



The power to do more

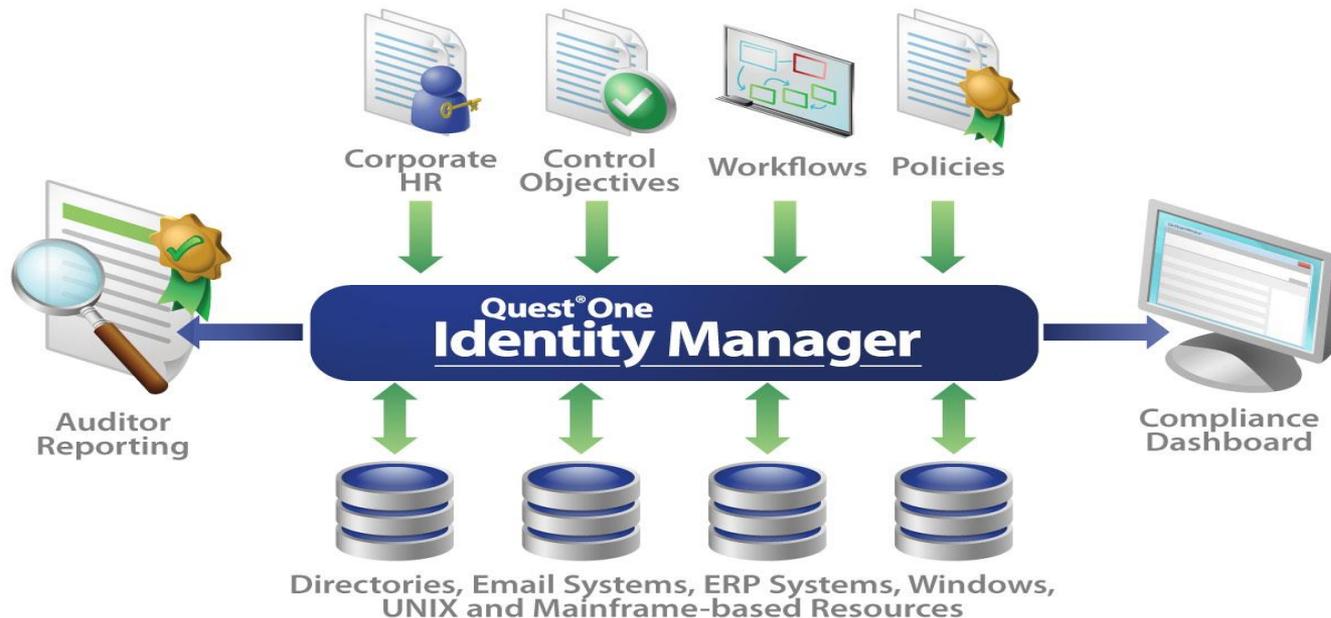
Управление доступом к корпоративным данным



Dell One Identity Manager –
гибкое решение
контроля доступа.

Гибкость в достижении единой цели

- Все элементы соединены в одно решение, где каждый человек несёт ответственность за свой участок работы.
- Каждый человек имеет возможность конфигурации «своих» элементов.
- Проект по внедрению имеет короткие фазы с чёткими достижимыми результатами.



Видение организации

Менеджеры должны легко видеть все роли и ресурсы подчинённых на одном простом экране.

Auditing - Employee details

Use the various tabs to see additional information about Albert Einstein.

Overview Requests Approvals Rule violations Roles and entitlements Business ownerships History

Access to shops (2)
Fruits & Vegetables Ltd.
Identity & Access Lifecycle

Identity Manager application roles (41)

Employee Albert Einstein

Form of address: Mr
Full name: Albert Einstein
Phone: +49 40 555 4564
Mobile phone:
Fax: +49 40 555 4599
Building:
Floor:
Room:
Central user account: ALBERTE
Central SAP user account: EINSTEIA
Default email address: ALBERTE@fruits.lan
Primary location: Hamburg
Primary department: Sales (10100200)
Primary cost center: 10100200 (Sales)
Primary business role: US
Manager: Albert Einstein
Deputy manager or supervisor:
Assistant deputy:
Certification pending: False
Disabled permanently: False
External: False

Active Directory user account 'Einstein Albert fruits.lan/EMEA/D/Einstein Albert [USER]'

Login name (pre Win2000): ALBERTE
Home directory: \\FRUIT-AD\ALBERTES
Email address: ALBERTE@fruits.lan

Additionally assigned to business role Operations (2)
Managers in Fruits
Staff

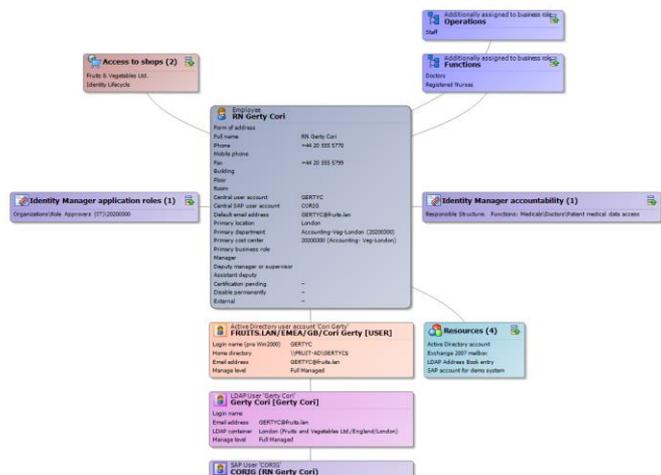
Additionally assigned to business role Functions (1)
Externals with sales permissions

Identity Manager accountability (60)

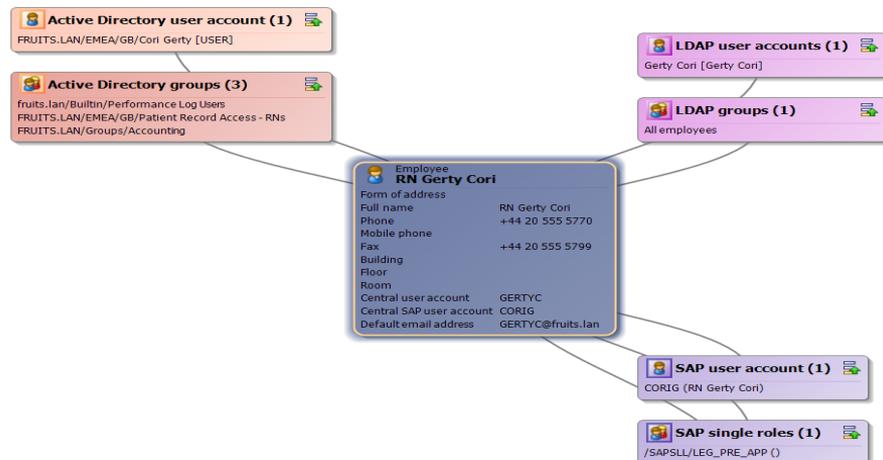
Resources (4)
Active Directory account
Exchange 2007 mailbox
LDAP Address Book entry
SAP account for demo system

Виды с точек зрения техники и бизнеса

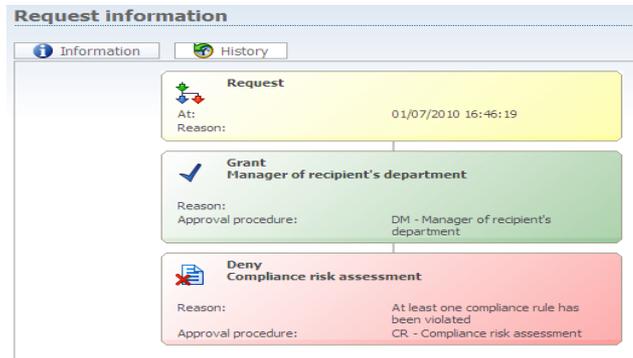
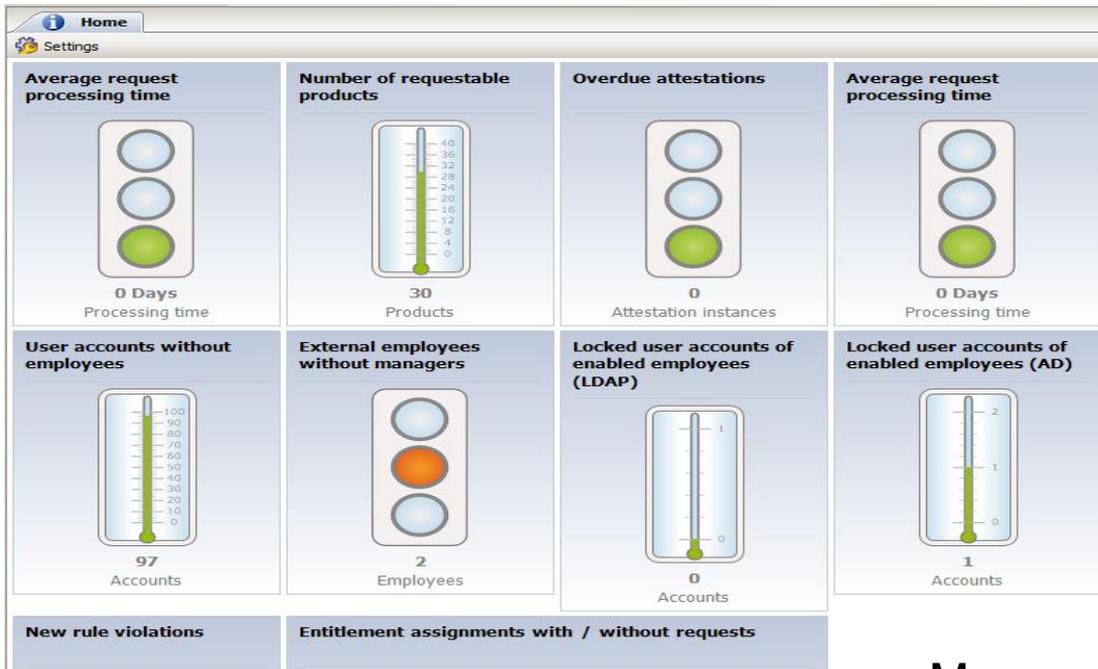
Бизнес-вид



Технический вид



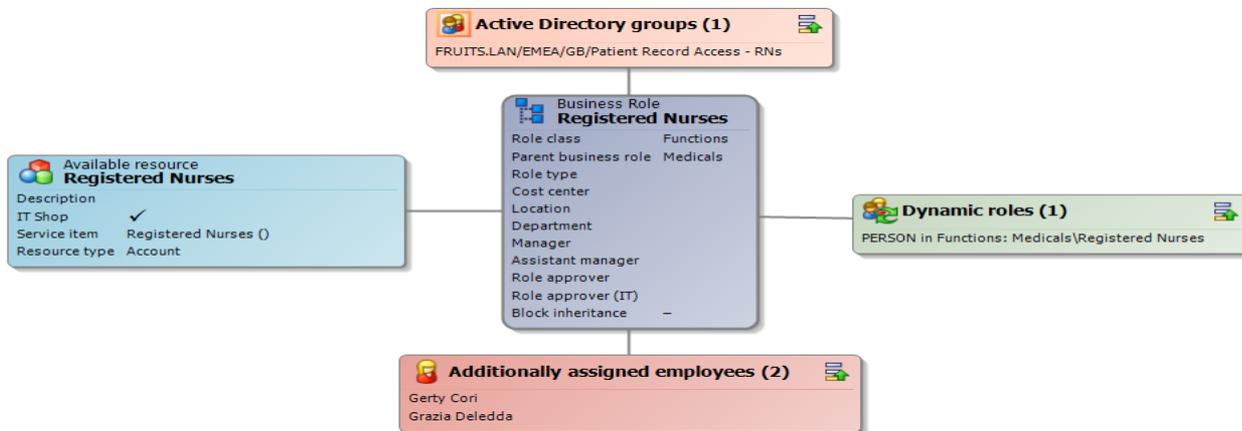
Панели с текущим статусом



Менеджеры должны легко находить текущий статус в целом и статус конкретных процессов.

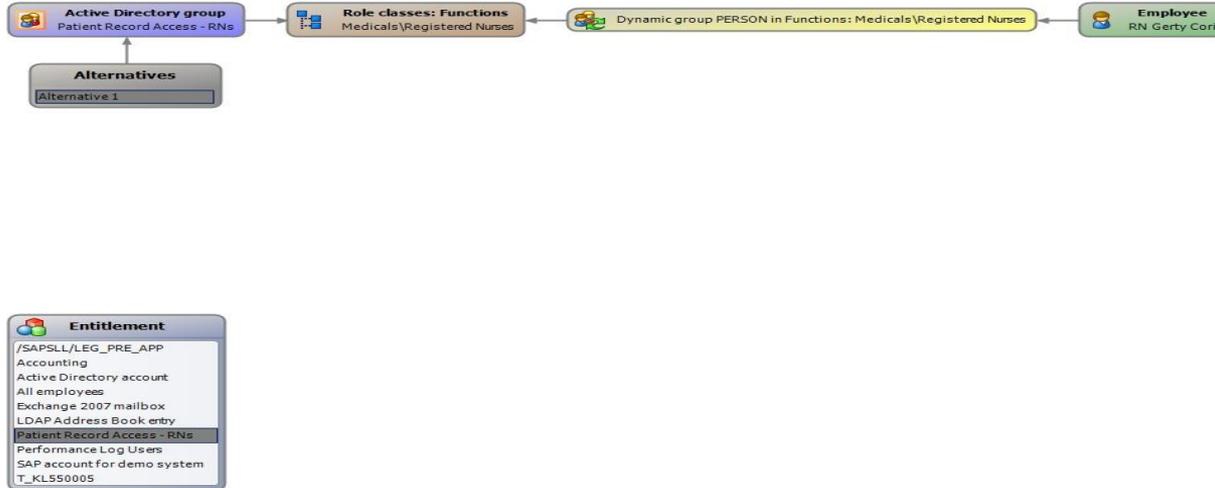
Конфигурация бизнес-ролей

Люди, отвечающие за бизнес, должны быть в состоянии строить нужные бизнес-роли в графическом интерфейсе, а не скриптами.



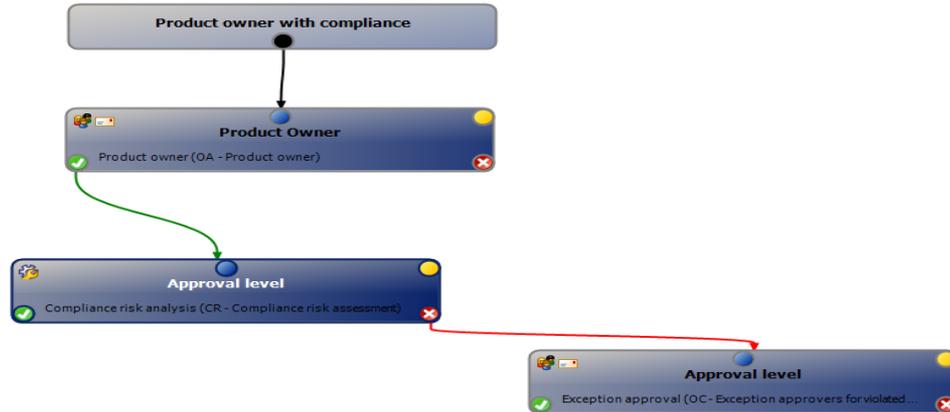
Аудит выдачи доступа

Люди, отвечающие за аудит должны видеть историю изменения доступа конкретных лиц



Постройка процессов одобрения

Бизнес-процессы должны строиться теми же людьми, которые отвечают за это в реальной жизни. Конструктор бизнес-процессов поможет в этом.



Пример аттестации

Attestation process 1/3/2012 2:49:47 AM (10)

Group by

IT Support

Count: 10

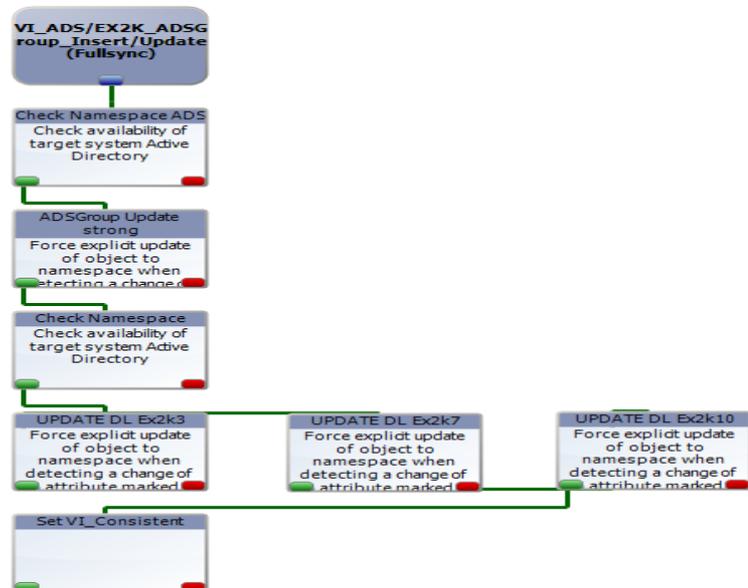
Last Name	First Name	Start Date	End Date		Approve	Reject
Stueer	Larry	02/27/2011 09:45:49	01/02/2012 00:46:35	Report	<input type="checkbox"/>	<input type="checkbox"/>
Smotter	Joe	02/18/2011 10:11:43	01/02/2012 00:46:35	Report	<input type="checkbox"/>	<input type="checkbox"/>
Timmerman	Christopher	02/10/2011 17:06:29	01/02/2012 00:46:35	Report	<input type="checkbox"/>	<input type="checkbox"/>
Wignis	Todd	02/27/2011 20:15:27	01/02/2012 00:46:35	Report	<input type="checkbox"/>	<input type="checkbox"/>
Travis	Randy	02/17/2011 14:08:34	01/02/2012 00:46:35	Report	<input type="checkbox"/>	<input type="checkbox"/>
Finn	Huck	02/11/2011 14:00:21	01/02/2012 00:46:35	Report	<input type="checkbox"/>	<input type="checkbox"/>
Batey	Elaine	02/11/2011 15:57:28	01/02/2012 00:46:31	Report	<input type="checkbox"/>	<input type="checkbox"/>
Harris	Eddy	02/15/2011 14:40:08	01/02/2012 00:46:35	Report	<input type="checkbox"/>	<input type="checkbox"/>
Parker	John	02/11/2011 13:47:42	01/02/2012 00:46:35	Report	<input type="checkbox"/>	<input type="checkbox"/>
Palligrove	Jane	02/27/2011 09:41:19	01/02/2012 00:46:35	Report	<input type="checkbox"/>	<input type="checkbox"/>

Rule violations (1)

Employees	Rule violation	Description	State	Approver
Batey, Elaine	Accounts Receivable with Accounts Payable Approver	Accounts Recieving cannot have Accounts Payable Approval authority. This is a toxic combination and a SOX Violation	 open	

Конструктор бизнес-процессов

Администратор должен иметь инструменты для постройки и изменения процессов.



Портал самообслуживания



Help for the IT service shop Scout Logout
You are logged in as: Domroese, Ulrich

- ▶ Home page
- ▶ Order IT service
 - ▶ Notes Account
 - ▶ Notes Mail-In DB
 - ▶ Notes Mail Distribution List
 - ▶ **Notes access group**
 - ▶ Reset password
- ▶ View drafts
- ▶ View requests
- ▶ Approve
- ▶ My Data

english ▼

Notes access group: Edit memberships for an employee

[Back](#)

i These changes must be approved by an administrator of the group. In case of approval, the changes will be automatically applied within 30 minutes.

• Choose employee: Search for: Name / ID → GO Dressel, Patrick (M121281)

• **List of memberships:**

▲ Groups:	
\$EMD_CI-AHE_acctest10_Depositor	X
\$KGA_CH-ICC_SRM ACL Test	X
\$MDA_CH-IEC_group-for-reset-of-your-brain	X
MDA_CH-IEC_KST-NEW	X
MDA_CH-IES_Dressel-Test	X

• **Add groups:**

Group name:

Employee for comparison: Search for: Name / ID → GO [/](#)

[Start search](#)

Order reason:

[Request change](#) [Save as draft](#) [Delete draft](#)

Портал должен быть достаточно простым, чтобы им могли пользоваться люди без специальных технических знаний.

Пример внедрения.

Задачи, поставленные заказчиком

- Автоматизация процесса управления предоставлением доступа
- Централизованное управление паролями пользователей
- Аудит имеющегося доступа
- Отчётность о предоставленном доступе
- Создание единого процесса и политики управления предоставлением доступа
- Интеграция с удостоверяющим центром

Интеграционные требования

- Интеграция с сервисной шиной:

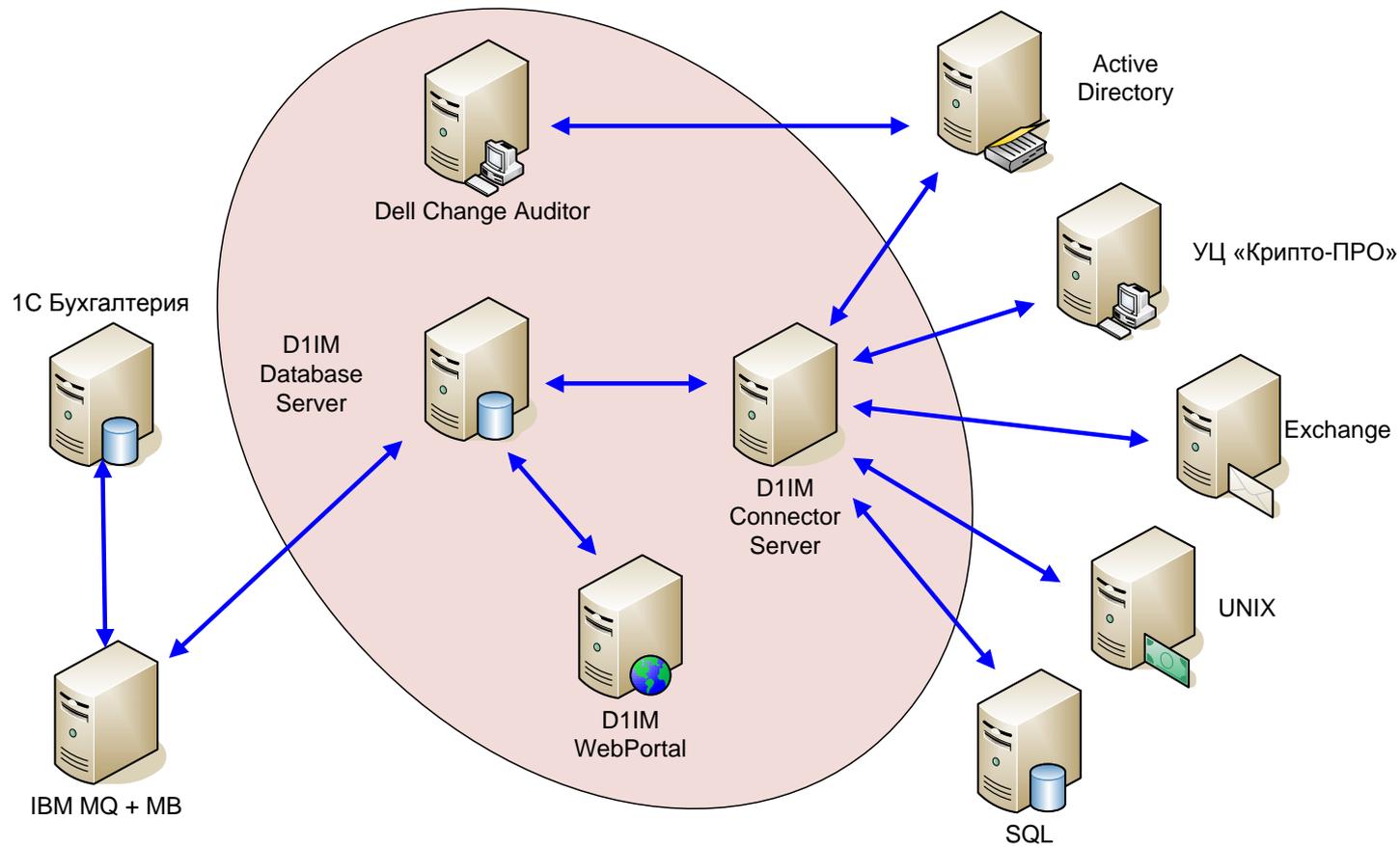
- Взаимодействие с системой кадрового учета реализуется посредством взаимодействия с сервисной шиной (ESB).

- Интеграция с почтовой системой:

- Управление почтовыми ящиками (создание, удаление, блокировка)
- Реализация метода утверждения запросов доступа к ресурсам посредством почтовых сообщений.

- Интеграция с УЦ:

- Интеграция с удостоверяющим центром «Крипто-ПРО», автоматизация процедур по выпуску/отзыву сертификатов.



MT809-Desk - Citrix Receiver

Самсонов Филипп Викторович - Outlook Web App - Windows Internet Explorer 10.1.206.30

https://mail.ahm1.ru/owa/

Outlook Web App

Почта > Входящие элементов: 27

Создать · Удалить · Переместить · Фильтр · Просмотр · Поиск во всем почтовом ящике

Входящие

От кого	Тема	Дата
q1idm_svc@ahm1.ru	Запрос на согласование прав доступа	20.03.2014
q1idm_svc@ahm1.ru	Запрос на согласование прав доступа	20.03.2014
q1idm_svc@ahm1.ru	запрос на согласование прав доступа	20.03.2014
q1idm_svc@ahm1.ru	запрос на согласование прав доступа	17.03.2014
q1idm_svc@ahm1.ru	запрос на согласование прав доступа	17.03.2014
q1idm_svc@ahm1.ru	Запрос на согласование прав доступа	17.03.2014
q1idm_svc@ahm1.ru	Запрос на согласование прав доступа	17.03.2014
q1idm_svc@ahm1.ru	Запрос на согласование прав доступа	17.03.2014
q1idm_svc@ahm1.ru	Reminder: approval required	17.03.2014
q1idm_svc@ahm1.ru	запрос на согласование прав доступа	17.03.2014
q1idm_svc@ahm1.ru	Запрос на согласование прав доступа	17.03.2014
q1idm_svc@ahm1.ru	запрос на согласование прав доступа	16.03.2014
q1idm_svc@ahm1.ru	запрос на согласование прав доступа	16.03.2014
q1idm_svc@ahm1.ru	Запрос на согласование прав доступа	16.03.2014
q1idm_svc@ahm1.ru	Запрос на согласование прав доступа	16.03.2014
q1idm_svc@ahm1.ru	Запрос на согласование прав доступа	16.03.2014
q1idm_svc@ahm1.ru	Запрос на согласование прав доступа	16.03.2014
q1idm_svc@ahm1.ru	Запрос на согласование прав доступа	16.03.2014
q1idm_svc@ahm1.ru	Запрос на согласование прав доступа	16.03.2014

Почта

Календарь

Контакты

Задачи

Общие ссылки

Запрос на согласование прав доступа

q1idm_svc@ahm1.ru

Кому: Самсонов Филипп Викторович

20 марта 2014 г., 14:02

Уважаемый(ая) Самсонов Филипп Викторович,

Требуется Ваше согласование для предоставления прав доступа к следующему ресурсу: 1С:Зарплата и кадры. Внутренний аудитор

Доступ запрашивается сотрудником: Толстая, Анна Владимировна

Доступ запрашивается для сотрудника: Толстая, Анна Владимировна

Обоснование:

Ваше решение:

[Согласовать](#) [Отказать](#)

Сообщение сгенерировано СУИД АИЖК

Система управления доступом АИЖК (<http://idm.ahm1.ru/ident/manager>)

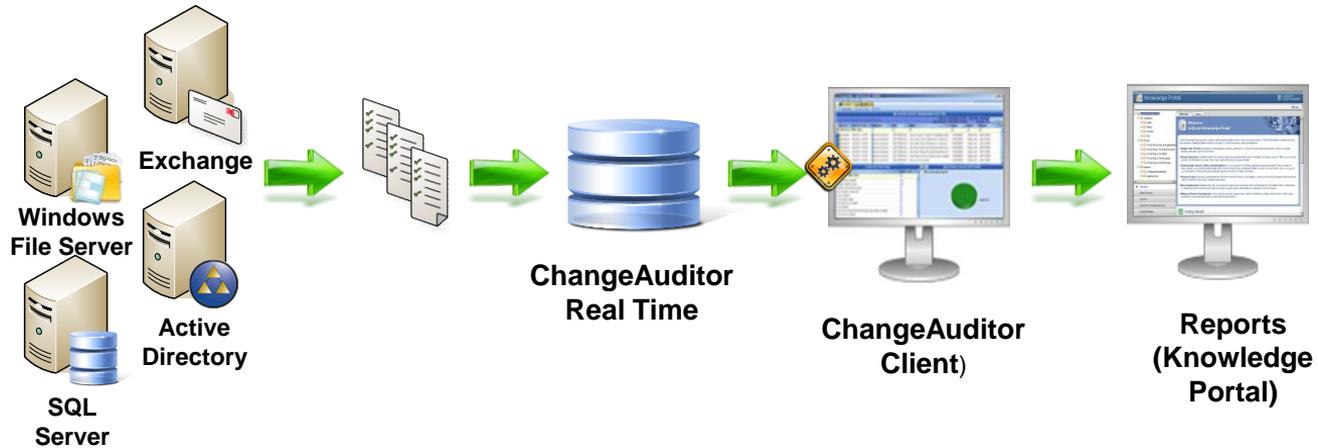
A3

ChangeAuditor for AD/Exchange/File Systems – расширенный аудит платформы Microsoft

ChangeAuditors+InTrust: аудит доступа и защита данных

- Решение Quest: ChangeAuditor+InTrust
- Основные возможности:
 - Аудит доступа в реальном времени.
 - Дополнительный уровень безопасности.
 - Защита критических данных от нежелательных изменений.
 - Применение защиты на основе членства в группах AD.
- Области контроля
 - ChangeAuditor - Active Directory, Microsoft Apps (Exchange, SQL, Sharepoint...), Microsoft Windows File Servers, Network Storage (EMC, NetApp).
 - InTrust – всё, т.е. серверы (Windows, Unix, AIX, Linux, ...), сетевые устройства, приложения и т.д.

Архитектура ChangeAuditor



InTrust с новым функционалом “IT Search”

Сегодня: InTrust – единая точка поиска IT-данных

**Search and
Visualization**



InTrust v11

**Aggregation
Correlation and Storage**



Collection

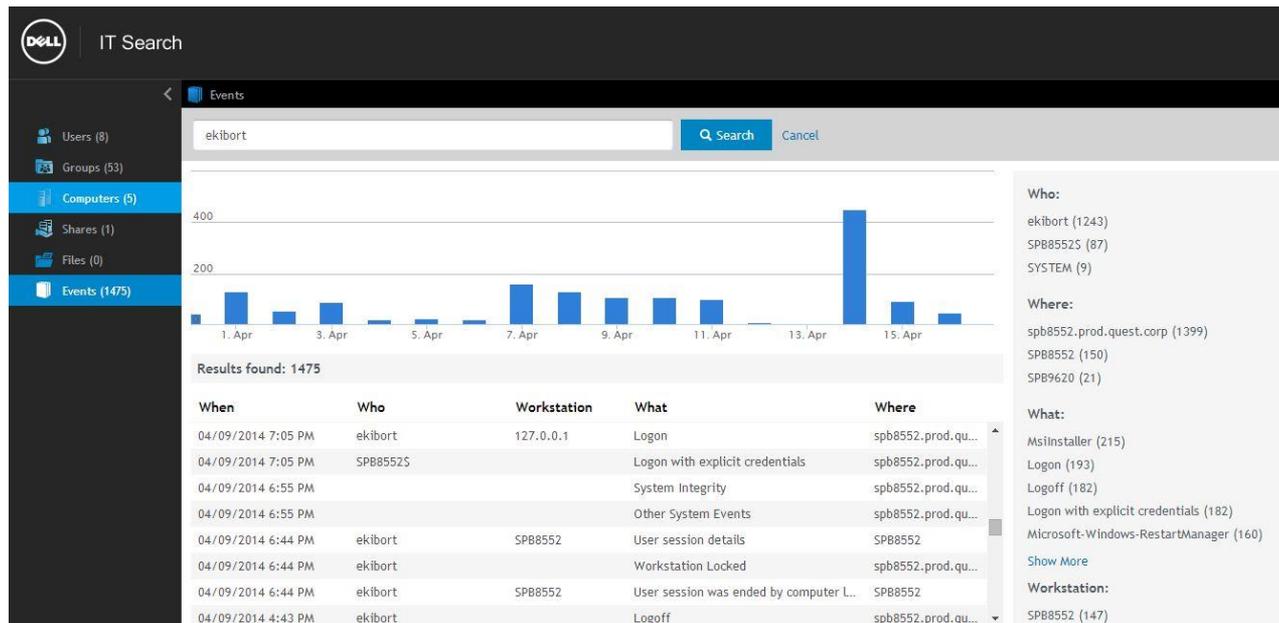


Data sources



InTrust становится «big data»-решением с IT Search

“IT Search ПОЗВОЛЯЕТ организации исследовать “big IT data”, включая логи, изменения, разрешения и т.д. для проведения разбора инцидентов безопасности и соответствия стандартам.



Поиск всех IT-данных в одном месте

The screenshot displays the InTrust IT Search application interface. The browser address bar shows the URL: `https://localhost/#/search/users?q=Lyudmila&p=1`. The application header includes the Dell logo, the text 'InTrust IT Search', and the user 'WIN-BMTLVGTNVSBAdministrator' with 'About' and 'Settings' links. The left sidebar contains navigation options: 'Users (3)', 'Groups (30)', 'Computers (0)', 'Shares (1)', 'Files (0)', and 'Events (215)'. The main search area has a search bar with 'Lyudmila' and buttons for 'Search' and 'Cancel'. Below the search bar, it indicates 'Results found: 3' and includes an 'Export' button. A table lists the search results with columns for Name, Department, Office, Manager, and Domain. A right-hand pane shows a summary of the results, categorized by 'Found in:', 'Title:', 'Department:', 'Office:', and 'Manager:'.

Name	Department	Office	Manager	Domain
 Lyudmila Epikhina Software Developer 3	R&D - Development	St. Petersburg	Eduard Kibort	prod.quest.corp
 Lyudmila Epikhina (Dell) Software Dev Engineer	QEST-R&D-97	RULED01-NA	Eduard Kibort (Dell)	prod.quest.corp
 Eduard Kibort Mgr, Software Developmen	R&D - Development	St. Petersburg	Yuri Golikov	prod.quest.corp

Found in:
E-mail (2)
Name (2)
Direct Reports (1)
LogonName (1)

Title:
Mgr, Software Development (1)
Software Dev Engineer (1)
Software Developer 3 (1)

Department:
R&D - Development (2)
QEST-R&D-97 (1)

Office:
St. Petersburg (2)
RULED01-NA (1)

Manager:
Eduard Kibort (1)

Взаимоотношения между событиями и конфигурацией

The screenshot displays the Dell InTrust IT Search web interface. The browser address bar shows a search query for a user. The interface includes a navigation sidebar on the left with categories like Users, Groups, Computers, Shares, Files, and Events. The main content area shows the profile of Lyudmila Epikhina, a Software Developer, with details such as Department (R&D - Development), Office (St. Petersburg), and contact information. A 'Member Of' tab is active, displaying a table of organizational units.

Display Name	Organizational Unit
DLSG_Lync.PublicAccess	prod.quest.corp/Dynamic Groups/IS Administration
Domain Users	prod.quest.corp/Users
HTTP_Access	prod.quest.corp/Groups/IS
Office_EMEA_RU.StPetersburg	prod.quest.corp/Dynamic Groups/Location
QDL.BU.WSM	prod.quest.corp/Groups/Business Unit
QDL.IS.Exchange2007MBCleanup2	prod.quest.corp/Dynamic Groups/IS Administration

Что делали пользователи?

The screenshot displays the InTrust IT Search application interface. At the top, the browser address bar shows the search query: `https://localhost/#/search/events?q=Who:%22Lyudmila%20Epikhina%22&p=3`. The application header includes the Dell logo, the text 'InTrust IT Search', the user 'WIN-BMTLVGTNVSB\Administrator', and links for 'About' and 'Settings'.

The main content area shows a breadcrumb trail: 'Users > Lyudmila Epikhina > Events'. Below this is a search bar containing 'Who:"Lyudmila Epikhina"' and a 'Search' button. A bar chart visualizes the event frequency over time, with a peak in late July. Below the chart, it states 'Results found: 25000' with an 'Export' button.

A table of search results is displayed with the following columns: When, Who, Workstation, What, and Where. The results show a series of file deletions and session events for the user 'lepikhin' on various workstations.

On the right side, a summary panel provides details for the search results:

- Found in:** Who (25057)
- Who:** lepikhin (24869), Lyudmila Epikhina (188)
- Where:** SPB8766VM3.prod.quest.corp (15578), SPB9620 (8978), SPB8766VM2.prod.quest.corp (378), spb8552.prod.quest.corp (74), SPB8766VM2 (33)
- What:** Logon (5225), Logoff (5213), Special Privileges assigned (5134), File/Folder Access (4601), Object Access (2698)

Куда имеют доступ пользователи?

The screenshot displays the Dell InTrust IT Search web interface. The browser address bar shows the URL: `https://localhost/#/search/files?q=Who:%22Lyudmila%20Epikhina%22%20.xlsx&p=3`. The interface includes a navigation sidebar on the left with categories: Users (0), Groups (0), Computers (0), Shares (0), Files (2), and Events (579). The main content area shows a search for "Who: 'Lyudmila Epikhina' .xlsx" with 2 results found. The results are listed in a table with columns for Computer and Path.

Computer	Path
SPB9620.PROD.QUEST.CORP	C:\Department Documents\Accounting\Balance Sheet.xlsx
SPB9620.PROD.QUEST.CORP	C:\Department Documents\IT\Plans\IT Search Deployment plan.xlsx

On the right side, a summary panel provides details for the found items:

- Found in:**
 - Path (2)
 - Permission (2)
- Computer:**
 - SPB9620.PROD.QUEST.CORP (2)
- Type:**
 - File (2)
- Account:**
 - PROD\epikhin (2)
 - SPB9620\Administrators (2)
 - NT AUTHORITY\SYSTEM (1)
 - PROD\adelikan (1)
 - PROD\egusev (1)
- Access type:**
 - Allow (2)

Как они получили ЭТОТ доступ?

The screenshot shows the InTrust IT Search application interface. The search query is: `Where:"SPB9620.PROD.QUEST.CORP" AND Path="C:\Department Documents\Accounting\Balance Sheet.xlsx"`. The search results show a file named **Balance Sheet.xlsx** located at `C:\Department Documents\Accounting\Balance Sheet.xlsx. The file's metadata includes: Computer: SPB9620.PROD.QUEST.CORP, Size: 8929, Type: File, Created: 07/31/2014 2:53 PM, Last Accessed: 07/31/2014 3:22 PM, Last Modified: 07/31/2014 3:22 PM, and Owner: SPB9620\Administrators. The permissions tab is active, displaying a table of permissions for the file.`

Account	Access Type	Permissions	Inheritance
PROD\egusev	Allow	Full control	Inherited
PROD\lepikhin	Allow	Full control	Explicit
PROD\lepikhin	Allow	Read and execute	Inherited

Actions:

- > [Who accessed this file](#)
- > [Who granted permissions to this file](#)

Производительность

>10ТВ

Данных

3-10 сек

До появления первых
результатов

50.000

Событий в секунду

7 лет

Возраст данных

1-10 мин

Среднее время
расследования

900 DC
ИЛИ

6300 Рабочих
станций

20:1

Уровень сжатия
(с индексированием)

>100

Встроенных поисков

10-100 млрд

Событий

Сегодня: InTrust – единая точка поиска IT-данных

**Search and
Visualization**



InTrust v11

**Aggregation
Correlation and Storage**



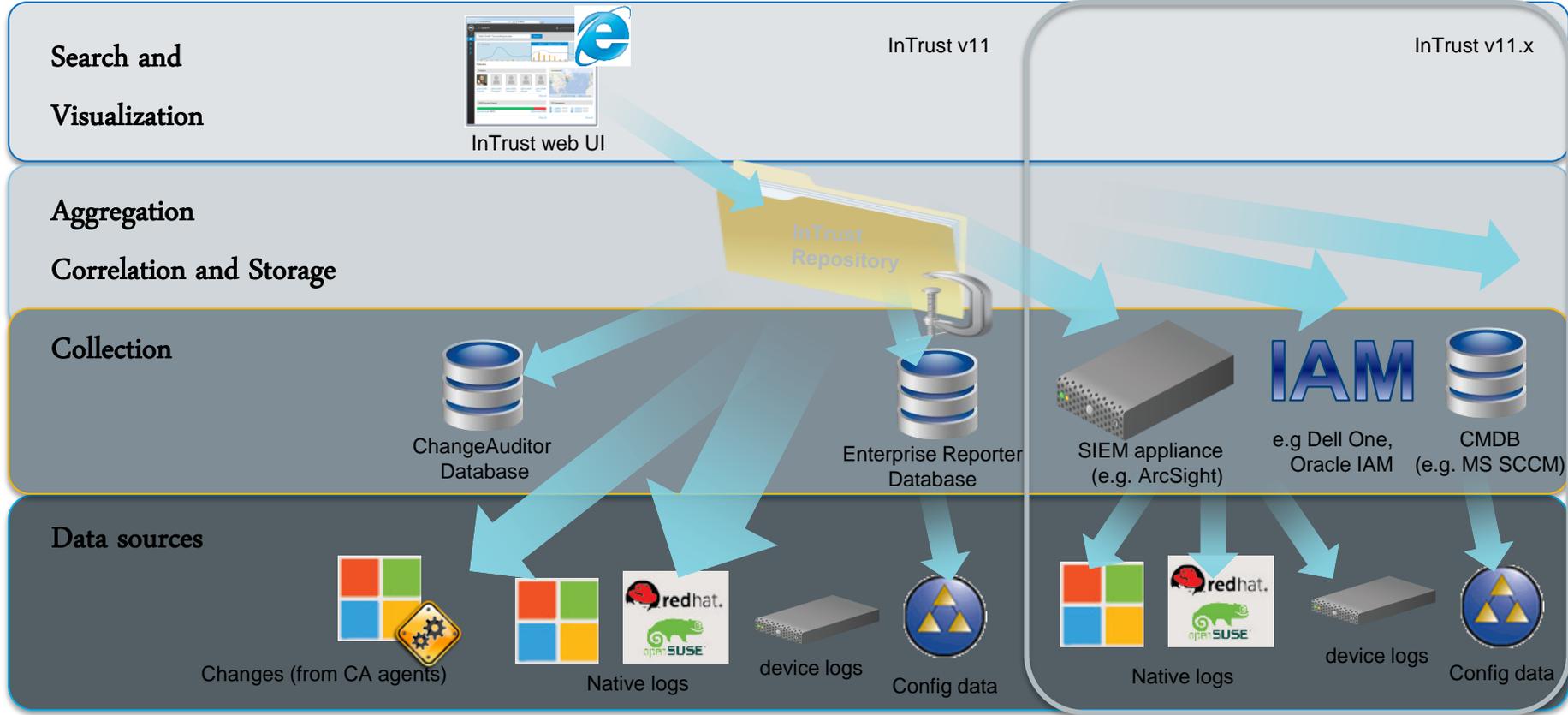
Collection

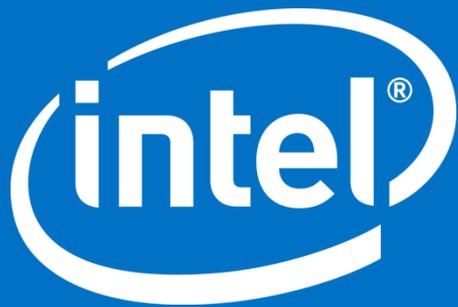


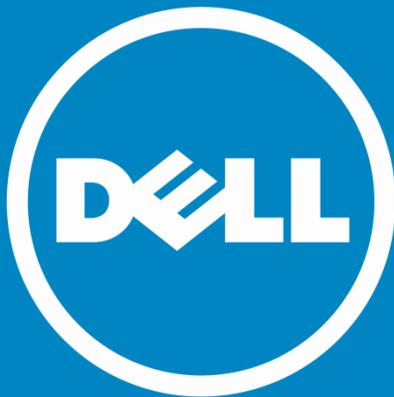
Data sources



Завтра: агрегация данных с не-Dell продуктов







The power to do more