ACNS 5.0.1 および Microsoft Active Directory を実行する CE との HTTP 要求認証の設定

目次

はじめに

この文書の設定例では、Cisco Content Engine をセットアップして、アクティブ ディレクトリ Lightweight Directory Access Protocol (LDAP) データベース検索を実行し、Web リソースへのユーザ アクセスを許可/制限する方法を示しています。

アクティブ ディレクトリ データベースは、Windows 2000 サーバのユーザ データベースです。 LDAP プロトコルは、認証を行うためにこのデータベースを照会することができます。 一般的に、Content Engine LDAP クライアントは、LDAP サーバのユーザ データベースを照会し、ユーザ アカウントの有効時間、特権、ユーザが属するグループなど、ユーザの認定証を取得します。 Cisco Application and Content Networking System (ACNS) 5.0 ソフトウェアでは、Content Engine LDAP クライアントも、Windows 2000 サーバ データベースのリモート アクティブディレクトリで設定されているユーザの認証と権限付与を行うことができます。

Miscrosoft Active Directory を LDAP サーバとして使用し Content Engine との認証を行うには、ある特定の手順を行う必要があります。 デフォルトでは、Microsoft Active Directory では匿名 LDAP クエリが許可されていません。 LDAP クエリを実行したりディレクトリを参照するには、Windows システムの管理者グループに属するアカウントの Distinguished Name (DN; 認定者名) を使用して、LDAP クライアントを LDAP サーバにバインドする必要があります。

Microsoft Active Directory を LDAP サーバとしてセットアップするには、管理者グループの 1 つのアカウントの完全な DN とパスワードを決定する必要があります。 たとえば、Active Directory 管理者が Active Directory Users and Computers Windows NT /2000 コントロール パネルのユーザ フォルダのアカウントを作成し、DNS ドメインが sns.cisco.com なら、生じる DN に次の構造があります: cn=<adminUsername>、cn=users、dc=sns、dc=cisco、dc=com

LDAP は、X.500 により提供される最高の品質を維持しながら、管理コストを削減するために開発されました。 LDAP は、TCP/IP 上で実行されるオープンなディレクトリ アクセス プロトコル

を実現します。 LDAP は X.500 データ モデルを保持し、ハードウェアとネットワーク インフラストラクチャへの適度な投資により、グローバル規模および数百万エントリにまでスケーラブルになっています。 結果として、小規模な組織でも十分利用可能な経済性のみならず、最大規模の企業をサポートできるような拡張性をも備えたグローバル ディレクトリ ソリューションになっています。

LDAP 対応の Cache Engine/Content Engine は、ユーザと LDAP サーバとの認証を行います。 HTTP クエリを使用して、Content Engine はユーザから認定証のセット（ユーザ ID とパスワード）を取得し、それらを LDAP サーバ内のものと比較します。 Content Engine が LDAP サーバを介してユーザを認証する場合、その認証のレコードは Content Engine の RAM（認証キャッシュ）にローカルに保存されます。 認証エントリが保持されている限り、そのユーザがそれ以降制限されたインターネット コンテンツにアクセスしようとする場合に、LDAP サーバのルックアップは必要ありません。 デフォルトは 480 分で、最小は 30 分、最大は 1440 分（24 時間）です。 これは、ユーザの最後のインターネット アクセスから、そのユーザのエントリが認証キャッシュから削除され、LDAP サーバとの再認証が強制されるまでの時間間隔です。

Cache Engine は、プロキシ モードと透過（WCCP）モードの両方のアクセスで LDAP 認証をサポートしています。 プロキシ モードでは、Cache Engine は認証データベースのキーとしてクライアントのユーザ ID を使用しますが、透過モードでは、Cache Engine は認証データベースのキーとしてクライアントの IP アドレスを使用します。 Cache Engine は、シンプルな（暗号化されていない）認証を使用して、LDAP サーバと通信します。

前提条件

要件

このドキュメントに関しては個別の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- ACNS 5.0.1 を実行する Cisco Content Engine 7325
- アクティブ ディレクトリを搭載した Microsoft Windows 2000 Advanced Server

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

設定

Cisco Content Engine 7325 (Cisco ACNS ソフトウェア リリース 5.0.1)

```
hostname V5CE7325
!
!
http authentication cache timeout 5
http proxy incoming 80 8080
!
ip domain-name cisco.com
!
interface GigabitEthernet 1/0
 ip address 10.48.67.23 255.255.254.0
 exit
interface GigabitEthernet 2/0
 shutdown
 exit
!
!
ip default-gateway 10.48.66.1
!
primary-interface GigabitEthernet 1/0
!
!
no auto-register enable
!
!
multicast accept-license-agreement
!
!
ip name-server 10.48.66.123

username admin password 1 CfxnDoKDWrBds
username admin privilege 15
!

ldap server base "dc=sns,dc=cisco,dc=com"
 !--- This is the base DN of the starting point for !---
the search in the LDAP database. ldap server userid-
attribute cn !--- Searching for the CN of the user. ldap
server host 10.48.66.217 primary !--- The LDAP server's
IP address number. ldap server administrative-dn
"cn=Administrator,cn=users,dc=sns,dc=cisco,dc=com" !---
This is the DN of the admin user. ldap server
administrative-passwd **** !--- This is the password for
the admin-user. ldap server version 3 !--- Use LDAP
version 3 for active directory. ldap server active-
directory-group enable !--- Allows users based on their
group memberships. ldap server enable ! authentication
login local enable primary authentication configuration
local enable primary ! access-lists 300 permit groupname
internet access-lists 300 deny groupname any !---
Defines what user groups are allowed. ! access-lists
enable ! ! cdm ip 10.48.67.25 cms enable ! ! end
```

確認

このセクションでは、設定が正常に動作しているかどうかを確認する際に役立つ情報を提供しています。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

注: debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

- show ldap：このコマンドは、設定の詳細を表示します。 次にコマンドの出力例を示します。

```
Allow mode:     disabled
Base DN:        dc=sns,dc=cisco,dc=com
Filter:         <none>
Retransmits:    2
Timeout:        5 seconds
UID Attribute:  cn
Group Attribute:         memberOf
Administrative DN:       cn=Administrator,cn=users,dc=sns,dc=cisco,dc=com
Administrative Password: ****
LDAP version:   3
LDAP port:      389
Server            Status
---------------   ---------
10.48.66.217      primary
<none>            secondary
```

- show access-lists：このコマンドは、有効になっている Access Control List（ACL; アクセス コントロール リスト）を表示します。
- show http-authcache：このコマンドは、認証キャッシュを表示します。 次にコマンドの出力例を示します。

```
V5CE7325#sh http-authcache
Apr 10 10:08:03 V5CE7325 -admin-shell:
   %CE-PARSER-6-350232:CLI_LOG:sh http-authcache
AuthCache
=====================
hash   835 : uid: gdufour nBkt: (nil) nLRU: (nil) pLRU: (nil)
lacc: 70 ipAddr: 144.254.9.45 keyType: UidPwd Based filterTp: 0 authUsed: 1
```

- debug https header trace：このコマンドを使用すると、Content Engine によって受信された要求の表示とトラブルシューティングを行うことができます。
- debug authentication http-request：このコマンドを使用すると、認証プロセスの表示とトラブルシューティングを行うことができます。 次にコマンドの出力例を示します。**認証の成功**

```
V5CE7325#sh http-authcache
Apr 10 10:08:03 V5CE7325 -admin-shell:
   %CE-PARSER-6-350232:CLI_LOG:sh http-authcache
AuthCache
=====================
hash   835 : uid: gdufour nBkt: (nil) nLRU: (nil) pLRU: (nil)
lacc: 70 ipAddr: 144.254.9.45 keyType: UidPwd Based filterTp: 0 authUsed: 1
```

要求の失敗（ユーザがインターネット グループのメンバでない場合）

```
V5CE7325#sh http-authcache
Apr 10 10:08:03 V5CE7325 -admin-shell:
   %CE-PARSER-6-350232:CLI_LOG:sh http-authcache
AuthCache
=====================
hash   835 : uid: gdufour nBkt: (nil) nLRU: (nil) pLRU: (nil)
```

```
lacc: 70 ipAddr: 144.254.9.45 keyType: UidPwd Based filterTp: 0 authUsed: 1
```

要求の失敗 (ユーザが LDAP データベースに存在しない場合)

```
V5CE7325#sh http-authcache
Apr 10 10:08:03 V5CE7325 -admin-shell:
   %CE-PARSER-6-350232:CLI_LOG:sh http-authcache
AuthCache
=====================
hash   835 : uid: gdufour nBkt: (nil) nLRU: (nil) pLRU: (nil)
lacc: 70 ipAddr: 144.254.9.45 keyType: UidPwd Based filterTp: 0 authUsed: 1
```

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- コンテンツ ネットワーキング Software Center (登録ユーザ専用)
- テクニカル サポートとドキュメント – Cisco Systems