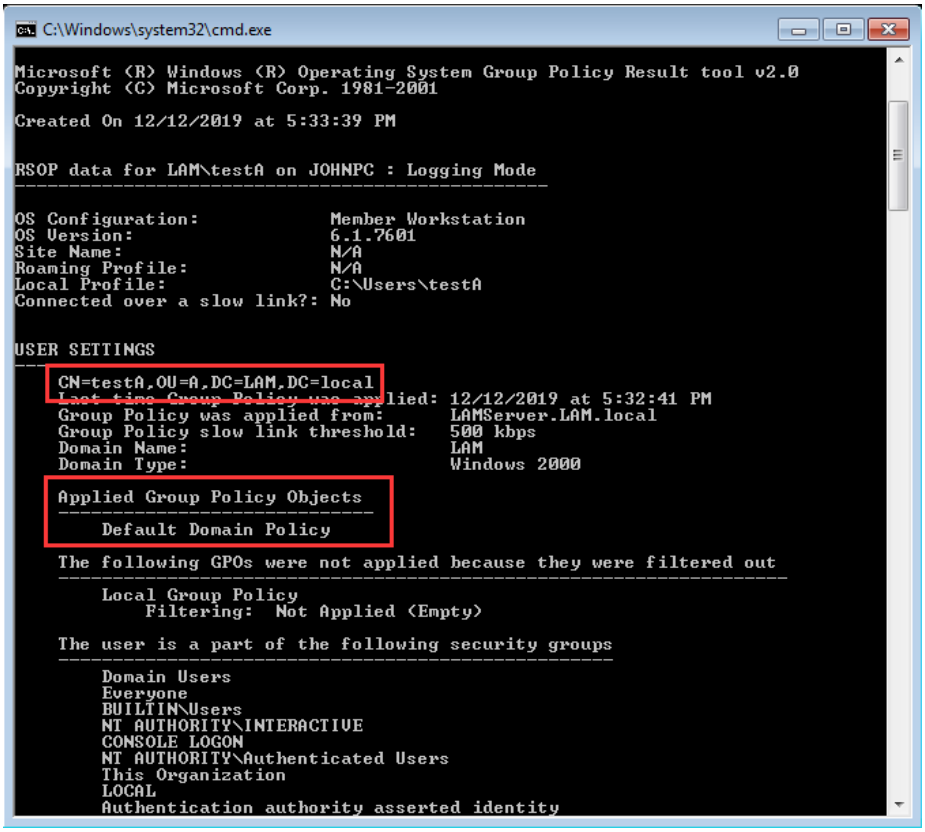
5 Configuration Guide with Screenshot

5.1 Configuration of AD domain Server

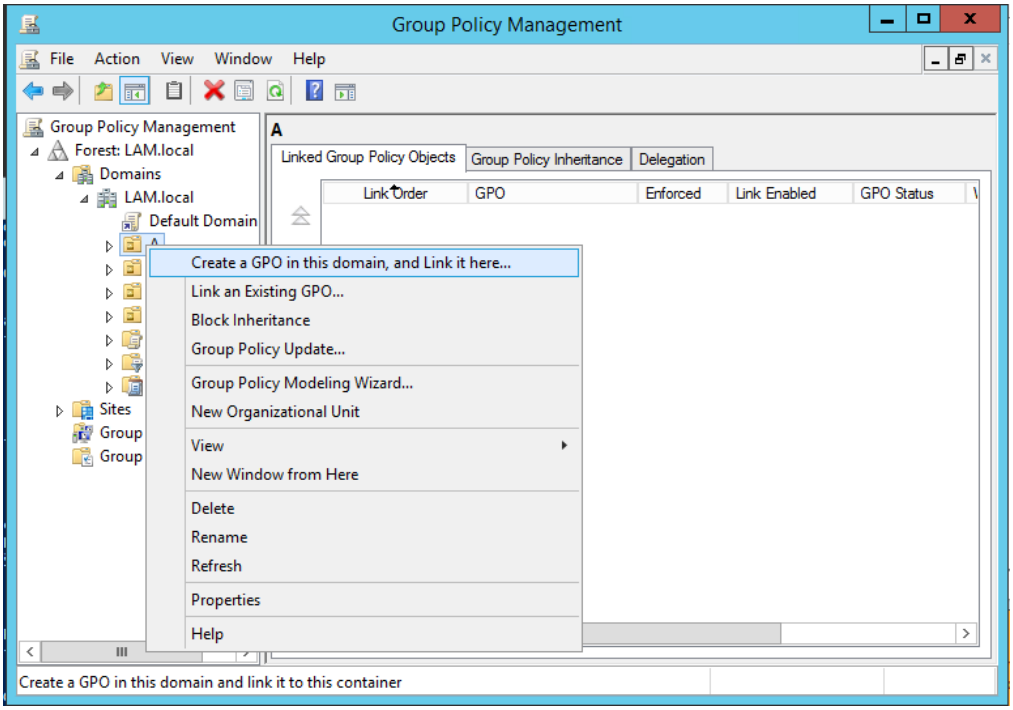
1. Enter [Start] - [Administrative tools] – [Active Directory Users and Computers], create three Organization unit (OU) as A, B, C. The diagram as below.



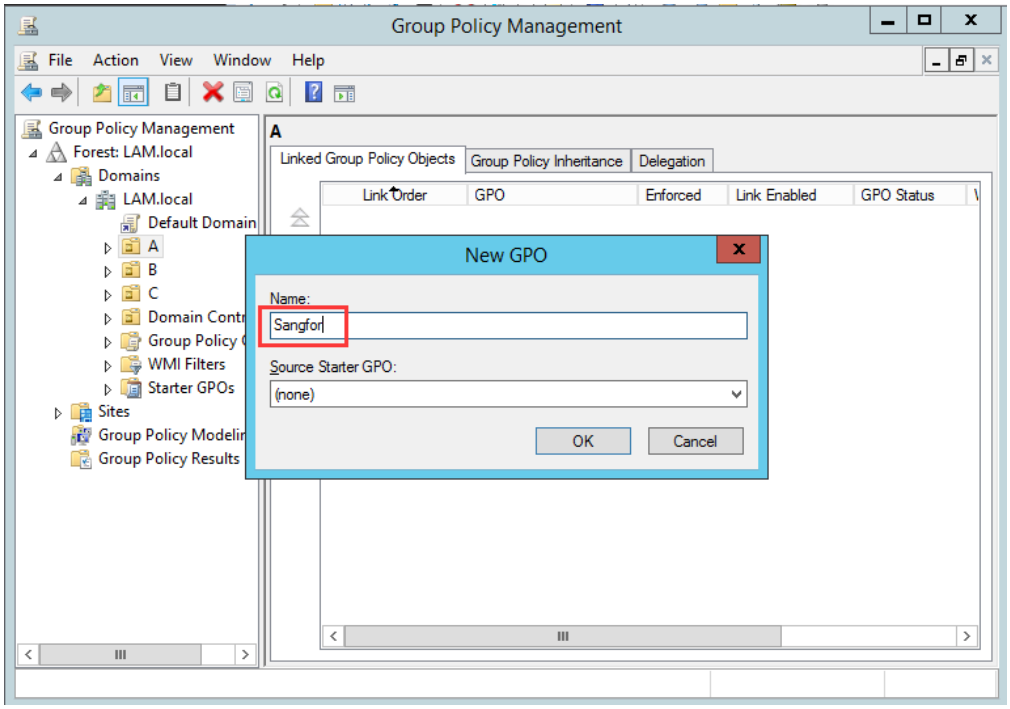
2. By using a PC to join the AD domain with testA user, which belong to A OU in AD domain. We able to checked the domain policy that related to user by using the command prompt, enter the command "gpresult/r". By now, you should able to see the user testA is associated with "Default Domain Policy", this policy is associated with all user. The diagram as below.



3. Create a Group policy with name "Sangfor" at [**Start**] - [**Administrative tools**] – [**Group Policy Management**]. Right click on A OU, you able to see "Create a GPO in this domain, and Link it here..", as diagram below.



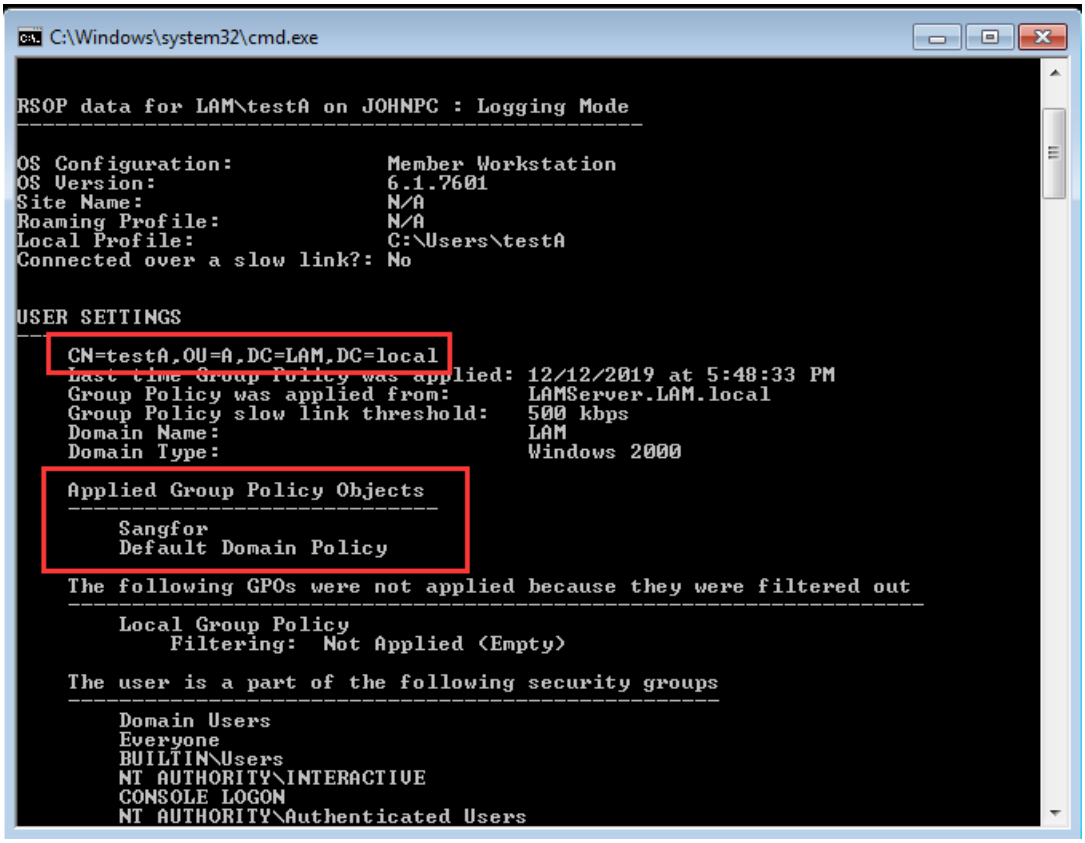
4. The next step is name the new GPO as “Sangfor“ and click OK. That is the step to assign the Sangfor group policy to A OU. The diagram as below.



5. When the configuration has complete, we need to activate the policy by right-click the OU and choose the “Group Policy Update“ option, and confirm the action in the Force Group Policy Update dialog by clicking “Yes“.

5.2 Testing Result

After log in again to the domain, we able to see the user testA is associated with the “Sangfor” group policy. The diagram as below.



6 Precaution

1. “gpresult” command is used to display or compute the Resultant Set of Policy (RSOP).
2. There has the difference between local group policy and domain group policy. You may use “gdedit.msc” command to open the local group policy edit.

Copyright © SANGFOR Technologies Inc. All rights reserved.
No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.
SANGFOR is the trademark of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders.
Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.The information in this document is subject to change without notice. To obtain the latest version, contact the international service center of SANGFOR Technologies Inc