Ferramenta NAC (CCA): Configurar e pesquise defeitos sinal de Windows do diretório ativo o único em (o SSO)

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Convenções
Configurar Windows SSO
Estabelecer o fornecedor AD SSO
Execute KTPass no DC
Configurar o SSO em CAS
Verifique que o serviço SSO está começado
Portas aberta ao DC
O cliente vê o agente SSO de execução
SSO terminado
Usuário SSO visto na lista de usuário on-line
Pesquise defeitos Windows SSO
Erro: Não podia começar o serviço SSO. Verifique por favor a configuração.
A authenticação do cliente não trabalha
Incapaz de executar o SSO nos indicadores 7 PC
Incapaz de configurar o apoio do cliente Linux para um usuário no ambiente NAC
O serviço SSO é começado, mas o cliente não executa o SSO
Kerbtray
Logs de CAS – Não pode começar o serviço SSO
Problemas conhecidos
Informações Relacionadas

Introdução

Este documento descreve como usar sinal do diretório ativo de Microsoft Windows o único (AD) sobre (SSO) a fim configurar e pesquisar defeitos o dispositivo do Cisco Network Admission Control (NAC), conhecido anteriormente como o acesso limpo de Cisco (CCA).

Pré-requisitos

Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Certifique-se do Windows 2000 SP4 ou Windows 2003 (padrão ou empresa) SP1 ou Windows 2003 R2 das corridas DC. Windows 2003 sem SP1 não é apoiado.
- Certifique-se que Windows SSO está apoiado em um ambiente AD somente. O ambiente do Windows NT não é apoiado. O agente limpo do acesso é exigido.
- Estabelecer a conta limpa do servidor de acesso (CAS) como descrito na ferramenta NAC de Cisco - Guia de Instalação e Configuração limpo do servidor de acesso, a liberação 4.1(2).

Componentes Utilizados

A informação neste documento é baseada a versão de software em 4.x da ferramenta NAC ou em mais tarde.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configurar Windows SSO

A informação nesta seção descreve como configurar as características apresentadas neste documento.

Estabelecer o fornecedor AD SSO

- Você não pode executar um teste da autenticação a um fornecedor AD SSO ou a um VPN SSO.
- O server da consulta LDAP é precisado somente se os usuários querem fazer regras do mapeamento para o AD SSO, de modo que após AD SSO, os usuários estejam colocados nos papéis baseados em atributos AD. Isto não é precisado de obter o funcionamento básico SSO (sem mapeamento do papel).

Execute KTPass no DC

KTPass é uma ferramenta disponível como parte de Windows 2000/2003 de ferramenta de suporte. Refira a ferramenta NAC de Cisco - Limpe o Guia de Instalação e Configuração do servidor de acesso, libere 4.1(2) para mais informação.

Quando você executa KTPass, é importante notar que o nome de computador que cai sempre entre “/” e “@” combina o nome do DC porque apareceria sob o Control Panel > o sistema > o nome de computador > completamente nome de computador no DC.

Também, certifique-se de que o nome de esfera que aparece após @ destacado está sempre em

letras de caixa.

```
C:\Program Files\Support Tools>ktpass -princ
 ccasso/prem-vm-2003.win2k3.local@WIN2K3.LOCAL -mapuser ccasso -pass Cisco123 -out
c:\test.keytab -ptype KRB5_NT_PRINCIPAL +DesOnly Using legacy password setting method //confirms
ccasso acct is mapped Successfully mapped ccasso/prem-vm-2003.win2k3.local to ccasso. Key
created. Output keytab to c:\test.keytab Keytab version: 0x502 keysize 80 ccasso/prem-vm-
2003.win2k3.local@WIN2K3.LOCAL ptype 1 (KRB5_NT_PRINCIPAL) vno 3 etype 0x17 (RC4-HMAC) keylength
16 (0xf2e787d376cbf6d6dd3600132e9c215d) Account ccasso has been set for DES-only encryption.
```

A fim apoiar Windows 7, você deve executar KTPASS segundo as indicações deste exemplo:

```
C:\Program Files\Support Tools>KTPASS.EXE -princ
newadsso/[adserver.]domain.com@DOMAIN.COM -mapuser newadsso -pass PasswordText -out
c:\newadsso.keytab -ptype KRB5_NT_PRINCIPAL
```

Também, certifique-se de que o nome de esfera que aparece após @ destacado está sempre em letras de caixa.

Configurar o SSO em CAS

Escolha **server CCA > controlam > autenticação > AUTH de Windows > diretório ativo SSO** a fim abrir o indicador AD, e verificam estes artigos:

- Domínio do diretório ativo: Necessidades do name= da esfera de kerberos de ser caixa.
- Servidor ative directory (FQDN): Certifique-se de que CAS pode resolver este nome através do DNS. Este campo não pode ser um endereço IP de Um ou Mais Servidores Cisco ICM NT. Usando os valores neste exemplo, você pode entrar a CAS através do Shell Seguro (ssh), e executa o “nslookup prem-vm-2003.win2k3.local”. Então, certifique-se que resolve com sucesso.
- Certifique-se que o FQDN combina o nome do server AD (DC) exatamente enquanto aparece sob o Control Panel > o sistema > o nome de computador | Nome de computador completo na máquina do servidor AD (DC).

Verifique que o serviço SSO está começado

Conclua estes passos:

1. Vai aos **server CCA > controla > o estado** a fim verificar que o serviço SSO está começado.
2. Execute este comando a fim verificar que CAS escuta agora em TCP 8910 (usado para Windows SSO).`[root@cs-ccas02 ~]#netstat -a | grep 8910 tcp 0 0 *:8910 *:* LISTEN`

Portas aberta ao DC

A fim abrir as portas apropriadas ao DC, termine estas etapas:

Nota: Para testar, abra sempre o acesso completo ao DC. Então, uma vez que o SSO trabalha, você pode amarrá-lo para tragar às portas específicas.

1. Certifique-se que as seguintes portas estão permitidas no papel não confiável ao diretório ativo:**TCP**: 88, 135, 445, 389/636, 1025, 1026**UDP**: 88, 389**Nota:** *A PORTA TCP 445* deve estar aberta para a senha do Windows restaurada para trabalhar corretamente.
2. Assegure-se de que o cliente execute o agente 4.0.0.1 CCA ou mais tarde.

3. Entre ao PC com as credenciais do domínio do Windows.**Nota:** Certifique-se que você está registrando no domínio e não na conta local.

O cliente vê o agente SSO de execução

SSO terminado

Usuário SSO visto na lista de usuário on-line

Pesquise defeitos Windows SSO

Erro: Não podia começar o serviço SSO. Verifique por favor a configuração.

Problema

Você recebe este erro:

Solução

Para resolver esse problema, siga estas etapas:

1. Verifique para certificar-se corretamente de corridas de KTPass. É importante verificar os campos como mencionado na corrediça X. Se KTPass foi executado incorretamente, suprima da conta e crie uma conta nova no AD e execute KTPass outra vez.
2. Certifique-se que o tempo em CAS está sincronizado com o DC.Esta etapa pode ser executada apontando os ambos ao mesmo Time Server. Nas instalações de laboratório, aponte CAS ao DC próprio pelo tempo (o DC executa o tempo de Windows). O Kerberos é sensível cronometrar e o enviesamento não pode ser maior do que os minutos 5 (300 segundos).**Nota:** Quando você tenta começar o serviço AD SSO de CAS, uma edição pôde ocorrer com o syncronization do tempo, NTP. Se o NTP está configurado, e os pulsos de disparo não syncronized, os serviços não funcionarão. Uma vez que fixado os serviços devem trabalhar.
3. Certifique-se que o domínio do diretório ativo está no upper-case (reino) e CAS pode resolver o FQDN no DNS. Para instalações de laboratório, você pode apontar a um DC que execute o DNS (o AD exige no servidor DNS do aluguer um).
4. Log em CAS diretamente como o <CAS-IP-endereço >/admin de https://. Então, os **logs do apoio do** clique e mudam o nível de registro para a comunicação do diretório ativo que registra à **informação**.
5. Recreie o problema e transfira os logs do apoio.

A authenticação do cliente não trabalha

Problema

O serviço AD SSO é começado, mas a authenticação do cliente não trabalha.

Solução

As portas UDP não estavam abertas no papel não autenticado. Depois que você adiciona estas portas às políticas de tráfego, a autenticação deve trabalhar.

Incapaz de executar o SSO nos indicadores 7 PC

Problema

O SSO não está trabalhando para as máquinas que executam o sistema operacional de Windows 7.

Solução 1

A fim resolver esta edição, permita a criptografia DES na máquina que executa o sistema operacional de Windows 7, e torne a colocar em funcionamento então o KTPass. Termine estas etapas a fim permitir o DES em Windows 7 PC:

1. Entre à máquina cliente de Windows 7 como um administrador.
2. Vá ao **começo > ao Control Panel > ao sistema e à Segurança > às ferramentas administrativas > à política de segurança local > às políticas local/Segurança > opções**.
3. Escolha a **segurança de rede > configuram os tipos de criptografia permitidos**.
4. Nos ajustes da segurança local catalogue, verifique as caixas de seleção para permitir todas as opções, exceto a opção futura dos tipos de criptografia.

Solução 2

A fim resolver esta edição, execute este comando no server de Windows 2003 (se precisa de apoiar também Windows 7):

```
C:\Program Files\Support Tools> ktpass.exe -princ
casuser/cca-eng-domain.cisco.com@CCA-ENG-DOMAIN.CISCO.COM-mapusercasuser -pass
Cisco123 -out c:\casuser.keytab -ptype KRB5_NT_PRINCIPAL
```

Para mais informação, consulte para configurar AD SSO em um ambiente de Windows 7.

Incapaz de configurar o apoio do cliente Linux para um usuário no ambiente NAC

Problema

Incapaz de configurar o apoio do cliente Linux para um usuário no ambiente NAC.

Solução

O agente da Web ou o agente não são apoiados em Linux. O NAC apoia Linux com início de uma sessão da Web somente sem nenhuma avaliação da postura. Uma vez que a máquina é autenticada com o início de uma sessão da Web, o usuário deve ser atribuído a um papel de usuário final que você configure. O usuário terá então o acesso de acordo com a política de tráfego do papel de usuário. Refira o Bug da Cisco CSCti54517 (clientes registrados somente) para mais informação.

O serviço SSO é começado, mas o cliente não executa o SSO

Isto é geralmente devido a algum problema de comunicação entre o DC/client PC ou entre o PC cliente e o CAS.

Estão aqui algumas coisas a verificar:

- O cliente tem chaves do Kerberos.
- As portas estão abertas ao DC assim que o cliente pode conectar, para receber logs do agente, e para receber entra CAS.
- O tempo ou o pulso de disparo no PC cliente são sincronizados com o DC.
- Confirme CAS está escutando na porta 8910. Um farejador de rastreamento no PC cliente igualmente ajudará.
- O agente CCA é 4.0.0.1 ou mais tarde.
- O usuário é entrado realmente usando a conta de domínio e não usando a conta local.

Kerbtray

Kerbtray pode ser usado para confirmar que o cliente obteve os bilhetes do Kerberos (TGT e ST). O interesse é para o bilhete do serviço (ST), que é para a conta de CAS que você criou no DC.

Kerbtray é uma ferramenta livre disponível das ferramentas de suporte de Microsoft. Pode igualmente ser usado para remover os bilhetes do Kerberos em uma máquina cliente.

Um ícone verde de Kerbtray na bandeja do sistema indica que o cliente tem bilhetes ativos do Kerberos. Contudo, você precisa de verificar que o bilhete está correto (válido) para a conta de CAS.

Logs de CAS – Não pode começar o serviço SSO

O arquivo de registro do interesse em CAS é /perfigo/logs/perfigo-redirect-log0.log.0.

O serviço AD SSO não começa em CAS é um problema de comunicação CAS-DC:

1. `SEVERE: startServer - SSO Service authentication failed. Clock skew too great (37) Aug 3, 2006 7:52:48 PM com.perfigo.wlan.jmx.admin.GSSServer loginToKDC` Isto significa que o pulso de disparo não está sincronizado entre CAS e o controlador de domínio.
2. `Aug 21, 2006 3:39:11 PM com.perfigo.wlan.jmx.admin.GSSServer loginToKDC INFO: GSSServer - SPN : [ccass/PreM-vM-2003.win2k3public.local@WIN2K3PUBLIC.LOCAL] Aug 21, 2006 3:39:11 PM com.perfigo.wlan.jmx.admin.GSSServer loginToKDC SEVERE: startServer - SSO Service authentication failed. Client not found in Kerberos database (6) Aug 21, 2006 3:39:11 PM com.perfigo.wlan.jmx.admin.GSSServer startServer WARNING: GSSServer loginSubject could not be created.` Isto significa que o username está incorreto. Note o nome de usuário errado “ccass”, o código de erro 6 e o último aviso.
3. `Aug 21, 2006 3:40:26 PM com.perfigo.wlan.jmx.admin.GSSServer loginToKDC INFO: GSSServer - SPN : [ccasso/PreM-vM-2003.win2k3public.local@WIN2K3PUBLIC.LOCAL] Aug 21, 2006 3:40:26 PM com.perfigo.wlan.jmx.admin.GSSServer loginToKDC SEVERE: startServer - SSO Service authentication failed. Pre-authentication information was invalid (24) Aug 21, 2006 3:40:26 PM com.perfigo.wlan.jmx.admin.GSSServer startServer WARNING: GSSServer loginSubject could not be created.` A senha está incorreta ou o reino é inválido (não no upper-case?). FQDN ruim? KTPass é executado incorretamente? Note o erro 24 e o último aviso.**Nota:** Certifique-se de que a versão de KTPass é 5.2.3790.0. A menos que houver uma versão ruim de KTPass que mesmo se o script está executado corretamente, o serviço SSO não começará.

Cliente – Problema de comunicação de CAS:

```
Aug 3, 2006 10:03:05 AM com.perfigo.wlan.jmx.admin.GSSHandler run
        SEVERE: GSS Error: Failure unspecified at GSS-API level (Mechanism level: Clock skew
too great (37))
```

Este erro é considerado quando o tempo do PC cliente não é sincronizado com o DC.

Nota: A diferença entre este erro e esse onde o tempo de CAS não é sincronizado com o DC.

Problemas conhecidos

- A identificação de bug Cisco CSCse64395 (clientes registrados somente) — o agente 4.0 não resolve o DNS para Windows SSO.Esta edição é resolvida no agente 4.0.0.1 CCA.
- Identificação de bug Cisco CSCse46141 (clientes registrados somente) — O SSO falha caso que CAS não pode alcançar o server AD durante a partida.A ação alternativa é ir aos **server CCA > controla a autenticação do [CAS_IP] > o AUTH de Windows > o diretório ativo SSO**, e clica a **atualização** a fim reiniciar o serviço AD SSO.
- Execute um reinício do perfigo do serviço em CAS. Há uma edição pondo em esconderijo quando as credenciais velhas estão postas em esconderijo em CAS e não usa o novo até que Tomcat esteja reiniciado.
- Você não pode limitar o início de uma sessão do usuário único para o SSO. Este é o comportamento normal para o SSO porque é um protocolo do Kerberos, e não há nenhuma opção para limitar o início de uma sessão do usuário único um protocolo do Kerberos.
- *Windows 7* e *Windows 2008* não apoiam o SSO enquanto o SSO usa a **criptografia DES** que não está apoiada por Windows 7 ou por Windows 2008.

Informações Relacionadas

- Página de suporte do Dispositivo Cisco NAC (Clean Access)
- Suporte Técnico e Documentação - Cisco Systems