Настройте ISE 2.2 PIC с поставщиком WMI Active Directory

Содержание

Введение

Этот документ описывает, как настроить и устранить неполадки платформы Identity Services Engine Пассивный Идентификационный Разъём (PIC ISE) развертывания с инструментарием управления Windows Active Directory (AD WMI) поставщик. PIC ISE является легковесной версией ISE, которая фокусируется на Пассивных функциях ID.

PIC ISE является одиночным решением для ID для всего портфолио Cisco Security, который использует пассивную идентичность только. Это означает, что авторизация или политика не

могут быть настроены на PIC ISE. Это поддерживает других Поставщиков (Агенты, WMI, Системный журнал, API) и может быть интегрировано через API REST. Это имеет способности сделать запрос оконечных точек (В Пользователя входят? Оконечная точка все еще связана?)

Предварительные условия

Требования

Cisco рекомендует иметь базовые знания об этих темах:

- Идентификационный механизм сервиса Cisco
- Microsoft Active Directory
- Microsoft WMI

Используемые компоненты

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

- Идентификационный Механизм Сервиса Cisco Пассивная Идентификационная версия 2.2.0.470 Разъёма
- Microsoft Windows 7 пакетов обновления 1
- Microsoft Windows server 2012 r2

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.

Общие сведения

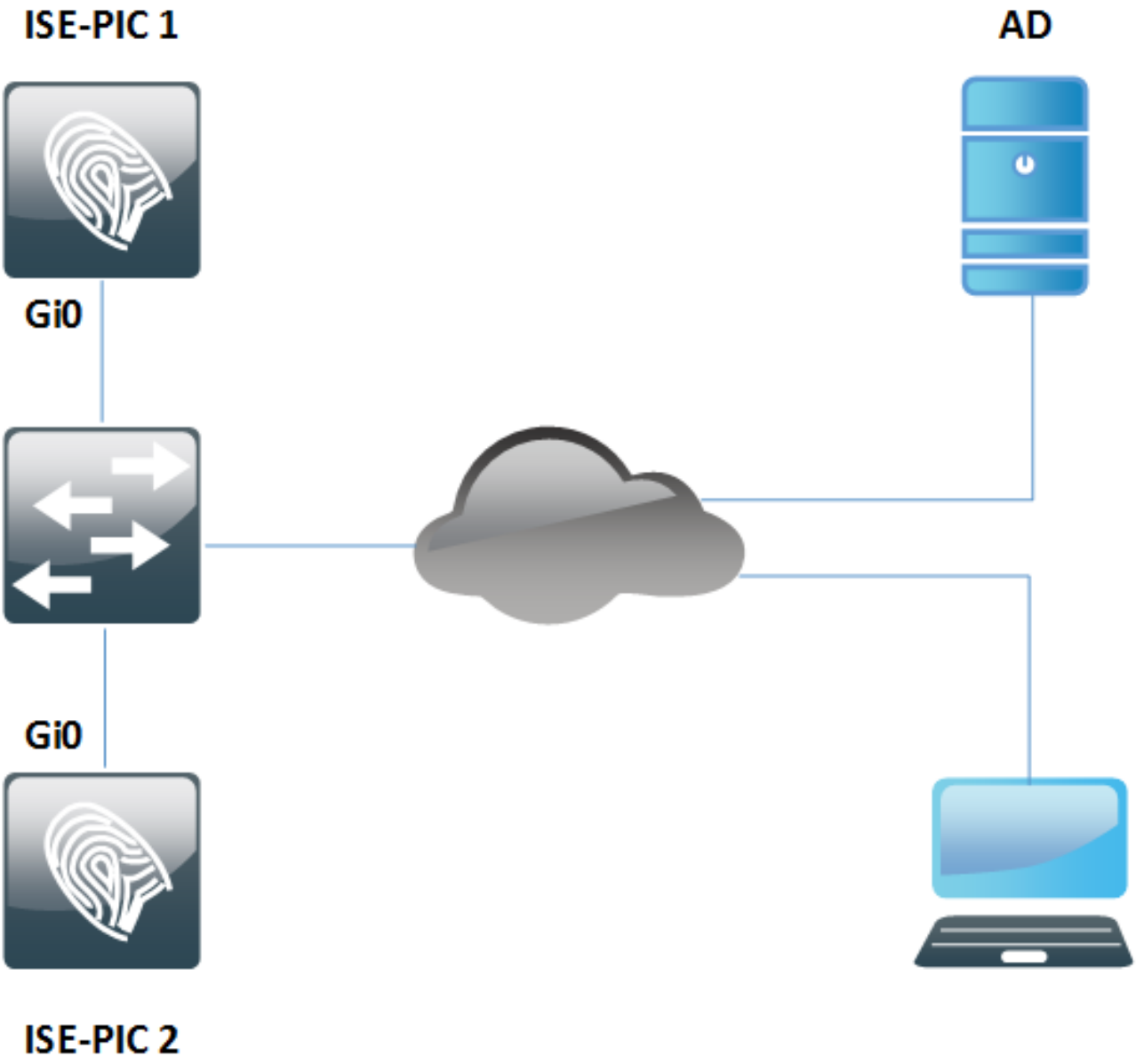
Максимальное количество узлов в развертываниях PIC ISE равняется 2. Данный пример показывает, как настроить развертывания PIC ISE для Высокой доступности, таким образом, используются 2 Виртуальных машины (VM). В развертываниях PIC ISE узлы могут иметь роли: Основной и Вторичный. В этом только одном узле может быть Основным за один раз, и роли могут только быть изменены вручную через GUI. В случае Первичного сбоя все функции все еще работают Вторичный за исключением UI. Только ручное продвижение Основному включает UI.

Данный пример показывает, как настроить Поставщика WMI для Active Directory. WMI состоит из ряда расширений к Windows Driver Model, которая предоставляет интерфейс операционной системы, через который оснащенные компоненты предоставляют сведения и уведомление. WMI является реализацией Microsoft управления предприятием на базе веб-интерфейса (WBEM) и стандартов Общей информационной модели (CIM) от Распределенной силы задачи управления (DMTF).

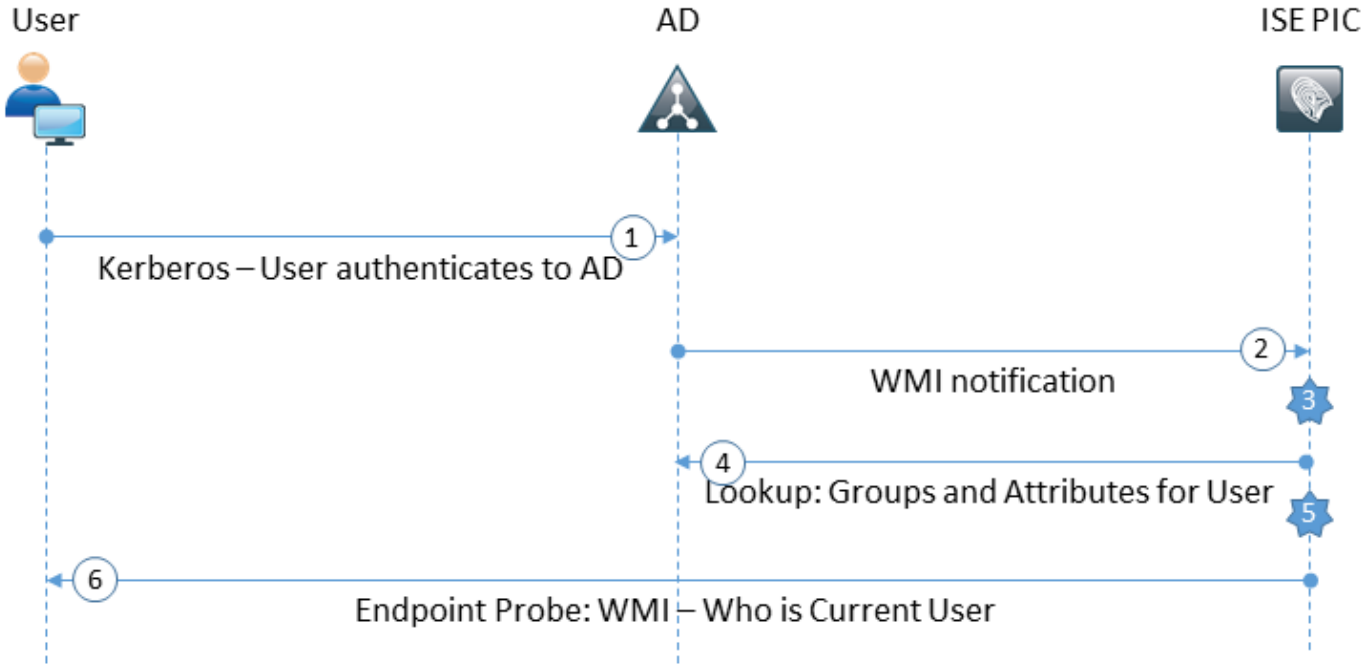
Примечание: Дополнительные сведения о WMI могут быть найдены на официальном узле Microsoft: О WMI

Схема сети

Информация в документе использует сетевую установку, показанную в образе:



Рабочий поток



1. Вход в систему к ПК и аутентифицируется на AD.

2. WMI уведомляет PIC ISE об этой аутентификации.

3. ISE добавляет привязку Username:IP_Address к его Каталогу Сеанса.

4. ISE получает Группы Пользователя и Атрибуты от AD.

5. ISE сохраняет эту информацию в свой Каталог Сеанса.

6. Каждые 4 часа (не конфигурируемый) PIC ISE выполняет Зонд Оконечной точки: Сначала это пробует WMI к Оконечной точке.Если WMI отказывает тогда выполнения PIC ISE ISEExec. Это делает запрос Оконечной точки для Пользователя, и включите WMI в следующий раз.Также PIC ISE получает MAC-адрес типа ОС и Оконечной точки.

   На PIC ISE это возможно только к Зондам Оконечной точки Позволить/запретить. Основной узел делает запрос всех оконечных точек, Вторичный узел для Высокой доступности только.

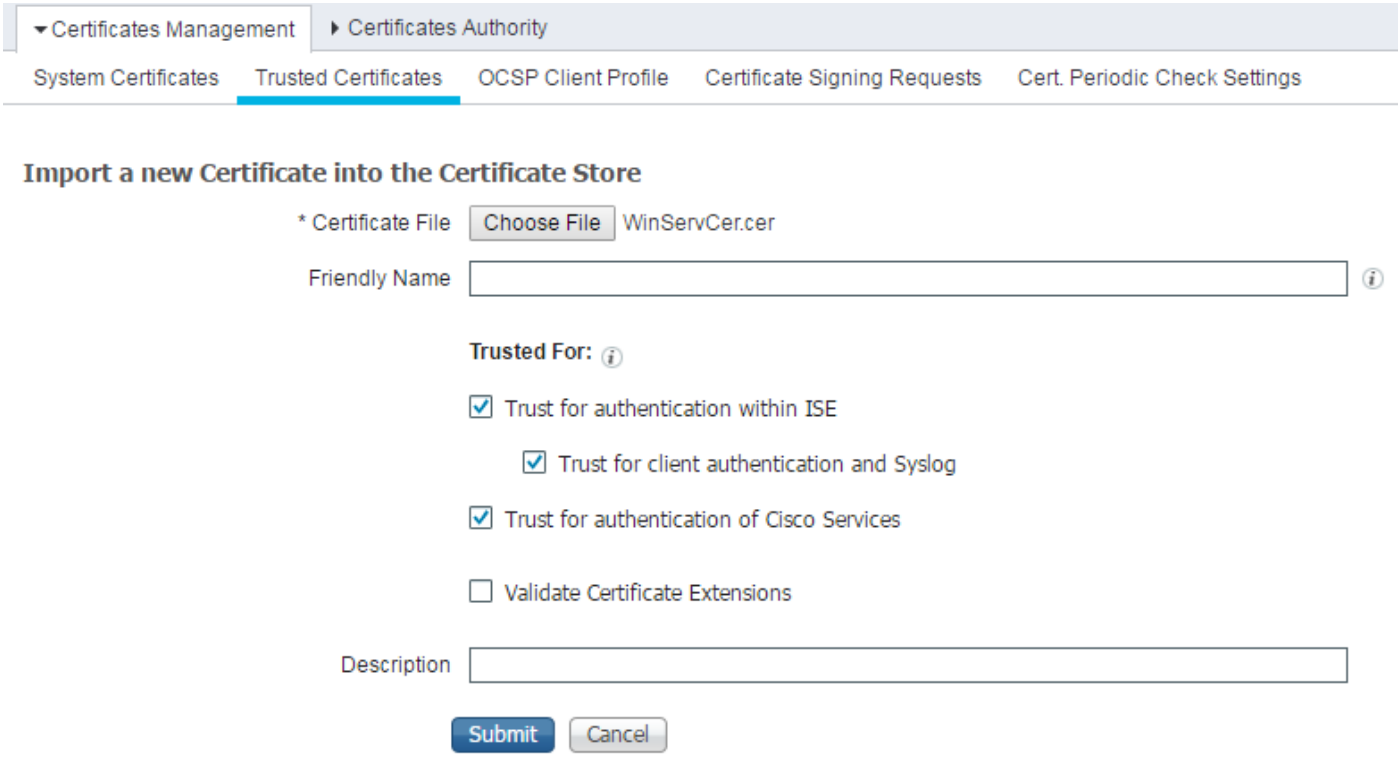
Настройка

Настройте развертывания PIC ISE

Шаг 1 (Необязательно). Установите надежные сертификаты.

Полная цепочка сертификатов вашего Центра сертификации (CA) должна быть установлена к хранилищу ISE, которому доверяют. Вход в систему к GUI PIC ISE и перешел к **Сертификатам> менеджмент Сертификатов> Надежные сертификаты**. Нажмите **Import** и выберите сертификат своего CA от вашего ПК.

Как показано в образе, нажмите **Submit** для сохранения изменений. Повторите этот шаг для всех сертификатов цепочки. Повторите шаги во вторичный узел также.

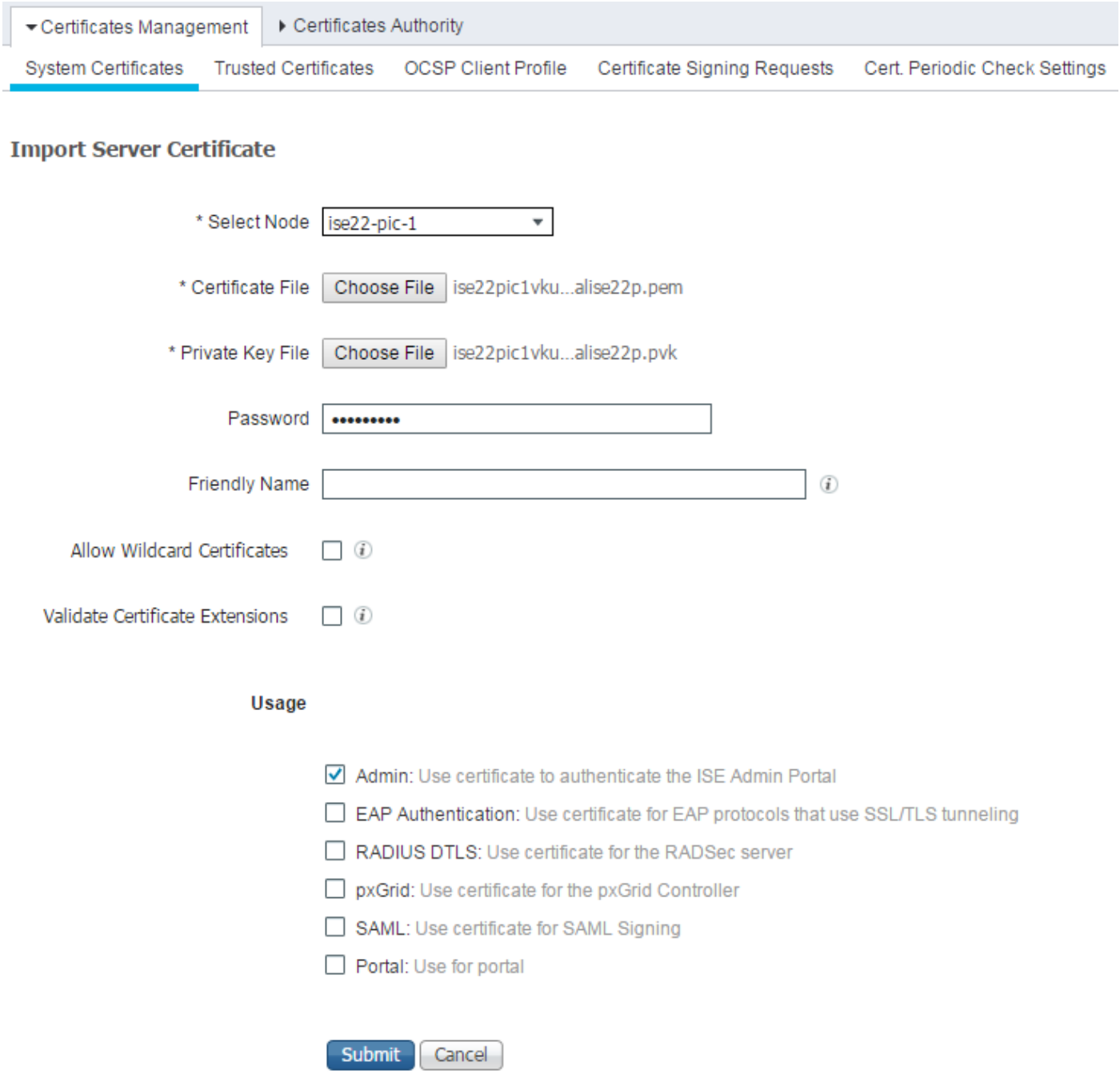


Шаг 2 (Необязательно). Установите системные сертификаты.

Вариант 1. Сертификаты уже генерируются CA наряду с секретным ключом.

Перейдите к **Сертификатам> менеджмент Сертификатов> Системные Сертификаты** и нажмите **Import**. Выберите **Certificate File** и **Private Key File**, введите *Поле Password*, если зашифрован секретный ключ.

Как показано в образе проверяют **Параметры использования**:



Примечание: Так как PIC ISE основывается на коде ISE и может легко быть преобразован в полнофункциональный ISE с соответствующими лицензиями, все параметры использования доступны. Роли, такие как **Аутентификация eap**, **RADIUS DTLS**, **SAML** и **Портал** не используются PIC ISE.

Нажмите **Submit** для установки сертификата. Повторите эту процедуру на вторичном узле также.

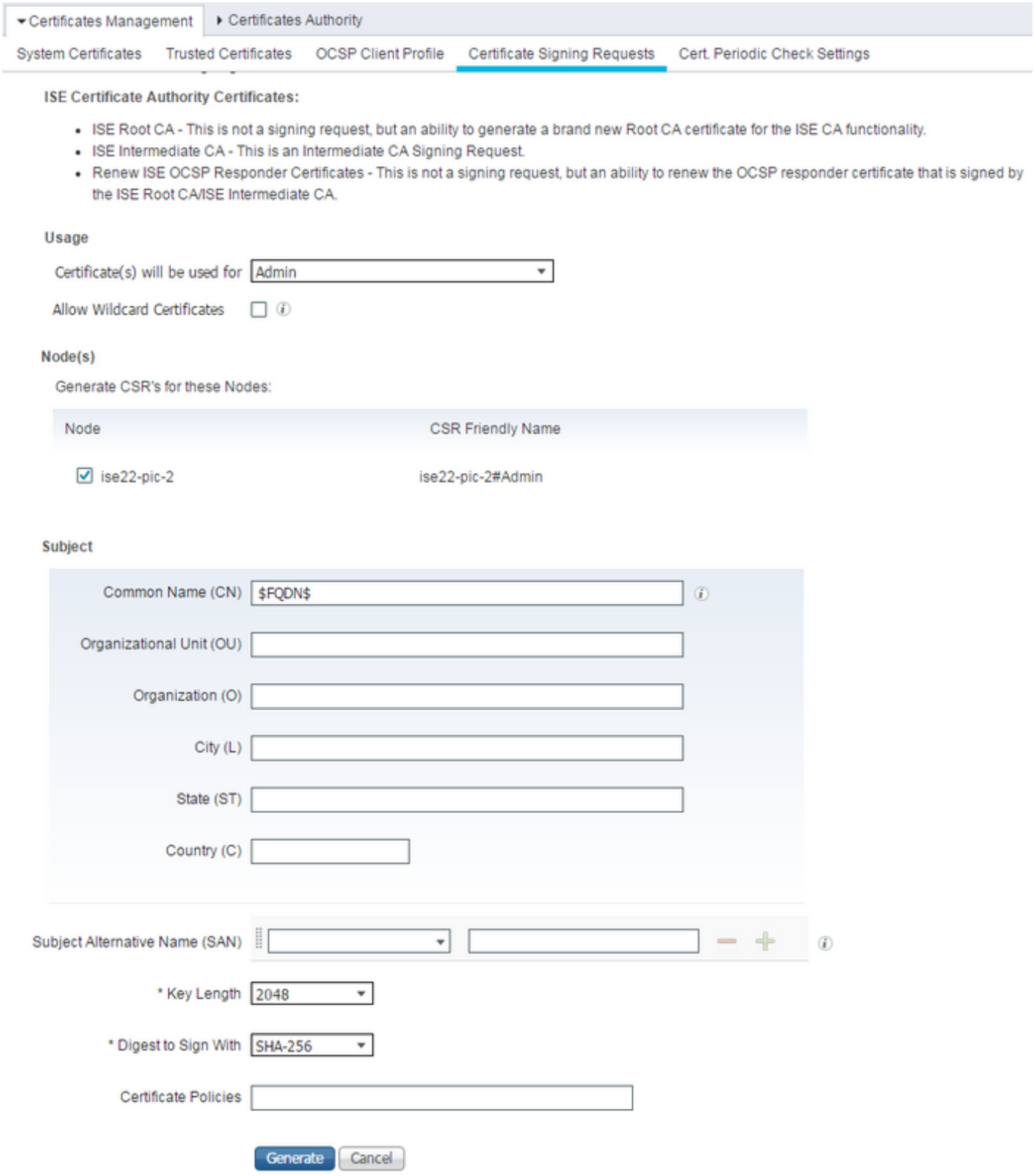
Примечание: Все сервисы на перезапусках узла PIC ISE после импорта серверного сертификата.

Вариант 2. Генерируйте Запрос подписи сертификата (CSR), подпишите его с CA и привяжите ISE.

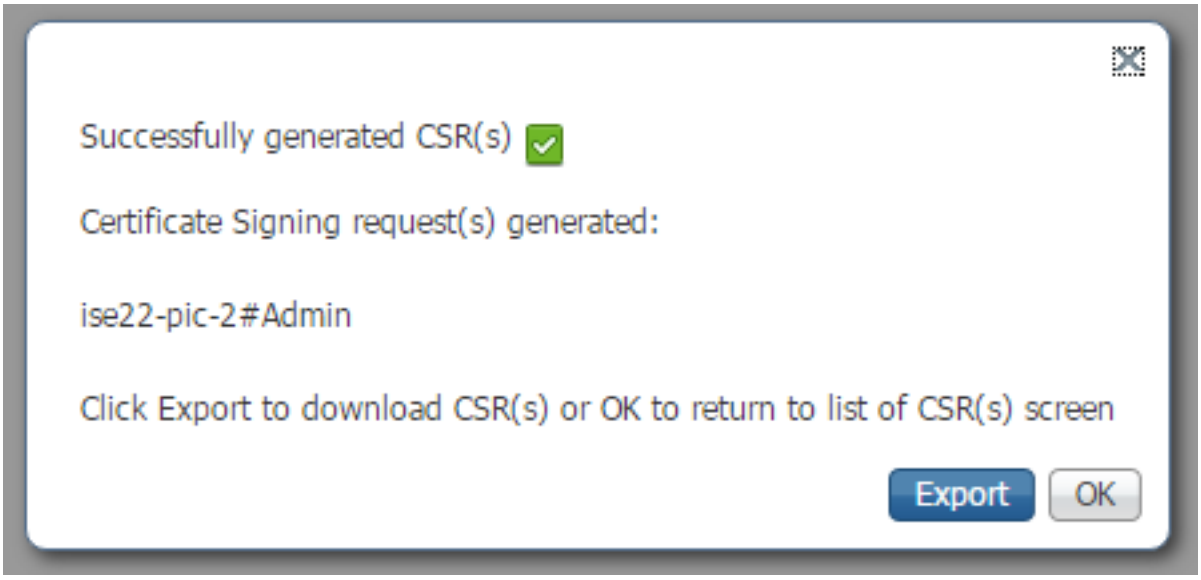
Перейдите к странице **Certificates> Certificates Management> Certificate Signing Requests** и

нажмите **Generate Certificate Signing Requests (CSR)**.

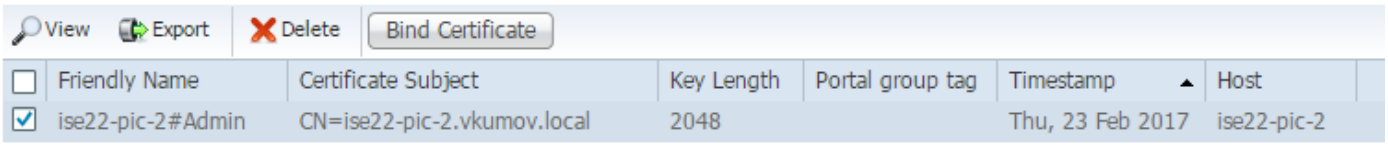
Выберите узел и использование, введите другие поля при необходимости:



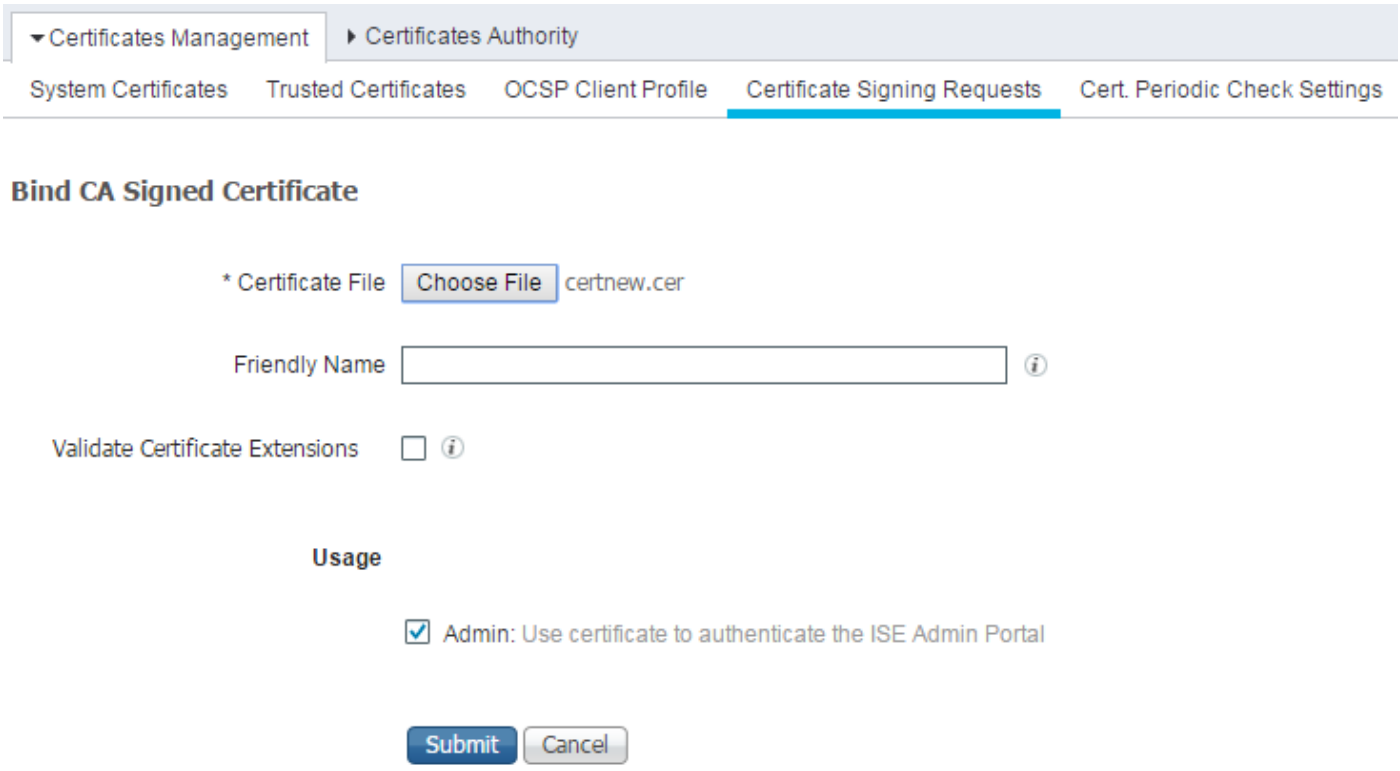
Нажмите **Generate.** Новое окно появляется с опцией для **Экспортирования** генерируемого CSR:



Нажмите **Export,** сохраните генерируемый ***.pem** файл и подпишите его с CA., Как только CSR подписан, перешли назад к странице **Certificates> Certificates Management> Certificate Signing Requests**, выбирают ваш CSR и нажимают **Bind Certificate**:



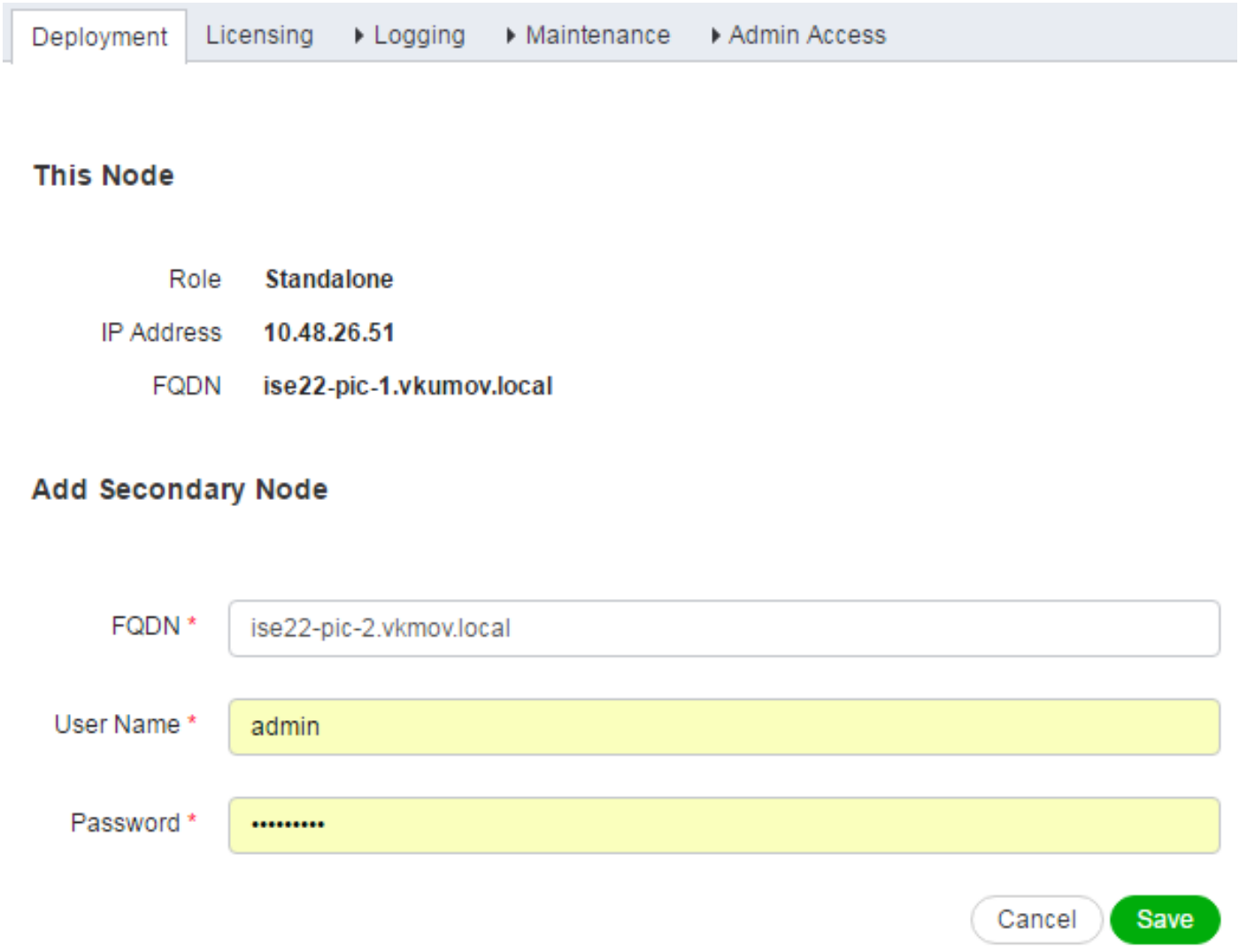
Выберите сертификат, который был подписан с вашим CA, и нажмите **Submit** для применения изменений:



Все сервисы на перезапуске узла PIC ISE после нажатия **Submit** для установки сертификата.

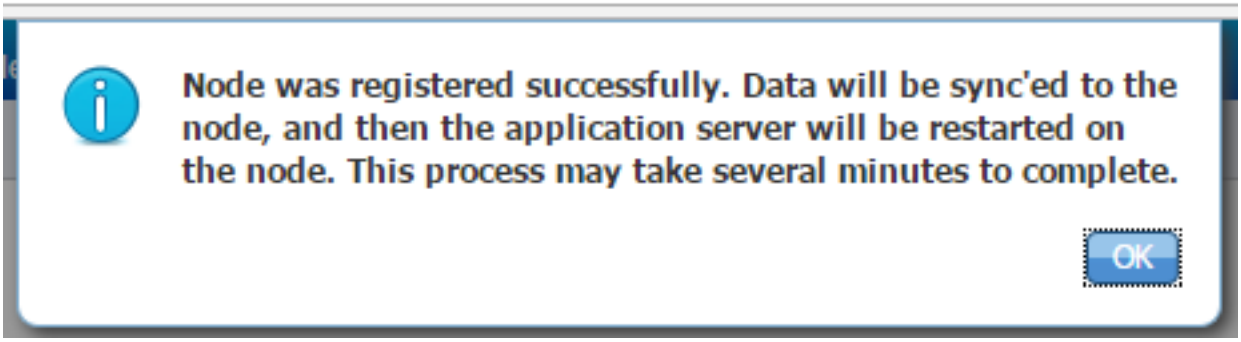
Шаг 3. Добавьте вторичный узел к развертываниям.

PIC ISE позволяет иметь 2 узла в развертываниях для Высокой доступности. Это не требует для имения двухстороннего доверия сертификатов (по сравнению с обычными развертываниями ISE). Для добавления вторичного узла к развертываниям перейдите к **странице Administration> Deployment** на основном узле PIC ISE, как показано в образе:

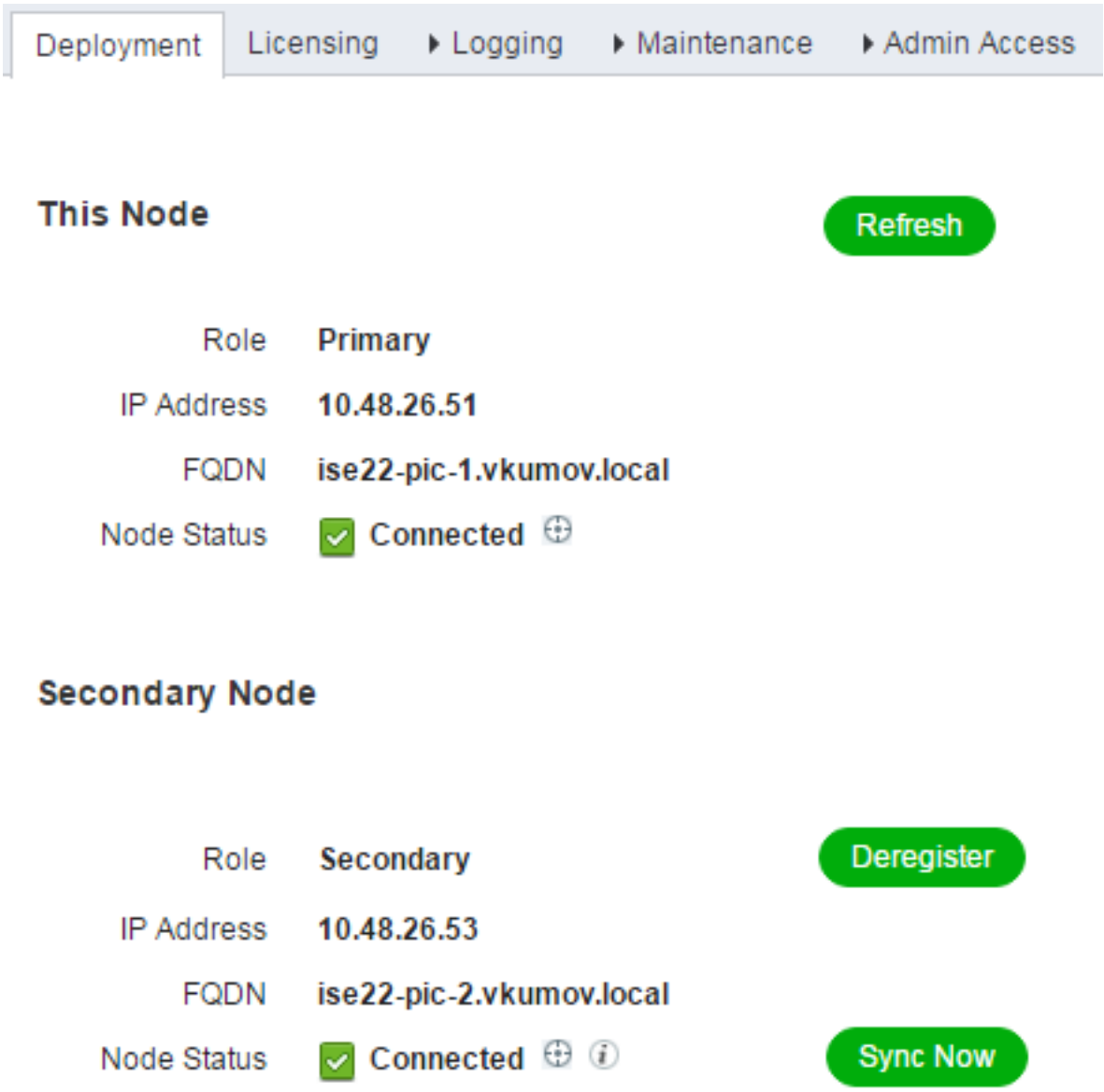


Введите Полное доменное имя (FQDN) вторичного узла, учетные данные администратора того узла и нажмите **Save**. В случае, если основной узел PIC ISE не в состоянии проверить сертификат admin второго узла, это просит подтверждение, прежде чем это установит тот сертификат в доверяемом хранилище.

В таком случае нажимают **Import Certificate и Proceed** для соединения узла с развертываниями. Необходимо получить уведомление, что узел добавлен успешно. Все сервисы на вторичных перезапусках узла.



В течение 10-20 минут должны синхронизироваться узлы, и статус узла должен измениться от **Происходящий** к **Подключено:**



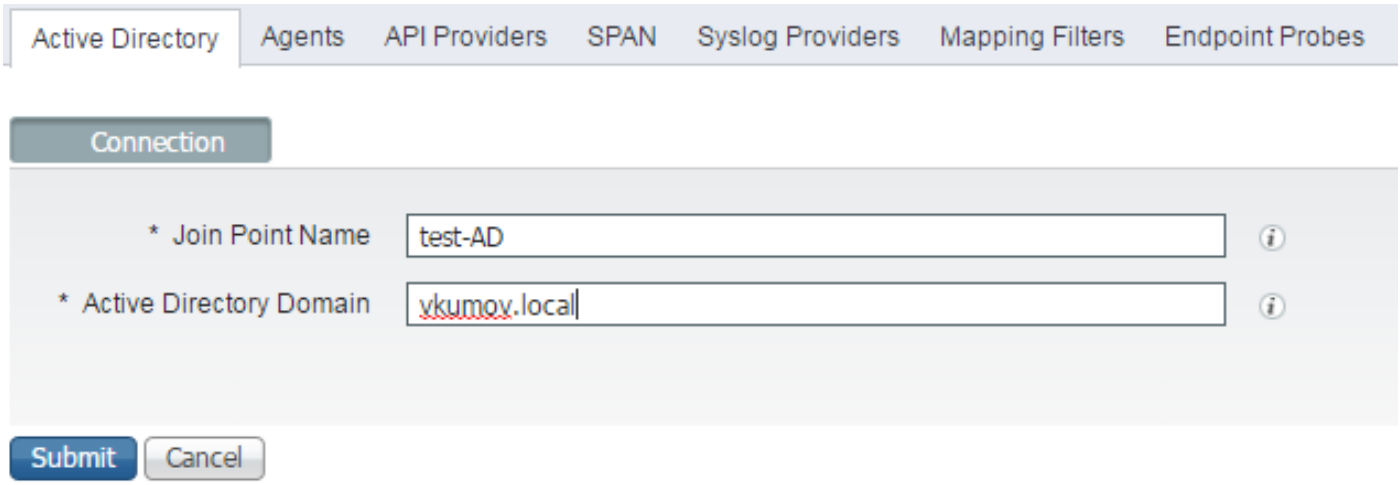
Настройте поставщиков Active Directory

PIC ISE использует инструментарий управления Windows (WMI) для сбора информации о сеансах от AD и действий как Pub/Sub communitation, что означает:

- PIC ISE подписывается на достоверные события
- Когда те события имеют место, WMI предупреждает PIC ISE: 4768 (билет Kerberos, предоставляющий) и 4770 (билет Kerberos обновление)Записи в Каталоге Сеанса истекают (Чистка)

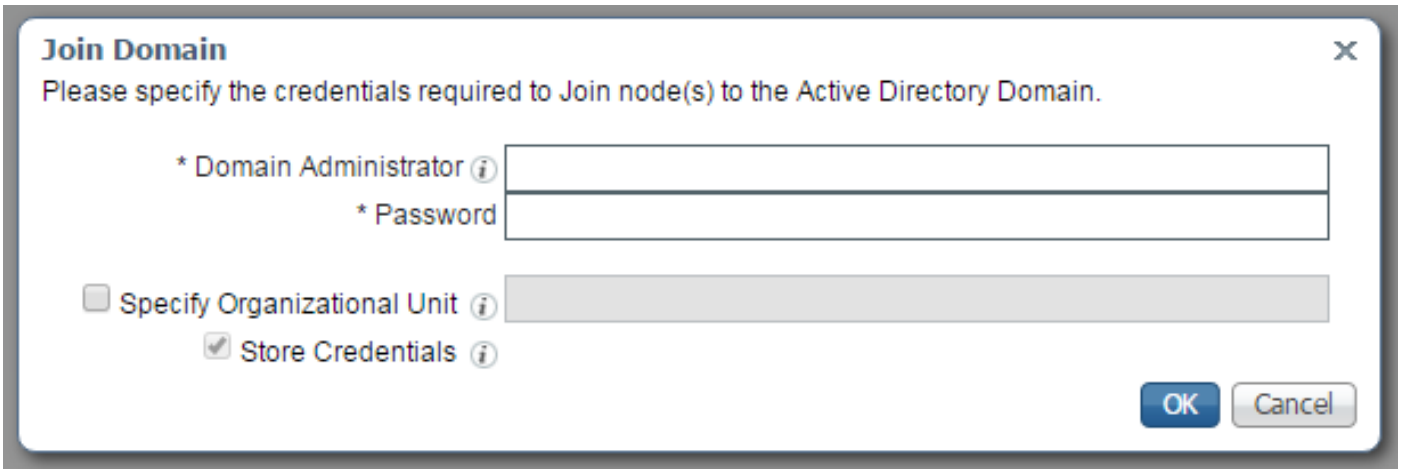
Шаг 1. Соедините PIC ISE с доменом.

Для соединения PIC ISE с доменом перейдите **Поставщикам> Active Directory** и **нажмите Add**:



Название Точки соединения заливки и **поля Domain Active Directory** и нажимают **Submit** для сохранения изменений. **Название Точки соединения** является названием, которое используется в PIC ISE только. **Домен Active Directory** является названием домена, где к PIC ISE нужно присоединиться, и это должно быть разрешимо с сервером DNS, настроенным на PIC ISE.

Если требуется соединить узлы с доменом, после того, как создание PIC ISE Точки соединения должно спросить вас. **Нажмите кнопку YES.** Окно должно появиться для вас для обеспечения учетных данных для присоединения к домену:



Заполните **Администратора домена** и **Поля Password** и нажмите **OK.**

Даже при том, что поле называют **Администратором домена** необязательно для использования администратора для **соединения** PIC ISE с доменом. У этого пользователя должны быть достаточные привилегии, чтобы создать и удалить учетные записи машины в домене или изменить пароли для ранее созданных учетных записей машины. Разрешения Учетной записи Active Directory, требуемые для выполнения различных операций, могут быть найдены в этом документе.

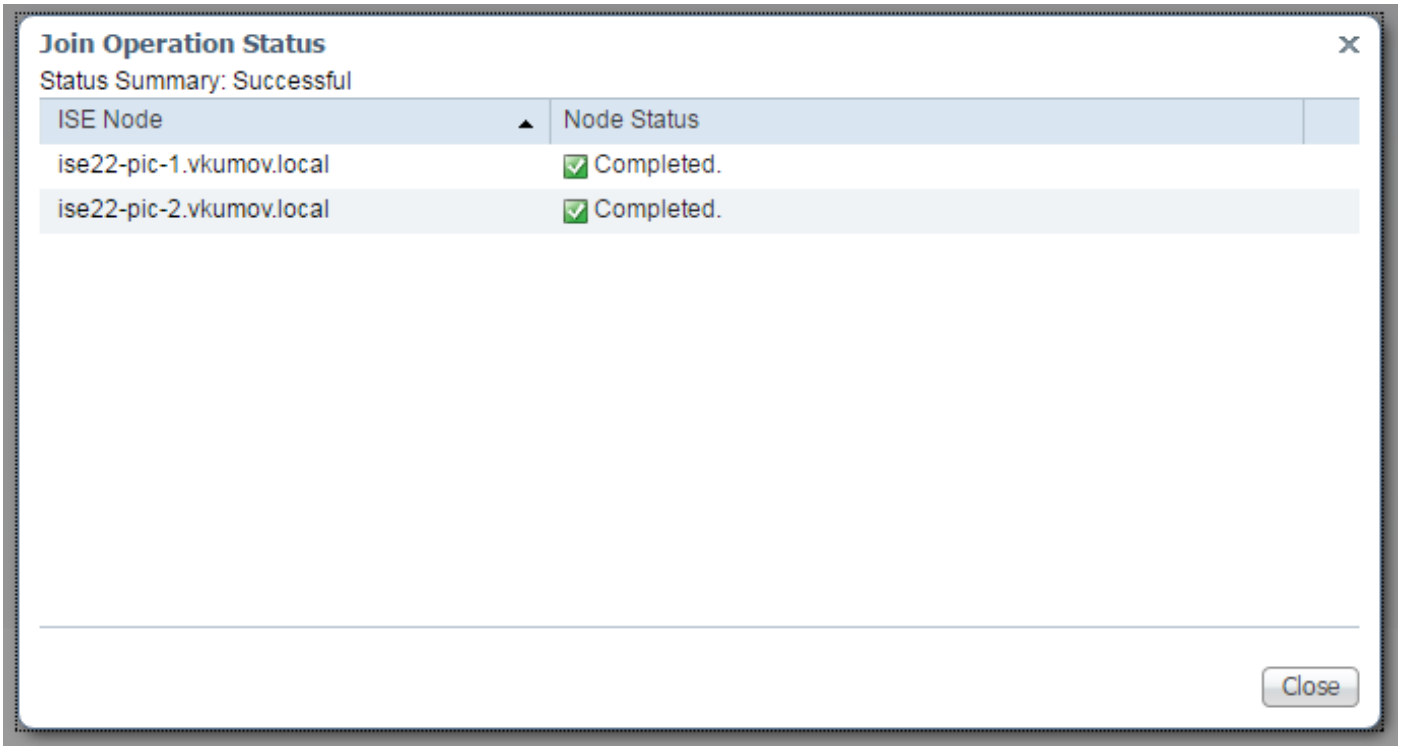
Если требуется использовать WMI, однако, это - учетные данные Администратора домена использования requiredto во время соединения. Опция **WMI config** требует:

- Изменения в реестре

- Разрешения для использования DCOM
- Разрешения для использования WMI Удаленно
- Доступ для чтения Журнала событий безопасности AD Доменного Controlle
- Windows Firewall должен позволить трафику от/к PIC ISE (соответствующий Windows Firewall policies будет создан во время **WMI Config**),

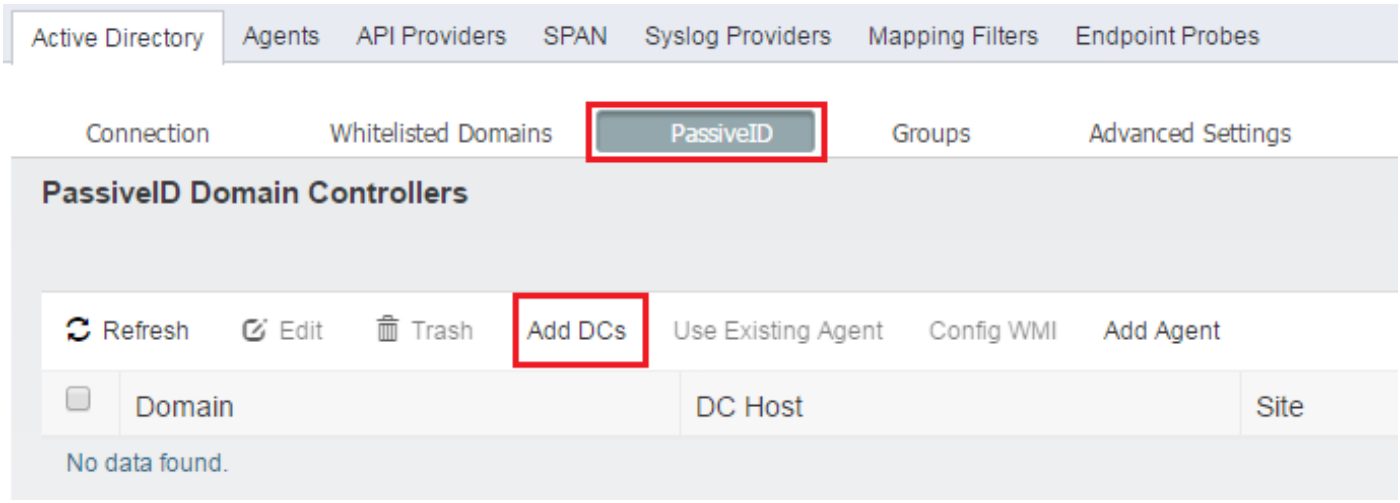
  Примечание: Учетные данные хранилища всегда быть включенными на PIC ISE, так как это требуется для Зондов Оконечной точки и конфигурации WMI. ISE хранит их зашифрованный внутренне.

Как показано в образе, PIC ISE показывает результат операции в новом окне:



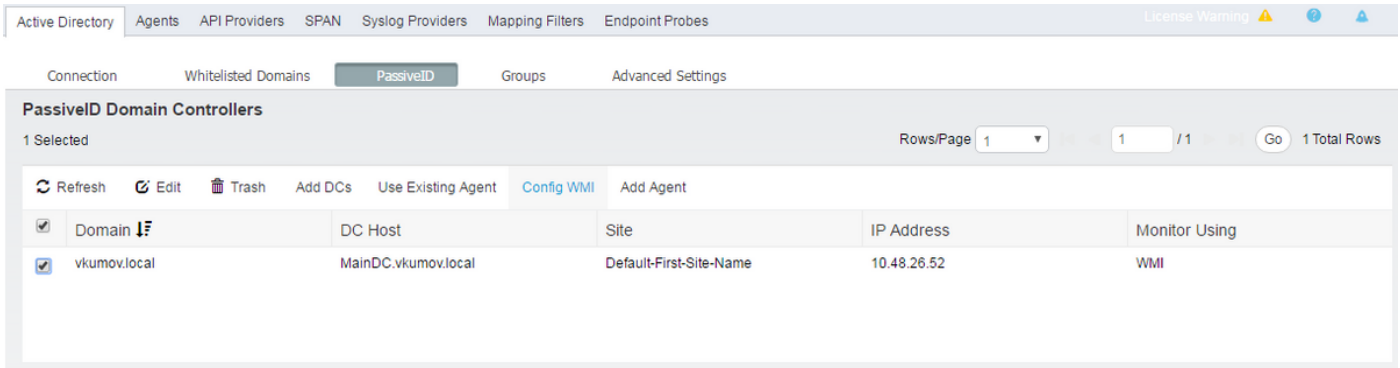
Шаг 2. Добавьте агентов PassiveID.

На AD странице domain перешли к вкладке PassiveID и **нажмите Add DC**, как показано в образе:

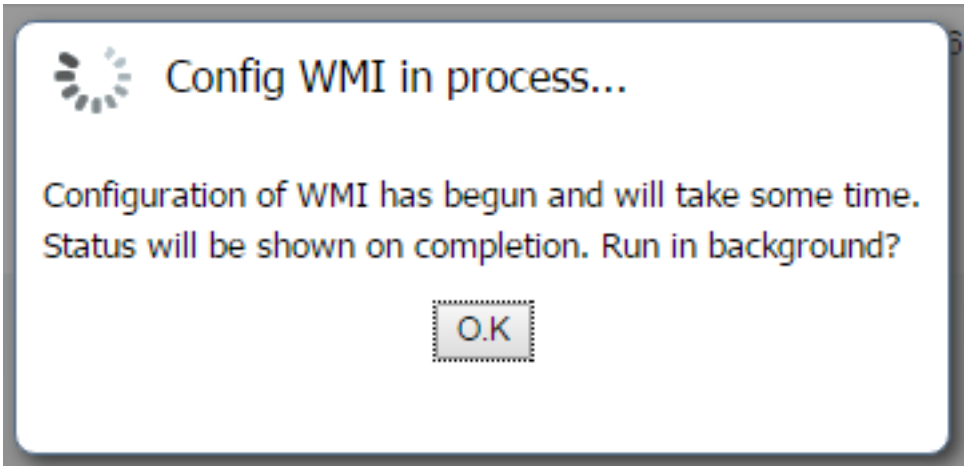


Новое окно появляется, и ISE загружает список всех доступных контроллеров домена. Выберите DC, где требуется настроить WMI и нажать **OK** для сохранения изменений, как показано в образе:

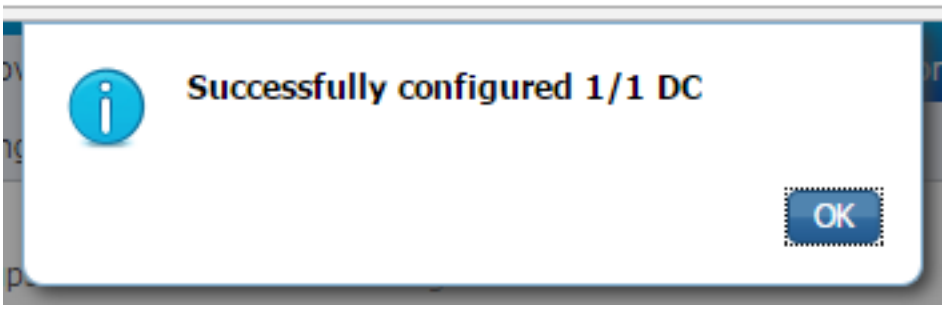
Выбрал DC, добавлены к списку **Контроллеров домена PassiveID.** Выберите свои DC и нажмите кнопку **Config WMI**:



PIC ISE показывает сообщение, что процесс конфигурирования происходит:



После нескольких минут это показывает вам сообщение, что WMI успешно настроен на выбранных DC:



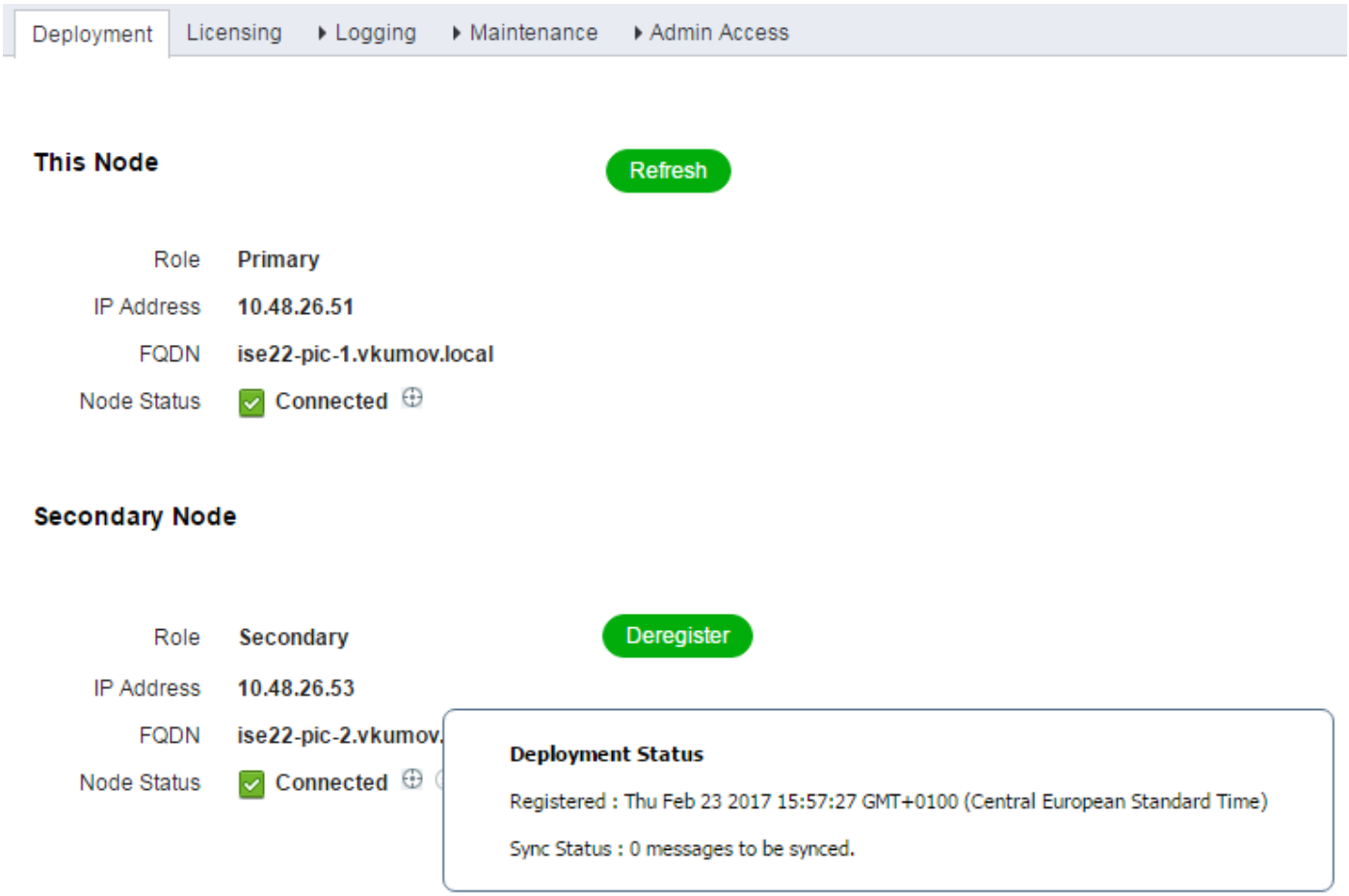
Проверка

Развертывания

Статус развертываний может быть проверен несколькими способов:

Страница Deployment

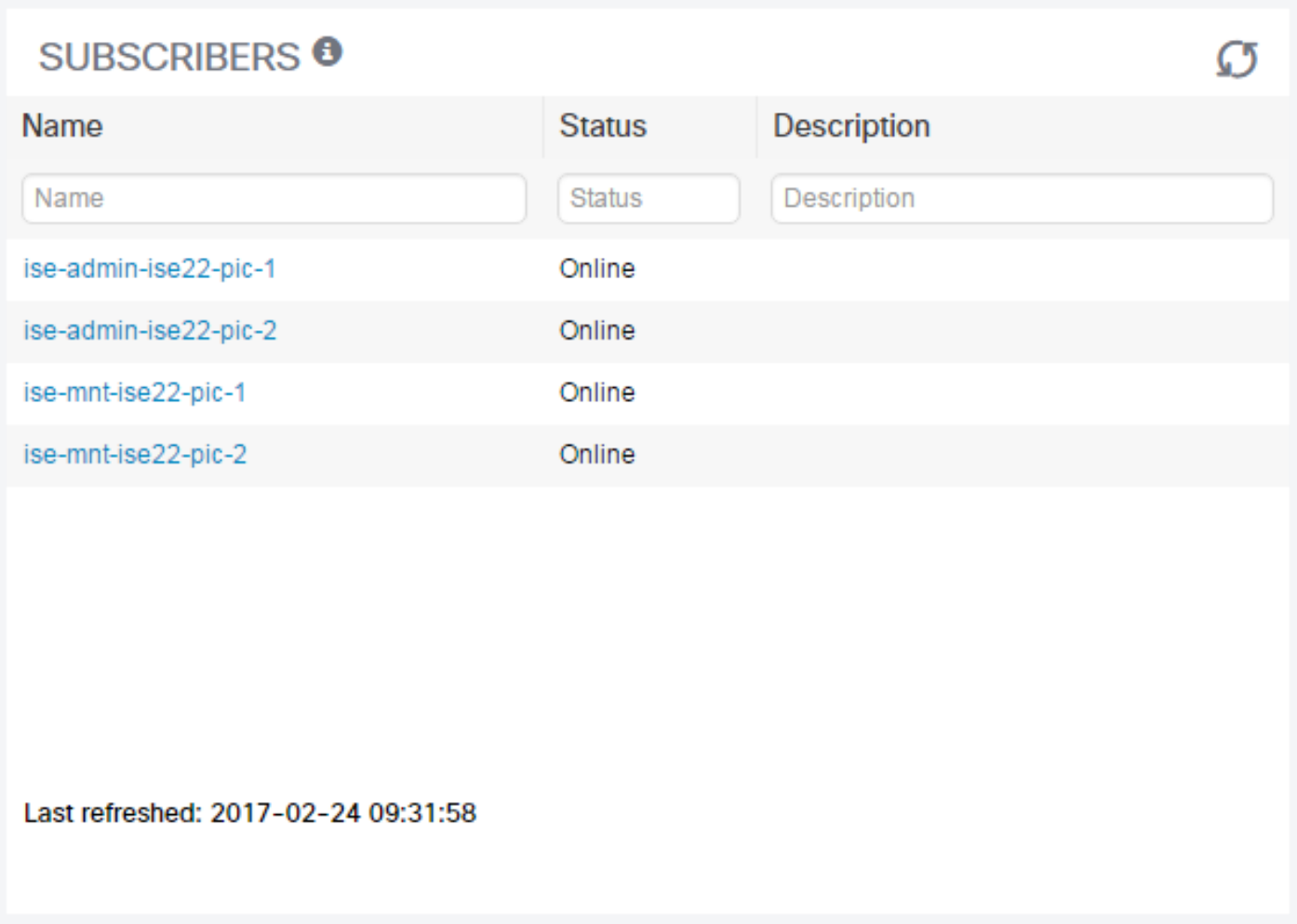
Перейдите к **странице Administration> Deployment**, текущее состояние развертываний может быть проверено:



От этой страницы вторичный узел может de, вычеркнутый из списка в случае необходимости. Ручная синхронизация может быть запущена, и **состояние синхронизации** может быть проверено.

Страница Dashboard

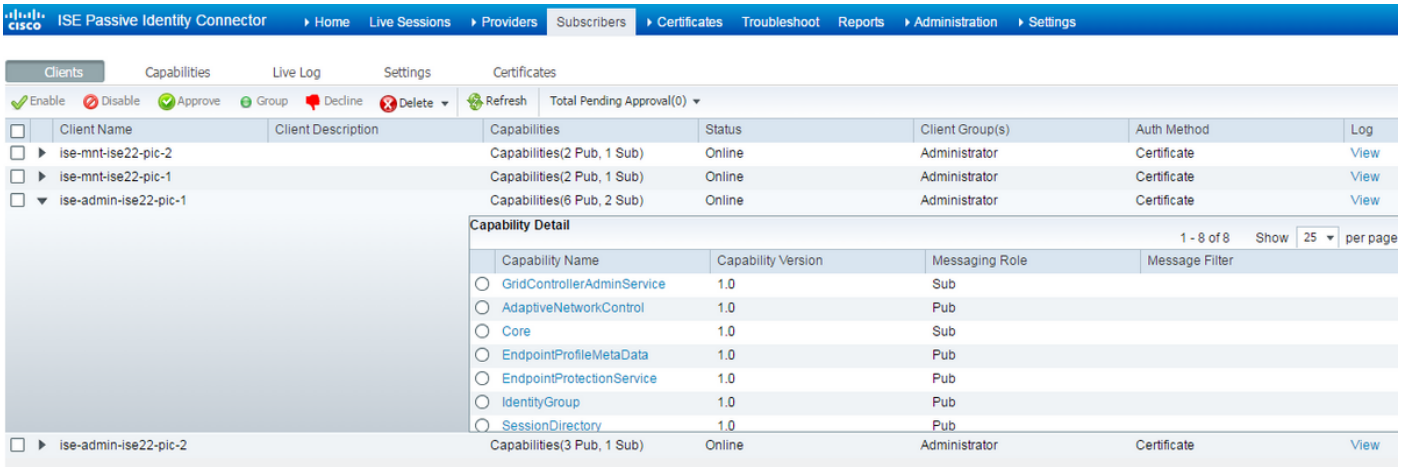
На основной странице ISE PIC существует dashlet **вызываемые абоненты**. С этим dashlet можно проверить текущий статус узлов PIC ISE, как показано в образе:



PIC ISE создает 2 абонентов для каждого узла - **admin** и **mnt.** Все они должны быть в **Онлайн-статусе**, что означает, что узлы reacheable и в рабочем состоянии.

Абоненты

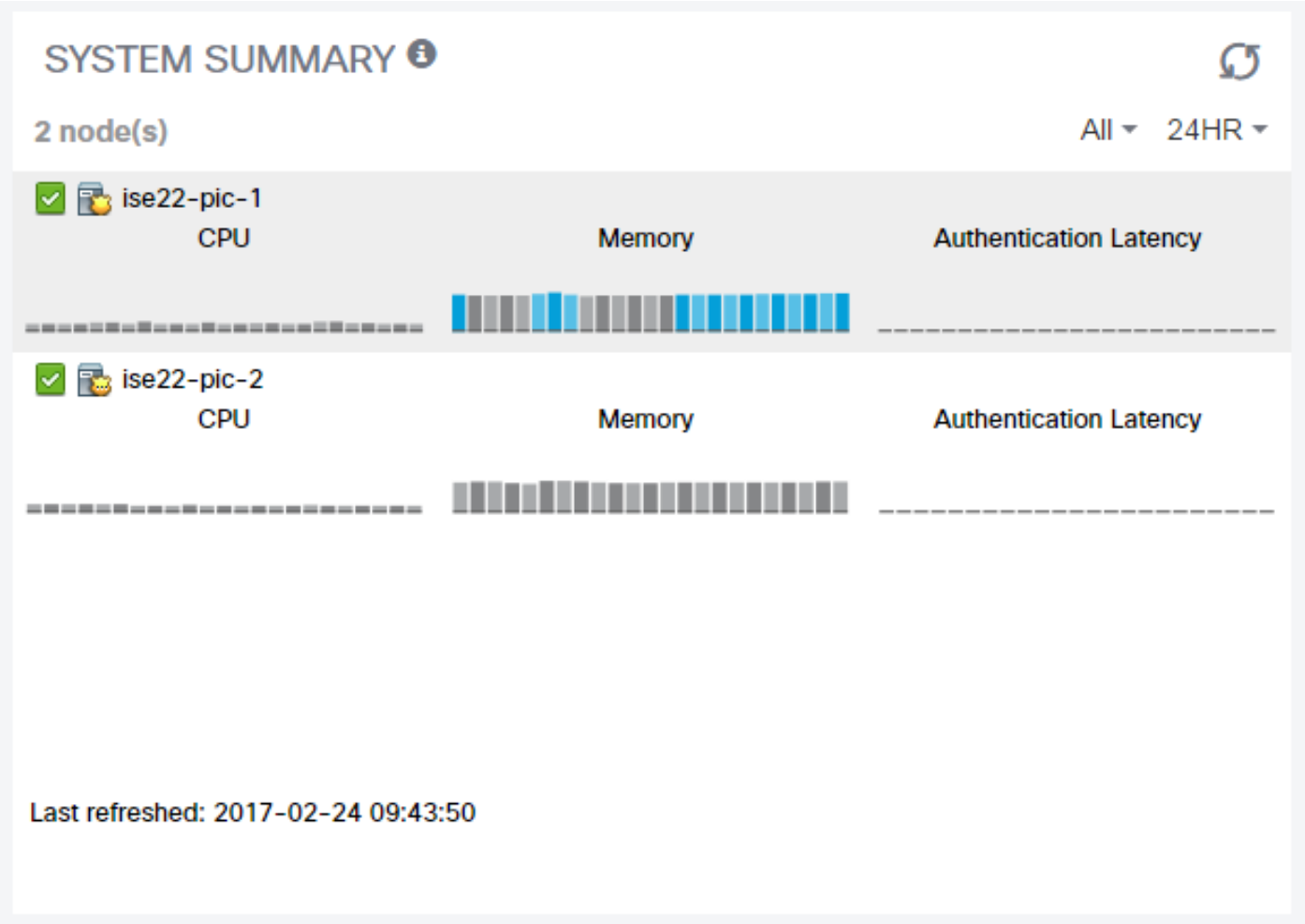
Страница **Subscribers** является расширенной версией абонентов dashlet от Домашней страницы PIC ISE. Эта страница показывает весь отнесенный pxGrid, однако статус узлов PIC ISE может быть проверен здесь также:



Системная сводка

PIC ISE позволяет контролировать Сводку состояния узлов также. Этот dashlet может быть

найден **дома> Информационная панель> Дополнительным**:

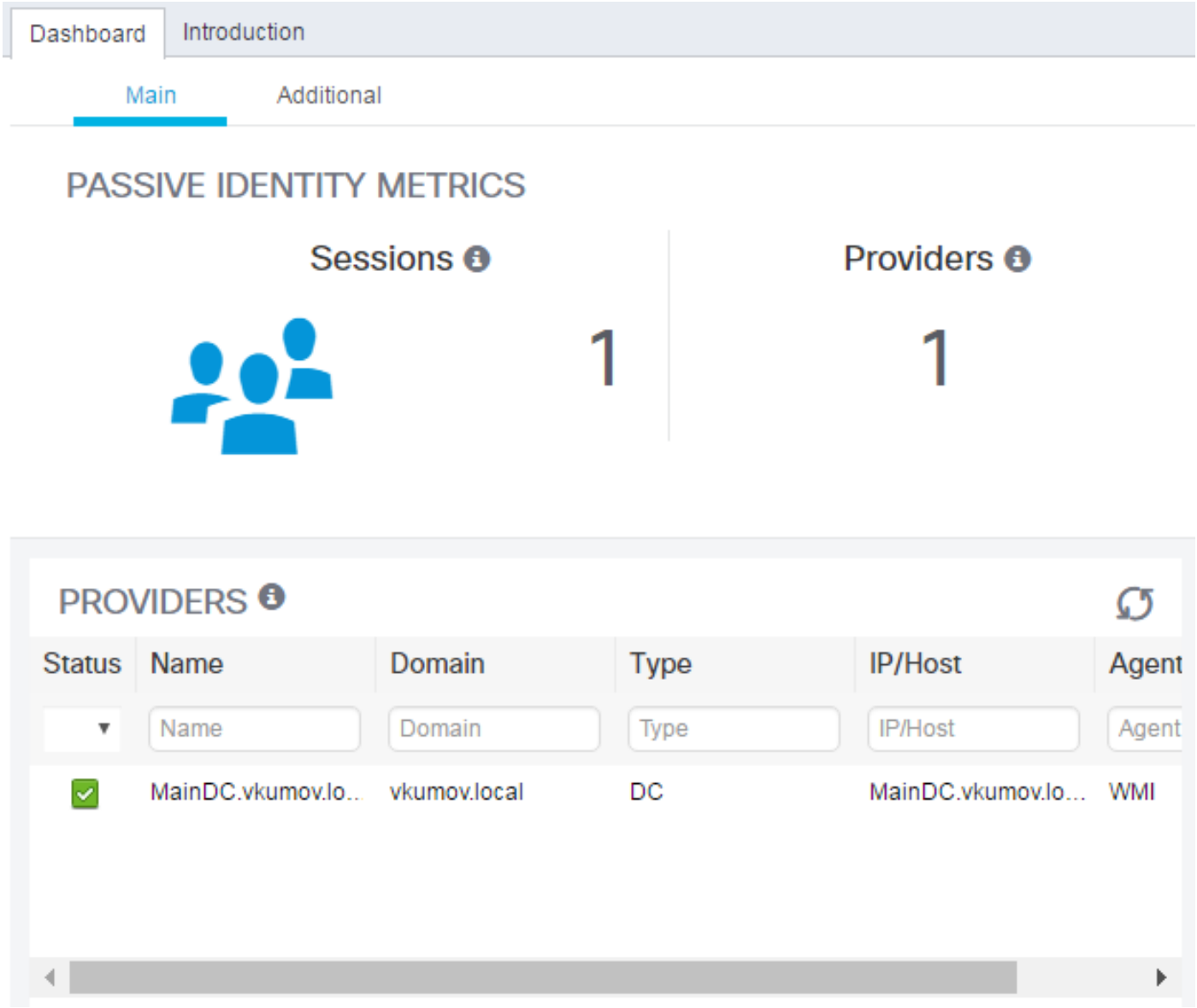


Опознавательная Задержка всегда 0ms, так как PIC ISE не выполняет аутентификаций/авторизаций.

Поставщики и сеансы

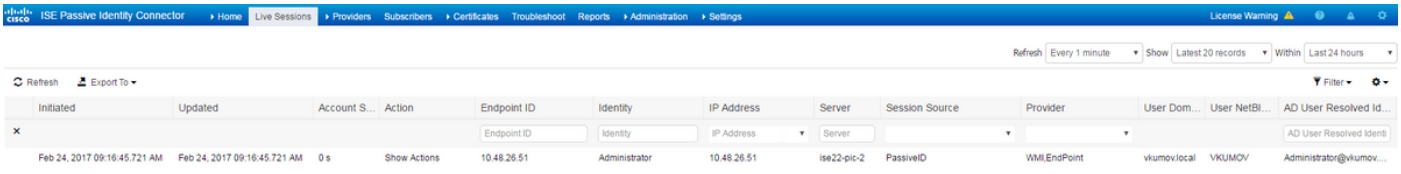
Домашняя страница

В то время как вы перешли к **странице Home> Dashboard,** статусы поставщиков, их количество и сумма найденных сеансов могут быть проверены:



Оперативные сеансы

Подробные сведения обо всех найденных пользовательских сеансах могут быть найдены в странице **Live Sessions**:



Это содержит такую информацию как:

- Поставщик - какие поставщики использовались для определения этого сеанса
- Инициируемый и Обновленный - метки времени, когда сеанс инициируется и обновляется соответственно
- IP-адрес- адрес Оконечной точки

- Действие - действия, которые может выполнить ISE (например, проверьте статус оконечной точки, или если PIC ISE интегрирован с pxGrid, тогда отправляют запрос для очистки сеанса),

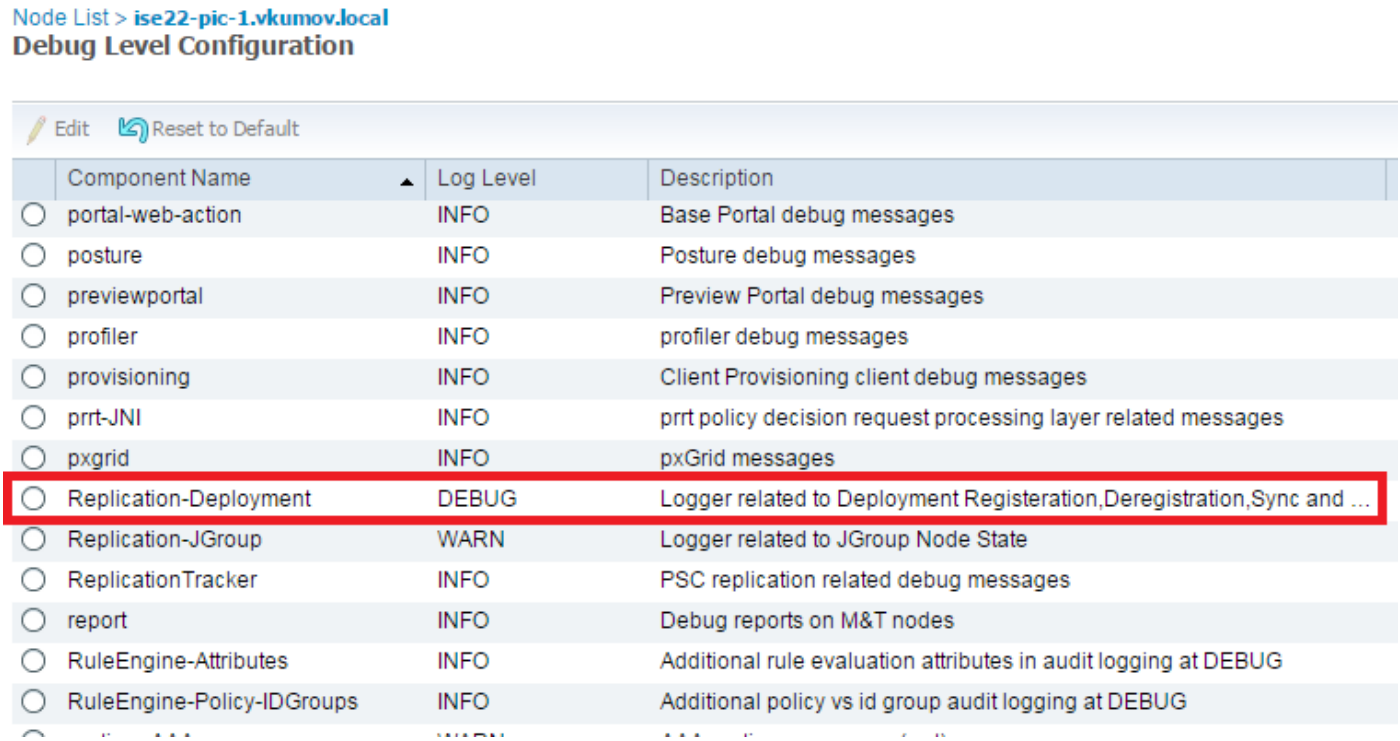
Устранение неполадок

Развертывания

Для устранения проблем проблем развертываний и репликации изучите те файлы журнала:

- replication.log
- deployment.log
- ise-psc.log

Для включения отладок перейдите к **администрированию> Регистрация> Конфигурация Журнала Отладки**:



Эти отладки записаны в **replication.log** файл. Вот пример процесса стандартной репликации:

```
2017-02-24 10:11:06,893 INFO [pool-215-thread-1][]
cisco.cpm.deployment.replication.PublisherImpl -:::- Calling the publisher job from
clusterstate processor
2017-02-24 10:11:06,893 DEBUG [pool-214-thread-1][]
cisco.cpm.deployment.replication.PublisherImpl -:::- Started executing publisher job
2017-02-24 10:11:06,894 DEBUG [pool-214-thread-1][]
cisco.cpm.deployment.replication.PublisherImpl -:::- Number of messages with no sequence number
is 0
2017-02-24 10:11:06,894 DEBUG [pool-214-thread-1][]
cisco.cpm.deployment.replication.PublisherImpl -:::- Finished executing publisher job
2017-02-24 10:11:06,895 DEBUG [pool-214-thread-1][]
api.services.persistance.dao.ChangeDataDaoImpl -:::- Data returned in getMinMaxBySequence
method=[id=[63ce2fe0-f8cd-11e6-b0ad-005056991a2e],startTime=[0],endTime=[0],applied=[false],data
length=[794],sequenceNumber=[502]2017-02-22 08:06:10.782]
2017-02-24 10:11:06,895 DEBUG [pool-214-thread-1][]
api.services.persistance.dao.ChangeDataDaoImpl -:::- Data returned in getMinMaxBySequence
```

method=[id=[3ded93c0-fa70-11e6-b684-005056990fbb],startTime=[0],endTime=[0],applied=[false],data length=[794],sequenceNumber=[1600]2017-02-24 10:04:26.364]
2017-02-24 10:11:06,895 DEBUG [pool-214-thread-1][]
cisco.cpm.deployment.replication.ClientNodeProxy -:::- Calling setClusterState(name: ise22-pic-1, minSequence: 502, sequence: 1600, active: {ise22-pic-1-5015})
2017-02-24 10:11:06,896 INFO [pool-214-thread-1][]
cisco.cpm.deployment.replication.PublisherImpl -:::- Finished sending the clusterState !!!
2017-02-24 10:11:06,899 DEBUG [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:- MonitorJob starting
2017-02-24 10:11:06,901 DEBUG [pool-216-thread-1][]
cisco.cpm.deployment.replication.ClientNodeProxy -:::NodeStateMonitor:- Calling getNodeStates()
2017-02-24 10:11:06,904 INFO [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:- Nodes in distrubution: {ise22-pic-2=nodeName: ise22-pic-2, **status: SYNC COMPLETED**, transientStatus: , lastStatusTime: 1487927436906, seqNumber: 1600, createTime: 2017-02-24 10:04:26.364} --- Nodes in cluster: [name: ise22-pic-2, Address: ise22-pic-2-38077, sequence: 1600, createtime: 2017-02-24 10:04:26.364]
2017-02-24 10:11:06,904 DEBUG [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:- Adding [nodeName: ise22-pic-2, **status: SYNC COMPLETED**, transientStatus: , lastStatusTime: 1487927436906, seqNumber: 1600, createTime: 2017-02-24 10:04:26.364] to liveDeploymentMembers
2017-02-24 10:11:06,905 DEBUG [pool-216-thread-1][]
api.services.persistance.dao.ChangeDataDaoImpl -:::NodeStateMonitor:- Data returned in getMinMaxBySequence method=[id=[63ce2fe0-f8cd-11e6-b0ad-005056991a2e],startTime=[0],endTime=[0],applied=[false],data length=[794],sequenceNumber=[502]2017-02-22 08:06:10.782]
2017-02-24 10:11:06,905 DEBUG [pool-216-thread-1][]
api.services.persistance.dao.ChangeDataDaoImpl -:::NodeStateMonitor:- Data returned in getMinMaxBySequence method=[id=[3ded93c0-fa70-11e6-b684-005056990fbb],startTime=[0],endTime=[0],applied=[false],data length=[794],sequenceNumber=[1600]2017-02-24 10:04:26.364]
2017-02-24 10:11:06,905 INFO [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:- Primary node current status minmum sequence[1600], cluster state: [name: ise22-pic-1, minSequence: 502, sequence: 1600, active: {ise22-pic-1-5015}]
2017-02-24 10:11:06,905 DEBUG [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:- Processing node state [name: ise22-pic-2, Address: ise22-pic-2-38077, sequence: 1600, createtime:2017-02-24 10:04:26.364]
2017-02-24 10:11:06,905 DEBUG [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:- ise22-pic-2 - [nodeName: ise22-pic-2, status: SYNC COMPLETED, transientStatus: , lastStatusTime: 1487927436906, seqNumber: 1600, createTime: 2017-02-24 10:04:26.364]
2017-02-24 10:11:06,905 DEBUG [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:- Adding nodeName: ise22-pic-2, status: SYNC COMPLETED, transientStatus: , lastStatusTime: 1487927436906, seqNumber: 1600, createTime: 2017-02-24 10:04:26.364 to liveJGroupMembers
2017-02-24 10:11:06,905 INFO [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:- No Of deployedNodes: [1], No Of liveJGroupNodes: [1], deadOrSyncInPrgMembersExist: [false], latestMinSequence: [502]
2017-02-24 10:11:06,905 DEBUG [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:- deadOrSyncInPrgMembersExist =[false], minSequence=[1598],clusterState=[502]

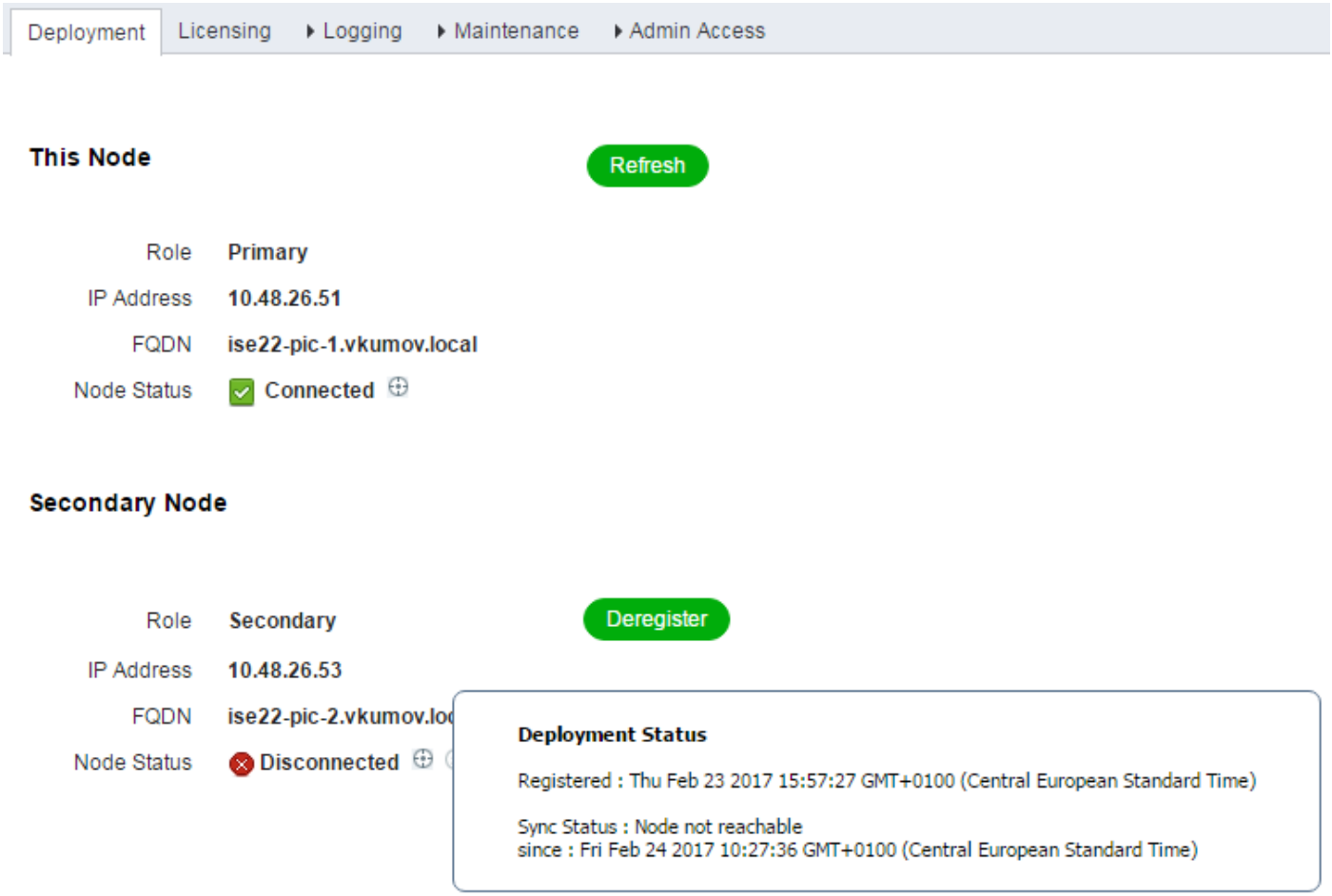
Сообщение от **ise-psc.log**:

2017-02-24 10:11:06,893 INFO [pool-215-thread-1][]
cisco.cpm.deployment.replication.PublisherImpl -:::- Calling the publisher job from clusterstate processor
2017-02-24 10:11:06,893 DEBUG [pool-214-thread-1][]
cisco.cpm.deployment.replication.PublisherImpl -:::- Started executing publisher job
2017-02-24 10:11:06,894 DEBUG [pool-214-thread-1][]
cisco.cpm.deployment.replication.PublisherImpl -:::- Number of messages with no sequence number

is 0
2017-02-24 10:11:06,894 DEBUG [pool-214-thread-1][]
cisco.cpm.deployment.replication.PublisherImpl -::::- Finished executing publisher job
2017-02-24 10:11:06,895 DEBUG [pool-214-thread-1][]
api.services.persistance.dao.ChangeDataDaoImpl -::::- Data returned in getMinMaxBySequence
method=[id=[63ce2fe0-f8cd-11e6-b0ad-005056991a2e],startTime=[0],endTime=[0],applied=[false],data
length=[794],sequenceNumber=[502]2017-02-22 08:06:10.782]
2017-02-24 10:11:06,895 DEBUG [pool-214-thread-1][]
api.services.persistance.dao.ChangeDataDaoImpl -::::- Data returned in getMinMaxBySequence
method=[id=[3ded93c0-fa70-11e6-b684-005056990fbb],startTime=[0],endTime=[0],applied=[false],data
length=[794],sequenceNumber=[1600]2017-02-24 10:04:26.364]
2017-02-24 10:11:06,895 DEBUG [pool-214-thread-1][]
cisco.cpm.deployment.replication.ClientNodeProxy -::::- Calling setClusterState(name: ise22-pic-
1, minSequence: 502, sequence: 1600, active: {ise22-pic-1-5015})
2017-02-24 10:11:06,896 INFO [pool-214-thread-1][]
cisco.cpm.deployment.replication.PublisherImpl -::::- Finished sending the clusterState !!!
2017-02-24 10:11:06,899 DEBUG [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:- MonitorJob starting
2017-02-24 10:11:06,901 DEBUG [pool-216-thread-1][]
cisco.cpm.deployment.replication.ClientNodeProxy -:::NodeStateMonitor:- Calling getNodeStates()
2017-02-24 10:11:06,904 INFO [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:- Nodes in
distrubution: {ise22-pic-2=nodeName: ise22-pic-2, **status: SYNC COMPLETED**, transientStatus: ,
lastStatusTime: 1487927436906, seqNumber: 1600, createTime: 2017-02-24 10:04:26.364} --- Nodes
in cluster: [name: ise22-pic-2, Address: ise22-pic-2-38077, sequence: 1600, createtime: 2017-02-
24 10:04:26.364]
2017-02-24 10:11:06,904 DEBUG [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:- Adding [nodeName:
ise22-pic-2, **status: SYNC COMPLETED**, transientStatus: , lastStatusTime: 1487927436906,
seqNumber: 1600, createTime: 2017-02-24 10:04:26.364] to liveDeploymentMembers
2017-02-24 10:11:06,905 DEBUG [pool-216-thread-1][]
api.services.persistance.dao.ChangeDataDaoImpl -:::NodeStateMonitor:- Data returned in
getMinMaxBySequence method=[id=[63ce2fe0-f8cd-11e6-b0ad-
005056991a2e],startTime=[0],endTime=[0],applied=[false],data
length=[794],sequenceNumber=[502]2017-02-22 08:06:10.782]
2017-02-24 10:11:06,905 DEBUG [pool-216-thread-1][]
api.services.persistance.dao.ChangeDataDaoImpl -:::NodeStateMonitor:- Data returned in
getMinMaxBySequence method=[id=[3ded93c0-fa70-11e6-b684-
005056990fbb],startTime=[0],endTime=[0],applied=[false],data
length=[794],sequenceNumber=[1600]2017-02-24 10:04:26.364]
2017-02-24 10:11:06,905 INFO [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:- Primary node
current status minmum sequence[1600], cluster state: [name: ise22-pic-1, minSequence: 502,
sequence: 1600, active: {ise22-pic-1-5015}]
2017-02-24 10:11:06,905 DEBUG [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:- Processing node
state [name: ise22-pic-2, Address: ise22-pic-2-38077, sequence: 1600, createtime:2017-02-24
10:04:26.364]
2017-02-24 10:11:06,905 DEBUG [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:- ise22-pic-2 - [
nodeName: ise22-pic-2, status: SYNC COMPLETED, transientStatus: , lastStatusTime: 1487927436906,
seqNumber: 1600, createTime: 2017-02-24 10:04:26.364]
2017-02-24 10:11:06,905 DEBUG [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:- Adding nodeName:
ise22-pic-2, status: SYNC COMPLETED, transientStatus: , lastStatusTime: 1487927436906,
seqNumber: 1600, createTime: 2017-02-24 10:04:26.364 to liveJGroupMembers
2017-02-24 10:11:06,905 INFO [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:- No Of
deployedNodes: [1], No Of liveJGroupNodes: [1], deadOrSyncInPrgMembersExist: [false],
latestMinSequence: [502]
2017-02-24 10:11:06,905 DEBUG [pool-216-thread-1][]
cisco.cpm.deployment.replication.NodeStateMonitorImpl -:::NodeStateMonitor:-
deadOrSyncInPrgMembersExist =[false], minSequence=[1598],clusterState=[502]

Общая проблема: вторичный узел не reacheable

Если бы вторичный узел становится unreacheable, он был бы отображен в **странице Administration> Deployment**:



ise-psc.log содержит это сообщение:

```
2017-02-24 10:43:21,587 INFO   [admin-http-pool155][]
admin.restui.features.deployment.DeploymentIDCUIApi -::::- Replication status for node ise22-
pic-2 = NODE NOT REACHABLE
```

Это сообщение объясняет, что не reacheable, например узел не отвечает на эхо-запрос:

```
2017-02-24 11:03:53,359 INFO   [counterscheduler-call-1][]
cisco.cpm.infrastructure.utils.GenericUtil -::::- Received pingNode response : Node is reachable
```

Действия для взятия: проверьте, разрешим ли FQDN socandary узла, проверьте базовое сетевое подключение между узлами.

В случае, если приложения не находятся в активном состоянии на вторичном узле или между узлами существует межсетевой экран, **ise-psc.log** может показать те сообщения:

```
2017-02-24 11:08:14,656 INFO   [Thread-10][] com.cisco.epm.util.NodeCheck -::::- Now checking
against secondary pap ise22-pic-2
2017-02-24 11:08:14,656 INFO   [Thread-10][] com.cisco.epm.util.NodeCheckHelper -::::-  inside
getHostConfigRemoteServer
2017-02-24 11:08:14,766 WARN   [Thread-10][]
deployment.client.cert.validator.HttpsCertPathValidatorImpl -::::- Error while connecting to
host: ise22-pic-2.vkumov.local. java.net.ConnectException: Connection refused
2017-02-24 11:08:14,871 WARN   [Thread-10][] com.cisco.epm.util.NodeCheckHelper -::::- Unable to
retrieve the host config from standby pap java.net.ConnectException: Connection refused
```

```
2017-02-24 11:08:14,871 WARN   [Thread-10][] com.cisco.epm.util.NodeCheckHelper -:::- returning
null from getHostConfigRemoteServer
2017-02-24 11:08:14,871 INFO   [Thread-10][] com.cisco.epm.util.NodeCheck -:::-
remotePrimaryConfig.getNodeRoleStatus() NULL
2017-02-24 11:08:14,871 INFO   [Thread-10][] com.cisco.epm.util.NodeCheck -:::-
remoteClusterInfo.getDeploymentName NULL
```

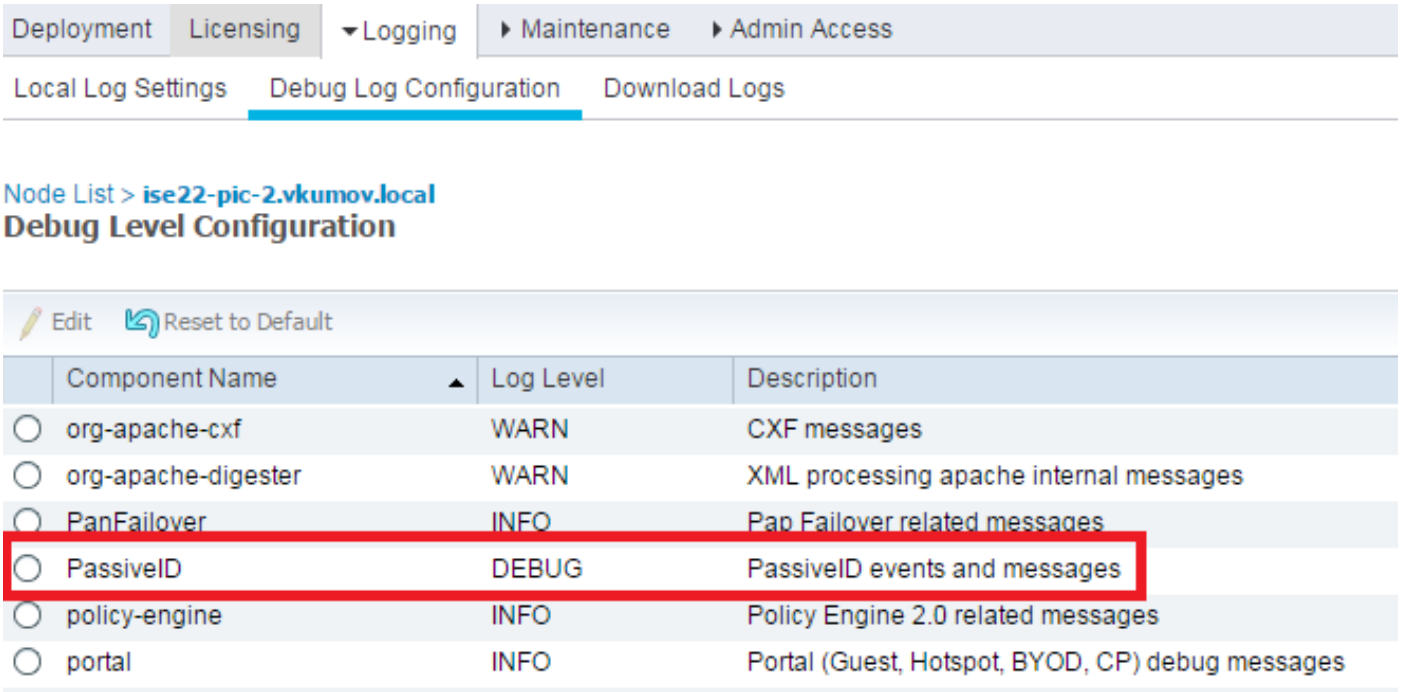
Действия для взятия: проверьте состояние приложения на вторичном узле, проверьте сетевое подключение, если все соединения разрешены между узлами.

Active Directory и WMI

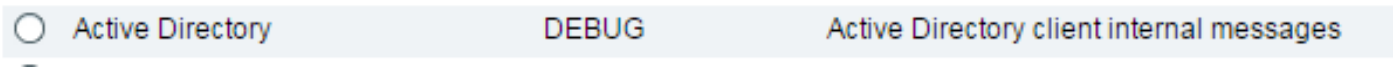
Для устранения проблем WMI Active Directory изучают те файлы:

- passive-wmi.log
- passive-endpoint.log
- ise-psc.log
- ad_agent.log

И полезные отладки могут, включил при **администрировании> Регистрация> Конфигурация Журнала Отладки**:



И:



Вот пример нового изученного сеанса от **пассивного-wmi.log** с включенными отладками:

```
2017-02-24 11:36:22,584 DEBUG  [Thread-11][] com.cisco.idc.dc-probe- New login event retrieved
from Domain Controller. Identity Mapping.ticket =
instance of __InstanceCreationEvent
{
SECURITY_DESCRIPTOR = {1, 0, 20, 128, 96, 0, 0, 0, 112, 0, 0, 0, 0, 0, 0, 0, 20, 0, 0, 0, 2, 0,
76, 0, 3, 0, 0, 0, 0, 0, 20, 0, 69, 0, 15, 0, 1, 1, 0, 0, 0, 0, 0, 5, 18, 0, 0, 0, 0, 0, 24, 0,
69, 0, 0, 0, 1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0, 0, 0, 24, 0, 65, 0, 0, 0, 1, 2,
0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 61, 2, 0, 0, 1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0, 1,
1, 0, 0, 0, 0, 0, 5, 18, 0, 0, 0};
```

```
TargetInstance =
instance of Win32_NTLogEvent
{
Category = 14339;
CategoryString = "Kerberos Authentication Service";
ComputerName = "MainDC.vkumov.local";
EventCode = 4768;
EventIdentifier = 4768;
EventType = 4;
InsertionStrings = {"Administrator", "vkumov.local", "S-1-5-21-2952046201-2792970045-1866348404-
500", "krbtgt", "S-1-5-21-2952046201-2792970045-1866348404-502", "0x40810010", "0x0", "0x12",
"2", "::1", "0", "", "", ""};
Logfile = "Security";
Message = "A Kerberos authentication ticket (TGT) was requested.
\n
\nAccount Information:
\n\tAccount Name:\t\tAdministrator
\n\tSupplied Realm Name:\tvkumov.local
\n\tUser ID:\t\t\tS-1-5-21-2952046201-2792970045-1866348404-500
\n
\nService Information:
\n\tService Name:\t\tkrbtgt
\n\tService ID:\t\tS-1-5-21-2952046201-2792970045-1866348404-502
\n
\nNetwork Information:
\n\tClient Address:\t\t::1
\n\tClient Port:\t\t0
\n
\nAdditional Information:
\n\tTicket Options:\t\t0x40810010
\n\tResult Code:\t\t0x0
\n\tTicket Encryption Type:\t0x12
\n\tPre-Authentication Type:\t2
\n
\nCertificate Information:
\n\tCertificate Issuer Name:\t\t
\n\tCertificate Serial Number:\t
\n\tCertificate Thumbprint:\t\t
\n
\nCertificate information is only provided if a certificate was used for pre-authentication.
\n
\nPre-authentication types, ticket options, encryption types and result codes are defined in RFC
4120.";
RecordNumber = 918032;
SourceName = "Microsoft-Windows-Security-Auditing";
TimeGenerated = "20170224103621.575178-000";
TimeWritten = "20170224103621.575178-000";
Type = "Audit Success";
};
TIME_CREATED = "131324061825752057";
};
 , Identity Mapping.dc-domainname = vkumov.local , Identity Mapping.dc-connection-type = Current
events , Identity Mapping.dc-name = MainDC.vkumov.local , Identity Mapping.dc-host =
MainDC.vkumov.local/10.48.26.52 ,
2017-02-24 11:36:22,587 DEBUG  [Thread-11][] com.cisco.idc.dc-probe- Replaced local IP. Identity
Mapping.ticket =
instance of __InstanceCreationEvent
{
SECURITY_DESCRIPTOR = {1, 0, 20, 128, 96, 0, 0, 0, 112, 0, 0, 0, 0, 0, 0, 0, 20, 0, 0, 0, 2, 0,
76, 0, 3, 0, 0, 0, 0, 0, 20, 0, 69, 0, 15, 0, 1, 1, 0, 0, 0, 0, 0, 5, 18, 0, 0, 0, 0, 0, 24, 0,
69, 0, 0, 0, 1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0, 0, 0, 24, 0, 65, 0, 0, 0, 1, 2,
0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 61, 2, 0, 0, 1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0, 1,
1, 0, 0, 0, 0, 0, 5, 18, 0, 0, 0};
TargetInstance =
```

instance of Win32_NTLogEvent
{
Category = 14339;
CategoryString = "Kerberos Authentication Service";
ComputerName = "MainDC.vkumov.local";
EventCode = 4768;
EventIdentifier = 4768;
EventType = 4;
InsertionStrings = {"Administrator", "vkumov.local", "S-1-5-21-2952046201-2792970045-1866348404-500", "krbtgt", "S-1-5-21-2952046201-2792970045-1866348404-502", "0x40810010", "0x0", "0x12", "2", "::1", "0", "", "", ""};
Logfile = "Security";
Message = "A Kerberos authentication ticket (TGT) was requested.
\n
\nAccount Information:
\n\tAccount Name:\t\tAdministrator
\n\tSupplied Realm Name:\tvkumov.local
\n\tUser ID:\t\t\tS-1-5-21-2952046201-2792970045-1866348404-500
\n
\nService Information:
\n\tService Name:\t\tkrbtgt
\n\tService ID:\t\tS-1-5-21-2952046201-2792970045-1866348404-502
\n
\nNetwork Information:
\n\tClient Address:\t\t::1
\n\tClient Port:\t\t0
\n
\nAdditional Information:
\n\tTicket Options:\t\t0x40810010
\n\tResult Code:\t\t0x0
\n\tTicket Encryption Type:\t0x12
\n\tPre-Authentication Type:\t2
\n
\nCertificate Information:
\n\tCertificate Issuer Name:\t\t
\n\tCertificate Serial Number:\t
\n\tCertificate Thumbprint:\t\t
\n
\nCertificate information is only provided if a certificate was used for pre-authentication.
\n
\nPre-authentication types, ticket options, encryption types and result codes are defined in RFC 4120.";
RecordNumber = 918032;
SourceName = "Microsoft-Windows-Security-Auditing";
TimeGenerated = "20170224103621.575178-000";
TimeWritten = "20170224103621.575178-000";
Type = "Audit Success";
};
TIME_CREATED = "131324061825752057";
};
 , Identity Mapping.dc-domainname = vkumov.local , Identity Mapping.dc-connection-type = Current events , Identity Mapping.probe = WMI , Identity Mapping.event-local-ip-address = ::1 , Identity Mapping.dc-name = MainDC.vkumov.local , Identity Mapping.dc-host = MainDC.vkumov.local/10.48.26.52 , Identity Mapping.server = ise22-pic-2 , Identity Mapping.event-ip-address = 10.48.26.52 ,
2017-02-24 11:36:22,589 DEBUG [Thread-11][] com.cisco.idc.dc-probe- Received login event. Identity Mapping.ticket =
instance of __InstanceCreationEvent
{
SECURITY_DESCRIPTOR = {1, 0, 20, 128, 96, 0, 0, 0, 112, 0, 0, 0, 0, 0, 0, 0, 20, 0, 0, 0, 2, 0, 76, 0, 3, 0, 0, 0, 0, 0, 20, 0, 69, 0, 15, 0, 1, 1, 0, 0, 0, 0, 0, 5, 18, 0, 0, 0, 0, 0, 24, 0, 69, 0, 0, 0, 1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0, 0, 0, 24, 0, 65, 0, 0, 0, 1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 61, 2, 0, 0, 1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0, 1, 1, 0, 0, 0, 0, 0, 5, 18, 0, 0, 0};

```
TargetInstance =
instance of Win32_NTLogEvent
{
Category = 14339;
CategoryString = "Kerberos Authentication Service";
ComputerName = "MainDC.vkumov.local";
EventCode = 4768;
EventIdentifier = 4768;
EventType = 4;
InsertionStrings = {"Administrator", "vkumov.local", "S-1-5-21-2952046201-2792970045-1866348404-
500", "krbtgt", "S-1-5-21-2952046201-2792970045-1866348404-502", "0x40810010", "0x0", "0x12",
"2", "::1", "0", "", "", ""};
Logfile = "Security";
Message = "A Kerberos authentication ticket (TGT) was requested.
\n
\nAccount Information:
\n\tAccount Name:\t\tAdministrator
\n\tSupplied Realm Name:\tvkumov.local
\n\tUser ID:\t\t\tS-1-5-21-2952046201-2792970045-1866348404-500
\n
\nService Information:
\n\tService Name:\t\tkrbtgt
\n\tService ID:\t\tS-1-5-21-2952046201-2792970045-1866348404-502
\n
\nNetwork Information:
\n\tClient Address:\t\t::1
\n\tClient Port:\t\t0
\n
\nAdditional Information:
\n\tTicket Options:\t\t0x40810010
\n\tResult Code:\t\t0x0
\n\tTicket Encryption Type:\t0x12
\n\tPre-Authentication Type:\t2
\n
\nCertificate Information:
\n\tCertificate Issuer Name:\t\t
\n\tCertificate Serial Number:\t
\n\tCertificate Thumbprint:\t\t
\n
\nCertificate information is only provided if a certificate was used for pre-authentication.
\n
\nPre-authentication types, ticket options, encryption types and result codes are defined in RFC
4120.";
RecordNumber = 918032;
SourceName = "Microsoft-Windows-Security-Auditing";
TimeGenerated = "20170224103621.575178-000";
TimeWritten = "20170224103621.575178-000";
Type = "Audit Success";
};
TIME_CREATED = "131324061825752057";
};
 , Identity Mapping.dc-domainname = vkumov.local , Identity Mapping.dc-connection-type = Current
events , Identity Mapping.probe = WMI , Identity Mapping.event-local-ip-address = ::1 , Identity
Mapping.dc-name = MainDC.vkumov.local , Identity Mapping.event-user-name = Administrator ,
Identity Mapping.dc-host = MainDC.vkumov.local/10.48.26.52 , Identity Mapping.server = ise22-
pic-2 , Identity Mapping.event-ip-address = 10.48.26.52 ,
```

Пример проверки оконечной точки от пассивного-endpoint.log (в этом случае оконечная точка была unreacheable от ISE):

```
2017-02-24 11:36:22,584 DEBUG  [Thread-11][] com.cisco.idc.dc-probe- New login event retrieved
from Domain Controller. Identity Mapping.ticket =
instance of __InstanceCreationEvent
{
```

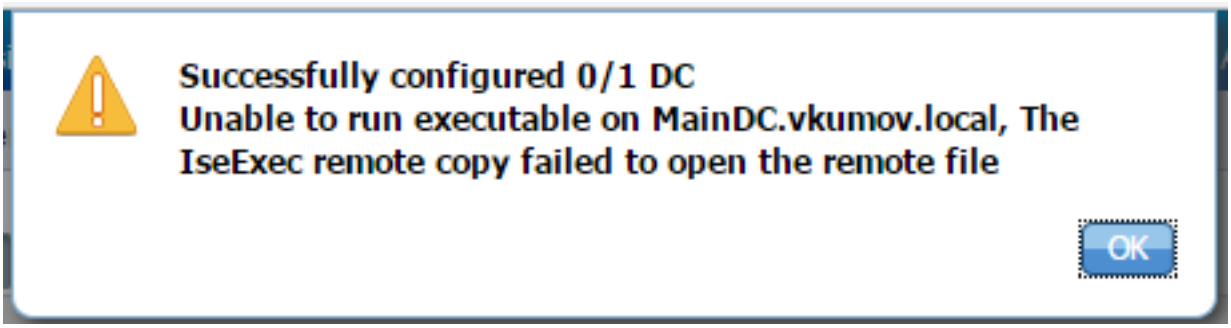
SECURITY_DESCRIPTOR = {1, 0, 20, 128, 96, 0, 0, 0, 112, 0, 0, 0, 0, 0, 0, 0, 20, 0, 0, 0, 2, 0,
76, 0, 3, 0, 0, 0, 0, 0, 20, 0, 69, 0, 15, 0, 1, 1, 0, 0, 0, 0, 0, 5, 18, 0, 0, 0, 0, 0, 24, 0,
69, 0, 0, 0, 1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0, 0, 0, 24, 0, 65, 0, 0, 0, 1, 2,
0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 61, 2, 0, 0, 1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0, 1,
1, 0, 0, 0, 0, 0, 5, 18, 0, 0, 0};
TargetInstance =
instance of Win32_NTLogEvent
{
Category = 14339;
CategoryString = "Kerberos Authentication Service";
ComputerName = "MainDC.vkumov.local";
EventCode = 4768;
EventIdentifier = 4768;
EventType = 4;
InsertionStrings = {"Administrator", "vkumov.local", "S-1-5-21-2952046201-2792970045-1866348404-
500", "krbtgt", "S-1-5-21-2952046201-2792970045-1866348404-502", "0x40810010", "0x0", "0x12",
"2", "::1", "0", "", "", ""};
Logfile = "Security";
Message = "A Kerberos authentication ticket (TGT) was requested.
\n
\nAccount Information:
\n\tAccount Name:\t\tAdministrator
\n\tSupplied Realm Name:\tvkumov.local
\n\tUser ID:\t\t\tS-1-5-21-2952046201-2792970045-1866348404-500
\n
\nService Information:
\n\tService Name:\t\tkrbtgt
\n\tService ID:\t\tS-1-5-21-2952046201-2792970045-1866348404-502
\n
\nNetwork Information:
\n\tClient Address:\t\t::1
\n\tClient Port:\t\t0
\n
\nAdditional Information:
\n\tTicket Options:\t\t0x40810010
\n\tResult Code:\t\t0x0
\n\tTicket Encryption Type:\t0x12
\n\tPre-Authentication Type:\t2
\n
\nCertificate Information:
\n\tCertificate Issuer Name:\t\t
\n\tCertificate Serial Number:\t
\n\tCertificate Thumbprint:\t\t
\n
\nCertificate information is only provided if a certificate was used for pre-authentication.
\n
\nPre-authentication types, ticket options, encryption types and result codes are defined in RFC
4120.";
RecordNumber = 918032;
SourceName = "Microsoft-Windows-Security-Auditing";
TimeGenerated = "20170224103621.575178-000";
TimeWritten = "20170224103621.575178-000";
Type = "Audit Success";
};
TIME_CREATED = "131324061825752057";
};
 , Identity Mapping.dc-domainname = vkumov.local , Identity Mapping.dc-connection-type = Current
events , Identity Mapping.dc-name = MainDC.vkumov.local , Identity Mapping.dc-host =
MainDC.vkumov.local/10.48.26.52 ,
2017-02-24 11:36:22,587 DEBUG [Thread-11][] com.cisco.idc.dc-probe- Replaced local IP. Identity
Mapping.ticket =
instance of __InstanceCreationEvent
{
SECURITY_DESCRIPTOR = {1, 0, 20, 128, 96, 0, 0, 0, 112, 0, 0, 0, 0, 0, 0, 0, 20, 0, 0, 0, 2, 0,

76, 0, 3, 0, 0, 0, 0, 0, 20, 0, 69, 0, 15, 0, 1, 1, 0, 0, 0, 0, 0, 5, 18, 0, 0, 0, 0, 0, 24, 0, 69, 0, 0, 0, 1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0, 0, 0, 24, 0, 65, 0, 0, 0, 1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 61, 2, 0, 0, 1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0, 1, 1, 0, 0, 0, 0, 0, 5, 18, 0, 0, 0};
TargetInstance =
instance of Win32_NTLogEvent
{
Category = 14339;
CategoryString = "Kerberos Authentication Service";
ComputerName = "MainDC.vkumov.local";
EventCode = 4768;
EventIdentifier = 4768;
EventType = 4;
InsertionStrings = {"Administrator", "vkumov.local", "S-1-5-21-2952046201-2792970045-1866348404-500", "krbtgt", "S-1-5-21-2952046201-2792970045-1866348404-502", "0x40810010", "0x0", "0x12", "2", "::1", "0", "", "", ""};
Logfile = "Security";
Message = "A Kerberos authentication ticket (TGT) was requested.
\n
\nAccount Information:
\n\tAccount Name:\t\tAdministrator
\n\tSupplied Realm Name:\tvkumov.local
\n\tUser ID:\t\t\tS-1-5-21-2952046201-2792970045-1866348404-500
\n
\nService Information:
\n\tService Name:\t\tkrbtgt
\n\tService ID:\t\tS-1-5-21-2952046201-2792970045-1866348404-502
\n
\nNetwork Information:
\n\tClient Address:\t\t::1
\n\tClient Port:\t\t0
\n
\nAdditional Information:
\n\tTicket Options:\t\t0x40810010
\n\tResult Code:\t\t0x0
\n\tTicket Encryption Type:\t0x12
\n\tPre-Authentication Type:\t2
\n
\nCertificate Information:
\n\tCertificate Issuer Name:\t\t
\n\tCertificate Serial Number:\t
\n\tCertificate Thumbprint:\t\t
\n
\nCertificate information is only provided if a certificate was used for pre-authentication.
\n
\nPre-authentication types, ticket options, encryption types and result codes are defined in RFC 4120.";
RecordNumber = 918032;
SourceName = "Microsoft-Windows-Security-Auditing";
TimeGenerated = "20170224103621.575178-000";
TimeWritten = "20170224103621.575178-000";
Type = "Audit Success";
};
TIME_CREATED = "131324061825752057";
};
 , Identity Mapping.dc-domainname = vkumov.local , Identity Mapping.dc-connection-type = Current events , Identity Mapping.probe = WMI , Identity Mapping.event-local-ip-address = ::1 , Identity Mapping.dc-name = MainDC.vkumov.local , Identity Mapping.dc-host = MainDC.vkumov.local/10.48.26.52 , Identity Mapping.server = ise22-pic-2 , Identity Mapping.event-ip-address = 10.48.26.52 ,
2017-02-24 11:36:22,589 DEBUG [Thread-11][] com.cisco.idc.dc-probe- Received login event. Identity Mapping.ticket =
instance of __InstanceCreationEvent
{

```
SECURITY_DESCRIPTOR = {1, 0, 20, 128, 96, 0, 0, 0, 112, 0, 0, 0, 0, 0, 0, 0, 20, 0, 0, 0, 2, 0,
76, 0, 3, 0, 0, 0, 0, 0, 20, 0, 69, 0, 15, 0, 1, 1, 0, 0, 0, 0, 0, 5, 18, 0, 0, 0, 0, 0, 24, 0,
69, 0, 0, 0, 1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0, 0, 0, 24, 0, 65, 0, 0, 0, 1, 2,
0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 61, 2, 0, 0, 1, 2, 0, 0, 0, 0, 0, 5, 32, 0, 0, 0, 32, 2, 0, 0, 1,
1, 0, 0, 0, 0, 0, 5, 18, 0, 0, 0};
TargetInstance =
instance of Win32_NTLogEvent
{
Category = 14339;
CategoryString = "Kerberos Authentication Service";
ComputerName = "MainDC.vkumov.local";
EventCode = 4768;
EventIdentifier = 4768;
EventType = 4;
InsertionStrings = {"Administrator", "vkumov.local", "S-1-5-21-2952046201-2792970045-1866348404-
500", "krbtgt", "S-1-5-21-2952046201-2792970045-1866348404-502", "0x40810010", "0x0", "0x12",
"2", "::1", "0", "", "", ""};
Logfile = "Security";
Message = "A Kerberos authentication ticket (TGT) was requested.
\n
\nAccount Information:
\n\tAccount Name:\t\tAdministrator
\n\tSupplied Realm Name:\tvkumov.local
\n\tUser ID:\t\t\tS-1-5-21-2952046201-2792970045-1866348404-500
\n
\nService Information:
\n\tService Name:\t\tkrbtgt
\n\tService ID:\t\tS-1-5-21-2952046201-2792970045-1866348404-502
\n
\nNetwork Information:
\n\tClient Address:\t\t::1
\n\tClient Port:\t\t0
\n
\nAdditional Information:
\n\tTicket Options:\t\t0x40810010
\n\tResult Code:\t\t0x0
\n\tTicket Encryption Type:\t0x12
\n\tPre-Authentication Type:\t2
\n
\nCertificate Information:
\n\tCertificate Issuer Name:\t\t
\n\tCertificate Serial Number:\t
\n\tCertificate Thumbprint:\t\t
\n
\nCertificate information is only provided if a certificate was used for pre-authentication.
\n
\nPre-authentication types, ticket options, encryption types and result codes are defined in RFC
4120.";
RecordNumber = 918032;
SourceName = "Microsoft-Windows-Security-Auditing";
TimeGenerated = "20170224103621.575178-000";
TimeWritten = "20170224103621.575178-000";
Type = "Audit Success";
};
TIME_CREATED = "131324061825752057";
};
 , Identity Mapping.dc-domainname = vkumov.local , Identity Mapping.dc-connection-type = Current
events , Identity Mapping.probe = WMI , Identity Mapping.event-local-ip-address = ::1 , Identity
Mapping.dc-name = MainDC.vkumov.local , Identity Mapping.event-user-name = Administrator ,
Identity Mapping.dc-host = MainDC.vkumov.local/10.48.26.52 , Identity Mapping.server = ise22-
pic-2 , Identity Mapping.event-ip-address = 10.48.26.52 ,
```

Общая проблема: PIC ISE бросает "Неспособный работать на исполняемом файле <name> DC... Ошибка

Если у пользователя, который используется для соединения PIC ISE с доменом, нет достаточного количества разрешений, PIC ISE бросает ошибку во время конфигурации WMI:



Соответствующие отладки могут быть найдены в **ad_agent.log** файле (Уровень журнала Active Directory должен быть установлен в DEBUG):

```
26/02/2017 19:15:45,VERBOSE,139954093012736,SMBGSSContextNegotiate: state =
1,lwio/server/smbcommon/smbkrb5.c:460
26/02/2017 19:15:45,VERBOSE,139956055955200,Session 0x7f49bc001430 is eligible for
reaping,lwio/server/rdr/session2.c:290
26/02/2017 19:15:45,VERBOSE,139954101405440,Error at ../../lsass/server/auth-providers/ad-open-
provider/provider-main.c:7503 [code: C0000022],lsass/server/auth-providers/ad-open-
provider/provider-main.c:7503
26/02/2017 19:15:45,VERBOSE,139954101405440,Extended Error code: 60190 (symbol:
LW_ERROR_ISEEXEC_CP_OPEN_REMOTE_FILE),lsass/server/auth-providers/ad-open-provider/provider-
main.c:7627
26/02/2017 19:15:45,VERBOSE,139954101405440,Error at ../../lsass/server/auth-providers/ad-open-
provider/provider-main.c:7628 [code: C0000022],lsass/server/auth-providers/ad-open-
provider/provider-main.c:7628
26/02/2017 19:15:45,VERBOSE,139954101405440,Error code: 5 (symbol:
ERROR_ACCESS_DENIED),lsass/server/auth-providers/ad-open-provider/provider-main.c:7782
26/02/2017 19:15:45,VERBOSE,139954101405440,Error code: 5 (symbol:
ERROR_ACCESS_DENIED),lsass/server/auth-providers/ad-open-provider/provider-main.c:7855
26/02/2017 19:15:45,VERBOSE,139954101405440,Error code: 5 (symbol:
ERROR_ACCESS_DENIED),lsass/server/api/api2.c:2713
26/02/2017 19:15:45,VERBOSE,139956064347904,(session:ee880a4e15e682f4-08401b84f371a140)
Dropping: LWMSG_STATUS_PEER_CLOSE,lwmsg/src/peer-task.c:625
26/02/2017 19:15:50,VERBOSE,139956055955200,RdrSocketRelease(0x7f496800b6e0, 38): socket is
eligible for reaping,lwio/server/rdr/socket.c:2239
```

Действия для взятия: воссоединитесь с узлами PIC ISE к домену с учетными данными Администратора домена или добавьте пользователя, который используется для, соединяют операцию с группой *Администраторов домена* в AD.