abrideanProvisor's Support of Exchange Resource Forests

Introduction

abrideanProvisor supports a wide range of Active Directory and Exchange configurations. For instance, Provisor can host multiple organizations concurrently in a single AD domain, while maintaining full segregation between the organizations. A typical example of this scenario would be a service provider environment. Provisor also supports deployments involving a single forest with a single domain or a single forest with child domain(s), as well as multi-forest deployments.

Although Active Directory facilitates consolidation of domains and forests many organizations choose to retain a multi-forest environment. There are multiple reasons why these companies retain a multi-forest environment, but they are generally either security-related or driven by operational processes.

Security Related Concerns:

- ✓ Need to limit the number of users and administrators having access to each environment
- ✓ Allow administrators to maintain full control over their own domains
- ✓ Avoid dependency on a centralized directory

Operational Processes:

- ✓ Existing applications and processes may require a specific domain name
- ✓ Excessive cost to modify the architecture and re-train users
  - Migration of users to new domains
  - Changes to user logins
  - Definition of new administrative roles
- ✓ Limit schema modifications to specific domains

It is challenging for organizations with multi-forest configurations to deploy a single, centralized Exchange solution due to the tight integration between Exchange and Active Directory. This tight integration also poses a challenge to organizations using a single forest environment if Active Directory cannot have its schema modified or if security/operational concerns inhibit Exchange Administrators from having access to Active Directory.

The above scenarios can be resolved through the creation of an Exchange Resource Forest (ERF) by using the ERF as a deployment option, organizations can resolve both their security and operational issues while at the same time centralizing Exchange.

Exchange Resource Forest

An Exchange Resource Forest is a Microsoft deployment option for centralizing Exchange messaging within an organization, while still maintaining one or more independent Active Directory domains for employee network access. This scenario is common in large enterprises or in disparate organizations where the enterprise is comprised of many independent departments or companies, each with its own IT department and Active Directory domains, yet still wishing to centralize their Exchange Messaging while minimizing the impact on employees.

The Exchange Resource Forest consists of an AD domain that is dedicated to running Exchange and is separate from the external AD domain(s) where the users are located. For every user account that exists in the external AD domain(s), an equivalent "placeholder" user account is created in the ERF and provisioned with a mailbox. The mailbox rights settings for each mailbox can be modified to allow access by the original user in the external AD domain. A one-way trust is established between the ERF and the external AD domains so users that authenticate to an external AD domain automatically gain access to the ERF environment. The security of the external AD domain is preserved since user and administrative accounts in the ERF environment do not automatically link back to the external AD domain.

Benefits of Using an Exchange Resource Forest

Improved Security

- ✓ Any errors or problems in the ERF are independent and have no impact on the corporate AD domain(s).
- ✓ The ERF ensures that the schema of the external AD domain(s) is/are not modified by installing Exchange or any other messaging/collaboration-related utilities.
- ✓ Exchange and AD administrators have access only to the resources they need to mange their environments.

Simplified Administration:

- ✓ Exchange managers are given complete control of Exchange without having to involve AD managers.
- ✓ AD managers can administer their own respective environment without involving Exchange managers.

Improved Employee Experience

- ✓ Users experience single sign-on authentication, since they only need to log on to the corporate AD to get access to their e-mail. They do not need to log into a separate mail service.

Challenges of Using an Exchange Resource Forest

When using an Exchange Resource Forest, organizations typically face the challenge of efficient and effective deployment and ongoing management.

- ✓ The set-up of a new employee requires that an account be created in both the relevant corporate domain and in the ERF.

- ✓ Mailbox creation is manually intensive
  a. The placeholder account in the ERF domain must be created, and then disabled to improve security.
  b. Each new placeholder account must be mail enabled.
  c. The mailbox rights for this account must be set correctly so that the user from the external AD domain has full access and is the owner of the mailbox. This is potentially an error prone task, and mistakes can

result in the user not having access to e-mail, or create a security breach with the wrong user gaining access to another user's e-mail.

d. Address Books must be maintained for each segregated business unit, as well as across the enterprise. This may involve complicated naming standards and setting special attributes in Active Directory on the accounts specifically for this purpose.
e. Distribution Lists must be managed from the ERF domain. Administrators from each company or division typically require access to the common ERF domain to do this, posing security concerns.

- ✓ When a user is removed from a corporate AD domain, the equivalent user account in the ERF needs to be manually removed and/or archived.

- ✓ Administration of mailbox settings must occur within the ERF domain, requiring a delegated administration tool for enabling this in a secure manner.

abrideanProvisor and the Exchange Resource Forest

Provisor offers an easy-to-use interface for the deployment and ongoing management of the Exchange Resource Forest.

Automate Manual Processes

- ✓ Provisor automates account setup and mailbox creation, as well as the creation of mailbox rights to enable the mailbox owner appropriate user access. This reduces administrative workload and prevents data entry errors and security breaches resulting from inaccurate manual data entry.
- ✓ Provisor also automates and enforces naming conventions, including setting specific attributes to help manage address book membership based on the users' department or business unit.

Improve Security & Performance

- ✓ Provisor offers a web based administration interface for different levels of responsibility. Security roles enable secure delegation of mailbox management. Individual companies or departments are allowed to manage only their own users' mailboxes without affecting or tampering with others.
- ✓ Provisor can be used to delegate management of accounts in both the corporate AD domain and the ERF. This allows the two account sets to be synchronized, which avoids unnecessary licensing costs and eliminates security vulnerabilities due to dormant accounts.