ITA_System Configuration/ Environment Construction Guide

ActiveDirectory association function

ーVersion1.9ー

Disclaimer

Trademark

- Linux is registered trademark or trademark of Linus Torvalds, registered in the U.S. and other countries.
- Red Hat is registered trademark or trademark of Red Hat, Inc., registered in the U.S. and other countries.
- Apache, Apache Tomcat, Tomcat are registered trademarks or trademarks of the Apache Software Foundation.
- Oracle and MySQL are registered trademarks of Oracle Corporation and its subsidiaries and affiliates in the U.S. and other countries.
- MariaDB is a registered trademark or trademark of the MariaDB Foundation.
- Ansible is registered trademark or trademark of Red Hat, Inc.
- Active Directory is a registered trademark or trademark of Microsoft Corporation in the U.S. and other countries.

※”Exastro IT Automation” is written as “ITA” in this document.

Table of contents

Introduction

This document describes the system configuration and environment construction required for using the ActiveDirectory Association (referred as AD Association in the following text) function in ITA.

To use the AD association function, it is assumed that the ITA basic function has been constructed. For details on constructing ITA basic functions, please refer to “System Configuration / Environment Construction Guide_Basic”.

1. Function

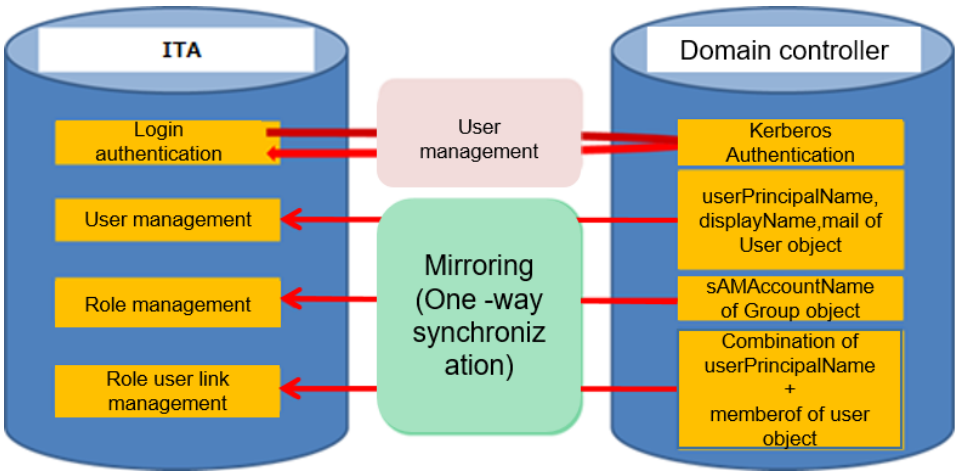
Active Directory association function provides following features.

Table 1-1 Function names

No	Function name	Application	WEB content	BackYard content
1	Active Directory authentication (kerberos authentication function) function.	Perform Active Directory authentication (Kerberos authentication) from ITA to Active Directory.	○	
2	Mirroring function.	In Active Directory user information and group information are mirrored to “User Management” and “Role Management” and “Role / User Linkage Management” on ITA. (One-way synchronization).		○

2. System configuration

The ActiveDirectory association function works with the domain controllers that made up by the domain used in user's organization.



※ userPrincipalName … Login ID of ActiveDirectory
※ displayName … displayName
※ sAMAccountName … Object name (in the figure above, the name of the group object)
※ memberof … Group name to which the user belongs

The Active Directory association function is not supported by configurations that has a proxy between ITA and the domain controller.

3. System requirements

Active Directory association function follows the requirement of ITA system, so please refer to [System Configuration/Environment construction guide_Basic].The requirements for Backyard function are as follows.

●BackYard

Table 3-1 Table for AD association function Backyard system requirements

Package	Version	Note
PHP	5.6	

Table 3-2 Table for AD association function required for external modules

External module	Version	Note
PEAR	1.10.3	

4. Preparing an external authentication configuration file

4.1 About external authentication configuration file

In ITA, the Active Directory association function is activated automatically when the following two conditions are satisfied.

①The external authentication configuration file exists in the specified directory.

②In the contents of the external authentication configuration file, there is at least one valid line.

To enable the Active Directory association function, it is necessary to place the external authentication configuration file in the specified directory. For details, refer 4.2_Deployment of external authentication configuration file.

In the description method there is also a fixed format for the external authentication configuration file. If the file is written in a format other than fixed format, error will occur.

For details, refer 4.3 Description of external authentication configuration file.

4.2 Deployment of external authentication configuration file

The file name and the deployment destination directory should be as follows.

■File name

・ExternalAuthSettings.ini

■Deployment destination path of directory

・~/ita-root/confs/webconfs/

4.3 Description of the external authentication configuration file

In the external authentication configuration file, [section] [key] is described as setting item.

The following is a configuration example.
For details of each section and each key, refer quick reference table, Table 4.3-1 ExternalAuthSetting.ini for setting values.

```
[Authentication_method]
AuthMode = 1

[Replication_Connect]
ConnectionUser = "Administrator"
UserPassword = "Password"
basedn = " ou=hogeUsers , dc= hoge,dc=local"

[DomainController_1]
host = ldap://127.0.0.1
port = 389
basedn = "ou=hogeUsers , dc=hoge , dc=local"
reconnection_count = 3
connect_protocolversion = 3
connect_timelimit = 30
search_timelimit = 30

[LocalAuthUserId]
IdList = "6 ,12"

[LocalRoleId]
IdList = "3 , 23"
```

Please refer to the table below for each section and each key.

※ All elements except connect_protocolversion are required elements.

Table 4.3-1 ExternalAuthSetting.ini Setting Value for Quick Reference

Section	Key	Description
Authentication_method	AuthMode	Set the authentication method. For ITA normally mode [1] is set.
Replication_Connect	ConnectionUser	In the mirroring function, specify an Active Directory user to search for the information on the Active Directory. Please specify a user who has the privilege to search all of the Active Directory information to be mirrored.
	UserPassword	Specify the password for the user specified in the [ConnectionUser] element.
	basedn	Specifies the base dn for the domain. The description method is based on "LDAP distinguished name description rules". The DC that consist the domain name must be specified. For specifying the search range, only OU can be specified. **※In ITA , the search range cannot be specified other than OU.**
DomainController_1 *1	host	Specify the DomainController host that configures the Active Directory to be linked.
	port	Specify the DomainController port that configures the Active Directory to be linked
	basedn	※ Specify the same content as in the case Replication_Connect
	reconnection_count	Specify the number of times If connection to the server fails due to poor communication it will automatically try to reconnect .If the connection cannot be made within the specified number of times, an error message will display on the login screen.
	connect_protocolversion	Users can specify the LDAP version. **※If the version is not specified, execute the process with version "3"**
	connect_timelimit	Specify the stand by time with connection to Domain controller. The connection will fail if the connection cannot be made within the specified time period.
	search_timelimit	Specifies the stand by time for kerberos authentication process in Active Directory. The process will fail, if the authentication cannot be made within the specified time period.

LocalAuthUserId	IdList	Users can specify which users on the ITA are not eligible for Active Directory association. （※Specify with the user ID of ITA.） Multiple values can be specified by separating them with commas.
LocalRoleId	IdList	Users can specify the roles that are not eligible to Active Directory linkage.**（※Specify with the ITA role ID.）**

*1 Users can specify up to three "DomainController". In that case, please add the section as "DomainController_2" and "DomainController_3". The key is the same as "DomainController_1". If more than one is specified, the process will be performed for each DomainController in order, but the process will not be performed for the next DomainController when it succeeds.

※ Users cannot specify DomainController with different domains.