



AAM Kerberos Relay Integration with SharePoint

How to Deploy A10 Thunder ADC's AAM Feature in a SharePoint Environment Using Kerberos Relay Authentication

Table of Contents

Overview.....	3
Deployment Prerequisites	3
The A10 Networks AAM Kerberos Relay Solution	4
Configuration Section	4
Authentication Logon	4
Configuring the AAM Authentication Logon	4
Virtual Server, Virtual Port and Server Configuration	7
Summary	9
Appendix:	10
Complete Configuration	10
About A10 Networks	11

Disclaimer

This document does not create any express or implied warranty about A10 Networks or about its products or services, including but not limited to fitness for a particular use and noninfringement. A10 Networks has made reasonable efforts to verify that the information contained herein is accurate, but A10 Networks assumes no responsibility for its use. All information is provided "as-is." The product specifications and features described in this publication are based on the latest information available; however, specifications are subject to change without notice, and certain features may not be available upon initial product release. Contact A10 Networks for current information regarding its products or services. A10 Networks' products and services are subject to A10 Networks' standard terms and conditions.

Overview

This document provides a detailed guide on how to deploy Kerberos Relay with Microsoft SharePoint, showing how the LDAP or RADIUS authentication protocol can be used for the Kerberos authentication process. User credentials are provisioned within the Active Directory and clients authenticate to A10 Networks® Thunder® ADC line of Application Delivery Controllers. After the client authentication to the Thunder ADC appliance is complete, Thunder ADC obtains a client’s username, receives ticket information from the Kerberos server, and allows the client traffic to pass to the backend/application servers.

In A10 Networks Advanced Core Operating System (ACOS®) release 4.0, there is a new service group type introduced in the Application Access Management (AAM) module which is designed for authentication purposes. This feature allows ACOS to load balance and manage multiple Key Distribution Center (KDCs). KDC works in conjunction with Active Directory (AD) and it provides session tickets and temporary keys to users and computers within an AD domain. Consequently, the primary Kerberos server’s purpose is to handle all authentication relay processing; the secondary server can be used as a backup or to support scalability to ensure the continuous availability of authentication services.

In a multiple KDC environment, you can only use an AAM service group that provides the round robin load-balancing algorithm. Authentication servers within the service group pool can also be given priority based on priority levels. The server with the higher priority number is the first authentication server to take a request. If authentication servers have the same priority number, then the round robin algorithm will determine the rotation.

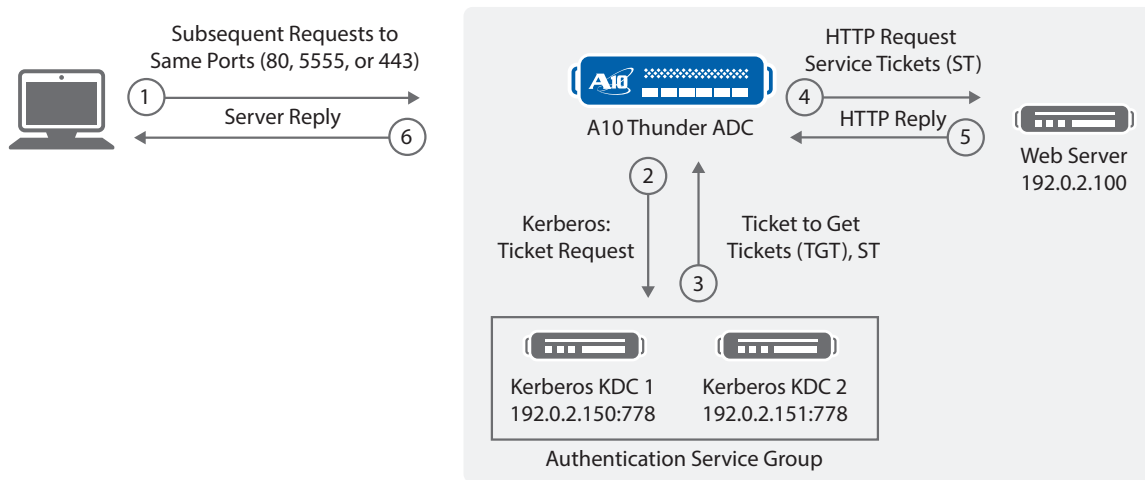


Figure 1: Kerberos Relay authentication process

Deployment Prerequisites

Client requirements:

- Browser: The latest versions of Internet Explorer 11 or higher, Mozilla version 38 or higher, or Chrome 22 or higher

ACOS requirements:

- 4.0.1 Px or higher

Application requirements:

- SharePoint Server 2010 or 2013 with the latest updates

The A10 Networks AAM Kerberos Relay Solution

In ACOS release 4.0 introduces a new set of features within the AAM module. Designed for authentication purposes, this feature allows ACOS to load balance and manage multiple KDCs, which provide session tickets and temporary keys to users and computers within an Active Directory domain. Consequently, the primary Kerberos server's purpose is to handle all authentication relay processing; the secondary server can be used as a backup or to support scalability to ensure the continuous availability of authentication services.

This integrated solution simplifies network authentication by using the A10 device as an authentication proxy. It offloads web and authentication servers, and it enables A10 Thunder ADC to handle the sending and initial processing of authentication challenges, forwarding credentials to SAML IdP and granting access.

Configuration Section

This section provides detailed CLI and GUI instructions on how to configure Kerberos Relay, and you will be tasked with creating the following configuration to support the A10 and SharePoint integration:

- Authentication logon
- Authentication server
- Authentication relay
- Authentication template
- AAA policy
- Service-principal name configured within the server port configuration

Note: For details on what these features are used for, please refer to the ACOS 4.x documentation for detailed information.

Authentication Logon

Configuring the AAM Authentication Logon

CLI Sample Configuration:

```
aam authentication logon http-authenticate hbasic
auth-method basic enable
```

GUI Sample Configuration:

Navigate to AAM > Auth Client > click Create

Enter the Name of the Authentication Logon: hbasic

Max Number of Retries: 3

Check the Enable Basic Logon option

The screenshot shows the configuration page for an authentication logon. The 'Name' field is set to 'hbasic'. The 'Max Number of Retries' is set to '3'. The 'Enable Basic Logon' checkbox is checked. The 'Auth Method' is set to 'http-authenticate'. The 'Auth Method' dropdown is set to 'hbasic'. The 'Auth Method' dropdown is set to 'hbasic'. The 'Auth Method' dropdown is set to 'hbasic'.

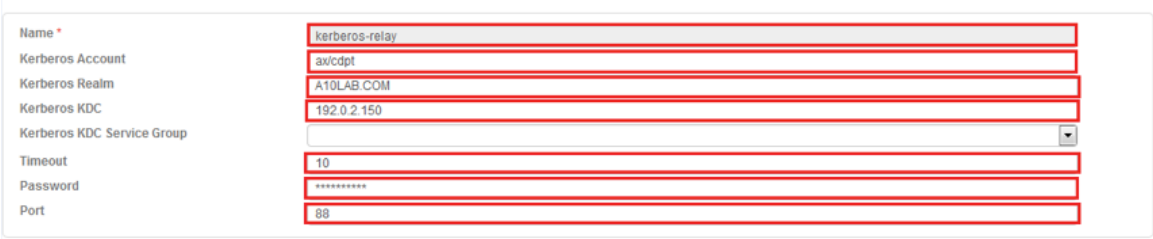
CLI Sample Configuration:

```
aam authentication server ldap ldap_serv
  host 192.0.2.150
  base cn=Users,dc=a10lab,dc=com
  admin-dn cn=Administrator,cn=Users,dc=a10lab,dc=com
  admin-secret *****
  default-domain a10lab
```

GUI Sample Configuration:

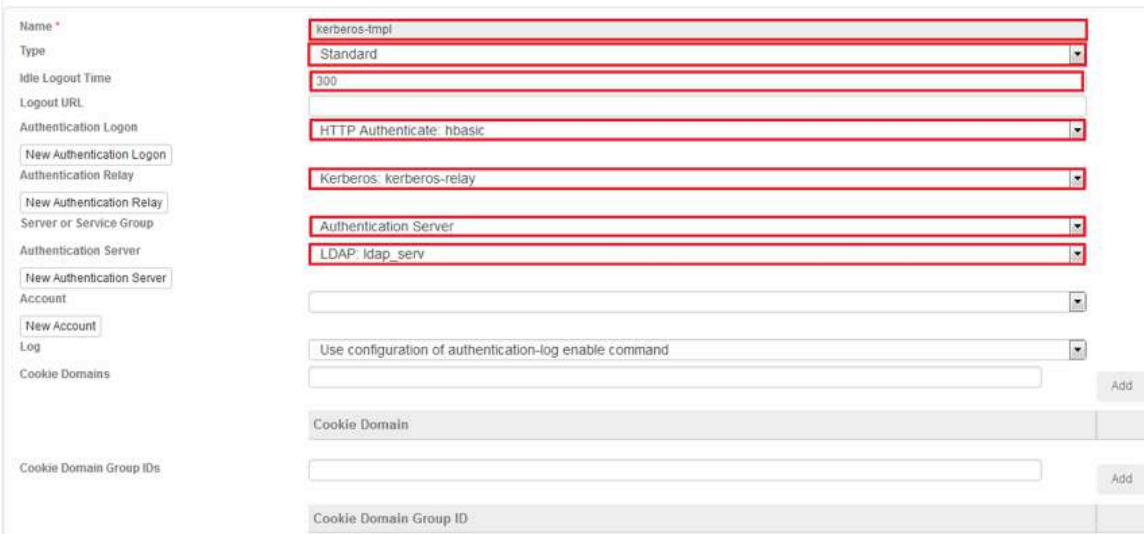


CLI Sample Configuration:



CLI Sample Configuration:

```
aam authentication template kerberos-tmpl
  logon hbasic
  relay kerberos-relay
  server ldap_serv
```

CLI Sample Configuration:

```
aam aaa-policy kerb-relay
  aaa-rule 1
    action allow
    authentication-template kerberos-tmpl
```

GUI Sample Configuration:

AAM >> AAA Policies >> Create

Create AAA Policy

Name *

Virtual Port Bindings Add

Virtual Ports

New VP

Cancel Create

Name * New VP

Virtual Port Bindings Add

Virtual Ports

AAA Rules Create

Index	Rule Action	Domain Name	Actions
No items to display.			

Cancel Update

Create AAA Rule

Index *

Domain Name

Access List

Action

Authorization Policy

New Authorization Policy

Authentication Template

New Authentication Template

URI Add

URI Match	URI

The policy can be defined as allow or deny. The index has to be configured as a unique number.

End state should look like this after the AAA Policy and AAA Rules are created.

Update AAA Policy

Name * New VP

Virtual Port Bindings Add

Virtual Ports

AAA Rules Delete Create

Index	Rule Action	Domain Name	Actions
1	allow		Edit

Cancel Update

Virtual Server, Virtual Port and Server Configuration

This section of the deployment provides a compound configuration for the virtual IP (VIP) address, virtual port, service group and server configuration. SharePoint requires three important ports to work properly: 443, 80 and 5555, which is an optional SharePoint Central Administration Web Application port.

Note: *The SharePoint Central Administration Web Application “5555” port is a non-standard configuration and administrators should choose the port they prefer for ease of management.*

With the three ports provided, these ports must be provisioned in the server and grouped in a pool using a service-group.

Service Group Configuration:

```
slb service-group mywsu-sg-443 tcp
  member sptest1 443
!
slb service-group mywsu-sg-80 tcp
  member sptest1 80
!
slb service-group mywsu-sg-5555 tcp
  member sptest1 5555
```

Once the servers and service-groups have been defined, configure the VIP with an IP address and virtual services and bind the AAA policy to the virtual services for port 80, 443 and 5555. Follow the sample configuration below and note that the configuration provided can also include client or server SSL for additional security. Refer to other SharePoint deployment guides for additional information regarding SharePoint security.

Virtual Server Configuration:

```
slb virtual-server sharepoint-vs 192.0.2.234
  port 80 https
    source-nat auto
    service-group mywsu-sg-80
    aaa-policy my-aaa-policy
  port 443 https
    source-nat auto
    service-group mywsu-sg-443
    aaa-policy my-aaa-policy
  port 5555 https
    source-nat auto
    service-group mywsu-sg-5555
    aaa-policy my-aaa-policy
slb server sptest1 192.0.2.100
  port 80 tcp
    service-principal-name HTTP/sptest1.a101lab.com
  port 443 tcp
    service-principal-name HTTPS/sptest1ssl.a101lab.com
  port 5555 tcp
    service-principal-name HTTP/sptest1.a101lab.com
```

Useful Commands When Validating Kerberos-Relay Deployments:

1. Check auth stats info:

```
AAM-SI-1#show aam authentication statistics | sec kerberos
```

```
-----
```

\ statistic Type\	Request Normal	Request Dropped	Response Success	Response Failure	Response Error	Response Timeout	Response Other
OCSP	0	0	0	0	0	0	0
RADIUS	0	0	0	0	0	0	0
LDAP	0	0	0	0	0	0	0
Windows-KERBEROS	18	0	8	10	0	0	0
Windows-NTLM-SMB	0	0	0	0	0	0	0
KERBEROS-RELAY	20	0	20	0	0	0	0
OCSP-STAPLING	0	0	0	0	0	0	0
SPN-KERBEROS	0	0	0	0	0	0	0

```
-----
```

```
-----
kerberos request send: 35
kerberos response get: 35
kerberos-relay request send: 20
kerberos-relay response get: 20
SPN kerberos request: 0
SPN kerberos response success: 0
SPN kerberos response failure: 0
AAM-SI-1#
```

2. Check auth-server stats info:

```
AAM-SI-1# show aam authentication statistics windows-kerberos
```

```
-----
```

Name	Request	Response	Timeout	Other-Err
dy-as-kdc-auth-relay	35	35	0	0

```
-----
```

3. Check kerberos-relay stats info:

```
kerberos-relay request send: 20
kerberos-relay response get: 20
Timeout error: 0
Job start error: 0
Polling control error: 0
Other error: 0

kerberos Authentication-relay name: dy-kdc-relay
Kerberos request send: 20
Kerberos response receive: 20
Current requets of user: 0
Kerberos tickets: 3
```


4. Check kerberos tickets info:

```
AAM-SI-1#show aam authentication klist
```

```
-----
```

```
Ticket cache: MEMORY:dy-kdc-relay
```

```
Default principal: HTTP/ sptest1.a10lab @example.com
```

```
Service principal: HTTP/win-gln4q4dh483@example.com
```

```
Client principal: client@example.com
```

```
timespan: 18:03 10,May,2015 - 03:58 11,Dec,2014
```

```
renew untill: 17:58 17,May,2015
```

```
flags: FRA
```

```
Service principal: HTTP/ sptest1.a10lab @ example.com
```

```
Client principal: client@ example.com
```

```
timespan: 17:58 10,May,2015 - 03:58 11,May,2015
```

```
renew untill: 17:58 17,May,2015
```

```
flags: FRA
```

```
Service principal: krbtgt/ example.com@example.com
```

```
Client principal: HTTP/ sptest1.a10lab @example.com
```

```
timespan: 17:58 10,May,2015 - 03:58 11,May,2015
```

```
renew untill: 17:58 17,May,2015
```

```
flags: FRIA
```

Note: The Kerberos tickets on Thunder ADC will be cached for 10 hours and every different Kerberos Relay profile will generate and cache its own tickets. You can use the “clear aam authentication kcache” command to clear all tickets on the Thunder ADC device.

Thunder ADC must have the same time/clock as the Kerberos server. Clock setting differences may cause the kerberos-auth to fail. If kerberos-auth keeps failing even when the clock settings are the same, check and make sure username and password are correct.

Summary

In summary, the configuration steps described in this deployment guide show how to set up Thunder ADC AAM integration with Kerberos Relay in the Microsoft SharePoint application. With ACOS 4.0, Thunder ADC can provide a wide array of authentication server capabilities which include LDAP, AD, NT LAN Manager (NTLM), Kerberos and SAML 2.0 options.

This integrated solution provides the following benefits:

- Minimizes the overwhelming nature of user interactions with traditional AAA servers
- Simplifies network authentication by using the A10 device as an authentication proxy
- Offloads web and authentication servers
- Enables A10 Thunder ADC to handle the sending and initial processing of authentication challenges, forwarding credentials to SAML IdP and granting access

By using Thunder ADC, significant benefits are achieved for all authentication deployments. For more information about A10 Thunder ADC products, please refer to the following URLs:

<https://www.a10networks.com/products/thunder-series/thunder-adc>

http://www.a10networks.com/products/application_delivery_controllers.php

Appendix:

Complete Configuration

```
aam authentication logon http-authenticate hbasic
  auth-method basic enable

aam authentication server ldap ldap_serv
  host 192.0.2.150
  base cn=Users,dc=a10lab,dc=com
  admin-dn cn=Administrator,cn=Users,dc=a10lab,dc=com
  admin-secret *****
  default-domain a10lab

aam authentication relay kerberos kerberos-relay
  kerberos-realm A10LAB.COM
  kerberos-kdc 192.0.2.150
  kerberos-account ax/cdpt
  password *****

slb server sptest1 192.0.2.100
  port 80 tcp
  service-principal-name HTTP/sptest1.a10lab.com
  port 443 tcp
  service-principal-name HTTPS/sptest1ssl.a10lab.com
  port 8888 tcp
  service-principal-name HTTP/sptest1.a10lab.com

aam authentication template kerberos-tmpl
  logon hbasic
  relay kerberos-relay
  server ldap_serv

aam aaa-policy kerb-relay
  aaa-rule 1
  action allow
  authentication-template kerberos-tmpl

slb service-group mywsu-sg-443 tcp
  member sptest1 443
!
slb service-group mywsu-sg-80 tcp
  member sptest1 80
!
slb service-group mywsu-sg-5555 tcp
  member sptest1 5555

slb virtual-server sharepoint-vs 192.0.2.234
  port 80 https
  source-nat auto
  service-group mywsu-sg-80
  template client-ssl cssl
  aaa-policy my-aaa-policy
  port 443 https
  source-nat auto
```

```
service-group mywsu-sg-443
template server-ssl s1
template client-ssl css1
aaa-policy my-aaa-policy
port 8888 https
source-nat auto
service-group mywsu-sg-5555
template client-ssl css1
aaa-policy my-aaa-policy
```

About A10 Networks

A10 Networks is a leader in application networking, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, California, and serves customers globally with offices worldwide. For more information, visit:

www.a10networks.com

Corporate Headquarters

A10 Networks, Inc
3 West Plumeria Ave.
San Jose, CA 95134 USA
Tel: +1 408 325-8668
Fax: +1 408 325-8666
www.a10networks.com

Part Number: A10-DG-16151-EN-01
July 2015

Worldwide Offices

North America
sales@a10networks.com
Europe
emea_sales@a10networks.com
South America
latam_sales@a10networks.com
Japan
jinfo@a10networks.com
China
china_sales@a10networks.com

Hong Kong
HongKong@a10networks.com
Taiwan
taiwan@a10networks.com
Korea
korea@a10networks.com
South Asia
SouthAsia@a10networks.com
Australia/New Zealand
anz_sales@a10networks.com

To learn more about the A10 Thunder Application Service Gateways and how it can enhance your business, contact A10 Networks at: www.a10networks.com/contact or call to talk to an A10 sales representative.