Contenido

Introducción

Este documento proporciona la información sobre validar la configuración del Lightweight Directory Access Protocol (LDAP) en el conjunto de administración de las Comunicaciones unificadas (UCSM) y los pasos para investigar los problemas del error de la autenticación ldap.

Guías de configuración:

[UCSM que configura la autenticación](#)

[Configuración del Active Directory de la muestra (AD)](#)

Verifique la Configuración LDAP UCSM

Aseegurese UCSM ha desplegado la configuración con éxito marcando máquina de estados finitos (FSM) el estatus y muestra completado en el 100%.

Del contexto del comando line interface(cli) UCSM

Del contexto del sistema operativo del nexo (NX-OS) CLI

Mejores prácticas de la Configuración LDAP

1. Cree los dominios adicionales de la autenticación en vez del reino cambiante de “Authenitcation nativo”

2. Utilice siempre el terreno local para la “autenticación de la consola”, en caso de que el usuario esté bloqueado hacia fuera de usar la “autenticación nativa”, admin todavía podría accederlo de la consola.

3. UCSM falla siempre de nuevo a la autenticación local si todos los servidores en el auténtico-dominio dado no pudieron responder durante el intento de inicio de sesión (no corresponde para el comando aaa de la prueba).

Validar la Configuración LDAP

Pruebe la autenticación ldap usando el comando NX-OS. “el comando aaa de la prueba” está disponible solamente de la interfaz CLI NX-OS.

1. Valide la configuración del específico del grupo LDAP.

El siguiente comando pasa a través de la lista de todos los servidores LDAP configurados basados en su orden configurado.

2. Valide la configuración de servidor LDAP específica

NOTA: la cadena del <password> será visualizada en la terminal.

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

Resolver problemas las fallas de registro LDAP

Esta sección proporciona la información sobre el diagnóstico de los problemas de la autenticación ldap.

Recreación de un problema #1 - No puede iniciar sesión

No puede iniciar sesión como usuario LDAP vía el Interfaz gráfica del usuario (GUI) UCSM y el CLI

El usuario recibe el **“error que autentica al servidor”** mientras que prueba la autenticación ldap.

Recomendación

Verifique la conectividad de red entre el servidor LDAP y la interfaz de administración de la interconexión de la tela (FI) por el ping del Internet Control Message Protocol (ICMP) y conexión Telnet del establecimiento del contexto del local-mgmt

Investigue la conectividad de red del Internet Protocol (IP) si UCSM no puede hacer ping al servidor LDAP o abrir a la sesión telnet en el servidor LDAP.

Verifique si el servicio de nombre del dominio (DNS) vuelve la dirección IP correcta al UCS para el nombre de host del servidor LDAP y aseegurese que el tráfico LDAP no está bloqueado entre estos dos dispositivos.

Recreación de un problema #2 - Puede registrar en el GUI, no puede registrar en SSH

El usuario LDAP puede iniciar sesión vía UCSM GUI pero no puede abrir a la sesión SSH en el FI.

Recomendación

Al establecer a la sesión SSH al FI como usuario LDAP, UCSM requiere el “ucs” prepended antes del Domain Name LDAP

* De la máquina de Linux/MAC

* Del cliente del putty

NOTA: El Domain Name es con diferenciación entre mayúsculas y minúsculas y debe hacer juego el Domain Name configurado en UCSM. La longitud máxima del nombre de usuario puede ser 32 chares que incluye el Domain Name.

“ucs-<domain-name> \ <user-name>” = 32 chares.

Recreación de un problema #3 - El usuario tiene privilegios solo lecturas

El usuario LDAP puede iniciar sesión sino tener privilegios solo lecturas aunque las correspondencias del ldap-grupo se configuran correctamente en UCSM.

Recomendación

Si no se extrajo ningunos papeles durante el proceso de ingreso LDAP, se permite al usuario remoto con el valor por defecto-papel (acceso del read only) o el acceso negado (ninguno-login) iniciar sesión a UCSM, sobre la base de la directiva del remote login.

Cuando el usuario remoto abre una sesión y dieron el usuario acceso de sólo lectura, en ese caso verifique los detalles de la calidad de miembro de grupo de usuarios en LDAP/AD.
Por ejemplo, podemos utilizar la utilidad ADSIEdit para el Active Directory MS. o ldapserach en caso de Linux/mac.

Puede también ser verificado con “el comando aaa de la prueba” del shell NX-OS.

Recreación de un problema #4 - No puede iniciar sesión con la “autenticación remota”

El usuario no puede iniciar sesión ni tiene acceso de sólo lectura a UCSM como usuario remoto

cuando la “autenticación nativa” fue cambiada al mecanismo de autenticación remota (LDAP los etc)

Recomendación

Como fallsback UCSM a la autenticación local para el acceso a la consola cuando no puede alcanzar el servidor de la autenticación remota, podemos seguir debajo de los pasos para recuperarlo.

1. Desconecte el cable de interfaz del mgmt del FI primario (el estado del cluster de la demostración indicaría cuál está actuando como primario)
2. Conecte con la consola del FI primario
3. Ejecute los siguientes comandos de cambiar la autenticación nativa

4. Conecte el cable de interfaz del mgmt
5. Inicie sesión vía UCSM usando la cuenta local y cree el auténtico-dominio para el grupo de la autenticación remota (ex LDAP).
NOTA: La desconexión de la interfaz del mgmt no afectaría a ningún tráfico del plano de los datos.

Recreación de un problema #4 - Trabajos de la autenticación ldap pero no con el SSL habilitado

La autenticación ldap está trabajando muy bien sin el Secure Socket Layer (SSL) pero falla cuando se habilita la opción de SSL.

Recomendación

El cliente LDAP UCSM utiliza las confianza-puntas configuradas (Certificados del Certificate Authority (CA)) mientras que establece la conexión SSL.

1. Aseegurese la confianza-punta fue configurado correctamente.

2. El campo de la identificación en el CERT debe ser el “nombre de host “del servidor LDAP. Aseegurese el nombre de host configurado en UCSM hace juego el nombre de host presente en el certificado y es válido.

3. Aseegurese UCSM se configura con “el IP address” del “nombre de host” no del servidor LDAP y es recheable de la interfaz del local-mgmt.

Recreación de un problema #5 - La autenticación falla después de que el proveedor LDAP cambie

La autenticación falla después de borrar al viejo servidor LDAP y de agregar al nuevo servidor LDAP

Recomendación

Cuando el LDAP se está utilizando en el reino, borrar y agregar de la autenticación de los nuevos servidores no se permite. De la versión del 2.1 UCSM, daría lugar al error FS.

Los pasos a seguir cuando es la eliminación/que agrega los nuevos servidores en la misma

transacción

1. Aseegurese todos los reinos de la autenticación usando el ldap se cambian al local y guardó la configuración.
2. Ponga al día a los servidores LDAP y verifiquelos que el estatus FS ha completado con éxito.
3. Cambie los reinos del auth de los dominios modificados en el paso 1, al LDAP.

Para el resto de las recreaciones de un problema - Hacer el debug del LDAP

Gire los debugs, intente iniciar sesión como usuario LDAP y recolectar después de los registros junto con el techsupport UCSM que captura el evento fallado del login.

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

2) Habilite los indicadores de siguiente del debug y salve a la sesión SSH hecha salir al archivo del registro.

3) Ahora abra un nuevo GUI o sesión CLI e intente iniciar sesión como usuario remoto (LDAP)
4) Una vez que usted recibió el mensaje de la falla de registro, **apague los debugs.**

Caputure del paquete del tráfico LDAP

En los escenarios donde requieren a la captura de paquetes, Ethanalyzer pueda utilizado para capturar el tráfico LDAP entre el FI y el servidor LDAP.

En el comando antedicho, el archivo del pcap se guarda bajo directorio de /workspace/diagnostics y se puede extraer del FI vía el contexto del local-mgmt CLI

Sobre el comando puede ser utilizado para capturar los paquetes para cualquier (LDAP, TACACS, RADIUS) tráfico remoto del authenitcation.
5. Relevante abre una sesión al conjunto del techsupport UCSM

En el techsupport UCSM, los registros relevantes están situados bajo **directorio <FI>/var/sysmgr/sam_logs**

Advertencias conocidas

CSCth96721
el rootdn del servidor LDAP en Sam debe permitir más que los caracteres 128

La versión UCSM que el 2.1 tiene anterior limitación de 127 caracteres para la base DN/la cadena del lazo DN.

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

--------- recorte ----------
El nombre distintivo específico en la jerarquía LDAP donde el servidor debe comenzar una

búsqueda cuando un usuario remoto abre una sesión y el sistema intenta conseguir el DN del usuario basado en su nombre de usuario. La longitud soportada máximo de la cadena es 127 caracteres.

El problema se repara en 2.1.1 y sobre la versión

CSCuf19514
La daemon LDAP causó un crash

El cliente LDAP puede causar un crash mientras que inicializa la biblioteca SSL si la llamada de los ldap_start_tls_s toma más de 60 secs para completar la inicialización. Esto podía suceder solamente en caso de la entrada DNS/de los retardos inválidos en la resolución de DNS.

Tome las medidas para dirigir los retardos y los errores de la resolución de DNS.