UCSM LDAP のトラブルシューティング ガイド

内容

はじめに

このドキュメントでは、Unified Computing System Manager(UCSM)でのLightweight Directory Access Protocol(LDAP)設定の検証について説明し、LDAP認証の失敗の問題を調査する手順を示します。

設定ガイド：

UCSM認証の設定

Active Directory(AD)の設定例

UCSM LDAP設定の確認

UCSMが有限状態マシン(FSM)のステータスをチェックして設定を正常に導入し、100 %で完了したと表示されていることを確認します。

UCSMコマンドラインインターフェイス(CLI)コンテキストから

```
ucs # scope security
ucs /security # scope ldap
ucs /security/ldap # show configuration
ucs /security/ldap # show fsm status
```

Nexusオペレーティングシステム(NX-OS)のCLIコンテキストから

```
ucs # scope security
ucs(nxos)# show ldap-server
ucs(nxos)# show ldap-server groups
```

LDAP設定のベストプラクティス

1.「ネイティブ認証」レルムを変更せずに、追加の認証ドメインを作成する

2.「コンソール認証」には常にローカルレルムを使用します。ユーザーが「ネイティブ認証」を使用してロックアウトされた場合、管理者は引き続きコンソールからアクセスできます。

3. ログイン試行中に特定のauth-domain内のすべてのサーバが応答に失敗すると、UCSMは常にローカル認証にフェールバックします（test aaaコマンドには適用されません）。

LDAP設定の検証

NX-OSコマンドを使用してLDAP認証をテストします。「test aaa」コマンドは、NX-OS CLIインターフェイスからのみ使用できます。

1. LDAPグループ固有の設定を検証します。

次のコマンドは、設定されているすべてのLDAPサーバのリストを、設定されている順序に基づいて表示します。

```
ucs(nxos)# test aaa group ldap <username> <password>
```

2. 特定のLDAPサーバ設定の検証

```
ucs(nxos)# test aaa server ldap <LDAP-server-IP-address or FQDN> <username> <password>
```

注1:<password>文字列が端末に表示されます。

注2:LDAPサーバのIPまたはFQDNは、設定済みのLDAPプロバイダーと一致する必要があります。

この場合、UCSMは特定のサーバに対して認証をテストし、指定されたLDAPサーバにフィルタが設定されていない場合は失敗する可能性があります。

LDAPログイン障害のトラブルシューティング

この項では、LDAP認証の問題の診断について説明します。

問題シナリオ#1：ログインできない

UCSMグラフィカルユーザインターフェイス(GUI)とCLIの両方からLDAPユーザとしてログインできない

LDAP認証のテスト中に「Error authenticating to server」が表示されます。

```
(nxos)# test aaa server ldap <LDAP-server> <user-name> <password>
error authenticating to server
bind failed for <base DN>: Can't contact LDAP server
```

推奨事項
インターネット制御メッセージプロトコル(ICMP)pingを実行し、ローカル管理コンテキストからTelnet接続を確立することによって、LDAPサーバとファブリックインターコネクト(FI)管理インターフェイス間のネットワーク接続を確認します

```
ucs# connect local
ucs-local-mgmt # ping <LDAP server-IP-address OR FQDN>
ucs-local-mgmt # telnet <LDAP-Server-IP-Address OR FQDN> <port-number>
```

UCSMがLDAPサーバにpingできない場合、またはLDAPサーバへのTelnetセッションを開けない場合は、インターネットプロトコル(IP)ネットワーク接続を調査します。

ドメインネームサービス(DNS)がLDAPサーバホスト名の正しいIPアドレスをUCSに返すかどうかを確認し、これら2つのデバイス間でLDAPトラフィックがブロックされていないことを確認します。

問題シナリオ#2:GUIにログインできるが、SSHにログインできない

LDAPユーザはUCSM GUIからログインできますが、FIへのSSHセッションを開くことができません。

推奨事項

LDAPユーザとしてFIへのSSHセッションを確立する場合、UCSMではLDAPドメイン名の前に「ucs – 」を付加する必要があります

* Linux/MACマシンから

```
ssh ucs-<domain-name>\\<username>@<UCSM-IP-Address>
ssh -l ucs-<domain-name>\\<username> <UCSM-IP-address>
ssh <UCSM-IP-address> -l ucs-<domain-name>\\<username>
```

* puttyクライアントから

```
Login as: ucs-<domain-name>\<username>
```

注：ドメイン名は大文字と小文字が区別され、UCSMで設定されたドメイン名と一致する必要があります。ユーザ名の最大長は、ドメイン名を含めて32文字です。

"ucs-<ドメイン名>\<ユーザ名>" = 32文字。

問題シナリオ#3：ユーザに読み取り専用権限がある

LDAPユーザはログインできますが、LDAPグループマップがUCSMで正しく設定されていても、読み取り専用権限を持ちます。

推奨事項
LDAPログインプロセスでロールが取得されなかった場合、リモートユーザはリモートログインポリシーに基づいて、default-roleで許可されるか（読み取り専用アクセス）、UCSMへのアクセスを拒否されるか(no-login)のいずれかになります。

リモートユーザがログインし、ユーザに読み取り専用アクセス権が与えられた場合、LDAP/ADのユーザグループメンバーシップの詳細を確認します。
たとえば、MS Active Directory用のADSIEDITユーティリティを使用できます。また、

Linux/Macの場合はldapserachを使用できます。

NX-OSシェルから「test aaa」コマンドを実行して確認することもできます。

問題シナリオ#4:「リモート認証」を使用してログインできない

「ネイティブ認証」がリモート認証メカニズム（ LDAPなど）に変更されたときに、ユーザがリモートユーザとしてUCSMにログインできないか、または読み取り専用アクセス権を持つ

推奨事項
リモート認証サーバに到達できない場合、UCSMはコンソールアクセスのためにローカル認証にフォールバックするため、次の手順に従って回復できます。

1. プライマリFIの管理インターフェイスケーブルを取り外します（ show cluster stateはどちらがプライマリとして動作しているかを示します）。
2. プライマリFIのコンソールに接続します
3. 次のコマンドを実行して、ネイティブ認証を変更します

```
scope security
show authentication
set authentication console local
set authentication default local
commit-buffer
```

4. 管理インターフェイスケーブルを接続する
5. ローカルアカウントを使用してUCSM経由でログインし、リモート認証(ex LDAP)グループの認証ドメインを作成します。
注：管理インターフェイスを切断しても、データプレーントラフィックには影響しません。

問題シナリオ#4:LDAP認証は機能するが、SSLが有効な場合は機能しない

LDAP認証はSecure Socket Layer(SSL)を使用せずに正常に機能しますが、SSLオプションを有効にすると失敗します。

推奨事項
UCSM LDAPクライアントは、SSL接続の確立中に、設定されたトラストポイント(認証局(CA)証明書)を使用します。

1. トラストポイントが正しく設定されていることを確認します。

2. certのidentifyフィールドは、LDAPサーバの「ホスト名」である必要があります。UCSMで設定

されたホスト名が、証明書に存在するホスト名と一致し、有効であることを確認します。

3. UCSMがLDAPサーバの「ipaddress」ではなく、「hostname」で設定されており、ローカル管理インターフェイスから再び取得できることを確認します。

問題シナリオ#5:LDAPプロバイダーの変更後に認証が失敗する

古いLDAPサーバを削除して新しいLDAPサーバを追加すると認証が失敗する

推奨事項
LDAPが認証レルムで使用されている場合、新しいサーバの削除と追加は許可されません。UCSM 2.1バージョンからは、FSM障害が発生します。

同じトランザクションで新しいサーバを削除または追加する際に実行する手順は、次のとおりです

1. ldapを使用するすべての認証レルムがローカルに変更され、設定が保存されていることを確認します。
2. LDAPサーバを更新し、FSMステータスが正常に完了したことを確認します。
3. 手順1で変更したドメインの認証レルムをLDAPに変更します。

その他すべての問題のシナリオ：LDAPのデバッグ

デバッグをオンにし、LDAPユーザとしてログインを試み、失敗したログインイベントをキャプチャするUCSM techsupportとともに次のログを収集します。

1) FIへのSSHセッションを開き、ローカルユーザとしてログインし、NX-OS CLIコンテキストに変更します。

```
ucs # connect nxos
```

2)次のデバッグフラグを有効にし、SSHセッションの出力をログファイルに保存します。

```
ucs(nxos)# debug aaa all <<< not required, incase of debugging authentication problems.
ucs(nxos)# debug aaa aaa-requests

ucs(nxos)# debug ldap all <<< not required, incase of debugging authentication problems.
ucs(nxos)# debug ldap aaa-request-lowlevel
ucs(nxos)# debug ldap aaa-request
```

3)ここで新しいGUIまたはCLIセッションを開き、リモート(LDAP)ユーザとしてログインを試みます
4)ログイン失敗メッセージを受信したら、デバッグをオフにします。

```
ucs(nxos)# undebug all
```

LDAPトラフィックのパケットキャプチャ

パケットキャプチャが必要なシナリオでは、Ethanalyzerを使用してFIとLDAPサーバ間のLDAPトラフィックをキャプチャできます。

```
ucs(nxos)# ethanalyzer local interface mgmt capture-filter "host <LDAP-server-IP-address>" detail limit
```

上記のコマンドでは、pcapファイルは/workspace/diagnosticsディレクトリに保存され、ローカル管理CLIコンテキストを介してFIから取得できます

上記のコマンドを使用して、任意のリモート(LDAP 、 TACACS 、 RADIUS)認証トラフィックのパケットをキャプチャできます。
5. UCSM techsupportバンドルの関連ログ

UCSM techsupportでは、関連するログは<FI>/var/sysmgr/sam_logsディレクトリにあります

```
httpd.log
svc_sam_dcosAG
svc_sam_pamProxy.log
```

```
NX-OS commands or from <FI>/sw_techsupport log file

ucs-(nxos)# show system internal ldap event-history errors
ucs-(nxos)# show system internal ldap event-history msgs
ucs-(nxos)# show log
```

既知の警告

CSCth96721
samのldapサーバのrootdnは128文字を超える必要があります

UCSMの2.1より前のバージョンでは、ベースDN/バインドDN文字列に127文字の制限があります。

http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/cli/config/guide/2.0/b_UCSM_CLI_Configurati

---------以下省略----------
リモートユーザがログインし、システムがユーザ名に基づいてユーザのDNを取得しようとするときにサーバが検索を開始する必要がある、LDAP階層内の特定の識別名。サポートされる文字列の最大長は127文字です。
0.----------

この問題は、2.1.1以降のリリースで修正されています

CSCuf19514
LDAPデーモンのクラッシュ

ldap_start_tls_s呼び出しが初期化を完了するのに60秒を超える場合、sslライブラリの初期化中にLDAPクライアントがクラッシュする可能性があります。これは、無効なDNSエントリまたはDNS解決の遅延が発生した場合にのみ発生する可能性があります。

DNS解決の遅延とエラーに対処する手順を実行します。

CSCvt31344:UCSインフラストラクチャを4.0.4から4.1にアップグレードした後でセキュアLDAPが失敗する

インフラストラクチャファームウェア4.1以降でのLDAPの更新により、UCSMではより厳格なLDAP設定要件が必要になりました。UCSMのアップグレード後、設定が調整されるまでLDAP認証が失敗する場合があります。詳細は、CSCvt31344のリリースノートを参照してください。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。