AAM Integrated Windows Authentication/ Basic NTLM

How to Deploy A10 Networks AAM NTLM Feature within Thunder ADC

Table of Contents

Disclaimer

Overview

The purpose of this document is to provide a guideline for administrators on how to deploy the A10 Networks® Application Access Management (AAM) module with Integrated Windows Authentication (IWA). IWA is a hash-based authentication service which is exchanged between clients and servers across the network. The A10 Networks Thunder® ADC line of Application Delivery Controllers is equipped with the authentication feature called AAM without additional license requirements, and one of the various authentication server options it supports is NT LAN Manager (NTLM). This guide covers the A10 AAM NTLM configuration in Microsoft Windows to enable authentication between clients and servers.

Deployment Prerequisites

Client Requirements:

- OS: Windows 7 or higher. For MAC OS, there are some versions of MAC OS that do not support NTLM authentication. Please use accordingly and refer to Apple documentation for supportability.
- Browser: Internet Explorer 11 or higher; Mozilla version 38 or higher; Chrome 22 or higher.

A10 Networks Advanced Core Operating System (ACOS®) Requirements:

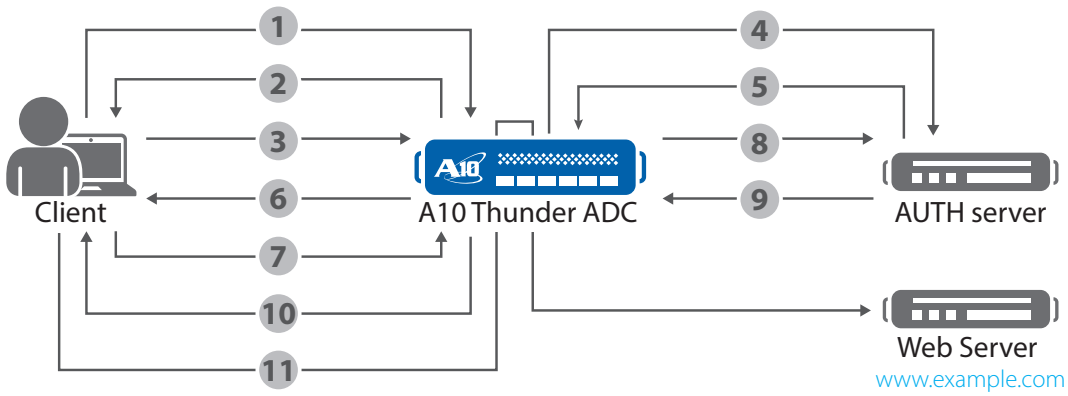
- 4.0.1 Px or higher

Authentication Server:

- Windows Server 2012 or Windows Server 2012 R2

Authentication Process

Figure 1 provides a detailed authentication flow that shows how the NT LAN Manager (NTLM) authenticates between clients and servers.



1 HTTP request
2 www-authentication: NTLM
3 HTTP-NTLM negotiation
4 NTLM negotiate/SMB*
5 NTLM challenge/SMB
6 HTTP-NTLM challenge
7 HTTP NTLM authenticate
8 NTLM authenticate/SMB
9 SMB session response
10 HTTP 200 OK
11 HTTP traffic

*Server Message Block

Figure 1. NTLM authentication flow with A10 Thunder ADC

Thunder ADC AAM Configuration

Template Configurations

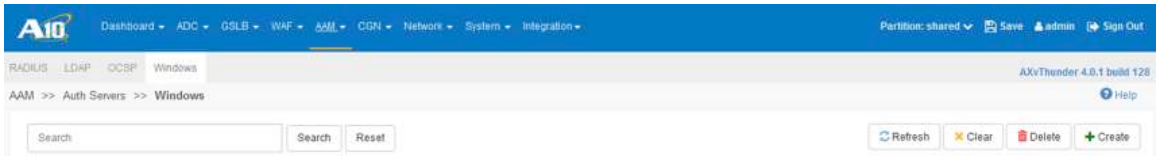
The best way to deploy the A10 AAM solution is to preconfigure all templates and then apply them to the Thunder ADC AAM configuration.

In this guide, the following templates will be used with the following names:

- Authentication server: "ntlmserver"
- AAM authentication logon template: "ntlm"
- Authentication template: "ntlmtemplate"
- AAA policy: "ntlmpolicy"

AAM Authentication Server Configuration

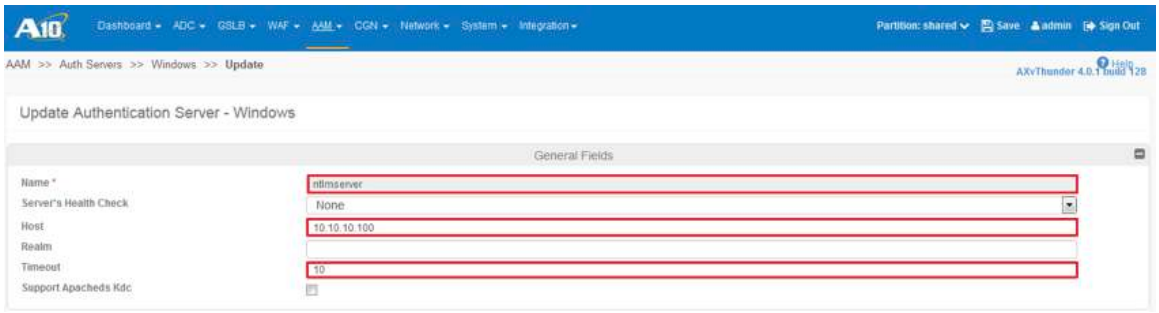
This section of the guide describes the steps needed to configure the AAM authentication server parameters. Before configuring this option on the Thunder ADC device, administrators must ensure that the authentication server is configured and available. To configure the authentication server parameters in the GUI, navigate to AAM > Auth Servers > Windows, then click "Create."



Enter the following information:

- Authentication name: ntlmserver
- Host: 10.10.10.100
- Timeout: 10

Once completed, click OK and save configuration.



Sample CLI Configuration:

```
aam authentication server windows ntlmserver
  host 10.10.10.100
  auth-protocol kerberos-disable
```

AAM Authentication Logon Configuration

As the first step to configure the Integrated IWA authentication template on the Thunder ADC device, navigate to AAM > Auth Clients.

- Click "Create" on the right-hand side of the dashboard
- Enter the name of the authentication client logon "ntlm"
- Enter the number of retries, for example "3"
- Select authentication options for the client login

In this guide, we will be checking "Enable NTLM Logon" as part of the configuration.

Sample CLI Configuration:

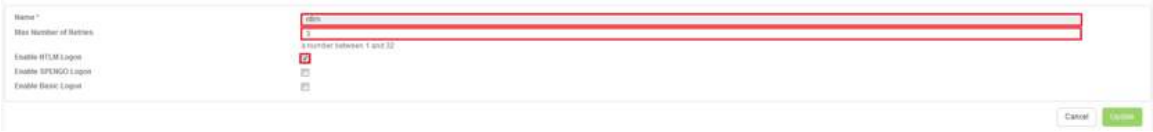
```
aam authentication logon http-authenticate "ntlm"
  auth-method ntlm enable
  logon "ntlm"
```

Authentication Template Configuration

This section of the guide covers the authentication template creation. Navigate to AAM > Authentication Templates and click "Create."

Enter the following parameters:

- Authentication template Name: "ntlmtemplate"
- Type: "Standard"
- Authentication logon: "HTTP Authenticate: NTLM"
- Server or service group: "Authentication Server"
- Authentication server: Windows: "ntlmserver"



Sample CLI Configuration:

```
aam authentication template ntlmtemplate
  logon ntlm
  server ntlmserver
```

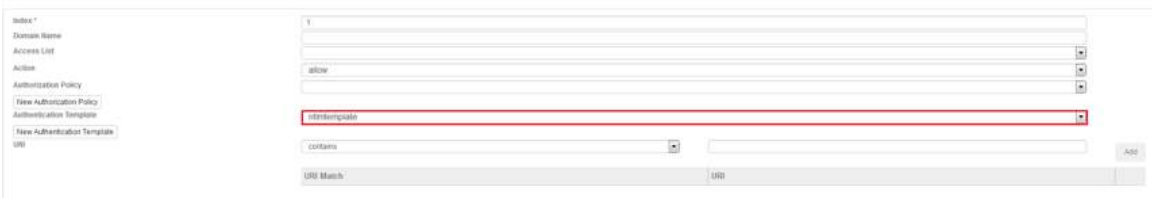
AAA Policy Configuration

This section of the guide explains how an administrator configures the AAA rules to allow or deny access. The rules are configured using a unique index number. To configure the AAA policy, navigate to the AAM > AAA Policies.

- Click "Create"
- Enter policy name: "ntlmpolicy" and click "Create" which redirects to the "Update AAA Policy" page
- Enter the virtual ports: "80+http"

- Configure the AAA rules:
  - Enter index: "1"
  - Rule action: "allow"
- Click OK and save configuration

In the AAA rules section, make sure that the authentication template is defined as "ntlmtemplate." Refer to the next section of the document for guidance about how to create an authentication template.



Sample CLI Configuration:

```
aam aaa-policy ntlmpolicy
  aaa-rule 1
    action allow
    authentication-template ntlmtemplate
```

Real Server Configuration

To configure the backend server (e.g., web server) and ports. Navigate to ADC > SLB > Servers.

Sample CLI Configuration:

```
slb server ser1 10.10.10.120
  port 80 tcp
```

Service-Group Configuration

To create a service group and add servers within the pool, navigate to ADC > SLB > Service Group.

Sample CLI Configuration:

```
slb service-group sg-ntlm tcp
  member ser1 80
```

***Note**: Additional servers can be added from the SG as needed.*

VIP and Virtual Port Configurations

This shows how to create a Virtual IP(VIP) for a web service (for example, www.example.com in this guide) and bind all of the template components preconfigured for authentication:

- Navigate to ADC > SLB > Virtual Server/Virtual Port

- In the general field of the virtual port, select the preconfigured AAA policy called "ntlmpolicy"

Sample CLI Configuration:

```
slb virtual-server vip-ntlm 10.153.0.100
  port 80 http
    source-nat pool 10.10.10.200
    service-group sg-ntlm
aaa-policy ntlmpolicy
```

Summary

This guide gives administrators the simple configuration steps needed to deploy A10 Networks Application Access Management (AAM) module with Integrated Windows Authentication (IWA). A10 Networks Thunder ADC line of Application Delivery Controllers comes with the AAM feature without additional license requirements, and one of the various authentication server options it supports is NT LAN Manager (NTLM). This guide covers the A10 AAM NTLM configuration in Microsoft Windows that enables authentication between clients and servers.

Appendix

```
aam authentication logon http-authenticate ntlm
  auth-method ntlm enable
  logon ntlm
aam authentication server windows ntlmserver
  host 10.10.10.120
  auth-protocol kerberos-disable
aam authentication template ntlmtemplate
  logon ntlm
  server ntlmserver
aam aaa-policy ntlmpolicy
  aaa-rule 1
    action allow
    authentication-template ntlmtemplate
slb server ser1 10.10.10.120
  port 80 tcp slb service-group sg-ntlm tcp
  member ser1 80
slb virtual-server authntlm 10.153.0.100
  port 80 http
    source-nat pool 10.10.10..200
    service-group sg-ntlm
aaa-policy ntlmpolicy
```

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-16150-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.