

Open Enterprise Server 2015 SP1

Domain Services for Windows: Best Practices Guide

June 2016

Legal Notices

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.novell.com/company/legal/>.

Copyright © 2016 Novell, Inc., a Micro Focus company. All Rights Reserved.

Contents

About This Guide	5
1 Analyzing Your Organization's Needs	7
Organizations Requiring Active Directory-Style Authentication and Authorization for Enterprise Applications	7
Organizations with High Bandwidth Connectivity and Workstations in the Domain	8
Organizations with Workstations as Part of the Domain at Remote Offices or Requiring Decentralized Administration	8
Organizations Introducing OES for the First Time	8
Installing both DSfW and other OES Services	9
Installing Only the DSfW Service	9
2 Designing and Planning Your Domain Implementation	11
Before You Design Your Domain Implementation	11
eDirectory Tree	12
Name-Mapped Installation	12
Non-Name-Mapped Installation	13
Need for Universal Password Policy	13
Naming Conventions	13
NetBIOS names	14
Domain NetBIOS Name	14
Domain Controller NetBIOS Name	14
DNS Domain Name	15
DNS Server Placement	15
DNS Zone Resolution	15
Domain Controller Placement	16
Sites and Subnets	16
Fault Tolerance	16
Scalability	16
Domain Controller Capacity	17
Third-Party Application Support	17
Time Synchronization	17
3 Preparing the IT Infrastructure	19
Tree Schema Extension	19
Partitioning	19
Existing DNS Server	20
Linux User Management	20
Domain Controller on Hypervisor	20
Installation	21
Provisioning Wizard	21

4 Domain Administration	23
Domain Health and Performance Checks	23
Post-Deployment Checks	23
Partition and Replication	24
Rename Domain Administrator	24
User, Group, and Computer Objects Management	24
Default Active Directory Containers and Password Policy Assignments for Computer Objects	25

About This Guide

This guide describes the best practices and guidelines for deploying Novell Domain Services for Windows. It addresses common challenges faced by organizations in DSfW infrastructure decision-making. It does not attempt to cover all possible scenarios of deployment, and there may be unique requirements that might need the support of Novell Services Deployment Consultants. This guide is not a replacement for any training material. We highly recommend that you read the related [product documentation](#).

This guide is divided into the following sections:

- ♦ [Chapter 1, “Analyzing Your Organization’s Needs,” on page 7](#)
- ♦ [Chapter 2, “Designing and Planning Your Domain Implementation,” on page 11](#)
- ♦ [Chapter 3, “Preparing the IT Infrastructure,” on page 19](#)
- ♦ [Chapter 4, “Domain Administration,” on page 23](#)

Audience

This guide is primarily intended for Novell Solution Deployment Consultants and DSfW Administrators with a thorough functional understanding of DSfW.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation.

Documentation Updates

For the most recent version of the *DSfW Best Practices Guide*, visit the [OES 2015 SP1 documentation website](http://www.novell.com/documentation/oes2015) (<http://www.novell.com/documentation/oes2015>).

Additional Documentation

For information about security issues and recommendations for Novell Domain Services for Windows, see the [OES 2015 SP1: Novell Domain Services for Windows Security Guide](#).

1 Analyzing Your Organization's Needs

Installation of DSfW (Forest Root Domain) in an enterprise introduces a logical DSfW forest with a single domain by extending the existing eDirectory tree or creating a new eDirectory tree. This forest can be further logically extended by introducing multiple sub-domains to support the needs of an organization. Understanding the needs of the organization in relation to the domain deployment scenarios described in this chapter is critical to a successful implementation. Organizations might require Active Directory-style authentication and authorization for all users in the eDirectory Tree. This need might arise either to support an Active Directory-based enterprise application or Member Server, or to provide Active Directory-style client workstation login and enterprise management.

- ♦ [“Organizations Requiring Active Directory-Style Authentication and Authorization for Enterprise Applications” on page 7](#)
- ♦ [“Organizations Introducing OES for the First Time” on page 8](#)

Organizations Requiring Active Directory-Style Authentication and Authorization for Enterprise Applications

Organizations might require Active Directory-style authentication and authorization to support an enterprise application with no Active Directory integrated workstations in the domain. The enterprise application can be any third-party service that integrates with Active Directory, such as Cisco ISE, Polycom, Citrix XENApp, XenDesktop, or VMWare. In such scenarios, the DSfW domain is expected to serve only a Windows server as a member server and have no workstations that require Active Directory-style logins.

Follow the guidelines given below for this deployment scenario:

- ♦ Create only one central domain representing the entire eDirectory tree.
- ♦ For existing OES environments, place the DSfW Forest Root Domain at the top-most partition (O or OU) in the existing eDirectory Tree and replicate all eDirectory partitions to the headquarters.
- ♦ Configure at least 2 domain controllers per domain for high availability and fault tolerance.
- ♦ Add additional domain controllers to meet the domain member server's third-party performance needs and for more scalability.

NOTE: For existing OES users, always use the existing eDirectory tree and select the partition that needs to be mapped to the domain. If you are unclear about the structure that needs to support the domain or if there are multiple Organization Containers to be covered, contact a Novell Service Partner or Novell Consulting for assistance.

- ♦ [“Organizations with High Bandwidth Connectivity and Workstations in the Domain” on page 8](#)
- ♦ [“Organizations with Workstations as Part of the Domain at Remote Offices or Requiring Decentralized Administration” on page 8](#)

Organizations with High Bandwidth Connectivity and Workstations in the Domain

For organizations that have a high bandwidth connection (at least 2 MBits) between their offices and use local Active Directory-style login, or that have workstation integration and Group Policies, follow the guidelines below:

- ♦ Configure a single central domain and support it with a local domain controller at each office. Use the Sites and Subnets feature to limit the Windows logon traffic to a local domain controller and to improve overall performance.
- ♦ Add an additional domain controller at the headquarters and one at the remote office for fault tolerance and scalability.

Organizations with Workstations as Part of the Domain at Remote Offices or Requiring Decentralized Administration

This deployment scenario includes organizations requiring a decentralized administration or having offices in remote locations that are connected using a low bandwidth connection and having workstations integrated to the Domain.

If there is a need to reduce replication or logon traffic over WAN due to a weak WAN link between offices, or to delegate domain administration tasks to remote offices, use the following recommendations:

- ♦ Split the remote office container (by partitioning) and map it to a child domain.
- ♦ Add additional domain controllers to the child domain for fault tolerance and scalability.
- ♦ (Optional) Configure the DSfW service on a standalone OES server if full eDirectory integration for OES service is not required.

NOTE: The multiple-domain approach leads to administration overheads, such as creating and maintaining domain-specific GPO policies and login scripts. Review the benefits and limitations of the single domain (multiple site feature) and multiple domain approach before introducing a child domain.

Organizations Introducing OES for the First Time

This section describes deployment scenarios for organizations introducing OES for the first time.

- ♦ [“Installing both DSfW and other OES Services” on page 9](#)
- ♦ [“Installing Only the DSfW Service” on page 9](#)

Installing both DSfW and other OES Services

This deployment scenario is applicable if you are new to OES and you need both non-DSfW OES services and DSfW in the same tree. The tree is used for a DSfW domain and provides workstation logins and GPO retrievals, and is used for OES services such as NSS, NCS, iPrint, DNS/DHCP, FTP, GroupWise, and ZCM satellite. Follow the recommendations given below for this deployment scenario:

- ♦ Define an eDirectory tree structure that meets the requirements of OES services.
- ♦ Deploy non-DSfW OES services first.
- ♦ Add an additional OES server to this eDirectory tree and configure a DSfW domain. Use the information in [“Organizations Requiring Active Directory-Style Authentication and Authorization for Enterprise Applications” on page 7](#) as appropriate to deploy the DSfW Domain.

Installing Only the DSfW Service

If you want to use OES to use only the DSfW Service in OES, you can follow a new eDirectory Tree approach and follow the recommendations in [“Organizations Requiring Active Directory-Style Authentication and Authorization for Enterprise Applications” on page 7](#).

If you prefer a custom eDirectory Tree structure with a Directory Objects notation of O and OU instead of the DSfW default Directory Objects notation of DC and CN, follow the guidelines in [“Organizations Requiring Active Directory-Style Authentication and Authorization for Enterprise Applications” on page 7](#). Configure the first OES server in the tree with only eDirectory, and introduce a second OES server with the DSfW configuration.

2 Designing and Planning Your Domain Implementation

The success of your domain implementation depends on how well you plan and design a domain that is suitable for your enterprise. Use the guidelines and recommendations in this chapter to plan and design your domain.

- ♦ “Before You Design Your Domain Implementation” on page 11
- ♦ “eDirectory Tree” on page 12
- ♦ “Need for Universal Password Policy” on page 13
- ♦ “Naming Conventions” on page 13
- ♦ “NetBIOS names” on page 14
- ♦ “DNS Domain Name” on page 15
- ♦ “DNS Server Placement” on page 15
- ♦ “Domain Controller Placement” on page 16
- ♦ “Third-Party Application Support” on page 17
- ♦ “Time Synchronization” on page 17

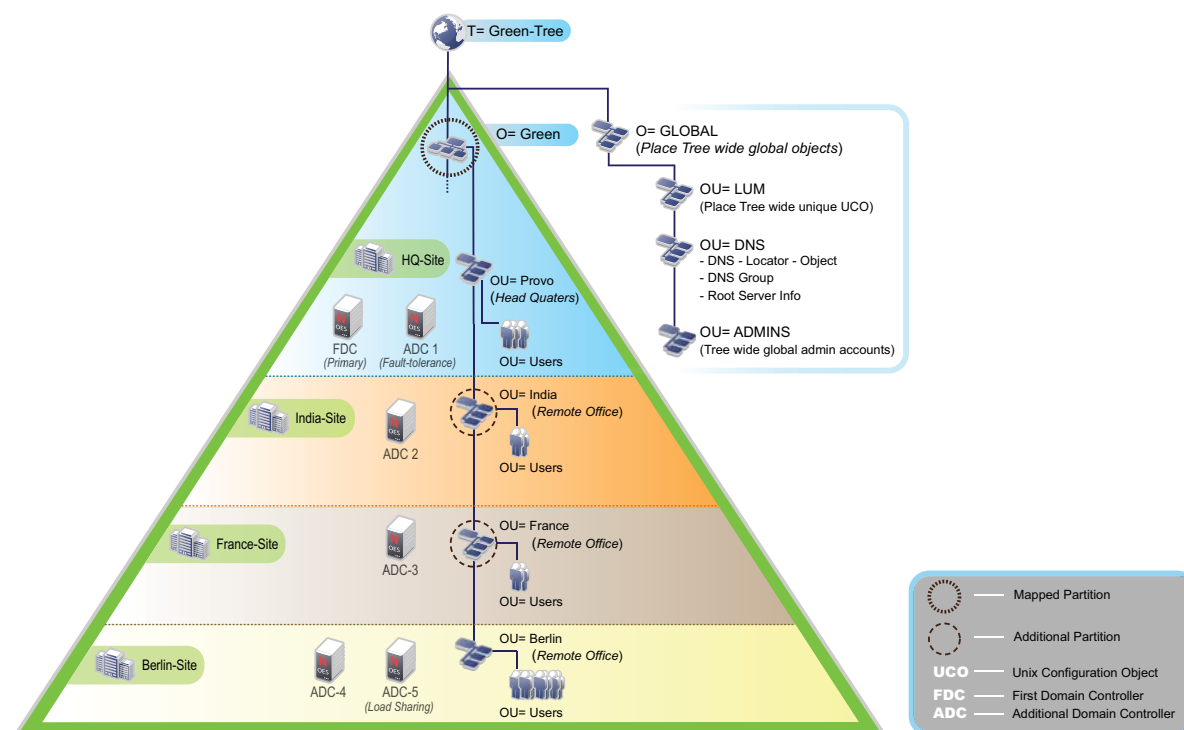
Before You Design Your Domain Implementation

Before you begin to design a domain that is suitable for your enterprise, ensure that you read and understand the following:

- ♦ For information about eDirectory, see the [eDirectory Documentation](#).
- ♦ DSfW emulates the Active Directory security model on top of eDirectory. Most of the security considerations for both Active Directory and eDirectory apply to DSfW. However, there are some key differences. For a functional overview, see [Domain Services for Windows Security Model](#).
- ♦ If you are creating a new eDirectory tree in your network, you must do some additional planning before you install the first server in the tree. For more information, see the [OES 2015: Planning and Implementation Guide](#).
- ♦ For information on requirements and guidelines for using DSfW on OES servers, see [Planning Your DSfW Implementation](#).
- ♦ For information on Active Directory planning guidelines by Microsoft, see [Best Practice Active Directory Design for Managing Windows Networks](#).
- ♦ For information about Forests, Domains, and Trust Relationships, see [Understanding DSfW in Relation to Active Directory](#).
- ♦ For information about DSfW in relation to Samba and IDM, see [Understanding DSfW in Relation to Samba](#) and [Understanding DSfW in Relation to IDM](#).

eDirectory Tree

The first DSfW server in a tree creates a forest, and only one forest can be created for each eDirectory tree. A DSfW domain can include one or more contiguous partitions. The figure below depicts mapping of multiple eDirectory partitions to a single DSfW domain and mapping each eDirectory partition to a respective DSfW domain.



- “Name-Mapped Installation” on page 12
- “Non-Name-Mapped Installation” on page 13

Name-Mapped Installation

Follow the guidelines in this section as you install DSfW into an existing tree:

- In a name-mapped installation scenario, only one top-level container (O or OU), including its sub-structure, can be integrated into the DSfW forest structure.
- Every DSfW domain must be mapped to a partition in eDirectory. The name of the domain and the organizational unit that is planned to be mapped can be different. For information on eDirectory partitioning, see [Managing Partitions and Replicas](#).
- After the DSfW domain is mapped to an eDirectory partition, its sibling partitions and its top-level partition in the eDirectory tree cannot be mapped to a DSfW domain. Ensure that you map a DSfW forest to the top-most partition in eDirectory tree, so that all the needed partitions can be brought under the DSfW domain.

- ♦ After DSfW is configured, the DSfW domain name and the first eDirectory partition that is mapped to the DSfW domain cannot be modified. For more information, see [Leveraging an Existing eDirectory Setup](#) and [Deploying DSfW in a Name-Mapped Setup](#).
- ♦ If the eDirectory tree has more than one organization that needs to be part of the domain, you must redesign or restructure eDirectory. Using “Alias objects” does not work. Instead, you can create a separate DSfW tree and use Identity Manager (IDM) to synchronize.

Non-Name-Mapped Installation

If you are introducing DSfW as a new tree in the enterprise, a container is created in DC (Domain Class) notation and is partitioned and mapped to the domain. This container is the root for all other subsequent domains. The name of the container to be created is derived from the DNS domain name.

Need for Universal Password Policy

The universal password policy set on the user objects enables the creation of Active Directory keys from the user's associated universal password policy during DSfW provisioning. It is mandatory to have all users enabled with the universal password policy so that all domain users are ready to access the domain services and functionality.

By default, DSfW creates NMAS password policies with universal password policy settings (retain password policies = no). However, if there are existing NMAS password policies in your environment, reuse them for the DSfW domain. Ensure that the universal password policy setting is enabled in those existing NMAS password policies.

The implementation of universal password policy impacts the login procedure of all users. We recommend that you implement universal password in your environment before deploying DSfW. When universal password policy is implemented before deploying DSfW, ensure that the **Retain existing Novell Password Policies on Users** check box is selected during DSfW installation.

Universal password policy implementation requires you to change the login of the Novell Client in an existing environment to an NMAS-based login. This is to ensure that NDS and the Universal Password is synchronized. For more information, see [Enabling Universal Password Policy for DSfW](#).

Naming Conventions

User, group, and computer objects are called security principals of the domain, and each object in the domain must have a unique name across the domain. Ensure the following:

- ♦ Objects are unique across the DSfW domain.
- ♦ Objects have single-valued CN attribute.
- ♦ User objects do not have a value assigned to the `uniqueID` attribute before DSfW is configured.
- ♦ Any workstation joining the domain has a unique and non-ambiguous network name.

User accounts with the same CN value in different eDirectory containers and part of the same DSfW domain results in duplicate DSfW user accounts. User accounts with duplicate names must be rectified before deploying the DSfW domain. To ensure uniqueness for objects in your tree, use tools such as the DSReport and iManager unique naming plugin.

Follow the guidelines below to prevent duplicate workstation names in your DSfW environment:

- ♦ Enable WINS on one domain controller for every forest, preferably the first domain controller in the tree.
- ♦ Configure WINS on the workstations before joining them to the domain (for example, using DHCP).
- ♦ Enable intruder lockout settings at the domain level.

NetBIOS names

Installing DSfW in an enterprise introduces a NetBIOS name for the domain controller and the domain. Ensure that you plan a unique NetBIOS name for the domain resources. Renaming NetBIOS names is not supported.

The maximum effective length of a NetBIOS name is 15 characters. By default, the NetBIOS name is derived from the first component of the corresponding resource DNS name. For example, the workstation NetBIOS name is derived from the workstation DNS name. For a workstation DNS name `novell.example.com`, the NetBIOS name is "novell". If the derived name exceeds 15 characters, only the first 15 characters are considered.

- ♦ [“Domain NetBIOS Name” on page 14](#)
- ♦ [“Domain Controller NetBIOS Name” on page 14](#)

Domain NetBIOS Name

The domain NetBIOS name is derived from the domain DNS name. For example, if the domain name is `provo.novell.com`, then "PROVO" is assigned as the NetBIOS name. We recommend that you do not modify the NetBIOS name. If you intend to have a custom NetBIOS name, choose the NetBIOS name carefully, so that it is unique across the organization network. Most often, the domain NetBIOS name is used by user for logon, so take special care when choosing the NetBIOS name.

Domain Controller NetBIOS Name

A domain controller's NetBIOS name is derived from the domain controller's DNS name. The NetBIOS name is restricted to 15 characters. If the hostname is more than 15 characters, only the first 15 characters are considered. There is no option to provide a custom NetBIOS name for a domain controller in a DSfW configuration.

DNS Domain Name

We recommend that you integrate into the existing DNS structure, if an existing DNS structure is present. You can reuse the domain name that is already used for servers and workstations, or create a child domain in the existing structure. Modifying the DSfW domain name after the DSfW configuration, and using third-party DNS services as designated primary is not supported.

DNS Server Placement

The first domain controller in the tree hosts the DNS server by default. For other DSfW installations, such as child and additional domain controllers, the DNS server is optional and is not enabled by default.

You can plan to introduce additional DNS servers in the Domain for the following situations:

- ♦ To achieve fault tolerance.
- ♦ To restrict DNS traffic in a remote office where an additional domain controller or a sub-domain is planned.
- ♦ If you need a complete delegated model of administration and you want every component to be local.

Follow the guidelines and recommendations given below:

- ♦ Configure at least two DNS servers hosting the DNS zones for DSfW. Both DNS servers should be configured during DSfW configuration.
- ♦ If the workstations need to use other DNS servers, add secondary zones of the DSfW DNS zones in these servers.
- ♦ Since it is difficult to post install and post configure DNS on a DSfW server, Novell recommends you to install and configure DNS on all domain controllers. It is not essential to use DNS service installed and configured on other OES servers and they can be deactivated on servers where it is not required.
- ♦ There can be only one designated primary DNS server for a specific DNS zone, and it must be running on one of the domain controllers for a domain. The forward lookup zone and all reverse lookup zones of clients that need to be dynamically updated in DNS must be hosted as a designated primary zone on the DSfW server. The dynamic updates are always sent from the clients to the DNS server that is hosting the designated primary zone.

DNS Zone Resolution

For most DNS deployments, you must have two central DNS servers that host every DNS Zone in the eDirectory tree. All remote DNS servers host zones for their location (forward and reverse) and forward the unresolved queries to the two central DNS servers. The DSfW DNS servers that are introduced at child domains must have forward list set to at least two trusted forest root domain DSfW DNS Servers.

The forest root domain DSfW DNS servers must be made authoritative (primary) for all the reverse lookup zones and for all the forward zones if a delegate zone approach is not possible. Ensure that you create the necessary reverse zones for all of the subnets used in your environment, using the DNS/DHCP Management Console.

The designated primary for a zone (forward or reverse) that is under the DSfW domain must be the server that handles the dynamic updates. This must either be the domain controller or the server that communicates with the DHCP server.

For information about DNS and DSfW integration, see [“DNS-DSfW Integration”](#).

Domain Controller Placement

Domain controllers should be located as close as possible to the workstation and the server that they connect to. Higher bandwidth and less latency between the domain controller and the client leads to higher performance.

- ♦ [“Sites and Subnets” on page 16](#)
- ♦ [“Fault Tolerance” on page 16](#)
- ♦ [“Scalability” on page 16](#)
- ♦ [“Domain Controller Capacity” on page 17](#)

Sites and Subnets

If you place domain controllers for one domain in multiple locations, you must use the Sites and Subnets feature. This helps to achieve optimal login performance for the clients by enabling them to connect to the closest available domain controller.

We recommend that you specify proper location names when specifying a site name, and that you avoid changing the site name later.

Fault Tolerance

We recommend that you have at least two domain controllers per domain for fault tolerance.

Scalability

Novell recommends you to add more domain controllers to a specific location based on the usage and the number of concurrent connections. The ideal configuration depends on factors such as domain controller concurrency, login traffic expected at fixed intervals, and expected growth. Thus, the recommendations described in [“Domain Controller Capacity” on page 17](#) are only indicative, and will need to be adjusted to suit your specific enterprise needs. Defining a configuration that provides the expected performance for an enterprise is a continuous process and needs to be worked out carefully.

Domain Controller Capacity

DSfW depends on many core services that are mutually dependent. Ensure that these services get enough resources such as Memory and CPU. Non-availability of resources for any of the DSfW services might lead to domain malfunction and slowness at the client workstation.

For an enterprise with user base up to 2000 users per domain and associated resources such as user workstations and shares, you must have at least two domain controllers. Each Domain controller must have at least 8 GB RAM and a Quad-Core CPU. For an enterprise with more than 2000 and less than 5000 concurrent logged in users per domain, you must have at least 4 Domain Controllers. Each Domain Controllers must have at least 16 GB RAM and a Quad-Core CPU.

NOTE: If the enterprise size is different from the ones mentioned in this section, we recommend that you contact Novell Services Qualified Partners or consultants.

Third-Party Application Support

Determine which third-party applications that are being used or planned rely on Active Directory for Single Sign-on Authentication. Verify whether these applications are supported by DSfW. Contact Novell Technical Services or Novell Consulting Services for any questions related to third-party application support.

For more information, see this Wiki page on Novell Website: [Applications known to work with DSfW](#). Other applications such as Blackberry Enterprise Server 10 and Cisco Applications also integrate well with DSfW. For more information about such applications, contact the OES DSfW Support forum. For information about compatibility of Citrix with DSfW, see [Citrix Compatibility](#).

Time Synchronization

Due to Kerberos, the functioning of DSfW and systems joined to the domain are critically time-dependent. DSfW domain joined systems automatically synchronize their time to the domain controller that they log in to. Plan for the right time source for all the domain controllers across the enterprise, and ensure that all servers in the tree; all domain controllers; and all workstations, servers, and services that join the domain have the same time. We recommend that you build a fault-tolerant time synchronization based on NTP that also synchronizes from multiple sources that provide the correct time. Domain Controllers must have at least two time sources set.

If you are planning to install domain controllers on hypervisor, ensure that the domain controller and the VM hypervisor host time is always synchronized with the same reliable NTP time source or to a parent domain controller that is out of the hypervisor. The VM infrastructure can cause time drifts. Avoid using VM tools to synchronize Domain controller time.

3 Preparing the IT Infrastructure

This chapter describes how to prepare the IT infrastructure to ensure a smooth configuration of the DSfW server.

- ♦ [“Tree Schema Extension” on page 19](#)
- ♦ [“Partitioning” on page 19](#)
- ♦ [“Existing DNS Server” on page 20](#)
- ♦ [“Linux User Management” on page 20](#)
- ♦ [“Domain Controller on Hypervisor” on page 20](#)
- ♦ [“Installation” on page 21](#)
- ♦ [“Provisioning Wizard” on page 21](#)

Tree Schema Extension

The DSfW installation creates a new eDirectory schema with Active Directory attributes and objectclass set. Installing DSfW in an existing eDirectory tree extends the schema. To install DSfW in an existing tree, ensure that all of the eDirectory servers holding the Tree Root partition are up and healthy.

In existing tree deployments, the DSfW installer extends the schema by contacting the eDirectory server that contains the read/write replica of the tree root partition. If the operation of extending the schema is done on a remote eDirectory server, it might take time for the extended schema to get replicated on the DSfW server that is being configured. Thus, you should extend the DSfW schema prior to the DSfW installation using the YaST plug-in Novell Schema Tool.

Before initiating the schema extension, perform an eDirectory health check and ensure that all servers are healthy. For more information on how to perform an eDirectory health check, see [TID 3564075](#). For more information on eDirectory schema management, see [Managing the Schema](#) and [Schema](#).

Partitioning

Ensure that the container (o or ou) that you are configuring as name mapped is partitioned before the start of the DSfW installation. DSfW extends the object with the new schema. Thus, we recommend that you clean up your eDirectory and merge all partitions that are not required.

If you previously had Novell NetWare in your environment, you must delete the old license objects (NLS objects).

Existing DNS Server

By default, the DSfW installation configures a DNS server in the forest root domain's first domain controller, and introduces a new DNS Locator object in the tree. If you have already configured Novell DNS Server in the same tree, using the existing DNS Locator object is mandatory. You can do this by providing the existing DNS Locator context in YaST during DSfW Configuration. This will ensure that if DSfW is configured to serve an existing domain, the existing DNS Zone is extended with DSfW-specific DNS settings instead of creating a duplicate DNS Zone.

In an existing environment, specify the existing DNS Locator object. Otherwise, a new DNS Locator Object will be created with a new zone for the same domain name. This new duplicate zone will need to be manually merged into the existing DNS Zone using Novell DNS/DHCP Console. A tree can contain multiple DNS Locators. However, we recommend that you have a unique DNS Locator object per tree. This ensures that there are no duplicate DNS Zones in the tree and it enables the zones to be managed in the DNS/DHCP console.

We recommend that you create the DNS entries for the new DSfW servers before installing DSfW. This is because servers can resolve each other using the name and IP address when installing DSfW into an existing tree. If there are new DNS zones created for the DSfW domains, you should create these zones before the DSfW installation. If existing DNS Zones are reused, ensure that the DSfW DNS server serving the domain is set as Designated Primary for the zones after deploying the domain controllers. This is applicable for all forward and reverse zones.

Linux User Management

Follow the guidelines given below:

- ♦ Place the Unix Configuration Object (UCO) in the upper layers of the tree in a separate container (for example, `ou=LUM,o=services`) and maintain a single UCO per tree. For any additional server installation in the same tree, ensure that the existing UCO is utilized during LUM configuration in YaST.
- ♦ Clean up the existing POSIX attributes on user and group objects before deploying the DSfW domain. The POSIX attributes include all the attributes that belong to the LUM schema extensions, such as `uidNumber`, `gidNumber`, `homeDirectory`, `loginShell`.
- ♦ If you have modified the default POSIX ID ranges, ensure that they do not clash with the DSfW ID ranges. The LUM default UID and GID number for the DSfW domain ranges from 0 to 65500.

Domain Controller on Hypervisor

Consider a cautious approach when placing the domain controller in a virtualized environment such as VMware, Citrix, or Microsoft hypervisor. Follow the guidelines given below:

- ♦ Ensure that you secure the host computer where the virtual domain controller is hosted and protect it from malicious users.
- ♦ Protect the domain controller's virtual hard disk files (for example the `.vmd` files). Ensure that only reliable administrators have access to the domain controller's VHD files.
- ♦ Directory operations are critically time-dependent. Ensure that the domain controller and hypervisor host time is always synchronized with the same reliable NTP time source and to a source that is outside the hypervisor. VM infrastructures can cause serious time drifts.

- ♦ Separate the virtualization internal traffic from the guest traffic.
- ♦ Consider reducing the weight or priority of SRV records on the Virtual domain controllers if it is an additional domain controller for your domain.
- ♦ Ensure that the virtual domain controller gets enough network bandwidth for users to authenticate faster.
- ♦ Implement VMWare High availability to ensure that the virtual domain controller is restarted in the event of ESX server failures.
- ♦ In a multi-server environment, avoid domain controller snapshot reverting for any install failures in the tree that includes physical domain controllers or pre-existing eDirectory server.

Installation

DSfW must be installed on a new OES server. The OES server can be configured on an existing SLES server or as a new install of SLES where OES is the add-on product. We recommend that you install SLES and OES together to provide update sources during the installation, to ensure that all available patches are installed in YaST before the DSfW configuration in YaST. Follow the recommendations given below:

- ♦ Create separate filesystems or partitions for boot, root, tmp, swap, and var.
- ♦ If you plan to use the existing password policies, ensure that the **Retain existing Novell Password Policies on Users** check box is selected.
- ♦ Always install and configure DNS.
- ♦ Replicate Schema and Configuration to all domain controllers in a domain.

Provisioning Wizard

Follow the recommendations given below after the DSfW installation is complete and before you initiate provisioning:

- ♦ Configure user space core dump creation before provisioning and reboot.
- ♦ Verify time synchronization


```
ntpq -p
```
- ♦ Verify name resolution (DNS and SLP) using `slptool` and `nslookup`.
- ♦ Ensure that the CA server can resolve the new server's name.
- ♦ Ensure that all existing DSfW servers are up and running.
- ♦ Add replicas manually before initiating provisioning. In a single-domain scenario, add replicas of all partitions. In a multi-domain scenario, add replicas of all child partitions that belong to the mapped partition and to the domain.
- ♦ Use `rpcclient` to verify samba.
- ♦ Use X server on the local console.
- ♦ Always enable and use custom provisioning and ensure that only the first eDirectory partition being mapped to the domain is added during initial provisioning. Add additional partitions later using the `domainctrl` tool.

4 Domain Administration

- ♦ [“Domain Health and Performance Checks” on page 23](#)
- ♦ [“Post-Deployment Checks” on page 23](#)
- ♦ [“Partition and Replication” on page 24](#)
- ♦ [“Rename Domain Administrator” on page 24](#)
- ♦ [“User, Group, and Computer Objects Management” on page 24](#)
- ♦ [“Default Active Directory Containers and Password Policy Assignments for Computer Objects” on page 25](#)

Domain Health and Performance Checks

You should periodically monitor the DSfW domain controller for the following:

- ♦ sysvolsync
- ♦ Gposync
- ♦ Time synchronization
- ♦ eDirectory health
- ♦ Syslog for critical errors from all DSfW services
- ♦ KDC log
- ♦ Samba and winbind logs

Perform `xadcntrl validate` to ensure that all DSfW services are healthy. Any unexpected errors can lead to domain controller malfunctioning or unnecessary load on domain controllers if not attended to. For more information, see [“Logging”](#). For information on eDirectory performance tuning, see [TID 3178089](#).

Post-Deployment Checks

Verify that all the services necessary for DSfW are configured correctly by executing the `xadcntrl validate` command. For detailed verification steps, see [TID 7001884](#) and [“Activities After DSfW Installation or Provisioning”](#).

Partition and Replication

The functioning and performance of a domain controller is highly dependent on replica placement. If you have less than 20 domain controllers, you should place the copy of the configuration and schema partition replicas local to the domain controller to improve the login performance. This is because the configuration and schema details are often queried for by DSfW services. Follow the partition and replication guidelines given below:

- ♦ You must have replicas of all partitions inside the DSfW domain boundary local to the respective domain controllers.
- ♦ Do not remove the replica of the domain's primary eDirectory partition from its respective domain controller, to avoid exhaustion of the Domain RID Pool.
- ♦ Do not merge the eDirectory partition that is mapped as the first partition of a DSfW domain.
- ♦ Do not partition DSfW default containers such as `OU=OESystemObjects`, `CN=Computers`, `OU=Domain Controllers`. Partitioning default containers will lead to critical DSfW service issues.
- ♦ Do not merge a configuration or schema partition that is created by the DSfW provisioning wizard.
- ♦ Always use the `domaincntrl` tool to add or remove additional partitions to domain after provisioning the server.

Rename Domain Administrator

By default, a domain administrator named “Administrator” is created under the `cn=users` container. We recommend that you rename this account and specify a strong password to avoid unauthorized attacks to the Domain Administrator account. It is also recommended that you create a decoy account named “Administrator” with normal user privileges. For more information, see [Protecting the Administrator Account](#).

User, Group, and Computer Objects Management

We recommend that you use iManager for user management in existing environments, and MMC (Microsoft Management Console) for other operations. Follow the guidelines given below to improve domain performance:

- ♦ When a user is a member of several groups, the login time can increase. Avoid adding users to too many groups.
- ♦ Having large number of groups in a domain might result in an increase in resource utilization, as a result of calculation of the effective group membership. Avoid adding too many groups.
- ♦ Avoid adding users directly to Universal groups. Instead, place users in global groups and add global groups in universal groups. Adding users directly to universal groups can delay user login.

For more information, see [Securing Active Directory Administrative Groups and Accounts](#).

Default Active Directory Containers and Password Policy Assignments for Computer Objects

All default containers are present in the domain DN attribute wellknownObjects. Ensure that the nsmpPasswordPolicyDN attribute in the domain controllers container (OU=Domain Controllers,DC=example,DC=com) and computers container (CN=Computers,DC=example,DC=com) points to the default password policy (CN=Default Password Policy,CN=Password Policies,CN=System,DC=example,DC=com). If the computers container is modified, ensure that the default password policy is assigned to it.

Avoid placing or importing users and computers into the same container. Create dedicated containers for computer objects. If computers are imported to multiple containers, ensure that the default password policy is applied to those containers.

