Red Hat
Enterprise Linux

FreeIPA Global Catalog challenges

Samba XP - 2020 May 27

Alexander Bokovoy
Red Hat / Samba team

Florence Blanc-Renaud
Red Hat

Red Hat

Who we are?

Alexander:

- Samba team member since 2003
- FreeIPA core developer since 2011

Florence

- LDAP server technology engineer since 2007
- FreeIPA core developer since 2016

Red Hat

This work wouldn't be possible without contribution of many engineers across multiple projects

Samba:

- Andreas Schneider
- Isaac Boukris
- Simo Sorce

389-ds LDAP server

- Thierry Bordaz
- William Brown
- Mark Reynolds
- Ludwig Krispenz

MIT Kerberos

- Greg Hudson
- Robbie Harwood
- Isaac Boukris
- Simo Sorce

and many others

Thank you all!

Red Hat

Why a need for a Global Catalog with FreeIPA

Allow access to Active Directory resources
for IPA users and services

Red Hat

FreeIPA and trust to Active Directory

Frankenstein's Active Directory: for Linux clients, not Windows

Uses 389-ds LDAP server, MIT Kerberos, and Samba NT domain controller code base to implement what Active Directory domain controller sees as a separate Active Directory forest

- LDAP schema optimized for Linux clients and POSIX identity management use cases
  - Flat directory information tree for users, groups, and services
  - No compatibility with Active Directory schema
  - LDAP objects specific to POSIX environment use cases (SUDO rules, own access control rules, etc)
- KDC based on MIT Kerberos, native two-factor authentication and modern pre-authentication methods
- NetLogon and LSA pipes with enough support to allow AD DCs to interoperate via a forest trust
- Integrated DNS server and Certificate Authority

Red Hat

Global Catalog: just a LDAP server?

It is not that simple...

Red Hat

Global Catalog: just a LDAP server?

Global Catalog Entries

LDAP is a communication protocol designed with flexibility and extensibility in mind

- Schema:
  - Syntaxes
  - Attribute types
  - Object Classes
  - Matching rules
- Organizational structure
- Extended operations
- Extended controls

Red Hat

Global Catalog: just a LDAP server?

Global Catalog Schema

Subset of Active Directory LDAP schema

Incompatible with quite a few traditional POSIX LDAP schemas

```
dn: CN=Common-Name,CN=Schema,CN=Configuration,DC=X
objectClass: top
objectClass: attributeSchema
cn: Common-Name
distinguishedName: CN=Common-Name,CN=Schema,CN=Configuration,DC=X
attributeID: 2.5.4.3
attributeSyntax: 2.5.5.12
isSingleValued: TRUE
showInAdvancedViewOnly: TRUE
lDAPDisplayName: cn
name: Common-Name
```


Red Hat

Global Catalog: just a LDAP server?

Global Catalog Entries

Global Catalog replicates partial set of attributes for all users, groups, and machines (and more, if needed) from the whole Active Directory forest

- objectGUID
- objectSid
- userAccountControl
- sAMAccountName
- sAMAccountType
- objectCategory
- nTSecurityDescriptor
- ...

Red Hat

Global Catalog: just a LDAP server?

Global Catalog Organizational Structure

In Active Directory, Global Catalog service exposes users and groups in the same container, with a cn=.. naming format

Global Catalog

- dc=ad,dc=com
  - cn=users
    - cn=oneuser
    - cn=onegroup

FreeIPA primary LDAP instance

- dc=ipa,dc=com
  - **cn=accounts**
    - cn=users
      - **uid**=oneuser
    - **cn=groups**
      - cn=onegroup

Red Hat

Global Catalog: just a LDAP server?

Global Catalog Behavior

In Active Directory, LDAP server has a special handling for search filters for many attributes by allowing alternative representations of attribute values and additional matching rules

- **(objectCategory=*type*)**
  Handled as (objectCategory=CN=*type*,CN=Schema,CN=Configuration,DC=X)
- **(objectSID=S-*1-5-21-3005052257-2375221410-442149667-1380*)**
  Transformed into (objectSID=*AQUAAAAAAAAUVAAAAYXUds6IAk40jq1oaZAUAAA==*) as objectSID is an octetString
- **(member:1.2.840.113556.1.4.1941:=*cn=oneuser,cn=users,DC=X*)**
  Find all the groups that *oneuser* is a memberof (direct or indirect membership)

Red Hat

Global Catalog: FreeIPA's implementation

3 main components

Schema converter

Takes AD schema as input

Maps syntaxes

Maps matching and ordering rules

Handles conflicts

Outputs a 389-ds compatible schema

Separate 389-ds instance

Uses ports 3268 and 3269

GC schema

Specific indexes

SASL auth mapped to read-only user

Synchronization daemon

Based on syncrepl (RFC 4533)

Monitors primary LDAP instance

Applies transformations

Updates entries in GC

Red Hat

Global Catalog: demo

Red Hat

Global Catalog Demo

Connect as IDM user on a windows machine

- member.win2016.test is a (machine) member of win2016.test domain
- idmuser@ipa.test is a user defined in IPA
- Scenario:
  - On member.win2016.test, add idmuser to the “Remote Desktop Users” local group
  - Use *runas /user:ipa.test\idmuser whoami* to check the user can be resolved
  - Connect to member.win2016.test with rdesktop as idmuser
  - Check idmuser properties with whoami

Red Hat

Global Catalog Demo

Access resources as IDM user

- member.win2016.test is a (machine) member of win2016.test domain
- idmuser@ipa.test is a user defined in IPA
- Scenario:
  - On member.win2016.test, aduser allows access to his doc.txt to idmuser
  - Connect to member.win2016.test with rdesktop as idmuser
  - Edit doc.txt as idmuser

Red Hat

Behind the scenes

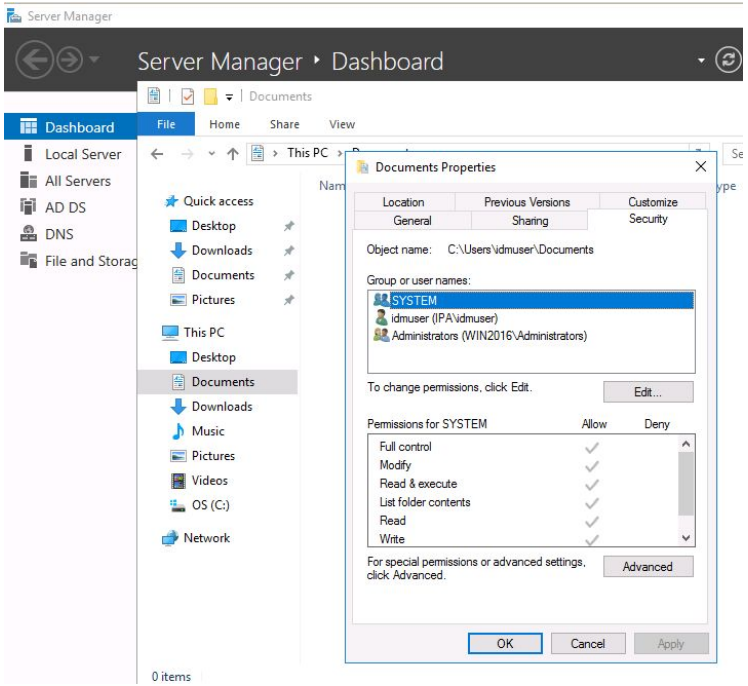
- Lookup an object in Global Catalog
- Translate an object name to SID
- Authenticate and authorize
- Kerberos extensions over trust boundary

Red Hat

Allow access to Active Directory resources for IPA users

Look up in IPA Global Catalog service

- "Security Tab"
  - To add a user to a permission, Windows client component will
    - look up a name in Global Catalog
    - Resolve name to SID via LSA call
    - Add SID to an ACL
  - The connection is done as the currently logged in user
    - Must be authenticated and authorized by the remote DC (IPA master)
    - Two-way forest trust and Kerberos authentication are required
    - LSA pipe connection implies successful Samba authentication and authorization
      - Authenticated identity must have POSIX identity
      - Requested name for SID translation must make sense to Samba



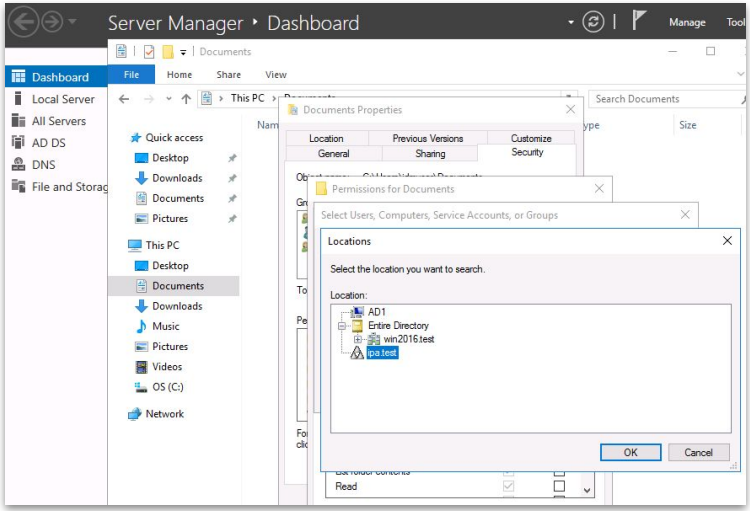
Red Hat

Global Catalog: behind the scenes

Lookup a name in Global Catalog

Expected LDAP server extensions

- Not enough to just have the same schema
- You cannot change clients' behavior
  - Filter rewriters
    - objectCategory support available in 389-ds 1.4.3.6 or later
    - objectSID support available in 389-ds git master now
- No support for AD-specific matching rules yet



2.45 Attribute objectSid

02/14/2019 • 2 minutes to read

This attribute specifies a binary value that specifies the security identifier (SID) of a security principal object. The SID is a unique value used to identify security principal objects. For more information on the SID data type, refer to [MS-DTYP] section 2.4.2. SID usage is also discussed in [MS-ADTS], in particular in section 3.1.1.1.3.

Because this is an attribute of String(SID) syntax, an application writing to this attribute via the LDAP protocol can specify a value for this attribute as a valid SDDL SID string, as specified in [MS-ADTS] section 3.1.1.3.1.2.5. The directory service will convert that value to its binary value equivalent.

```
cn: Object-Sid
ldapDisplayName: objectSid
attributeId: 1.2.840.113556.1.4.146
attributeSyntax: 2.5.5.17
omSyntax: 4
isSingleValued: TRUE
schemaIdGuid: bf9679e8-0de6-11d0-a285-00aa003049e2
systemOnly: TRUE
```

3.1.1.3.4.4 LDAP Matching Rules (extensibleMatch)

03/30/2020 • 2 minutes to read

The following sections describe the matching rules supported by DCs when performing LDAP search requests. Unlike, for example, extended controls and extended operations, there is no attribute exposed by the DC that specifies which matching rules it supports. The identifiers for these matching rules are used in an extensibleMatch clause in the filter portion of a SearchRequest, as described in [RFC2251] section 4.5.1. Matching rules are identified by an OID that corresponds to a human-readable name, as shown in the following table.

Capability name	OID
LDAP_MATCHING_RULE_BIT_AND	1.2.840.113556.1.4.803
LDAP_MATCHING_RULE_BIT_OR	1.2.840.113556.1.4.804
LDAP_MATCHING_RULE_TRANSITIVE_EVAL	1.2.840.113556.1.4.1941
LDAP_MATCHING_RULE_DN_WITH_DATA	1.2.840.113556.1.4.2253

Windows 2000 operating system, Windows Server 2003 operating system, Windows Server 2003 R2 operating system, and Active Directory Application Mode (ADAM) support the LDAP_MATCHING_RULE_BIT_AND and LDAP_MATCHING_RULE_BIT_OR matching rules. Windows Server 2008 operating system and later support those two rules and the LDAP_MATCHING_RULE_TRANSITIVE_EVAL rule, in both AD DS and AD LDS. Windows Server 2012 R2 operating system and later support those three rules and the LDAP_MATCHING_RULE_DN_WITH_DATA rule, in both AD DS and AD LDS.

3.1.1.3.1.3.5 Searches Using the objectCategory Attribute

03/30/2020 • 2 minutes to read

When an LDAP search filter F contains a clause C of the form "(objectCategory=**V**)", if **V** is not a DN but there exists an object O such that O!objectClass = classSchema and O!lDAPDisplayName = **V**, then the server treats the search filter as if clause C was replaced in F with the clause "(objectCategory=**V'**)", where **V'** is O!defaultObjectCategory.

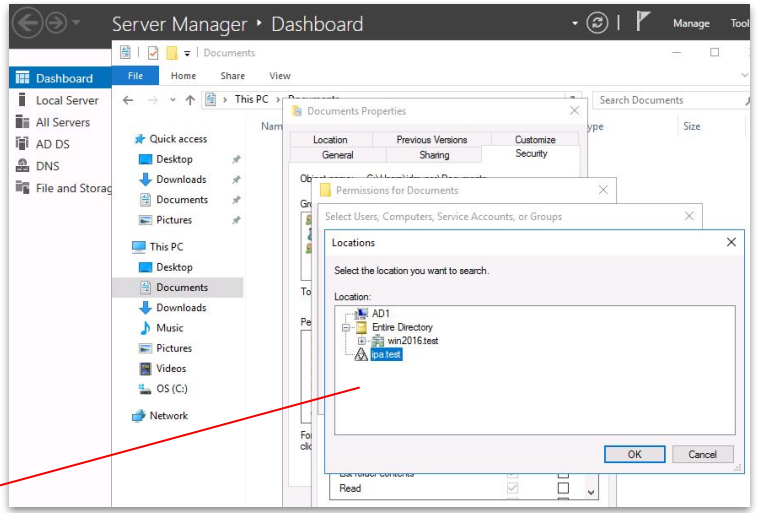
For example, if the LDAP search filter contains clause "(objectCategory=contact)", because the defaultObjectCategory of class contact is CN=person,CN=schema,CN=configuration,DC=Fabrikam,DC=com, Active Directory will treat the clause as "(objectCategory=CN=person,CN=schema,CN=configuration,DC=Fabrikam,DC=com)".

Allow access to Active Directory resources for IPA users

Look up in IPA Global Catalog service

- Requested name to SID translation must make sense to Samba
  - For a forest lookup user or group name would be qualified with forest name instead of NetBIOS name for the forest root domain
    - ipa.test\admins, not IPA\admins
    - Samba will fail this lookup as it expects only NetBIOS name here

```
[2020/01/13 11:12:39.859134,  1, pid=33253, effective(1732401004, 1732401004), real(1732
      lsa_LookupNames3: struct lsa_LookupNames3
         in: struct lsa_LookupNames3
             handle                   : *
                 handle: struct policy_handle
                     handle_type              : 0x00000000 (0)
                     uuid                     : 0000000e-0000-0000-1c5e-a750e5810000
             num_names                : 0x00000001 (1)
             names: ARRAY(1)
                 names: struct lsa_String
                     length                   : 0x001e (30)
                     size                     : 0x0020 (32)
                     string                   : *
                         string                   : 'ipa.test\admins'
             sids                     : *
                 sids: struct lsa_TransSidArray3
                     count                    : 0x00000000 (0)
                     sids                     : NULL
             level                    : LSA_LOOKUP_NAMES_UPLEVEL_TRUSTS_ONLY2 (6)
             count                    : *
                 count                    : 0x00000000 (0)
             lookup_options           : LSA_LOOKUP_OPTION_SEARCH_ISOLATED_NAMES (0)
             client_revision          : LSA_CLIENT_REVISION_2 (2)
```




```
diff --git a/source3/passdb/lookup_sid.c b/source3/passdb/lookup_sid.c
index 82c47b3145b..26bdb31149e 100644
--- a/source3/passdb/lookup_sid.c
+++ b/source3/passdb/lookup_sid.c
@@ -114,7 +114,8 @@ bool lookup_name(TALLOC_CTX *mem_ctx,
        DEBUG(10, ("lookup_name: flags = 0x0%x\n", flags));

        if (((flags & LOOKUP_NAME_DOMAIN) || (flags == 0)) &&
-           strequal(domain, get_global_sam_name())))
+           (strequal(domain, get_global_sam_name()) ||
+            strequal(domain, lp_realm())))
        {

                /* It's our own domain, lookup the name in passdb */
```

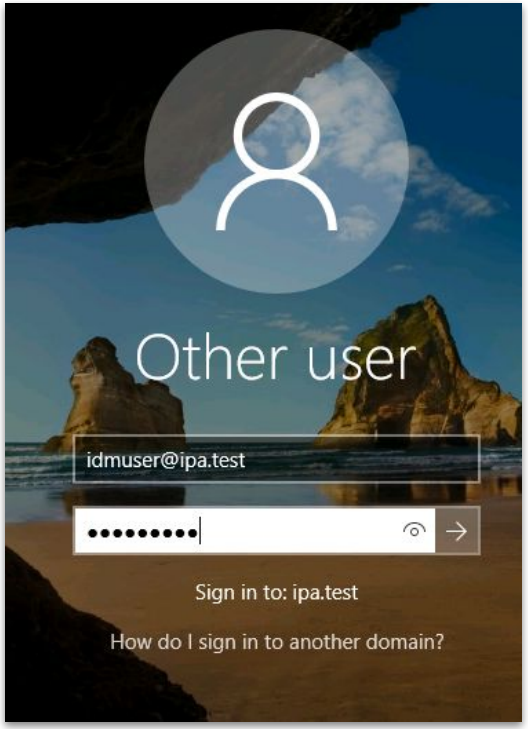
Authentication and authorization

Logon to Windows workstation

- Windows logon uses enterprise principal name type
  - Any UPN associated with the trusted forest would work
- Windows workstation attempts to authenticate against own DC
  - AD DC issues cross-realm client referral to IPA KDC
- IPA KDC handles AS-REQ and then TGS-REQ for cross-realm TGT back to AD
  - Windows workstation asks own DC to lookup user name to SID with LSA LookupNames3 call, level 6 (LOOKUP_NAMES_UPLEVEL_TRUSTS_ONLY2)
  - This call gets relayed to IPA DC for a response over the trust link
  - Same happens for the SID obtained from LookupNames3, by using LSA LookupSids2 request

several times

- Actual logon process goes forward, relying on MS-PAC content of the original Kerberos ticket



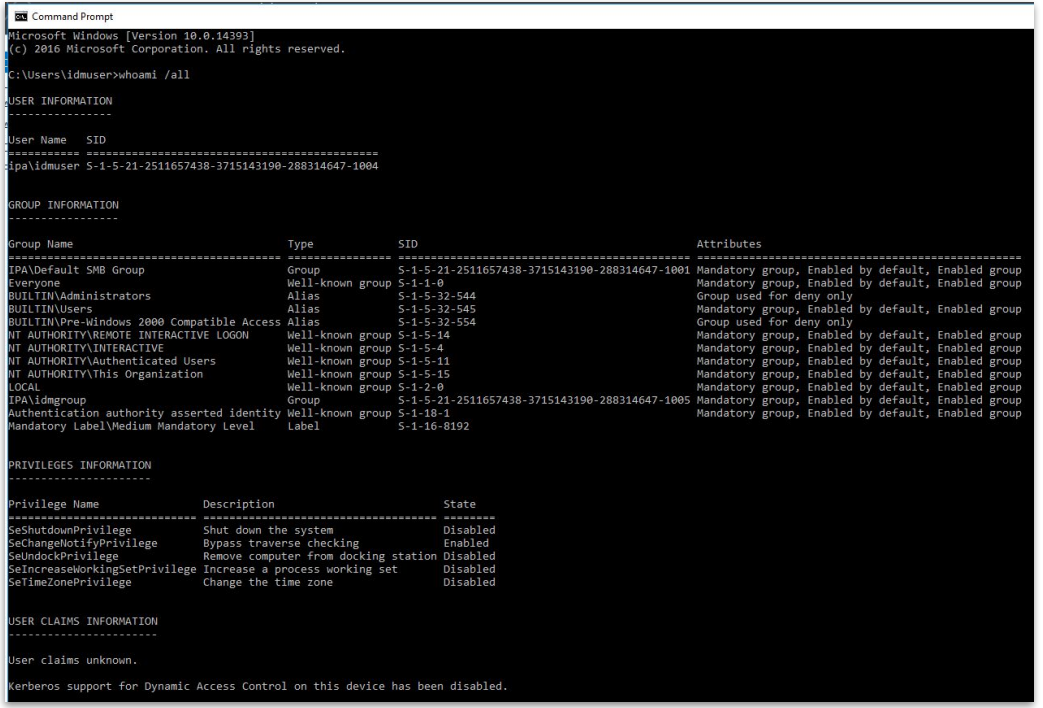
Red Hat

Global Catalog: behind the scenes

Authorization

Logon to Windows workstation

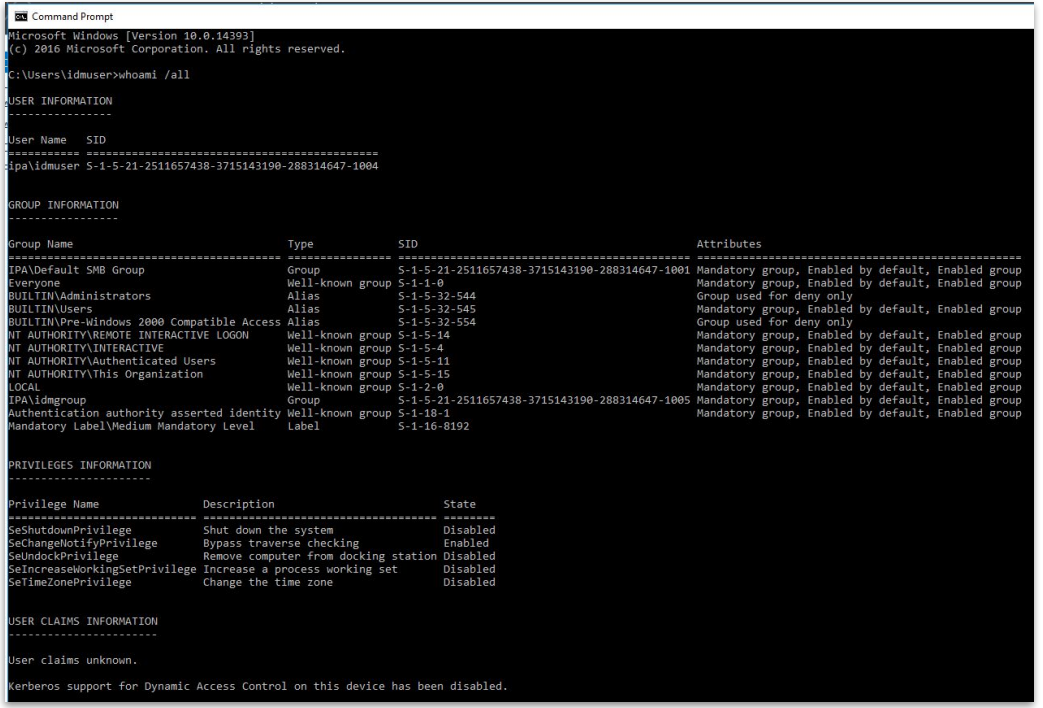
- Windows requires PAC record presence in the Kerberos tickets
  - Content of PAC is important but there is a level of acceptance
- FreeIPA issues tickets with PAC for users and selected Kerberos services
  - Didn't work for S4U2Self protocol transition over trust
  - Still issues with MIT Kerberos and User-to-User authentication
- KERB_VALIDATION_INFO (INFO3 structure) needs to be properly set up
  - Logon time must be set to a reasonable value (or a password reset will be recommended by Windows)
  - Group membership should include also a primary group
  - Optional but expected: extra SIDs should encode asserted identities
- UPN_DNS_INFO buffer has to exist



Red Hat

Kerberos extensions over trust boundary

- Windows applications rely on S4U extensions
  - A lot: workstation to workstation requests, remote terminal access, security token refreshes
- S4U2Proxy delegation is supported in FreeIPA
- Constrained delegation support added in MIT Kerberos 1.18
  - Not integrated yet in FreeIPA
- S4U2Self
  - Recently fixed in FreeIPA for cross-realm operations
  - User-to-User still fails when aliases are used in the second ticket (remote terminal access)
- No support for claims yet



Red Hat

Future plans

- Add group lookup support in FreeIPA PASSDB module
- Add group lookup support to tdbsam and tests to Samba to allow lookup of groups via PASSDB
- Complete 389-ds support for matching rules required by Active Directory clients
- Fix principal aliases lookup in MIT Kerberos
  - Needed for MIT-based Samba AD DC as well
- Teach SSSD to use IPA global catalog when trust is between IPA and IPA domains

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.


linkedin.com/company/red-hat


youtube.com/user/RedHatVideos


facebook.com/redhatinc


twitter.com/RedHat

Red Hat