Guia de solução de problemas UCSM LDAP

Contents

Introdução

Este documento fornece informações sobre como validar a configuração do Lightweight Diretory Access Protocol (LDAP) no Unified Computing System Manager (UCSM) e as etapas para investigar problemas de falha de autenticação LDAP.

Guias de configuração:

Configuração de autenticação do UCSM

Exemplo de configuração do Ative Diretory (AD)

Verificar a configuração LDAP do UCSM

Certifique-se de que o UCSM tenha implantado a configuração com êxito verificando o status da Máquina de Estado Finito (FSM) e se ela aparece concluída a 100%.

Do contexto da Interface de Linha de Comando (CLI) do UCSM

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

Do contexto CLI do Nexus Operating System (NX-OS)

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

Práticas recomendadas de configuração LDAP

1. Crie domínios de autenticação adicionais em vez de alterar o território da "Autenticação Nativa "

2. Sempre usar território local para 'autenticação de console'. Caso o usuário seja impedido de usar 'autenticação nativa', o administrador ainda poderá acessá-lo a partir do console.

3. O UCSM sempre retornará à autenticação local se todos os servidores em um determinado domínio de autenticação não responderem durante a tentativa de login (não aplicável para o comando test aaa).

Validando configuração LDAP

Teste a autenticação LDAP usando o comando NX-OS. O comando 'test aaa' está disponível somente na interface CLI do NX-OS.

1. Valide a configuração específica do grupo LDAP.

O comando a seguir percorre a lista de todos os servidores LDAP configurados com base em sua ordem configurada.

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

2. Validar a configuração específica do servidor LDAP

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

OBSERVAÇÃO 1: a sequência de **<password>** será exibida no terminal.

OBSERVAÇÃO 2: o IP ou FQDN do servidor LDAP deve corresponder a um provedor LDAP configurado.

Nesse caso, o UCSM testa a autenticação em relação a um servidor específico e pode falhar se não houver um filtro configurado para o servidor LDAP especificado.

Solução de problemas de falhas de login LDAP

Esta seção fornece informações sobre como diagnosticar problemas de autenticação LDAP.

Cenário de problema #1 - Não é possível fazer logon

Não é possível efetuar login como usuário LDAP via GUI (Graphical User Interface, interface gráfica do usuário) e CLI do UCSM

O usuário recebe "Error authenticating to server" enquanto testa a autenticação LDAP.

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

Recomendação
Verificar a conectividade de rede entre o servidor LDAP e a interface de gerenciamento da Interconexão de estrutura (FI) pelo ping do Protocolo de Mensagens de Controle da Internet (ICMP - Internet Control Message Protocol) e estabelecendo a conexão telnet a partir do contexto de gerenciamento local.

```
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>
```

Investigue a conectividade de rede do Internet Protocol (IP) se o UCSM não puder fazer ping no servidor LDAP ou abrir a sessão telnet para o servidor LDAP.

Verifique se o Serviço de Nome de Domínio (DNS) retorna o endereço IP correto para o UCS para o nome de host do servidor LDAP e certifique-se de que o tráfego LDAP não esteja

bloqueado entre esses dois dispositivos.

Cenário de problema #2 - Pode fazer login na GUI, não pode fazer login no SSH

O usuário LDAP pode fazer login através da GUI do UCSM, mas não pode abrir a sessão SSH para FI.

Recomendação

Ao estabelecer uma sessão SSH para FI como usuário LDAP, o UCSM requer que " ucs- " seja colocado antes do nome de domínio LDAP

* Do computador Linux/MAC

```
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>
```

* Do putty client

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

OBSERVAÇÃO: o nome de domínio diferencia maiúsculas de minúsculas e deve corresponder ao nome de domínio configurado no UCSM. O comprimento máximo do nome de usuário pode ser de 32 caracteres, o que inclui o nome do domínio.

"ucs-<domain-name>\<user-name>" = 32 caracteres.

Cenário de problema #3 - O usuário tem privilégios somente leitura

O usuário LDAP pode fazer login, mas tem privilégios somente leitura, mesmo que os mapas de grupo ldap estejam configurados corretamente no UCSM.

Recomendação
Se nenhuma função tiver sido recuperada durante o processo de login LDAP, o usuário remoto poderá fazer login no UCSM com a função padrão (acesso somente leitura) ou com o acesso negado (sem login), com base na política de login remoto.

Quando o usuário remoto faz login e recebe acesso somente leitura, nesse caso, verifique os detalhes de associação do grupo de usuários no LDAP/AD.
Por exemplo, podemos usar o utilitário ADSIEDIT para MS Ative Diretory. ou ldapserach no caso de Linux/Mac.

Também pode ser verificado com o comando " test aaa " no shell do NX-OS.

Cenário de problema #4 - Não é possível fazer logon com 'Autenticação Remota'

O usuário não pode fazer login ou tem acesso somente leitura ao UCSM como usuário remoto quando a " Autenticação nativa " foi alterada para o mecanismo de autenticação remota (LDAP etc)

Recomendação
Como o UCSM retorna à autenticação local para acesso de console quando não consegue alcançar o servidor de autenticação remota, podemos seguir as etapas abaixo para recuperá-lo.

1. Desconecte o cabo de interface de gerenciamento do FI primário (show cluster state indicaria qual está funcionando como Primário)
2. Conecte-se ao console do FI principal
3. Execute os seguintes comandos para alterar a autenticação nativa

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

4. Conecte o cabo de interface de gerenciamento
5. Faça login via UCSM usando a conta local e crie um domínio de autenticação para o grupo de autenticação remota (ex LDAP).
OBSERVAÇÃO: Desconectar a interface de gerenciamento NÃO afetaria nenhum tráfego de plano de dados.

Cenário de problema #4 - Autenticação LDAP funciona, mas não com SSL habilitado

A autenticação LDAP está funcionando bem sem SSL (Secure Socket Layer), mas falha quando a opção SSL está habilitada.

Recomendação

O cliente LDAP do UCSM usa os pontos de confiança configurados (certificados da Autoridade de Certificação) ao estabelecer a conexão SSL.

1. Verifique se o ponto de confiança foi configurado corretamente.

2. O campo de identificação no certificado deve ser o " nome do host "do servidor LDAP. Certifique-se de que o nome de host configurado no UCSM corresponda ao nome de host presente no certificado e seja válido.

3. Verifique se o UCSM está configurado com 'hostname' e não com 'ipaddress' do servidor LDAP e se ele pode ser recuperado da interface de gerenciamento local.

Cenário de problema #5 - A autenticação falha após as alterações do provedor LDAP

A autenticação falha após excluir o servidor LDAP antigo e adicionar o novo servidor LDAP

Recomendação
Quando o LDAP está sendo usado no domínio de autenticação, não é permitido excluir e adicionar novos servidores. A partir da versão 2.1 do UCSM, isso resultaria em falha do FSM.

As etapas a serem seguidas ao remover/adicionar novos servidores na mesma transação são

1. Certifique-se de que todos os territórios de autenticação usando ldap sejam alterados para local e salvos na configuração.
2. Atualize os servidores LDAP e verifique se o status do FSM foi concluído com êxito.
3. Altere os domínios de autenticação dos domínios modificados na etapa 1 para LDAP.

Para todos os outros cenários de problema - Depurando LDAP

Ative as depurações, tente fazer login como usuário LDAP e reúna os seguintes logs junto com o suporte técnico do UCSM que captura o evento de login com falha.

1) Abra uma sessão SSH para FI e faça login como usuário local e altere para o contexto CLI do NX-OS.

```
ucs # connect nxos
```

2) Ative os seguintes sinalizadores de depuração e salve a saída da sessão SSH no arquivo de registro.

```
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) Agora, abra uma nova sessão de GUI ou CLI e tente fazer login como usuário remoto (LDAP)
4) Depois de receber a mensagem de falha de login, desative as depurações.

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

Captura de pacotes do tráfego LDAP

Em cenários onde a captura de pacotes é necessária, o Ethanalyzer pode ser usado para capturar o tráfego LDAP entre o FI e o servidor LDAP.

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

No comando acima, o arquivo pcap é salvo no diretório /workspace/diagnostics e pode ser recuperado do FI através do contexto CLI de gerenciamento local

O comando acima pode ser usado para capturar pacotes para qualquer tráfego de autenticação remoto (LDAP, TACACS, RADIUS).
5. Logs relevantes no pacote de suporte técnico do UCSM

No suporte técnico do UCSM, os registros relevantes estão localizados no <FI>/var/sysmgr/sam_logs diretory

```
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
```

Caveats conhecidos

CSCth96721
rootdn do servidor ldap no sam deve permitir mais de 128 caracteres

A versão do UCSM anterior à 2.1 tem um limite de 127 caracteres para a string DN base/DN de ligação.

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

---------- de recorte de ---------
O nome distinto específico na hierarquia LDAP onde o servidor deve iniciar uma pesquisa quando um usuário remoto faz login e o sistema tenta obter o DN do usuário com base em seu nome de usuário. O comprimento máximo da cadeia de caracteres é de 127 caracteres.

O problema foi corrigido na versão 2.1.1 e superior

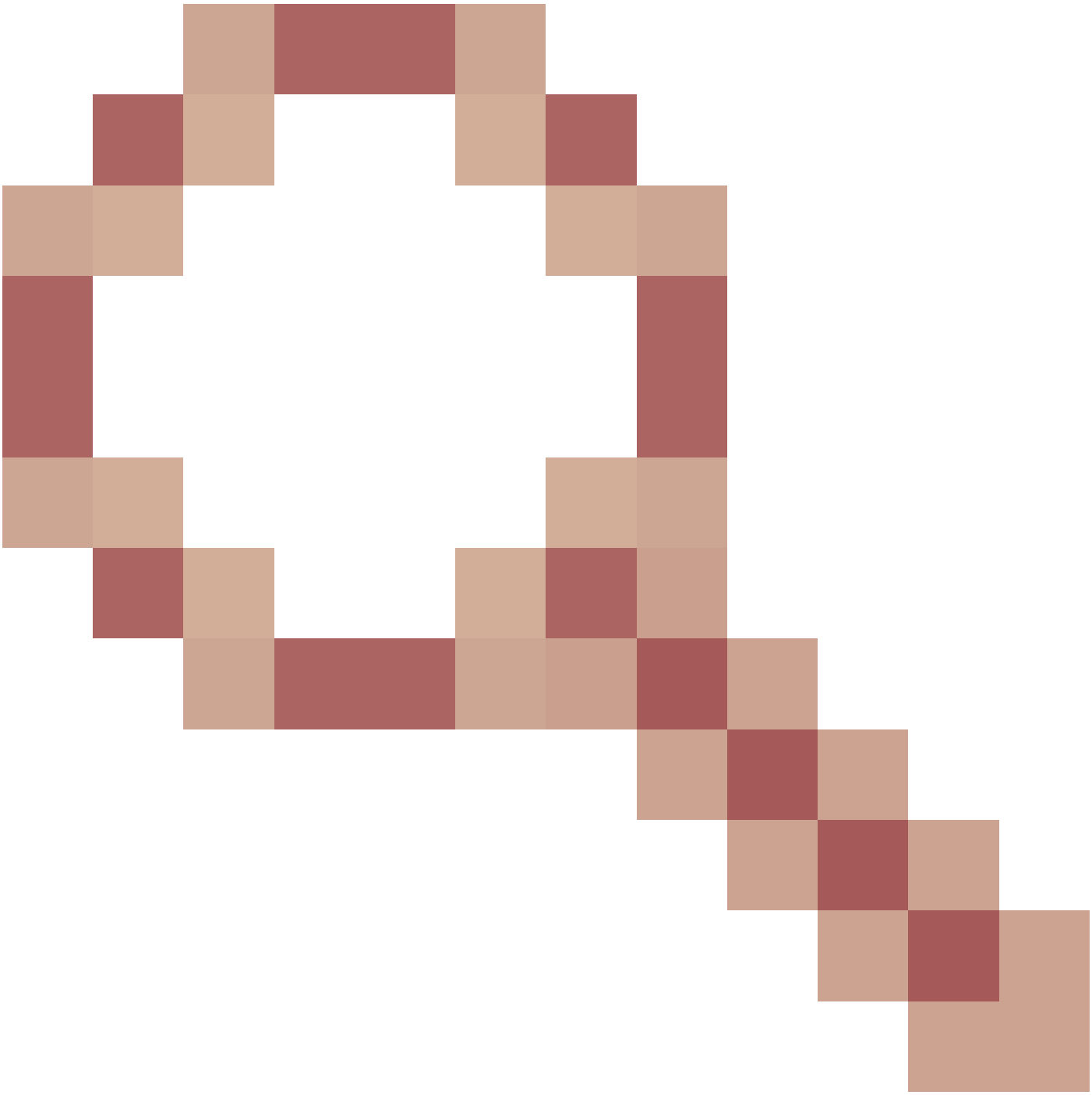
CSCuf19514
daemon LDAP travou

O cliente LDAP pode travar durante a inicialização da biblioteca ssl se a chamada ldap_start_tls_s levar mais de 60 segundos para concluir a inicialização. Isso só poderia acontecer em caso de entrada de DNS inválida / atrasos na resolução DNS.

Tome medidas para resolver os atrasos e erros de resolução de DNS.

CSCvt31344 - LDAP seguro falha após atualização de infra do UCS de 4.0.4 para 4.1

As atualizações de LDAP no firmware de infraestrutura 4.1 e posterior resultaram em requisitos de configuração LDAP mais rigorosos no UCSM. Após a atualização do UCSM, a autenticação LDAP pode falhar, até que a configuração seja ajustada. Consulte as notas de versão do CSCvt31344



para obter detalhes.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.