Full credit is given to the above companies including the OS that this PDF file was generated!

Rocky Enterprise Linux 9.2 Manual Pages on command 'sssd-ipa.5'

$ man sssd-ipa.5

SSSD-IPA(5) File Formats and Conventions SSSD-IPA(5)

NAME

sssd-ipa - SSSD IPA provider

DESCRIPTION

This manual page describes the configuration of the IPA provider for sssd(8). For a detailed syntax reference, refer to the ?FILE FORMAT? section of the sssd.conf(5) manual page.

The IPA provider is a back end used to connect to an IPA server. (Refer to the freeipa.org web site for information about IPA servers.) This provider requires that the machine be joined to the IPA domain; configuration is almost entirely self-discovered and obtained directly from the server.

The IPA provider enables SSSD to use the sssd-ldap(5) identity provider and the sssd-krb5(5) authentication provider with optimizations for IPA environments. The IPA provider accepts the same options used by the sssd-ldap and sssd-krb5 providers with some exceptions. However, it is neither necessary nor recommended to set these options.

The IPA provider primarily copies the traditional ldap and krb5 provider default options with some exceptions, the differences are listed in the ?MODIFIED DEFAULT OPTIONS? section.

As an access provider, the IPA provider uses HBAC (host-based access control) rules. Please refer to freeipa.org for more information about HBAC. No configuration of access provider is required on the client side.

If ?auth_provider=ipa? or ?access_provider=ipa? is configured in sssd.conf then the id_provider must also be set to ?ipa?.

The IPA provider will use the PAC responder if the Kerberos tickets of users from trusted realms contain a PAC. To make configuration easier the PAC responder is started automatically if the IPA ID provider is configured.

CONFIGURATION OPTIONS

Refer to the section ?DOMAIN SECTIONS? of the sssd.conf(5) manual page for details on the configuration of an SSSD domain.

ipa_domain (string)

Specifies the name of the IPA domain. This is optional. If not provided, the configuration domain name is used.

ipa_server, ipa_backup_server (string)

The comma-separated list of IP addresses or hostnames of the IPA servers to which SSSD should connect in the order of preference. For more information on failover and server redundancy, see the ?FAILOVER? section. This is optional if autodiscovery is enabled. For more information on service discovery, refer to the ?SERVICE DISCOVERY? section.

ipa_hostname (string)

Optional. May be set on machines where the hostname(5) does not reflect the fully qualified name used in the IPA domain to identify this host. The hostname must be fully qualified.

dyndns_update (boolean)

Optional. This option tells SSSD to automatically update the DNS server built into FreeIPA with the IP address of this client. The update is secured using GSS-TSIG. The IP address of the IPA LDAP connection is used for the updates, if it is not otherwise

specified by using the ?dyndns_iface? option.

NOTE: On older systems (such as RHEL 5), for this behavior to work

reliably, the default Kerberos realm must be set properly in

/etc/krb5.conf

NOTE: While it is still possible to use the old ipa_dyndns_update

option, users should migrate to using dyndns_update in their config

file.

Default: false

dyndns_ttl (integer)

The TTL to apply to the client DNS record when updating it. If

dyndns_update is false this has no effect. This will override the

TTL serverside if set by an administrator.

NOTE: While it is still possible to use the old ipa_dyndns_ttl

option, users should migrate to using dyndns_ttl in their config

file.

Default: 1200 (seconds)

dyndns_iface (string)

Optional. Applicable only when dyndns_update is true. Choose the

interface or a list of interfaces whose IP addresses should be used

for dynamic DNS updates. Special value ?*? implies that IPs from

all interfaces should be used.

NOTE: While it is still possible to use the old ipa_dyndns_iface

option, users should migrate to using dyndns_iface in their config

file.

Default: Use the IP addresses of the interface which is used for

IPA LDAP connection

Example: dyndns_iface = em1, vnet1, vnet2

dyndns_auth (string)

Whether the nsupdate utility should use GSS-TSIG authentication for

secure updates with the DNS server, insecure updates can be sent by

setting this option to 'none'.

Default: GSS-TSIG

dyndns_auth_ptr (string)

Whether the nsupdate utility should use GSS-TSIG authentication for secure PTR updates with the DNS server, insecure updates can be sent by setting this option to 'none'.

Default: Same as dyndns_auth

ipa_enable_dns_sites (boolean)

Enables DNS sites - location based service discovery.

If true and service discovery (see Service Discovery paragraph at the bottom of the man page) is enabled, then the SSSD will first attempt location based discovery using a query that contains "_location.hostname.example.com" and then fall back to traditional SRV discovery. If the location based discovery succeeds, the IPA servers located with the location based discovery are treated as primary servers and the IPA servers located using the traditional SRV discovery are used as back up servers

Default: false

dyndns_refresh_interval (integer)

How often should the back end perform periodic DNS update in addition to the automatic update performed when the back end goes online. This option is optional and applicable only when dyndns_update is true.

Default: 0 (disabled)

dyndns_update_ptr (bool)

Whether the PTR record should also be explicitly updated when updating the client's DNS records. Applicable only when dyndns_update is true.

This option should be False in most IPA deployments as the IPA server generates the PTR records automatically when forward records are changed.

Default: False (disabled)

dyndns_force_tcp (bool)

Whether the nsupdate utility should default to using TCP for communicating with the DNS server.

Default: False (let nsupdate choose the protocol)

dyndns_server (string)

The DNS server to use when performing a DNS update. In most setups, it's recommended to leave this option unset.

Setting this option makes sense for environments where the DNS server is different from the identity server.

Please note that this option will be only used in fallback attempt when previous attempt using autodetected settings failed.

Default: None (let nsupdate choose the server)

dyndns_update_per_family (boolean)

DNS update is by default performed in two steps - IPv4 update and then IPv6 update. In some cases it might be desirable to perform IPv4 and IPv6 update in single step.

Default: true

ipa_deskprofile_search_base (string)

Optional. Use the given string as search base for Desktop Profile related objects.

Default: Use base DN

ipa_hbac_search_base (string)

Optional. Use the given string as search base for HBAC related objects.

Default: Use base DN

ipa_host_search_base (string)

Deprecated. Use ldap_host_search_base instead.

ipa_selinux_search_base (string)

Optional. Use the given string as search base for SELinux user maps.

See ?ldap_search_base? for information about configuring multiple search bases.

Default: the value of ldap_search_base

ipa_subdomains_search_base (string)

Optional. Use the given string as search base for trusted domains.

See ?ldap_search_base? for information about configuring multiple search bases.

Default: the value of cn=trusts,%basedn

ipa_master_domain_search_base (string)

Optional. Use the given string as search base for master domain object.

See ?ldap_search_base? for information about configuring multiple search bases.

Default: the value of cn=ad,cn=etc,%basedn

ipa_views_search_base (string)

Optional. Use the given string as search base for views containers.

See ?ldap_search_base? for information about configuring multiple search bases.

Default: the value of cn=views,cn=accounts,%basedn

krb5_realm (string)

The name of the Kerberos realm. This is optional and defaults to the value of ?ipa_domain?.

The name of the Kerberos realm has a special meaning in IPA - it is converted into the base DN to use for performing LDAP operations.

krb5_confd_path (string)

Absolute path of a directory where SSSD should place Kerberos configuration snippets.

To disable the creation of the configuration snippets set the parameter to 'none'.

Default: not set (krb5.include.d subdirectory of SSSD's pubconf directory)

ipa_deskprofile_refresh (integer)

The amount of time between lookups of the Desktop Profile rules against the IPA server. This will reduce the latency and load on the IPA server if there are many desktop profiles requests made in a short period.

Default: 5 (seconds)

ipa_deskprofile_request_interval (integer)

The amount of time between lookups of the Desktop Profile rules against the IPA server in case the last request did not return any rule.

Default: 60 (minutes)

ipa_hbac_refresh (integer)

The amount of time between lookups of the HBAC rules against the IPA server. This will reduce the latency and load on the IPA server if there are many access-control requests made in a short period.

Default: 5 (seconds)

ipa_hbac_selinux (integer)

The amount of time between lookups of the SELinux maps against the IPA server. This will reduce the latency and load on the IPA server if there are many user login requests made in a short period.

Default: 5 (seconds)

ipa_server_mode (boolean)

This option will be set by the IPA installer (ipa-server-install) automatically and denotes if SSSD is running on an IPA server or not.

On an IPA server SSSD will lookup users and groups from trusted domains directly while on a client it will ask an IPA server.

NOTE: There are currently some assumptions that must be met when SSSD is running on an IPA server.

? The ?ipa_server? option must be configured to point to the IPA server itself. This is already the default set by the IPA installer, so no manual change is required.

? The ?full_name_format? option must not be tweaked to only print short names for users from trusted domains.

Default: false

ipa_automount_location (string)

The automounter location this IPA client will be using

Default: The location named "default"

Please note that the automounter only reads the master map on startup, so if any autofs-related changes are made to the sssd.conf, you typically also need to restart the automounter daemon after restarting the SSSD.

VIEWS AND OVERRIDES

SSSD can handle views and overrides which are offered by FreeIPA 4.1 and later version. Since all paths and objectclasses are fixed on the server side there is basically no need to configure anything. For completeness the related options are listed here with their default values.

ipa_view_class (string)

Objectclass of the view container.

Default: nsContainer

ipa_view_name (string)

Name of the attribute holding the name of the view.

Default: cn

ipa_override_object_class (string)

Objectclass of the override objects.

Default: ipaOverrideAnchor

ipa_anchor_uuid (string)

Name of the attribute containing the reference to the original object in a remote domain.

Default: ipaAnchorUUID

ipa_user_override_object_class (string)

Name of the objectclass for user overrides. It is used to determine if the found override object is related to a user or a group.

User overrides can contain attributes given by

? ldap_user_name

? ldap_user_uid_number

? ldap_user_gid_number

? ldap_user_gecos

? ldap_user_home_directory

? ldap_user_shell

? ldap_user_ssh_public_key

Default: ipaUserOverride

ipa_group_override_object_class (string)

Name of the objectclass for group overrides. It is used to determine if the found override object is related to a user or a group.

Group overrides can contain attributes given by

? ldap_group_name

? ldap_group_gid_number

Default: ipaGroupOverride

MODIFIED DEFAULT OPTIONS

Certain option defaults do not match their respective backend provider defaults, these option names and IPA provider-specific defaults are listed below:

KRB5 Provider

? krb5_validate = true

? krb5_use_fast = try

? krb5_canonicalize = true

LDAP Provider - General

? ldap_schema = ipa_v1

? ldap_force_upper_case_realm = true

? ldap_sasl_mech = GSSAPI

? ldap_sasl_minssf = 56

? ldap_account_expire_policy = ipa

? ldap_use_tokengroups = true

LDAP Provider - User options

? ldap_user_member_of = memberOf

? ldap_user_uuid = ipaUniqueID

? ldap_user_ssh_public_key = ipaSshPubKey

? ldap_user_auth_type = ipaUserAuthType

LDAP Provider - Group options

? ldap_group_object_class = ipaUserGroup

? ldap_group_object_class_alt = posixGroup

? ldap_group_member = member

? ldap_group_uuid = ipaUniqueID

? ldap_group_objectsid = ipaNTSecurityIdentifier

- ? ldap_group_external_member = ipaExternalMember

SUBDOMAINS PROVIDER

The IPA subdomains provider behaves slightly differently if it is configured explicitly or implicitly.

If the option 'subdomains_provider = ipa' is found in the domain section of sssd.conf, the IPA subdomains provider is configured explicitly, and all subdomain requests are sent to the IPA server if necessary.

If the option 'subdomains_provider' is not set in the domain section of sssd.conf but there is the option 'id_provider = ipa', the IPA subdomains provider is configured implicitly. In this case, if a subdomain request fails and indicates that the server does not support subdomains, i.e. is not configured for trusts, the IPA subdomains provider is disabled. After an hour or after the IPA provider goes online, the subdomains provider is enabled again.

TRUSTED DOMAINS CONFIGURATION

Some configuration options can also be set for a trusted domain. A trusted domain configuration can be set using the trusted domain subsection as shown in the example below. Alternatively, the ?subdomain_inherit? option can be used in the parent domain.

```
[domain/ipa.domain.com/ad.domain.com]
ad_server = dc.ad.domain.com
```

For more details, see the sssd.conf(5) manual page.

Different configuration options are tunable for a trusted domain depending on whether you are configuring SSSD on an IPA server or an IPA client.

OPTIONS TUNABLE ON IPA MASTERS

The following options can be set in a subdomain section on an IPA master:

- ? ad_server
- ? ad_backup_server
- ? ad_site
- ? ldap_search_base

- ? ldap_user_search_base
- ? ldap_group_search_base
- ? use_fully_qualified_names

OPTIONS TUNABLE ON IPA CLIENTS

The following options can be set in a subdomain section on an IPA client:

- ? ad_server
- ? ad_site

Note that if both options are set, only ?ad_server? is evaluated.

Since any request for a user or a group identity from a trusted domain triggered from an IPA client is resolved by the IPA server, the ?ad_server? and ?ad_site? options only affect which AD DC will the authentication be performed against. In particular, the addresses resolved from these lists will be written to ?kdcinfo? files read by the Kerberos locator plugin. Please refer to the sssd_krb5_locator_plugin(8) manual page for more details on the Kerberos locator plugin.

FAILOVER

The failover feature allows back ends to automatically switch to a different server if the current server fails.

Failover Syntax

The list of servers is given as a comma-separated list; any number of spaces is allowed around the comma. The servers are listed in order of preference. The list can contain any number of servers.

For each failover-enabled config option, two variants exist: primary and backup. The idea is that servers in the primary list are preferred and backup servers are only searched if no primary servers can be reached. If a backup server is selected, a timeout of 31 seconds is set. After this timeout SSSD will periodically try to reconnect to one of the primary servers. If it succeeds, it will replace the current active (backup) server.

The Failover Mechanism

The failover mechanism distinguishes between a machine and a service.

The back end first tries to resolve the hostname of a given machine; if this resolution attempt fails, the machine is considered offline. No further attempts are made to connect to this machine for any other service. If the resolution attempt succeeds, the back end tries to connect to a service on this machine. If the service connection attempt fails, then only this particular service is considered offline and the back end automatically switches over to the next service. The machine is still considered online and might still be tried for another service.

Further connection attempts are made to machines or services marked as offline after a specified period of time; this is currently hard coded to 30 seconds.

If there are no more machines to try, the back end as a whole switches to offline mode, and then attempts to reconnect every 30 seconds.

Failover time outs and tuning

Resolving a server to connect to can be as simple as running a single DNS query or can involve several steps, such as finding the correct site or trying out multiple host names in case some of the configured servers are not reachable. The more complex scenarios can take some time and SSSD needs to balance between providing enough time to finish the resolution process but on the other hand, not trying for too long before falling back to offline mode. If the SSSD debug logs show that the server resolution is timing out before a live server is contacted, you can consider changing the time outs.

This section lists the available tunables. Please refer to their description in the sssd.conf(5), manual page.

dns_resolver_server_timeout

Time in milliseconds that sets how long would SSSD talk to a single DNS server before trying next one.

Default: 1000

dns_resolver_op_timeout

Time in seconds to tell how long would SSSD try to resolve single DNS query (e.g. resolution of a hostname or an SRV record) before trying the next hostname or discovery domain.

Default: 3

dns_resolver_timeout

How long would SSSD try to resolve a failover service. This service resolution internally might include several steps, such as resolving DNS SRV queries or locating the site.

Default: 6

For LDAP-based providers, the resolve operation is performed as part of an LDAP connection operation. Therefore, also the ?ldap_opt_timeout? timeout should be set to a larger value than ?dns_resolver_timeout? which in turn should be set to a larger value than ?dns_resolver_op_timeout? which should be larger than ?dns_resolver_server_timeout?.

SERVICE DISCOVERY

The service discovery feature allows back ends to automatically find the appropriate servers to connect to using a special DNS query. This feature is not supported for backup servers.

Configuration

If no servers are specified, the back end automatically uses service discovery to try to find a server. Optionally, the user may choose to use both fixed server addresses and service discovery by inserting a special keyword, ?_srv_?, in the list of servers. The order of preference is maintained. This feature is useful if, for example, the user prefers to use service discovery whenever possible, and fall back to a specific server when no servers can be discovered using DNS.

The domain name

Please refer to the ?dns_discovery_domain? parameter in the sssd.conf(5) manual page for more details.

The protocol

The queries usually specify _tcp as the protocol. Exceptions are documented in respective option description.

See Also

For more information on the service discovery mechanism, refer to RFC

2782.

EXAMPLE

The following example assumes that SSSD is correctly configured and example.com is one of the domains in the [sssd] section. This examples shows only the ipa provider-specific options.

```
[domain/example.com]
id_provider = ipa
ipa_server = ipaserver.example.com
ipa_hostname = myhost.example.com
```

SEE ALSO

sssd(8), sssd.conf(5), sssd-ldap(5), sssd-ldap-attributes(5), sssd-krb5(5), sssd-simple(5), sssd-ipa(5), sssd-ad(5), sssd-files(5), sssd-sudo(5), sssd-session-recording(5), sss_cache(8), sss_debuglevel(8), sss_obfuscate(8), sss_seed(8), sssd_krb5_locator_plugin(8), sss_ssh_authorizedkeys(8), sss_ssh_knownhostsproxy(8), sssd-ifp(5), pam_sss(8). sss_rpcidmapd(5) sssd-systemtap(5)

AUTHORS

The SSSD upstream - https://github.com/SSSD/sssd/

SSSD 07/10/2023 SSSD-IPA(5)