Содержание

Введение

Этот документ описывает решение аутентификаций платформы Identity Services Engine (ISE), отказывающих против Active Directory (AD) из-за ошибки 24371 вызванный недостаточными привилегиями учетной записи машины ISE.

Предварительные условия

Требования

Cisco рекомендует иметь базовые знания об этих темах:

- Конфигурация и устранение проблем ISE
- Microsoft Active Directory

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Версия 1.3.0.876 ISE
- Версия 2008 R2 Microsoft AD

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Проблема

AD аутентификации отказывают из-за ошибки 24371

В ISE 1.3 и выше, аутентификации могут отказать против AD с ошибкой 24371. Подробный опознавательный отчёт для сбоя будет иметь шаги подобными показанным здесь:

AD статус показывает присоединенный и связанный, и требуемые AD группы были добавлены правильно в конфигурации ISE.

Решение

Модифицируйте разрешения для учетной записи машины ISE на AD

Ошибка в подробном опознавательном отчёте подразумевает, что учетная запись машины ISE на Active Directory, не имеет достаточных привилегий для выборки маркерных групп.

> **Примечание:** Исправление сделано на AD сторонах A, которые оно не в состоянии дать соответствующим полномочиям учетной записи машины ISE. Вы, возможно, должны разъединить/повторно подключить ISE к AD после этого.

Текущие привилегии учетной записи машины могут быть проверены с помощью dsacls команды как показано в данном примере:

```
Open a command prompt on your AD with administrator privilege.
The dsquery command can be used to find the Fully Qualified Domain Name (FQDN) of the ISE.
C:\Users\admin> dsquery computer -name lab-ise1  //here lab-ise1 is the hostname of the
ISE"CN=lab-ise1,CN=Computers,DC=ciscolab,DC=local"The dsacls command can now be used to find the
privileges assigned to the machine accountC:\Windows\system32> dsacls "CN=lab-
ise1,CN=Computers,DC=ciscolab,DC=local" >> C:\dsacl_output.txt
```

Выходные данные долго и поэтому перенаправляются в текстовый файл **dsacl_output.txt**, который может тогда быть открыт и просмотрен должным образом в текстовом редакторе, таком как блокнот.

Если учетная запись будет иметь разрешения для чтения маркерных групп, то она будет иметь эти записи в **dsacl_output.txt** файле:

```
Open a command prompt on your AD with administrator privilege.
The dsquery command can be used to find the Fully Qualified Domain Name (FQDN) of the ISE.
C:\Users\admin> dsquery computer -name lab-ise1  //here lab-ise1 is the hostname of the
ISE"CN=lab-ise1,CN=Computers,DC=ciscolab,DC=local"The dsacls command can now be used to find the
privileges assigned to the machine accountC:\Windows\system32> dsacls "CN=lab-
ise1,CN=Computers,DC=ciscolab,DC=local" >> C:\dsacl_output.txt
```

Если разрешения не присутствуют, то это может быть добавлено с помощью этой команды:

```
C:\Windows\system32>dsacls "CN=Computers,DC=ciscolab,DC=local" /I:T /G "lab-
ise1$":rp;tokenGroups
```

Если FQDN или точная группа не известны, эта команда может быть быстро выполнена для домена или OU согласно этим командам:

```
C:\Windows\system32>dsacls "DC=ciscolab,DC=local" /I:T /G "lab-ise1$":rp;tokenGroups
C:\Windows\system32>dsacls "OU=ExampleOU,DC=ciscolab,DC=local" /I:T /G "lab-
ise1$":rp;tokenGroups
```

Команды ищут лабораторную-работу-ise1 хоста во всем домене или OU соответственно.

Не забудьте заменять группу и подробные данные имени хоста в командах с соответствующей группой и названием ISE от ваших развертываний. Эта команда допускает, что машина ISE считает привилегию считать маркерные группы. Это должно быть выполнено на одном контроллере домена только и должно реплицировать в другие контроллеры автоматически.

Вопрос может быть сразу решен путем выполнения команды на контроллере домена, в настоящее время связываемом на ISE.

Контроллер текущего домена может быть просмотрен при **администрировании> Управление идентификацией> Внешние Идентификационные Источники>, Active Directory> Выбирает точку соединения AD.**

Дополнительные сведения

- Информация относительно других разрешений учетной записи может быть найдена в Интеграция Active Directory с Cisco ISE 1.3
- Microsoft Technet Link