

Приглашаем Вас принять участие в конкурсе на поставку и сопровождение лицензий

Varonis DataPrivilege for 500 users

1. Описание конкурса

Позиции	Описание		
Наименование товара	Лицензии <i>Varonis DataPrivilege for 500 users</i>		
Модель, спецификация	Наименование	Артикул	Количество
	Лицензии Varonis DataPrivilege for 500 users	VDP-500L	1
	Annual Software Subscription & Support for DataPrivilege® for 500 users	VSSPDP1-500L	1
	Professional Services - Installation, basic training and configuration	VPRS-8D	1
	Дополнительная информация в <u>Приложении 1</u>		
Сроки и периодичность закупок	Разовая закупка лицензий		
Минимальные требования к поставщику работ (услуг):			
- опыт, квалификация	Уровень партнерства: партнер Varonis		
- наличие выполненных проектов	Опыт работы с ключевыми клиентами		
- условия оплаты	Предоставление лицензий на основании заключенного договора поставки. Оплата по факту поставки на основании договора поставки. Факт поставки будет закрыт актом, после предоставления ПО с русифицированным интерфейсом. Срок поставки составляет 60 дней с момента размещения заказа на приобретение.		
- срок работы на рынке	не менее 3 лет		
Условия принятия коммерческих предложений:	<p>Коммерческие предложения принимаются только по электронной почте на адрес tender@bank.rs.ru и hizbulin@bank.rs.ru в любом распространенном графическом формате (сканированные документы *.jpg или *.pdf). Обязательно указывать тему: «Коммерческое предложение <i>Varonis</i> от «<u>название организации</u>».</p> <p>Коммерческие предложения полученные на другие почтовые адреса не рассматриваются.</p>		

- Конкурсные предложения принимаются 25 февраля 2010 г. с 10.00 до 17.00 мск на фирменном бланке, заверенные печатью компании **ТОЛЬКО по адресам** tender@bank.rs.ru и hizbulin@bank.rs.ru.
- В конкурсном предложении указать цену за единицу (включая общую стоимость), условия оплаты (ЦБ РФ + 0%) по факту поставки, а также сроки поставки.
- Предложения, полученные после 17.00 ___ февраля 2010 года, а также полученные на другие почтовые ящики рассматриваться не будут.**
- Подтвердить получение приглашения на участие в конкурсе.
- Выслать Карточку Сведений об организации по электронной почте вместе с конкурсным предложением.

I. Краткое описание функций системы

Система управления доступом к файловым ресурсам должна обеспечивать ответственному сотруднику от подразделения возможность подать запрос на получение доступа к файловым ресурсам, а лицам, ответственным за доступ к ресурсам – удовлетворить либо отклонить запрос.

II. Основные технические требования:

Система должна работать на следующей программной платформе:

- Операционная система Microsoft Windows Server 2003 или 2008 (Standard или Enterprise Edition), 32-bit или 64-bit.
- СУБД Microsoft SQL Server 2005 SP2/SP3 (Standard или Enterprise Edition)
- Microsoft Internet Information Server (IIS) версии 6 или 7.

Система должна обеспечивать следующий уровень интеграции с информационной средой компании:

1. Взаимодействие со службой каталогов Active Directory:
 - 1.1. Чтение информации о пользователе/группе
 - 1.2. Создание новых групп безопасности в выделенном для этого контейнере (OU) – при необходимости.
 - 1.3. Изменение членства в существующих группах AD
2. Работа с файловыми серверами Windows 2000, 2003, 2008, а также Network Appliance (NetApp):
 - 2.1. Чтение структуры папок на файловом сервере, а также списков контроля доступа,
 - 2.2. Добавление групп или индивидуальных пользователей в ACL вновь создаваемых папок – при необходимости.
3. Обмен информацией с пользователями системы с использованием существующего SMTP-сервера.
 - 3.1. Отправление оповещений и отчётов через существующий SMTP-сервер

III. Основные требования к функциональности

1. Программа должна поддерживать следующие способы управления доступом пользователей к файловым ресурсам:
 - 1.1. Добавление пользователя(ей) в доменную группу, имеющую необходимый доступ к соответствующей папке файлового ресурса. В связи с тем, что существуют запросы на предоставление доступа к конкретному ресурсу группе лиц, иногда достигающие до 300-400 пользователей, реализована возможность включения большого кол-ва пользователей в доменную группу по одной заявке с использованием специальной утилиты Bulk Upload Tool. Реализация аудита событий массового добавления в группу с помощью утилиты Bulk Upload Tool будет реализована в течение **45 дней с момента размещения заказа на приобретение ПО.**
 - 1.2. Добавление учётной записи пользователя(ей) напрямую в ACL файлового ресурса, но не более 5 пользователей. Если доступ требуется более 5

пользователям, администратор программы имеет возможность из графического интерфейса создать в AD новые группы и прописать их в список контроля доступа папки с необходимыми правами.

2. Наличие Web-интерфейса, отсутствие требования по установке клиентской части на рабочие станции пользователей.
3. В одной заявке можно одновременно запрашивать доступ к множеству файловых ресурсов (до 32-х) с разным уровнем доступа.
4. Язык интерфейса – русский. **Полная поддержка русского языка будет реализована в программе в течение 60 дней с момента размещения заказа на приобретение ПО.**
5. Автоматическая авторизация в Web-интерфейсе программы пользователей, авторизованных в домене, без необходимости повторного ввода учётных данных.
6. Обеспечение выполнения заданного срока действия прав доступа, с автоматическим закрытием доступа по истечении срока, назначенного при удовлетворении заявки.
7. Все участники процесса должны иметь возможность получать уведомления о новых заявках, а также об изменении статуса существующих заявок, по электронной почте.
8. Должна быть предусмотрена возможность назначения нескольких обязательных уровней авторизации для конкретного ресурса.
9. Авторизатор должен иметь возможность удовлетворить заявку как в неизменном (исходном) виде, так и внеся изменения в уровень предоставляемых прав доступа, а также в срок действия назначенных прав доступа.
10. В случае, если заявка не была обработана в течение заданного времени, предусмотрена возможность, через заданное число дней, автоматического напоминания для авторизаторов всех уровней, а также, через заданное число дней, эскалация на ответственного (ответственных) за ресурс.
11. После прохождения всех ступеней авторизации, включая Администратора, доступ должен предоставляться автоматически, без участия администраторов или специалистов службы поддержки.

IV. Роли пользователей в системе.

Программа должна обеспечивать наличие следующих ролей, в соответствии с которыми программа предоставляет полномочия пользователям:

- Администратор;
- Ответственный за ресурс;
- Авторизатор;
- Специалист службы поддержки;
- Ответственный сотрудник от подразделения.

Администратор должен обладать в системе следующими правами:

1. Определять разделы файловых ресурсов, на которых требуется организовать управление правами доступа.
2. Назначать «ответственных за ресурс», ответственных за организацию управления доступом к файловым ресурсам в их зоне ответственности.
3. Назначать других администраторов, а также специалистов службы поддержки (Service Desk/Help Desk).
4. Выполнять настройки программы, в том числе параметры взаимодействия с AD и файловыми серверами.

5. Получать отчёты о работе программы, текущих правах доступа и об истории обработки запросов.
6. Иметь возможность определить, для доступа к каким ресурсам используется та или иная группа.
7. Авторизовывать доступ.

Ответственный за ресурс должен иметь в системе следующие полномочия в пределах своей зоны ответственности:

1. Определять конкретные ресурсы (папки), к которым требуется индивидуально контролировать доступ.
2. Назначать сотрудников (авторизаторов), которые будут утверждать запросы на доступ к ресурсам в пределах их ответственности.
3. Получать информацию обо всех необработанных запросах доступа, а также иметь возможность найти любой запрос, поданный и авторизованный ранее.
4. Самостоятельно одобрять/отклонять запросы, предназначенные для обработки авторизаторами нижнего уровня.
5. Участвовать в процессе авторизации (т.е. самому быть авторизатором).
6. Самостоятельно подавать запросы на доступ к ресурсам за других сотрудников.
7. Автоматически получать по электронной почте отчёты о текущих правах доступа к ресурсам, а также обо всех запросах, поданных в течение заданного интервала времени.
8. Иметь возможность определить, для доступа к каким ресурсам используется та или иная группа
9. По заданному графику проводить аудит существующих прав доступа к ресурсам.

Авторизатор должен обладать в системе следующими возможностями в пределах своей зоны ответственности:

1. Наблюдать в системе (а также получать по электронной почте) необработанные запросы на доступ к ресурсам, для которых он является авторизатором.
2. Отклонить запрос, объяснив причину, либо отправить запрос на уточнение Администраторам.
3. Удовлетворить запрос, как в исходном виде, так и внося изменения в уровень доступа и срок действия прав доступа к ресурсу.
4. Самостоятельно подавать запросы на доступ к ресурсам за других сотрудников.
5. Найти в системе любые запросы, которые он обрабатывал в прошлом.
6. Автоматически получать по электронной почте отчёты о текущих правах доступа к ресурсам, а также обо всех запросах, поданных в течение заданного интервала времени.
7. Иметь возможность определить, для доступа к каким ресурсам используется та или иная группа

Специалист службы поддержки должен иметь возможность наблюдать в системе все текущие заявки на предоставление доступа, для оказания помощи пользователям.

Ответственный сотрудник от подразделения должен иметь доступ к следующим сервисам, предоставляемым системой:

1. Выбор файлового ресурса, к которому требуется получить доступ. Для удобства поиска, файловые ресурсы отображаются в виде дерева.
2. Выбор требуемого уровня доступа из предложенных системой.
3. Выбор срока действия запрошенных прав доступа (включая «бессрочно»).
Наблюдение в системе своих заявок, как активных, так и закрытых (отклонённых и удовлетворённых).

4. Получение по электронной почте сообщений от системы о статусе прохождения заявки, в том числе об удовлетворении или отклонении заявки.
5. Отображение списка авторизаторов, через которых должна пройти конкретная заявка, с их контактной информацией.

V. Поиск информации о правах доступа, назначенных с момента внедрения системы управления доступом

Возможность поиска и отображения информации о правах доступа должна обеспечиваться при выполнении следующих условий:

1. Пользователи системы управления правами доступа должны иметь следующие возможности по поиску и отображению архивной информации.
 - 1.1. Поиск заявок, поданных в течение заданного интервала времени.
 - 1.2. Поиск заявок, относящихся к определённому ресурсу (папке) на файловой системе.
 - 1.3. Поиск заявок на изменение прав доступа конкретному сотруднику,
 - 1.4. Логические операции И, ИЛИ, НЕ над условиями из п.п. 1.1. – 1.3.
 - 1.5. В результате выполнения запроса система управления правами доступа должна выдать в своём Web-интерфейсе список заявок, удовлетворяющих условиям поиска.