Active Directory Domains and Forests Concept for DeltaV™ Systems

This white paper provides information about Active Directory Domains and Forests concept applied to DeltaV™ systems.
Table of Contents

Introduction .................................................................................................................................................................................. 3
Domains and Forests within DeltaV systems................................................................................................................................ 3
DeltaV systems configuration to allow single sign-on through two-way trust between Forests .............................................. 6
Conclusion .................................................................................................................................................................................. 9
Introduction

Active Directory (AD) was introduced with the release of the Microsoft Windows Server 2000 operating system, and since then supported by Emerson in order to allow DeltaV systems to be deployed in domain environments, primarily for security purposes – but also to simplify the integration of several endpoints on larger networks.

It is assumed that the intended reader of this document is familiar with Active Directory (Domains and Forests). The concept of Parent/Child relationships among domains is not covered in this document neither – please refer to the white paper “The Pros and Cons of DeltaV as a Child Domain” for more information on this specific topic.

Domains within the same Forest cannot be considered completely isolated as there are many inherent connections between those domains that cannot be removed. The concept of Forests actually creates the security boundaries necessary to control the access permissions to the directories between domains.

DeltaV systems work in conjunction with certain AD features to provide a more secure and manageable production environment. This document describes the configuration changes pertaining to DeltaV software that need to be considered in order to enable two-way trust between DeltaV systems and a root Forest and allow customers to enjoy a single sign-on experience throughout the Forests.

For security reasons Emerson recommends to deploy each DeltaV system on its own Forest/domain without any type of relationship with other Forests/Domains.

Domains and Forests within DeltaV systems

Standard supported deployments would have individual domains for each DeltaV installation (single System ID) with its own set of domain Controllers (primary and backup). In most of the cases the domains are also part of their own individual Forests, hence no implicit trust is per default set between them, which would mean that each System ID (own domain / Forest) has its own users within that scope.

Figure 1 – Domains and Forests with no trust.

Whenever single sign-on is required for multiple DeltaV System IDs, customers would normally pick one of the two options listed below:

- Establish a parent/child relationship (domain tree) within the same forest;
- Establish a trust between different Forests containing single DeltaV domains.

A single Forest with implicit trust between different domains is not currently supported as each DeltaV System ID utilizes the same IP range set for the DeltaV endpoints and embedded nodes, hence IP duplication would cause DNS (Domain Name System) issues that would need to be remediated by means of an engineered solution.

As mentioned previously, the parent/child approach will not be covered in this white paper, but on Figure 2 you can see the representation of multiple Forests and established two-way trusts between them, which is the main topic of this white paper.
Although a single Forest has implicit trust between domains (no need for additional configuration), the domains are not considered security boundaries and therefore each DeltaV System ID / installation would need to be implemented in different Organizational Units within the AD concept so that specific management and security policies are handled on a per system basis rather than globally within the Forest context.

In the other hand, the Forests are security boundaries and therefore each DeltaV System ID has its own management and security policies in place. As highlighted in Figure 3, a system administrator of Forest 1 is not inherently able to manipulate Forest 2’s security policies, nor vice-versa, which instead is possible on a single Forest approach by design. The caveat here is that transitive two-way trust between Forests needs to be manually configured and appropriate measures should be in place to make sure cross-forest administrator privileges are not provided inadvertently during system configuration.
When Forests are connected by a Forest Trust, the authentication requests are routed between Forests to provide access to resources in both Forests. However, it is important to emphasize that Forest Trusts can only be established between Forest Root domains which is not an issue here since the DeltaV System ID domain is also the Forest Root Domain on our use cases.

Once the trust is established and the DeltaV configuration is adjusted to meet the single sign-on behavior, the user credentials within the main automation Forest are used to log into the DeltaV systems within any other Forest that has an established trust to the main automation one. Figure 4 illustrates this scenario where the main automation Forest does not have to be running DeltaV applications necessarily. This concept also allows for multi-vendor integration since the individual Forests are not shared in regards to management and security policies.

Figure 4 – Main Automation Forest connected to DeltaV systems.
DeltaV systems configuration to allow single sign-on using two-way trust between Forests

The steps below do not show how to deploy individual Forests nor how to establish a two-way trust between Forests since these are standard steps pertaining to the operating system. Instead we are highlighting the additional steps that are required within DeltaV systems to make sure the single sign-on experience can be achieved by means of two-way trust established between Forests. For this example, we are considering a simplified sketch based on two Forests with a single domain each: DEMO.System and ICS.Automation.

Figure 5 shows the creation of new user accounts within the ICS.Automation domain which will be used to log into any other Forests to which a two-way trust is establish with (the Demo System in this case):

Figure 5 – Accounts creation within the main automation Forest.
Once created the users need to be added to the corresponding DeltaV groups within the DeltaV Forests (Demo System in this case). This step is done within the DeltaV Forest Active Directory Users and Computers applet.

**Figure 6 – Adding main automation Forest users to the DeltaV Groups.**

The next step is to ‘Allow log on locally’ to the new users which shall be added to the Local Group Policies within the DeltaV Forest (Computer Configuration / Windows Settings / Security Settings / Local Policies / User Rights Assignment).

**Figure 7 – Allow log on locally for the created users within the main automation Forest.**
The final step is to create DeltaV database accounts using DeltaV User Manager within each DeltaV system Forest, and associate them with the main automation Forest domain name (ICS Automation in this case). The new DeltaV database accounts shall NOT be assigned to a local Windows account.

![Figure 8 – DeltaV database account creation.](image8.png)

Figures 9 and 10 show how a user configured at the main automation Forest (username: Jake) experiences the logon process into the DeltaV system Forest (Demo System).

![Figure 9 – New user logon experience.](image9.png)
Conclusion

We highly recommend the use of domain environments for DeltaV systems, and Forest Trusts should only be used if required and should be implemented accordingly, following a thorough system design to make sure the security posture is considered at all levels of the system.

Single sign-on is a solution for convenience, but it may also impose a security issue that needs to be evaluated carefully. If credentials are compromised in this specific case where trusts are established across multiple Forests, multiple systems can be compromised with a single exploit.

Special care is required during upgrades and migrations since most of the settings to allow the two-way trust to work correctly with DeltaV systems are performed manually and not covered by the DeltaV system upgrade tools.

It is important to emphasize that DNS plays an important role in the effective implementation of domains and Forests connections, and within AD environments in general. Please make sure DNS is also included in the thorough system design prior to implementing the Forest Trusts in your systems.