UCSM LDAP 문제 해결 가이드

목차

소개

이 문서에서는 UCSM(Unified Computing System Manager)에서 LDAP(Lightweight Directory Access Protocol) 컨피그레이션의 유효성을 검사하는 방법과 LDAP 인증 실패 문제를 조사하는 단계를 제공합니다.

구성 가이드:

[UCSM 인증 구성](#)

[샘플 AD(Active Directory) 구성](#)

UCSM LDAP 컨피그레이션 확인

UCSM이 FSM(Finite State Machine) 상태를 확인하여 컨피그레이션을 성공적으로 구축했으며 100%로 완료되었는지 확인합니다.

UCSM CLI(Command Line Interface) 컨텍스트에서

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

Nexus 운영 체제(NX-OS) CLI 컨텍스트에서

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

LDAP 구성 모범 사례

1. "Native Authentication" 영역을 변경하는 대신 추가 인증 도메인을 생성합니다.

2. 항상 '콘솔 인증'에 로컬 영역을 사용합니다. 사용자가 '기본 인증'을 사용하지 못하도록 잠겨 있는 경우 관리자는 여전히 콘솔에서 액세스할 수 있습니다.

3. 로그인 시도 중에 지정된 auth-domain의 모든 서버가 응답하지 못한 경우 UCSM은 항상 로컬 인증으로 다시 실패합니다(test aaa 명령에는 해당되지 않음).

LDAP 컨피그레이션 검증

NX-OS 명령을 사용하여 LDAP 인증을 테스트합니다.'test aaa' 명령은 NX-OS CLI 인터페이스에서만 사용할 수 있습니다.

1. LDAP 그룹별 컨피그레이션을 검증합니다.

다음 명령은 구성된 순서에 따라 구성된 모든 LDAP 서버 목록을 거칩니다.

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

2. 특정 LDAP 서버 컨피그레이션을 검증합니다.

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

참고 1:<password> 문자열이 터미널에 표시됩니다.

참고 2:LDAP 서버 IP 또는 FQDN은 구성된 LDAP 제공자와 일치해야 합니다.

이 경우 UCSM은 특정 서버에 대해 인증을 테스트하며 지정된 LDAP 서버에 대해 구성된 필터가 없으면 실패할 수 있습니다.

LDAP 로그인 실패 문제 해결

이 섹션에서는 LDAP 인증 문제 진단에 대한 정보를 제공합니다.

문제 시나리오 #1 - 로그인할 수 없습니다.

UCSM GUI(Graphical User Interface) 및 CLI를 모두 통해 LDAP 사용자로 로그인할 수 없습니다.

사용자가 LDAP 인증을 테스트하는 동안 **"서버에 대한 인증 오류"**를 수신합니다.

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

권장 사항
ICMP(Internet Control Message Protocol) ping 및 로컬 관리 컨텍스트에서 텔넷 연결을 설정하여 LDAP 서버와 FI(Fabric Interconnect) 관리 인터페이스 간의 네트워크 연결을 확인합니다.

```
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>
```

UCSM이 LDAP 서버에 대해 ping하거나 텔넷 세션을 열 수 없는 경우 IP(Internet Protocol) 네트워크 연결을 조사합니다.

DNS(Domain Name Service)가 LDAP 서버 호스트 이름에 대해 UCS에 올바른 IP 주소를 반환하는지 확인하고 두 디바이스 간에 LDAP 트래픽이 차단되지 않았는지 확인합니다.

문제 시나리오 #2 - GUI에 로그인할 수 있으며 SSH에 로그인할 수 없습니다.

LDAP 사용자는 UCSM GUI를 통해 로그인할 수 있지만 FI에 대한 SSH 세션을 열 수 없습니다.

권장 사항

LDAP 사용자로 FI에 SSH 세션을 설정하는 경우 UCSM은 LDAP 도메인 이름 앞에 " ucs-"를 추가해야 합니다.

* Linux/MAC 시스템에서

```
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 클라이언트에서

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

참고:도메인 이름은 대/소문자를 구분하며 UCSM에 구성된 도메인 이름과 일치해야 합니다.최대 사용자 이름 길이는 도메인 이름을 포함하는 32자입니다.

"ucs-<domain-name>\<user-name>" = 32자

문제 시나리오 #3 - 사용자에게 읽기 전용 권한이 있음

LDAP 사용자는 로그인할 수 있지만 UCSM에서 ldap-group 맵이 올바르게 구성되었더라도 읽기 전

용 권한이 있습니다.

권장 사항
LDAP 로그인 프로세스 중에 역할이 검색되지 않은 경우 원격 사용자는 원격 로그인 정책에 따라 기본 역할(읽기 전용 액세스) 또는 UCSM에 로그인하기 위한 액세스(no-login)가 거부됩니다.

원격 사용자 로그인 및 사용자에게 읽기 전용 액세스 권한이 부여된 경우 이 경우 LDAP/AD에서 사용자 그룹 구성원 자격 세부사항을 확인합니다.
예를 들어 MS Active Directory용 ADSIEDIT 유틸리티를 사용할 수 있습니다.Linux/Mac의 경우 ldapserach를 선택합니다.

또한 NX-OS 셸에서 " test aaa " 명령을 사용하여 확인할 수 있습니다.

문제 시나리오 #4 - '원격 인증'으로 로그인할 수 없습니다.

"Native Authentication(기본 인증) "이 원격 인증 메커니즘(LDAP 등)으로 변경된 경우 사용자는 원격 사용자로 UCSM에 로그인하거나 읽기 전용 액세스 권한을 가질 수 없습니다.

권장 사항
UCSM이 원격 인증 서버에 연결할 수 없는 경우 콘솔 액세스를 위한 로컬 인증으로 폴백할 때 다음 단계에 따라 복구할 수 있습니다.

1. 기본 FI의 관리 인터페이스 케이블을 분리합니다(show cluster state는 Primary로 작동 중인 것을 나타냅니다.)
2. 기본 FI의 콘솔에 연결합니다.
3. 다음 명령을 실행하여 기본 인증을 변경합니다.

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

4. 관리 인터페이스 케이블을 연결합니다.
5. 로컬 계정을 사용하여 UCSM을 통해 로그인하여 원격 인증(예: LDAP) 그룹을 위한 인증 도메인을 생성합니다.
참고:관리 인터페이스의 연결을 끊어도 데이터 평면 트래픽에는 영향을 주지 않습니다.

문제 시나리오 #4 - LDAP 인증은 작동하지만 SSL은 활성화되지 않음

SSL(Secure Socket Layer) 없이 LDAP 인증이 제대로 작동하지만 SSL 옵션이 활성화되면 실패합니다.

권장 사항
UCSM LDAP 클라이언트는 SSL 연결을 설정하는 동안 구성된 신뢰 지점(CA(Certificate Authority) 인증서)을 사용합니다.

1. 신뢰 지점이 올바르게 구성되었는지 확인합니다.

2. 인증서의 ID 필드는 LDAP 서버의 " 호스트 이름 "이어야 합니다.UCSM에 구성된 호스트 이름이 인증서에 있는 호스트 이름과 일치하고 유효한지 확인합니다.

3. UCSM이 LDAP 서버의 'ipaddress'가 아닌 'hostname'으로 구성되어 있고 로컬 관리 인터페이스에서 다시 확인할 수 있는지 확인합니다.

문제 시나리오 #5 - LDAP 제공자가 변경된 후 인증이 실패합니다.

이전 LDAP 서버를 삭제하고 새 LDAP 서버를 추가한 후 인증이 실패합니다.

권장 사항
인증 영역에서 LDAP를 사용하는 경우 새 서버를 삭제하고 추가할 수 없습니다.UCSM 2.1 버전에서는 FSM 오류가 발생합니다.

동일한 트랜잭션에서 새 서버를 제거/추가할 때 수행하는 단계는 다음과 같습니다.

1. ldap를 사용하는 모든 인증 영역이 로컬 영역으로 변경되고 컨피그레이션이 저장되었는지 확인합니다.
2. LDAP 서버를 업데이트하고 FSM 상태가 성공적으로 완료되었는지 확인합니다.
3. 1단계에서 수정된 도메인의 인증 영역을 LDAP로 변경합니다.

기타 모든 문제 시나리오의 경우 - LDAP 디버깅

디버그를 켜고 LDAP 사용자로 로그인하고 실패한 로그인 이벤트를 캡처하는 UCSM 기술 지원과 함께 다음 로그를 수집합니다.

1) FI에 대한 SSH 세션을 열고 로컬 사용자로 로그인하고 NX-OS CLI 컨텍스트로 변경합니다.

```
ucs # connect nxos
```

2) 다음 디버그 플래그를 활성화하고 SSH 세션 출력을 로그 파일에 저장합니다.

```
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) 이제 새 GUI 또는 CLI 세션을 열고 원격(LDAP) 사용자로 로그인 시도
4) 로그인 실패 메시지를 수신한 후에는 **디버그를 끕니다.**

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

LDAP 트래픽의 패킷 캡처

패킷 캡처가 필요한 시나리오에서 Ethanalyzer를 사용하여 FI와 LDAP 서버 간의 LDAP 트래픽을

캡처할 수 있습니다.

```
ucs(nxos)# ethanalyzer local interface mgmt capture-filter "host
```

위의 명령에서 pcap 파일은 /workspace/diagnostics 디렉토리에 저장되며 로컬 관리 CLI 컨텍스트를 통해 FI에서 검색할 수 있습니다.

위의 명령을 사용하여 원격(LDAP, TACACS, RADIUS) 인증 트래픽에 대한 패킷을 캡처할 수 있습니다.
5. UCSM 기술 지원 번들의 관련 로그

UCSM 기술 지원에서 관련 로그는 **<FI>/var/sysmgr/sam_logs 디렉토리** 아래에 있습니다.

```
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
```

알려진 주의 사항

CSCth96721
sam에서 ldap 서버의 루트dn은 128자를 초과해야 합니다.

2.1 이전의 UCSM 버전은 기본 DN/바인드 DN 문자열에 대해 127자 제한을 가집니다.

http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/cli/config/guide/2.0/b_UCSM_CLI_Configuration_Guide_2_0_chapter_0111.html#task_0FC4E8245C6D4A64B5A1F575DAEC6127

— snip —
원격 사용자가 로그인하고 시스템이 사용자 이름을 기반으로 사용자의 DN을 가져오려고 시도할 때 서버가 검색을 시작해야 하는 LDAP 계층 구조의 특정 고유 이름입니다.지원되는 최대 문자열 길이는 127자입니다.
—

2.1.1 이상의 릴리스에서 문제가 해결됨

CSCuf19514
LDAP 디먼이 충돌함

ldap_start_tls_s 호출이 초기화를 완료하는 데 60초 이상 걸리는 경우 LDAP 클라이언트가 ssl 라이브러리를 초기화하는 동안 충돌할 수 있습니다.이는 잘못된 DNS 항목/DNS 확인 지연의 경우에만 발생할 수 있습니다.

DNS 확인 지연 및 오류를 해결하는 단계를 수행합니다.