

Active Directory Domain Services (ADDS)

Novedades – Instalación – Configuración – RBAC -
Troubleshooting



TecTimes
Blog de Tecnología

Detalles del Evento

El 04 y 05 de Marzo de 2013 se realizó, en la Ciudad de Buenos Aires, un encuentro de capacitación que contó con la presencia de profesionales de la Administración de Tecnologías Microsoft y Consultoría IT, cuyo tema central fue la tecnología Active Directory Domain Services de Windows Server 2012.

La capacitación tuvo una duración de 6 horas distribuidas en dos jornadas. El orador fue Pablo Ariel Di Loreto y participaron profesionales de distintas empresas de Tecnología y Servicios IT de la Ciudad de Buenos Aires.

Si deseás recibir más info y/o los materiales del evento, contactate por los siguientes medios:

- Email: pablodiloreto@Hotmail.com
- Twitter: [@PabloDiLoreto](https://twitter.com/PabloDiLoreto)
- Web: <http://www.tectimes.net>

Agenda

- Objetivo.
- Alcance.
- Presentación de Roles de Active Directory.
- Introducción a Active Directory Domain Services.
- Roles FSMO en Active Directory Domain Services.
- IPD de Active Directory Domain Services.
- Lab: Instalación de ADDS en Windows Server 2012.
- Lab: Configuración Ejemplo de ADDS.
- Lab: RBAC en ADDS.
- Lab: Troubleshooting de ADDS.
- Cierre.

Objetivo



- Conocer los conceptos fundamentales de Active Directory Domain Services en Windows Server 2012.
- Conocer las directivas fundamentales de Planeamiento y Diseño de ADDS.
- Conocer las premisas de RBAC en ADDS.
- Conocer el troubleshooting básico de ADDS.

Alcance

- Presentación teórica de ADDS en Windows Server 2012.
- Lab de Instalación de ADDS en Windows Server 2012.
- Lab de ejemplo ADDS en Windows Server 2012.
- Lab de Troubleshooting básico para ADDS en Windows Server 2012.



Presentación de Roles de Active Directory

ADCS, ADDS, ADFS, ADLDS, ADRMS

Roles de Active Directory

¿Cuáles son los Roles de Active Directory?

(ADCS) ACTIVE DIRECTORY
CERTIFICATE SERVICES

(ADDS) Active Directory
Domain Services

(ADFS) Active Directory
Federation Services

(ADLDS) Active Directory
Lightweight Directory Services

(ADRMS) Active Directory
Rights Management Services

Introducción a ADDS

Introducción a Active Directory Domain Services.

Introducción a ADDS

Definición y Funcionamiento de ADDS

¿Qué es Active Directory Domain Services?

¿Cómo funciona Active Directory Domain Services?

Introducción a ADDS

Definición y Funcionamiento de ADDS

¿Qué es Active Directory Domain Services?

- Es la implementación de Microsoft del servicio de directorio en una red distribuida de computadoras.

¿Cómo funciona Active Directory Domain Services?

Introducción a ADDS

Definición y Funcionamiento de ADDS

¿Qué es Active Directory Domain Services?

- Es la implementación de Microsoft del servicio de directorio en una red distribuida de computadoras.

¿Cómo funciona Active Directory Domain Services?

- Similar a otras estructuras LDAP (Lightweight Directory Access Protocol).
- Base de datos centralizada.
- Objetos.
- Control, Administración y Consulta.

Introducción a ADDS

Elementos y Características de ADDS

¿Qué elementos componen a Active Directory?

¿Qué características analizaremos de ADDS?

Introducción a ADDS

Elementos y Características de ADDS

¿Qué elementos componen a Active Directory?

- El Bosque.
- Los Dominios.
- Las OUs.
- La Autenticación..

¿Qué características analizaremos de
ADDS?

Introducción a ADDS

Elementos y Características de ADDS

¿Qué elementos componen a Active Directory?

- El Bosque.
- Los Dominios.
- Las OUs.
- La Autenticación..

¿Qué características analizaremos de ADDS?

- El Esquema (Schema).
- El Catálogo Global (Global Catalog).
- Servicio de Replicación.
- Roles de Maestro (FSMO).

Introducción a ADDS

Bosques y Dominios en ADDS

¿Qué es un Forest de Active
Directory?

¿Qué es un Domain de Active
Directory?

Introducción a ADDS

Bosques y Dominios en ADDS

¿Qué es un Forest de Active Directory?

- Es el límite de seguridad de nuestra infraestructura de Active Directory Domain Services. Puede tener uno o más Dominios.

¿Qué es un Domain de Active Directory?

Bosques y Dominios en ADDS

¿Qué es un Forest de Active Directory?

- Es el límite de seguridad de nuestra infraestructura de Active Directory Domain Services. Puede tener uno o más Dominios.

¿Qué es un Domain de Active Directory?

- Es el límite de administración de nuestra infraestructura de Active Directory Domain Services.

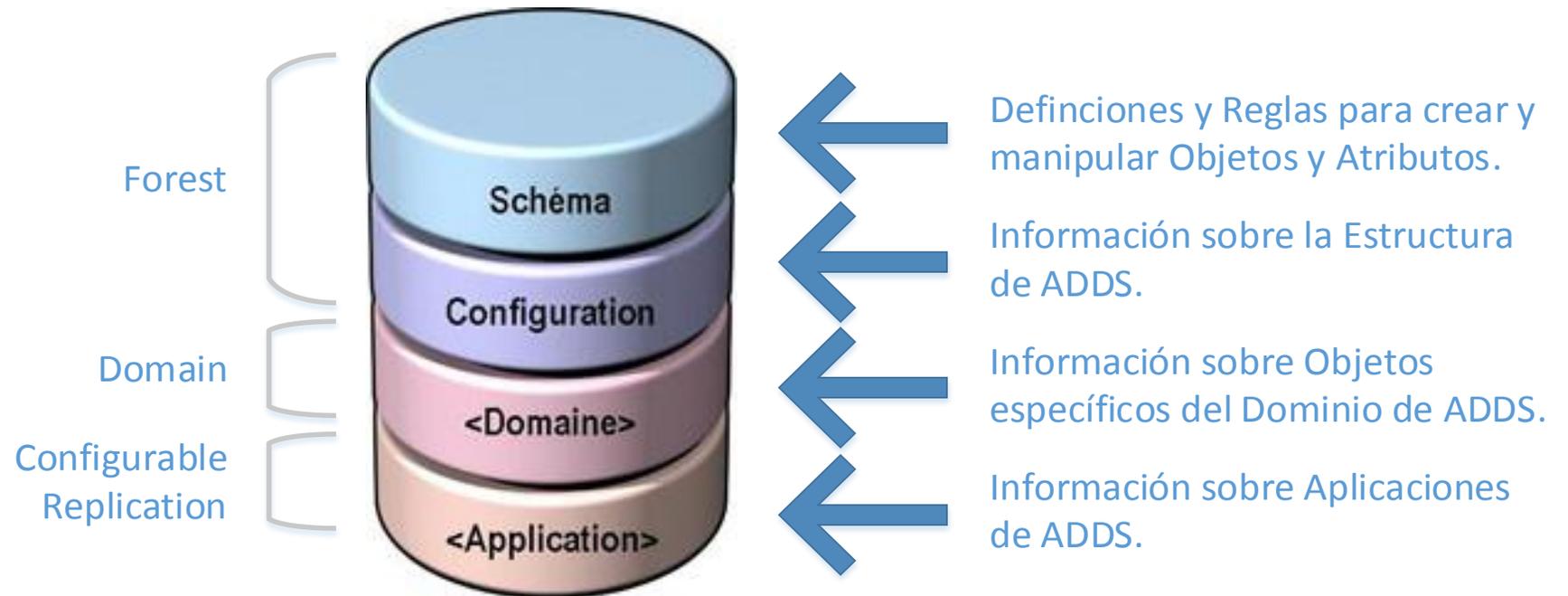
Introducción a ADDS

Particiones de ADDS



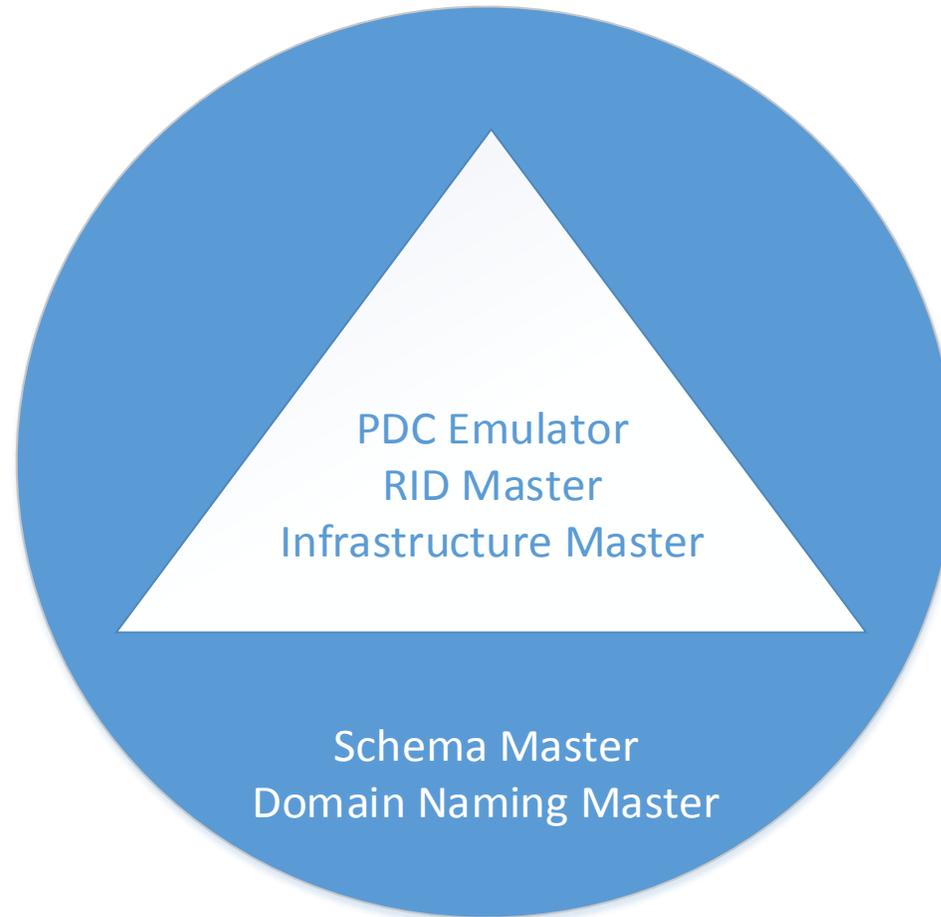
Introducción a ADDS

Particiones de ADDS



Introducción a ADDS

Roles FSMO



Roles FSMO – Schema Master

- Solo un controlador de dominio a nivel bosque (del Forest Root Domain) lo puede albergar.
- Es el responsable de procesar cualquier cambio que se realice en el Esquema de Active Directory, sin importar desde donde se lance el cambio (desde que equipo).
- La ausencia de éste rol en la operatoria diaria puede pasar desapercibido, debe estar disponible cuando son necesarios realizar cambios en el Esquema de Active Directory.
- La no disponibilidad del rol genera errores en los updates de esquema, por ejemplo si estamos realizando los cambios en una instalación de Exchange Server.

Introducción a ADDS

Roles FSMO – Domain Naming Master

- Solo un controlador de dominio a nivel bosque (del Forest Root Domain) lo puede albergar.
- Es el responsable de procesar las adiciones y remociones de dominios y particiones de aplicación en un bosque.
- La ausencia de éste rol en la operatoria diaria puede pasar desapercibido, debe estar disponible cuando se agregan o quitan dominios o aplicaciones que requieran cambios en la partición de aplicación.
- La no disponibilidad del rol genera la imposibilidad de agregar o quitar dominios del forest o modificar la partición de aplicación.

Introducción a ADDS

Roles FSMO – PDC Emulator

- Solo un controlador de dominio a nivel dominio lo puede albergar.
- Recibe las actualizaciones de contraseñas cuando son cambiadas por la computadora del usuario y por cuentas de usuario del resto de los DCs.
- Recibe consultas por el resto de controladores de dominio ante eventos de ingreso erróneo de contraseñas.
- Es el controlador de dominio destino por defecto ante cambios en GPOs.
- Es el controlador de dominio destino por defecto para aplicaciones que realizan operaciones de escritura sobre el servicio de directorio.
- Es el controlador de dominio destino por defecto para algunas herramientas administrativas de Active Directory.
- Mantiene la coordinación de hora para el dominio, en el que se basan las decisiones para identificar el último horario de escritura para objetos.
- Es utilizado por equipos clientes que no soportan el esquema multi-master, como Windows 98.

Roles FSMO – PDC Emulator

- La ausencia de éste rol en la operatoria diaria no pasa desapercibido y puede generar algunos dolores de cabeza a los administradores. Es recomendable que esté online las 24 horas del día los 365 días del año.
- La no disponibilidad del rol genera:
 - Demoras ante ingresos erróneos de contraseña.
 - No-coordinación de horario entre controladores de dominio.
 - No-operación de algunas herramientas administrativas de Active Directory.
 - Errores en la herramienta “Entorno de Red” en equipos con hasta Windows 2003 y XP.
 - Otros dolores de cabeza en la operatoria diaria!

Roles FSMO – RID Master

- Solo un controlador de dominio a nivel dominio lo puede albergar.
- Es el responsable de alocar los grupos activos y en espera de RID (Relative Identifier) a los restantes DCs.
- La ausencia de éste rol en la operatoria diaria puede pasar desapercibido, debe estar disponible cuando se asignan RIDs.
- Cuando un controlador de dominio tiene pocos RIDs disponibles, éste le debe solicitar al RID Master otro rango de RIDs.
- Cuando se promueve un nuevo controlador de dominio en un dominio existente, de no estar disponible este rol dicho controlador de dominio generará errores.

Introducción a ADDS

Roles FSMO – Infrastructure Master

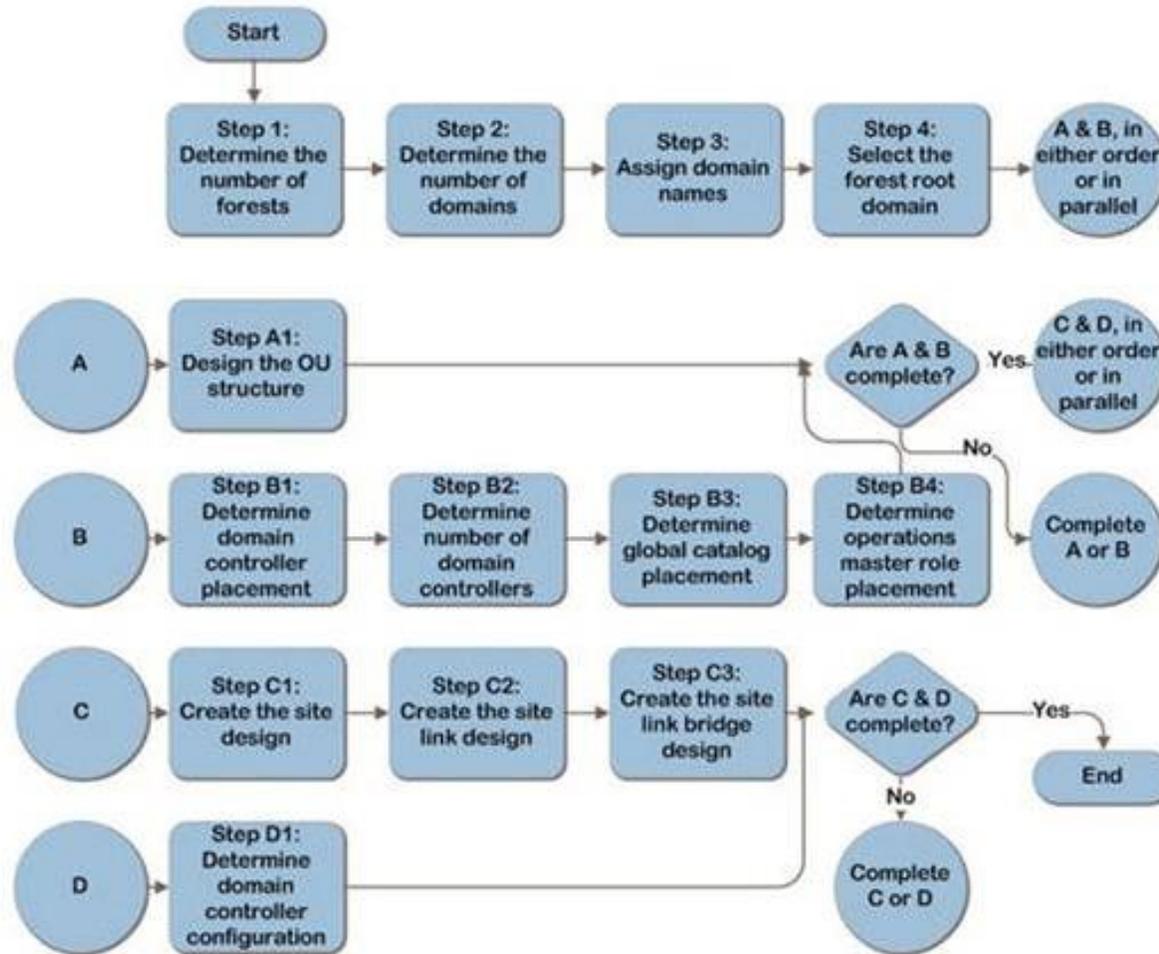
- Solo un controlador de dominio a nivel dominio lo puede albergar.
- Es el responsable de actualizar las referencias entre dominios.
- Es el responsable de traducir los SID a nombres en las referencias de cuentas entre dominios.
- La ausencia de éste rol en la operatoria diaria puede pasar desapercibido, salvo en casos de cambios de referencias o pertenencias a grupos de usuario entre dominios.
- La no disponibilidad de este rol puede provocar que las referencias a objetos entre dominios no muestre los datos del usuario, sino su SID.

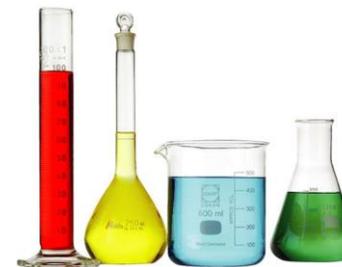
IPD de Active Directory Domain Services

Infrastructure Planning & Design for ADDS

IPD de ADDS

Presentación de flujo de IPD for ADDS





Lab: Instalación de ADDS

Instalación de ADDS en Windows Server 2012

Lab: Instalación

Alcance del Laboratorio:

- Instalación del rol ADDS en Windows Server 2012



Lab: Configuración

Lab: Configuración Ejemplo de ADDS

Lab: Configuración

Alcance del Laboratorio:

- Configuración de OUs ejemplo.
- Configuración de Políticas Básicas.



Lab: RBAC en ADDS

RBAC en ADDS

Lab: Configuración

Alcance del Laboratorio:

- Delegación de Tareas Administrativas para ADDS.



Lab: Troubleshooting de ADDS

Troubleshooting básico para ADDS

Lab: Configuración

Alcance del Laboratorio:

- Comandos básicos de Troubleshooting para ADDS.

Gracias!!



TecTimes

Blog de Tecnología

<http://www.tectimes.net/>

Datos de Contacto

- Email: pablodiloreto@Hotmail.com
- Twitter: [@PabloDiLoreto](https://twitter.com/PabloDiLoreto)
- Web: <http://www.tectimes.net>