Guía de Troubleshooting de LDAP de UCSM

Contenido

Introducción

Este documento proporciona información sobre la validación de la configuración del protocolo ligero de acceso a directorios (LDAP) en Unified Computing System Manager (UCSM) y los pasos para investigar los problemas de falla de autenticación LDAP.

Guías de Configuración:

[Configuración de la Autenticación de UCSM](#)

[Ejemplo de configuración de Active Directory (AD)](#)

Verificar la configuración LDAP de UCSM

Asegúrese de que UCSM ha implementado la configuración correctamente comprobando el estado de la Máquina de estado finito (FSM) y de que muestra completada al 100%.

Desde el contexto de la interfaz de línea de comandos (CLI) de UCSM

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

Desde el contexto CLI de Nexus Operating System (NX-OS)

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

Prácticas recomendadas de configuración LDAP

1. Crear dominios de autenticación adicionales en lugar de cambiar el rango de "Autenticación nativa"

2. Utilice siempre el rango local para 'autenticación de consola'. En caso de que el usuario no pueda utilizar 'autenticación nativa', el administrador podrá acceder a él desde la consola.

3. UCSM siempre falla en la autenticación local si todos los servidores en el dominio de autenticación dado fallaron en responder durante el intento de inicio de sesión (no se aplica para el comando test aaa) .

Validación de la configuración LDAP

Pruebe la autenticación LDAP con el comando NX-OS. El comando 'test aaa' sólo está disponible en la interfaz CLI de NX-OS.

1. Validar la configuración específica del grupo LDAP.

El siguiente comando pasa por la lista de todos los servidores LDAP configurados en función de su orden configurado.

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

2. Validar la configuración específica del servidor LDAP

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

NOTA 1: <password> se mostrará en el terminal.

NOTA 2: La IP o FQDN del servidor LDAP debe coincidir con un proveedor LDAP configurado.

En este caso, UCSM prueba la autenticación con un servidor específico y puede fallar si no hay ningún filtro configurado para el servidor LDAP especificado.

Resolución de problemas de fallas de inicio de sesión LDAP

Esta sección proporciona información sobre el diagnóstico de problemas de autenticación LDAP.

Situación de problema nº 1: no se puede iniciar sesión

No se puede iniciar sesión como usuario LDAP a través de la interfaz gráfica de usuario (GUI) de UCSM y CLI

El usuario recibe **"Error al autenticarse en el servidor"** mientras se prueba la autenticación 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
```

Recomendación

Verifique la conectividad de red entre el servidor LDAP y la interfaz de administración de Fabric Interconnect (FI) mediante ping de protocolo de mensajes de control de Internet (ICMP) y el establecimiento de una conexión telnet desde el contexto de administración 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 la conectividad de red de protocolo de Internet (IP) si UCSM no puede hacer ping con el servidor LDAP o abrir sesión telnet con el servidor LDAP.

Verifique si el servicio de nombres de dominio (DNS) devuelve la dirección IP correcta a UCS para el nombre de host del servidor LDAP y asegúrese de que el tráfico LDAP no esté bloqueado entre estos dos dispositivos.

Situación de problema nº 2: puede iniciar sesión en la GUI, no puede iniciar sesión en SSH

El usuario LDAP puede iniciar sesión a través de UCSM GUI pero no puede abrir la sesión SSH a FI.

Recomendación

Al establecer la sesión SSH a FI como usuario LDAP, UCSM requiere que " ucs- " se anteponga antes del nombre de dominio LDAP

* Desde la máquina 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>
```

* Del cliente de putty

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

NOTE: El nombre de dominio distingue entre mayúsculas y minúsculas y debe coincidir con el nombre de dominio configurado en UCSM. La longitud máxima del nombre de usuario puede ser de 32 caracteres que incluye el nombre de dominio.

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

Situación de problema nº 3: el usuario tiene privilegios de solo lectura

El usuario LDAP puede iniciar sesión pero tiene privilegios de sólo lectura aunque los mapas ldap-group estén correctamente configurados en UCSM.

Recomendación

Si no se recuperó ninguna función durante el proceso de inicio de sesión LDAP, se permite al usuario remoto con la función predeterminada (acceso de sólo lectura) o acceso denegado (sin inicio de sesión) para iniciar sesión en UCSM, según la política de inicio de sesión remoto.

Cuando el usuario remoto inicia sesión y se le da acceso de sólo lectura, en ese caso verifique los detalles de pertenencia al grupo de usuarios en LDAP/AD.
Por ejemplo, podemos utilizar la utilidad ADSIEDIT para MS Active Directory. o ldapserach en caso de Linux/Mac.

También se puede verificar con el comando " test aaa " del shell de NX-OS.

Situación de problema nº 4: no se puede iniciar sesión con 'Autenticación remota'

El usuario no puede iniciar sesión o tiene acceso de sólo lectura a UCSM como usuario remoto cuando " Autenticación nativa " se cambió a mecanismo de autenticación remota (LDAP etc)

Recomendación

Como UCSM se devuelve a la autenticación local para el acceso a la consola cuando no puede alcanzar el servidor de autenticación remoto, podemos seguir los siguientes pasos para recuperarlo.

1. Desconecte el cable de interfaz de administración de FI principal (show cluster state indicaría cuál actúa como Primario)
2. Conexión a la consola del FI principal
3. Ejecutar los siguientes comandos para cambiar la autenticación nativa

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

4. Conecte el cable de interfaz de administración
5. Inicie sesión a través de UCSM mediante la cuenta local y cree un dominio de autenticación para el grupo de autenticación remota (ex LDAP).
NOTE: La desconexión de la interfaz de administración NO afectaría a ningún tráfico del plano de datos.

Situación de problema nº 4 - La autenticación LDAP funciona pero no con SSL

habilitado

La autenticación LDAP funciona correctamente sin Secure Socket Layer (SSL), pero falla cuando la opción SSL está activada.

Recomendación

El cliente LDAP de UCSM utiliza los puntos de confianza configurados (certificados de Autoridad de Certificación (CA)) al establecer la conexión SSL.

1. Asegúrese de que el punto de confianza se configuró correctamente.

2. El campo de identificación en cert debe ser el " hostname " del servidor LDAP. Asegúrese de que el nombre de host configurado en UCSM coincida con el nombre de host presente en el certificado y sea válido.

3. Asegúrese de que UCSM esté configurado con 'hostname' no con 'ipaddress' del servidor LDAP y que se pueda reprogramar desde la interfaz de administración local.

Escenario de problema nº 5: la autenticación falla después de que el proveedor LDAP cambie

La autenticación falla después de eliminar el servidor LDAP antiguo y agregar el nuevo servidor LDAP

Recomendación

Cuando se utiliza LDAP en el rango de autenticación, no se permite la eliminación y adición de nuevos servidores. De la versión 2.1 de UCSM, se produciría un error de FSM.

Los pasos que se deben seguir al eliminar/agregar nuevos servidores en la misma transacción son

1. Asegúrese de que todos los rangos de autenticación que utilizan ldap se cambien a local y guarden la configuración.
2. Actualice los servidores LDAP y verifique que el estado de FSM se haya completado correctamente.
3. Cambie los rangos de autenticación de dominios modificados en el paso 1, a LDAP.

Para todos los demás escenarios de problemas - Depuración LDAP

Active las depuraciones, intente iniciar sesión como usuario LDAP y recopile los registros siguientes junto con la compatibilidad técnica de UCSM que captura el evento de inicio de sesión fallido.

1) Abra una sesión SSH en FI e inicie sesión como usuario local y cambie al contexto CLI de NX-OS.

```
ucs # connect nxos
```

2) Habilite los siguientes indicadores de depuración y guarde el resultado de la sesión SSH en el archivo 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) Ahora abra una nueva sesión GUI o CLI e intente iniciar sesión como usuario remoto (LDAP)
4) Una vez que haya recibido el mensaje de error de inicio de sesión, **apague las depuraciones.**

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

Captura de paquetes del tráfico LDAP

En escenarios donde se requiere captura de paquetes, Ethanalyzer puede utilizarse para capturar el tráfico LDAP entre FI y servidor LDAP.

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

En el comando anterior, el archivo pcap se guarda en el directorio /workspace/diagnostics y se puede recuperar de FI a través del contexto CLI de administración local

El comando anterior se puede utilizar para capturar paquetes para cualquier tráfico de autenticación remota (LDAP, TACACS, RADIUS).
5. Registros relevantes en el paquete de soporte técnico UCSM

En UCSM techsupport, los registros relevantes se encuentran en el **<FI>/var/sysmgr/sam_logs directory**

```
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
```

Advertencias conocidas

CSCth96721
la raíz del servidor ldap en sam debe tener más de 128 caracteres

La versión de UCSM anterior a 2.1 tiene una limitación de 127 caracteres para el DN base / cadena DN de enlace.

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

nfiguration_Guide_2_0_chapter_0111.html#task_0FC4E8245C6D4A64B5A1F575DAEC6127

---------snip----------
El nombre distinguido específico en la jerarquía LDAP donde el servidor debería comenzar una búsqueda cuando un usuario remoto inicia sesión y el sistema intenta obtener el DN del usuario basado en su nombre de usuario. La longitud máxima de cadena admitida es de 127 caracteres.
—

El problema se soluciona en la versión 2.1.1 y posteriores

CSCuf19514
Demonio LDAP dañado

El cliente LDAP puede fallar mientras se inicializa la biblioteca ssl si la llamada ldap_start_tls_s tarda más de 60 segundos en completar la inicialización. Esto sólo podría ocurrir en caso de entrada DNS no válida / retrasos en la resolución DNS.

Tome medidas para solucionar los retrasos y errores de resolución de DNS.