Policy for Deployment and Management of Active Directory Services

University of the Western Cape Policy *ICS/2004.03*

Background

This document provides a policy for the deployment and usage of additional Active Directory infrastructures within the University of the Western Cape environment. The document is broken down into the Logical, Physical and Services Design sections. This document must be read and adhered to by anyone wishing to create additional Active Directory environments within the University of the Western Cape.

Scope

The Active Directory Policy provides requirements regarding the establishment of active directory infrastructure using:

- Microsoft Windows servers;
- SAMBA servers running on non-Microsoft systems such as GNU/Linux, BSD Unix, and Macintosh OS-X and up.

Design Concepts

1.1 Logical Design

UWC has single forest and a single domain structure to provide enterprise wide Active Directory services.

If the requirement arises for additional and/or separate Active Directory environment(s), the following options are available:

1.1.1 New Forest and Domain

This option will create a new Active Directory Forest and Domain, which allows for future logical expansion capabilities.

If the requirement for a separate Active Directory Forest exists, the following must be adhered to:

- The DNS namespace for the proposed forest must be unique. Currently the AD.UWC.AC.ZA and UWC.AC.ZA DNS namespaces are in use and cannot be duplicated.
- The NetBIOS name for the proposed forest must be unique. Currently the ADUWC NetBIOS name is in use and cannot be duplicated.
- In order to facilitate correct name resolution and resource access within the new forest, the correct DNS infrastructure must be established.
- If the requirement for resource access between the existing and the new forest exists, then the appropriate trust relationships and security measures must be established. Additionally, the appropriate name resolution infrastructure must be established.
- Administrative users within the newly created forest will have autonomous control of the forest. No delegation of authority is required.

1.1.2 New Tree within the existing AD.UWC.AC.ZA forest

This option will create a new Active Directory Tree within the existing production forest.

If the requirement for a separate Active Directory Tree exists, the following must be adhered to:

- The Active Directory namespace for the proposed Tree must be unique in the forest.
- Currently the AD.UWC.AC.ZA and UWC.AC.ZA DNS namespaces are in use and cannot be duplicated.
- The NetBIOS name for the proposed Tree must be unique. Currently the ADUWC NetBIOS name is in use and cannot be duplicated.
- In order to facilitate correct name resolution and resource access within the new Tree, the correct DNS infrastructure must be established.
- In order to create the new Tree within the existing forest, a user with sufficient administrative rights in the existing forest is required.
- If Schema modifications are required as a result of the creation of the new Tree or to facilitate resources within the new Tree, this must be performed at forest level on the Schema Master FSMO Role holder. Due to the nature and impact of such changes, proper change control mechanisms must be adhered to. A user with sufficient administrative rights in the existing forest is required.
- Administrative users within the newly created Tree will have autonomous control of the Tree. No delegation of authority is required.
- Enterprise administrators residing in the forest root domain will retain autonomous control over the entire forest, including the newly created Tree

1.1.3 New Domain within the existing AD.UWC.AC.ZA forest

This option will create a new Active Directory Child Domain within the existing production forest.

If the requirement for a separate Active Directory Child Domain exists, the following must be adhered to:

- The Active Directory namespace for the proposed Child Domain must be unique in the forest.
- The Active Directory namespace for the proposed Child Domain must be a child of the existing AD.UWC.AC.ZA domain.
- Currently the AD.UWC.AC.ZA and UWC.AC.ZA DNS namespaces are in use and cannot be duplicated.
- The NetBIOS name for the proposed Child Domain must be unique. Currently the ADUWC NetBIOS name is in use and cannot be duplicated.
- In order to facilitate correct name resolution and resource access within the new Child Domain, the correct DNS infrastructure must be established.
- In order to create the new Child Domain within the existing forest, a user with sufficient administrative rights in the existing forest is required.
- If Schema modifications are required as a result of the creation of the new Child Domain or to facilitate resources within the new Child Domain, this must be performed at forest level on the Schema Master FSMO Role holder. Due to the nature and impact of such changes, proper change control mechanisms must be adhered to. A user with sufficient administrative rights in the existing forest is required.
- Administrative users within the newly created Child Domain will have autonomous control of the Child Domain. No delegation of authority is required, but is possible.
- Enterprise administrators residing in the forest root domain will retain autonomous control over the entire forest, including the newly created Child Domain.

1.1.4 New Organizational Unit (OU) within the existing AD.UWC.AC.ZA Domain

This option will create a new Active Directory OU within the existing production Domain.

If the requirement for a separate Active Directory OU exists, the following must be adhered to:

- The name for the proposed OU must be unique within the domain.
- In order to create the new OU within the existing domain, a user with sufficient administrative rights in the existing forest is required.
- If Schema modifications are required as a result of the creation of the new OU or to facilitate resources within the new OU, this must be performed at forest level on the Schema Master FSMO Role holder. Due to the nature and impact of such changes, proper change control mechanisms must be

adhered to. A user with sufficient administrative rights in the existing forest is required.
- In order to facilitate a distributed (delegated) administrative model for this OU, administrative users can be delegated sufficient rights for the OU.
- Domain administrators residing in the domain will retain autonomous control over the entire domain, including the newly created OU.
- Enterprise administrators residing in the forest root domain will retain autonomous control over the entire forest, including the newly created OU.

1.2.3 New Active Directory Subnet

This option is available when creating a new Forest, Tree or Child Domain. If a new Active Directory Subnet is created, the following must be adhered to:

- The Active Directory Subnet name must be unique within the forest.
- In order to create the new Subnet and associate the Subnet with an Active Directory Site, a user with sufficient administrative rights in the forest is required.

1.2.4 Existing Active Directory Subnet

If an existing Active Directory Subnet is to be used, the following must be adhered to:

- The IP address structure of the new computers must adhere to the existing Active Directory Subnet classifications as defined in the existing Forest.

1.3 Active Directory Services

1.3.1 Domain Name System (DNS)

1.3.1.1 New Active Directory Forest

When a new Active Directory Forest is created,

- a Stub Zone for this DNS namespace must be created on the existing Unix BIND DNS server.
- The Stub Zone will reference the authoritative DNS servers for the new Forest.

1.3.1.2 New Tree within the existing AD.UWC.AC.ZA forest

When a Tree is created within the existing Active Directory Forest,

- a Stub Zone for this DNS namespace must be created on the existing Unix BIND DNS server.
- The Stub Zone will reference the authoritative DNS servers for the new Tree.
- In order to create the new zone and a user with sufficient administrative rights in the forest is required.

1.3.1.3 New Child Domain within the existing AD.UWC.AC.ZA forest

When a Child Domain is created within the existing Active Directory Forest,

- a Stub Zone for this DNS namespace must be created on the existing Unix BIND DNS server.
- The Stub Zone will reference the authoritative DNS servers for the new Child Domain.
- In order to create the new zone and a user with sufficient administrative rights in the forest is required.

1.3.2 Dynamic Host Configuration Protocol (DHCP)

- No DHCP server may be installed to facilitate new Active Directory Forests, Trees or Domains. The Enterprise DHCP server currently established will be utilized for all dynamic IP configurations.
- If a separate IP address structure is required, an IP address range will need to be acquired and assigned.

1.3.3 Windows Internet Name Service (WINS)

- The WINS service would only be required to support backward compatibility to legacy operating systems and services requiring NetBIOS name resolution.
- The WINS server IP address can be made available using the DHCP scope options or manually, as required.

1.3.3.1 New Active Directory Forest

- When a new Active Directory Forest is created, the NetBIOS names will be registered with the enterprise WINS server in the existing forest for NetBIOS name resolution.

1.3.3.2 New Tree within the existing AD.UWC.AC.ZA forest

- When a new Active Directory Tree is created, the NetBIOS names will be registered with the enterprise WINS server in the existing Active Directory Forest for NetBIOS name resolution.

1.3.3.3 New Child Domain within the existing AD.UWC.AC.ZA forest

- When a new Active Directory Tree is created, the NetBIOS names will be registered with the enterprise WINS server in the existing Active Directory Forest for NetBIOS name resolution.

1.4 Patch Management

It is a requirement that all the most recent software updates (service packs, patches and hotfixes) available from Microsoft (or the GNU/Linux distributor and the SAMBA project for GNU/Linux servers) are tested and applied to the newly deployed computers to ensure stability and security.

Procedures and Guidelines

ICS will advise on active directory deployment strategies, and management issues.

Any department wishing to work with ICS to deploy active directory must contact ICS by phoning 2000 or e-mailing: helpdesk@uwc.ac.za to begin the process.

In the case of active directory deployments, ICS will work with the departments in question to ensure that existing active directory services comply with this policy.

Responsible Organization

The Office of the Executive Director for Information and Communication Services will be responsible for this policy and for any appeals of ICS decisions relating to active directory deployments. This policy will be reviewed yearly by ICS, and changes will be authorized by the approval of the Information Systems Committee (CISC). ICS will review active directory standards on an annual basis and recommend changes to this policy as needed.