

Unified User Management Win/Jet Connector Application Architecture

Version 1.3

Table of content

1	ABSTRACT	3
2	CUSTOMER CONDITIONS	3
3	KEY REQUIREMENTS	4
4	SOLUTION ALTERNATIVES	4
5	ASYMMETRIC REPLICATION CONNECTOR	5
6	JOMDEV WEBWARE'S UUM WIN/JET CONNECTOR	6
7	SAMPLE CONFIGURATION	7
8	HISTORY	8
9	RELATED DOCUMENTS	8

1 Abstract

Microsoft Access as well as applications using DAO, OLEDB, ADO or ADO+ interfaces to Jet databases rely on the Jet Engine's security services and user data repositories for authentication and access restriction purposes. This paper outlines how to integrate Jet user data management, i.e. workgroup file management into the companies core Windows user management to deliver enhanced functionality and lower total cost of ownership. This paper is written for readers who have a basic understanding of the Windows Server security architecture and the Jet Engine's security model as well.

2 Customer Conditions

Microsoft Access databases became pervasive throughout most organizations. With the rise of Microsoft Access as one of the premier Windows database management systems and the use of those databases in other applications such as Visual Basic, more and more mission critical information is being stored in them.

Due to the grown power of office technologies like Jet and the wide spread knowledge in scripting languages, IT departments increasingly often have to deal with a huge number of weakly designed quick-apps, typically built directly by LoB's. Many of these applications have become an important part in the corporation's day-to-day business but are hard to move to a reliable, scalable and secure operation when the number of users grows or users have to cooperate over net boundaries. Maintenance chores are extremely difficult to accomplish, because the popularity of distributed applications has led to a proliferation of repositories that contain similar information about users and resources. As users are added or updated, all these repositories must be kept up-to-date and synchronized with each other.

In the user account management domain of Jet based applications the system administrator's need is effectively addressed by *c:JAM - Central Jet Accounts Manager*. *c:JAM* helps IT professionals transferring Jet based applications to a secure, scalable and centrally managed operation. This document goes one step further and outlines how to integrate Jet user account management into the overall network administration.

Consolidated user account management is one of the most important aspects of information security in today's heterogenous client server environments. In several projects we experience an increasing need to connect Jet workgroup management to the companies *official* user information repositories. Implementing a consistent security management into a wide spread set of Jet databases is a challenge and will likely fail where not integrated into the organizations core IT processes.

3 Key Requirements

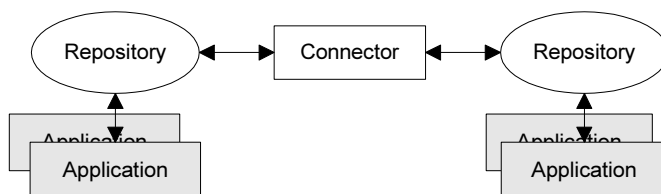
Consolidated user account management as outlined in this document should meet the following conditions

- Information about newly hired employees should be quickly propagated to all Jet based systems that require user authentication. The same process should be quickly performed in reverse when employees leave.
- Information about significant organizational, hierarchical as well as functional changes of employees should be as quickly propagated to all Jet based systems that require user authentication.
- Particular user management tasks may have to be delegated to local Access administrators. Fine tuning and selective overriding of general replication rules by Jet workgroup administration should be possible as well.
- Windows Server and Jet workgroup group accounts should not be enforced to have a one to one relationship or to be equally named. A configurable group mapping should allow for transformation of line group concepts (reflecting organizational structures) into functional group concepts (focussing on application roles).
- Hierarchical directory structures like domain trees and organizational units should be mappable to a single or specific sets of Jet workgroups as required. A topological translation virtually embodies hierarchical structures in a configuration of distributed Jet workgroups.
- The system should be ➤ simple, ➤ reliable, ➤ scalable and ➤ easily adoptable to organizational structures.

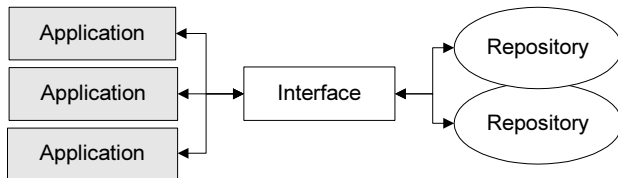
4 Solution Alternatives

Theoretically, the simplest unified user management solution is to have a single enterprise repository that holds all information about users, roles and applications in the company. For many reasons, including availability of suitable applications, particular security requirements and political issues, this goal will not be achieved quickly - if ever. Therefore companies have to look for solutions that link different user data repositories and applications together. With the assumption that repository data will continue to exist in many places, solutions must provide

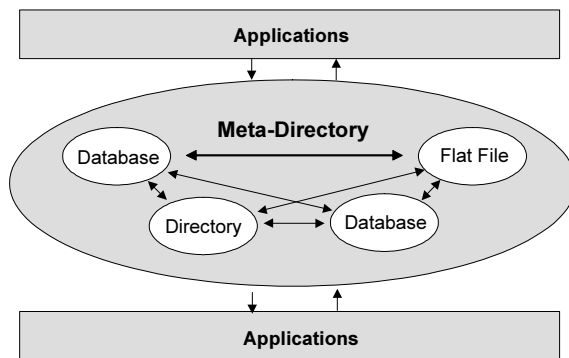
- **Replication** functionality, to distribute changes made in one directory or repository to other repositories in the enterprise affected by the change. Approaches focussed on techniques like this try to simplify management by keeping pairs of repositories synchronized



- **Connectivity**, to enable the sharing of user data between many different platforms, directories, databases or other kinds of repositories. Approaches focussed on techniques like this try to simplify writing applications and administrative scripts that are less dependent from specific platforms and may access multiple directory services and database technologies with a single programming interface



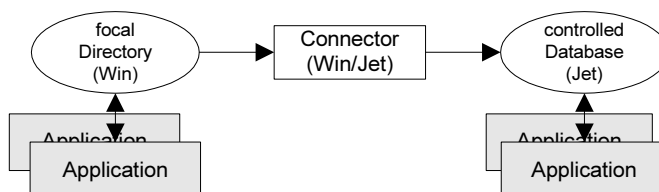
- **Data integrity** mechanisms, to enforce ownership rules and ensure that related user data remains consistent throughout the organization. Approaches combining data integrity management, replication and connectivity techniques try to encapsulate directories, databases, and other types of user data repositories into a 'directory of directories'. Given the complexity of the meta-directory challenge, however, such an approach may never be fulfilled.



Instead, companies should plan to implement a combination of techniques, ensuring that different platforms, directories and user data repositories can work together and that the total number of repositories that they need to manage is continuously reduced and consolidated in the long run.

5 Asymmetric Replication Connector

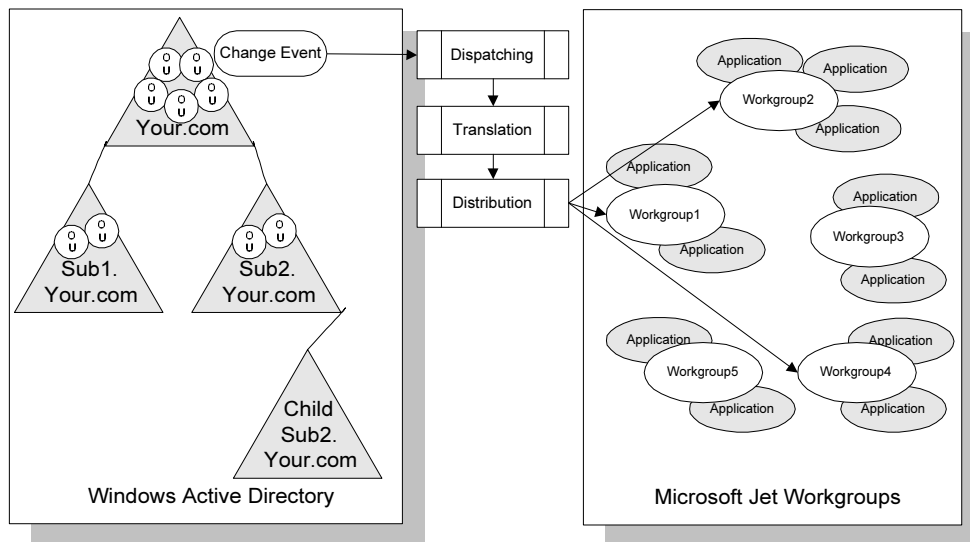
The solution presented in this paper makes use of an asymmetrical replication pattern between different repositories.



A replication connector is an application that knows how to recognize changes in one repository and propagate them to another one. Connectors are versatile enough, to handle situations where one side is a directory and the other is a database or an application specific repository. Connectors

simplify management by enabling administrators to designate one directory as management focal point where they make changes and rely on replication connectors to push the changes out to other repositories. Connectors typically maintain a one-to-one relationship, so organizations need a specific connector for each pair of repositories that they want to manage. A disadvantage may be, that they don't provide any functionality for single sign on approaches. On the other hand, because they require just installation and basic configuration, replication connectors also are quite simple to deploy.

A connector is responsible for change event processing. Change events occur any time administrators, applications or users somewhere add, delete, or modify user information data. Without the ability to detect and process changes, user information quickly becomes disorganized. Connectors therefore must provide features to detect changes, perform necessary data format and semantic translations, and then trigger related updates in all repositories that should reflect the change. For example, if an administrator adds a person to the development group in the product marketing department, this change event needs to cause any Microsoft Access application, that this person will use to reflect this addition.



6 Jomdev Webware's UUM Win/Jet connector

This guide outlines how to automate and control Jet workgroup management via connector by Windows Server user management. The outlined solution is not intended to replace the Jet workgroup repositories by one of the companies core directory services or to suspend the independence of the Jet engine's security system by any other means. Instead Windows Server user management events are replicated to a set of distributed Jet workgroups.

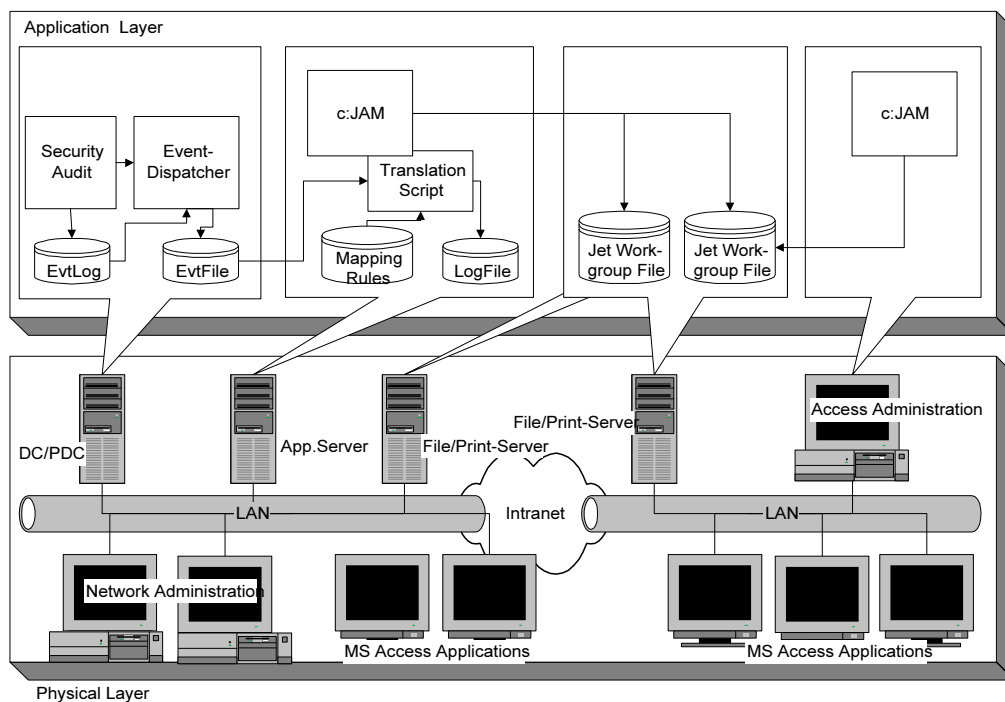
The UUM Win/Jet connector uses the built in Windows Server security auditing as its event source. Windows Server event auditing is as easily configurable in a Windows NT domain as in Active Directory or mixed environments and it is flexible enough to be easily adaptable to present and future directory topologies.

The UUM Win/Jet connector adds three components to the operating systems security auditing

- The **Event Dispatcher**, alerted by Windows Server audit events, analyzes the security event log, resolves internal identifiers (SIDs) and filters required events. The Event Dispatcher is implemented as a small Windows service with low resource consumption. The event log remains untouched.
- Translation is done by the **Translation Script**, a script which can be customized easily. Translation includes event mapping, group mapping and topological translation. This script is implemented as a set of VBScript methods and event procedures, stored in a c:JAM workgroup file. Group mapping rules are specified as simple ASCII files.
- Distribution is done by **c:JAM - Central Jet Accounts Manager**. The c:JAM shareware application is specifically designed to manage distributed Jet workgroups in medium and large networks. The workgroup configuration is maintained via the c:JAM GUI and stored in a single c:JAM workgroup file. A JScript and VBScript scripting and event handling engine is provided for customization and integration purposes.

7 Sample Configuration

The figure below outlines a sample Win/Jet Connector configuration, assuming a single user account domain topology and two Jet workgroup files residing on file-/print-servers in different LANs. The network administrations user management activities generate security audit events on the domain controller hosting the account domain (DC/PDC), where an instance of the Event Dispatcher is installed. The Event Dispatcher is alerted by these audit events, analyzes the security event log (EvtLog) and creates an event output file (EvtFile).



In the figure above an application server (App.Server) is used to run c:JAM as a background process. A c:JAM timer event periodically executes the Translation Script. This script takes the Event

Dispatcher's event output file and the mapping rule files as its input and causes c:JAM to distribute updates to the two configured Jet workgroup information files.

The sample configuration also assumes, that particular user management cases are delegated to a local Access administration. While all newly hired employees, which need access to Jet applications, are immediately provided with the required access permissions via the network administration, particular access permissions for developers are maintained by local Access administrators. In this sample configuration these Access administrators use c:JAM as their GUI to manage additional permissions.

8 History

The Win/Jet Connector has been developed in conjunction with a customer security project in 1998. The risk controlling department of a leading european bank group, dealing with many hundreds of Microsoft Access databases, assigned development and implementation of a consistent security management for their databases to the project. In 1999 the Win/Jet Connector has been put into production as part of the technical infrastructure of our project's results.

With the release of c:JAM v1.4 and it's build-in scripting support in Jan. 2000 the Win/Jet Connector has been redesigned and got a more simple architecture.

Due to engagements in other projects it has not been possible to bring UUM Win/Jet Connector to the market before the end of 2002. Now UUM Win/Jet Connector combines the maturity and simplicity of a turnkey business solution with high scalability, adjustability and the experience derived from customer projects.

9 Related Documents

Unified User Management. Win/Jet Connector. Product Specification

Unified User Management. Win/Jet Connector. Quick Start

Unified User Management. Event Dispatcher Service. Administration Guide

Unified User Management. Win/Jet Translation Script. Administration Guide

c:JAM – Central Jet Accounts Manager. Online Documentation