

Содержание

[Вопрос:](#)

Вопрос:

Как использовать LDAP, Принимают, что Запрос проверяет получателей входящих сообщений с помощью Microsoft Active Directory (LDAP)?

Примечание: Следующий пример интегрируется со стандартными развертываниями Microsoft Active Directory, невзирая на то, что принципы могут быть применены ко многим типам реализаций LDAP.

Вы сначала создадите запись Сервера LDAP, в этот момент необходимо задать сервер каталогов, а также запрос, который выполнит Устройство Безопасности электронной почты. Запрос тогда включен или применен на вашего входящего (общего) слушателя. Эти параметры настройки Сервера LDAP могут быть разделены другими слушателями и другими частями конфигурации, такими как карантинный доступ конечного пользователя.

Упростить конфигурацию LDAP делает запрос на вашем устройстве IronPort, мы рекомендуем использовать браузер LDAP, который позволяет вам посмотреть на вашу схему, а также все атрибуты, на которые можно сделать запрос против.

Для Microsoft Windows можно использовать:

Для Linux или UNIX, можно использовать `ldapsearch` команда.

Во-первых, необходимо определить Сервер LDAP для запроса. В данном примере псевдоним "PublicLDAP" дан для *myldapservr*. пример. Сервер LDAP *com*. Запросы направлены к порту TCP 389 (по умолчанию).

Примечание: Если ваша Реализация Active Directory будет содержать субдомены, то вы не будете в состоянии сделать запрос для пользователей в sub домене с помощью основного DN корневого домена. Однако при использовании Active Directory, можно также сделать запрос LDAP против Сервера глобального каталога (GC) на порте TCP 3268. Когда дополнительная информация запрошена, GC содержит частичную информацию для *все* объекты в лесу Active Directory и предоставляет рекомендации рассматриваемому субдомену. Если вы не можете "найти" пользователей в своих субдоменах, оставить основной DN в root и заставить IronPort использовать порт GC.

GUI:

1. Создайте новый Профиль Сервера LDAP со значениями, расположенными ранее от вашего сервера каталогов (Администрирование системы> LDAP) . Пример: Название профиля сервера: *PublicLDAP* Host name: *myldapserver. пример. com* Authentication method: *Пароль использования: включенный* Имя пользователя: *cn=ESA, cn=Users, dc=example, dc=com* Password: *password* Тип сервера: *Active Directory* Порт: *3268* BaseDN: *dc=example, dc=com* Удостоверьтесь, что использовали кнопку "Test Server" для проверки параметров настройки перед продолжением. Успешные выходные данные должны быть похожими:
2. Использование тот же экран для определения LDAP принимает запрос. Следующий пример проверяет адрес получателя против более общих атрибутов, любого "почтового" OR "proxyAddresses": Name: *PublicLDAP*. acceptQueryString: *(/ (отправляют по почте =) (proxyAddresses=smtp:{a}))* Можно использовать кнопку "Test Query", чтобы проверить, что поисковый запрос возвращает результаты для допустимой учетной записи. Успешные выходные данные, ищущие адрес учетной записи сервиса ["EKAadmin@example.com"](mailto:EKAadmin@example.com), должны быть похожими:
3. Примените это новое принимает запрос Входящему Слушателю (Сеть> Слушатели). Разверните опции LDAP Queries> Ассерт и выберите свой запрос *PublicLDAP.accept*.
4. Наконец, передайте изменения для включения этих параметров настройки.

CLI:

1. Во-первых, вы используете *ldapconfig* команду для определения Сервера LDAP для устройства для привязки с, и запросы для принятия получателя (*ldapaccept* подкоманда), направляя (*ldaprouting* подкоманда), и подменяя (подкоманда подмены) настроены.
2. Во-вторых, необходимо определить запрос для выполнения против Сервера LDAP, который вы только что настроили.
3. Как только вы настроили запрос LDAP, необходимо применить политику LDAPассерт к Входящему Слушателю.
4. Для активации изменений, внесенных в слушателя, передайте изменения.