Test Lab Guide: Demonstrate Permissions with SharePoint Server 2013

Test Lab Guide: Demonstrate Permissions with SharePoint Server 2013

Joe Davies
Microsoft Corporation

Published: May 2013

Applies to: SharePoint Server 2013

Summary: This paper contains a brief introduction to SharePoint Server 2013 and step-by-step instructions for configuring and demonstrating permissions behavior for intranet and team sites based on the Test Lab Guide: Configure Intranet and Team Sites with SharePoint Server 2013. This paper does not describe how to install and configure SharePoint Server 2013 in a pilot or production environment. For more information, see Install and deploy SharePoint 2013.

Date	Description
August 4, 2013	Updated to include a link to the new overview video.
May 7, 2013	Initial publication

Contents

Contents 2
Introduction 3
Test Lab Guides 3
In this guide 4
Test lab overview 5
Hardware and software requirements 6
Steps for Configuring the SharePoint Server 2013 Permissions Test Lab 7
Step 1: Set up intranet and team sites test lab 7
Step 2: Prepare groups and accounts and initial permissions 7
Step 3: Configure a secured Human Resources subsite 10
Step 4: Configure a subsite for vendor use 13
Step 5: Configure an archives subsite 16
Snapshot the Configuration 19
Additional Resources 19

Introduction

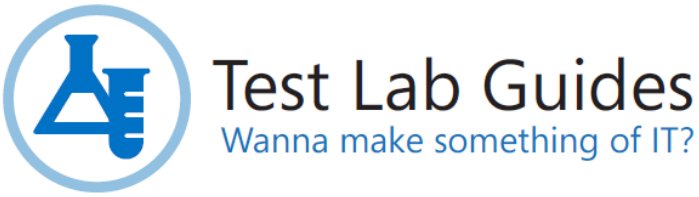
Microsoft® SharePoint® Server 2013 makes it easy for people to work together. SharePoint Server 2013 enables you and your employees to set up web sites to share information with others, manage documents from start to finish, and publish reports to help everyone make informed decisions.

SharePoint Server 2013 has the following capabilities:

- **Sites** Provides a single infrastructure for all your business web sites. Share documents with colleagues, manage projects with partners, and publish information to customers.
- **Communities** Delivers great collaboration tools—and a single platform to manage them. Make it easy for people to share ideas and work together the way they want.
- **Composites** Offers tools and components for creating do-it-yourself business solutions. Build no-code solutions to rapidly respond to business needs.
- **Content** Makes content management easy. Set up compliance measures ”behind the scenes”—with features like document types, retention polices, and automatic content sorting—and then let people work naturally in Microsoft Office.
- **Insights** Gives everyone access to the information in databases, reports, and business applications. Help people locate the information to make good decisions.
- **Search** Cuts through the clutter. A unique combination of relevance, refinement, and social cues helps people find the information and contacts they need to get their jobs done.

For more information about Microsoft SharePoint Server 2013, see the SharePoint 2013 Product Information site and SharePoint 2013 for IT pros.

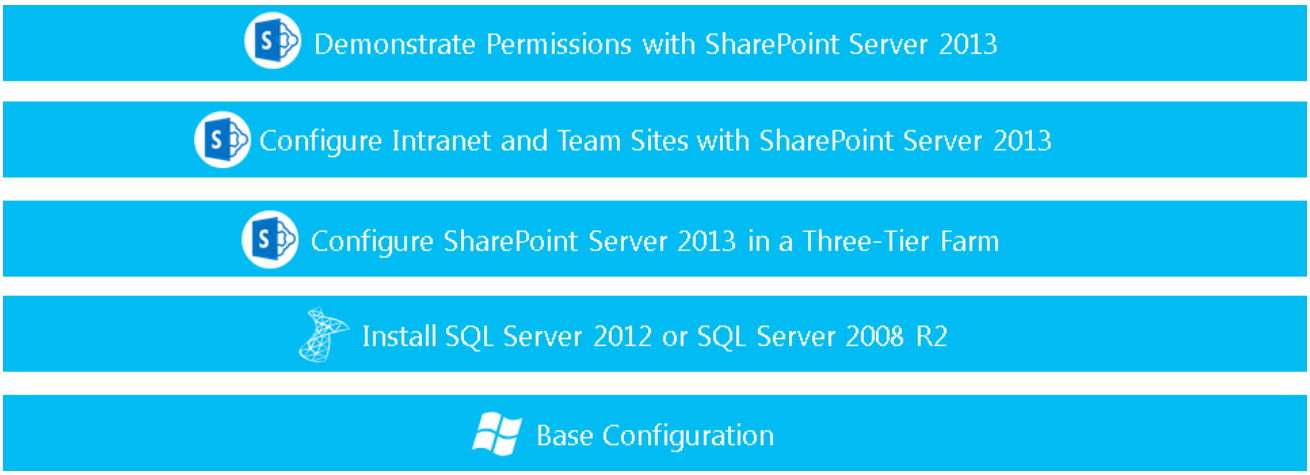
Test Lab Guides



Microsoft Test Lab Guides (TLGs) are a set of documents that step you through the configuration and demonstration of a Microsoft technology or product in a standardized test lab environment, which starts with a common base configuration that mimics a simplified intranet and the Internet. TLGs are designed to be modular, extensible, and stackable to configure complex, multi-product solutions. TLGs make learning about products, technologies, and solutions easier by providing that crucial hands-on, “I built it out myself” experience.

For more information, see Test Lab Guides at http://microsoft.com/testlabguides.

A TLG stack is a set of dependent TLGs that, when configured from the bottom of the stack, create a meaningful test lab configuration. This TLG is at the top of the following TLG stack:



In this guide

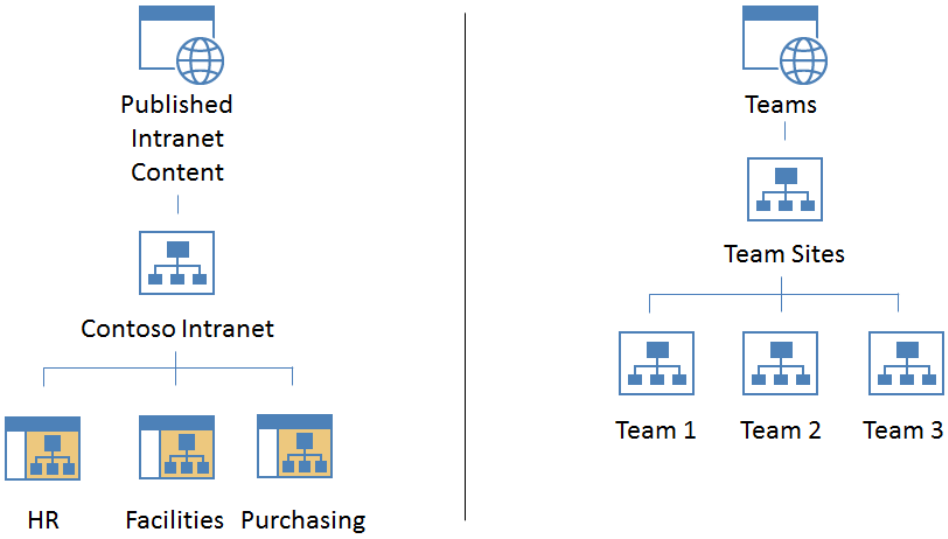
This paper explains how to configure and then demonstrate the behavior of SharePoint permissions in three scenarios:

- Locking down a subsite so that only members of a specific department can access it
- Creating a subsite that the vendors of an organization can access
- Creating an Archives subsite so that documents can be added, viewed, and changed, but not deleted

Our starting point is the web applications, site collections, and subsites for intranet departments and teams as configured in the Test Lab Guide: Configure Intranet and Team Sites with SharePoint Server 2013, which consists of the following:

- The Published Intranet Content web application, which contains the Contoso Intranet site collection and the three subsites for the Human Resources (HR), facilities, and purchasing departments.
- The Teams web application, which contains the Team Sites root site collection and site collections for Teams 1, 2, and 3.

See the following figure.



For a short video that describes the configuration of this test lab, see the SharePoint Permissions TLG overview.

For information about permissions in SharePoint 2013, see the following:

- Permissions planning for sites and content in SharePoint 2013
- Configure custom permissions in SharePoint 2013
- User permissions and permission levels in SharePoint 2013

Important

The following instructions configure a SharePoint Server 2013 test lab by using the minimum number of computers. Individual computers are needed to separate services provided on the network and to clearly show the desired functionality. This configuration is neither designed to reflect best practices nor does it reflect a desired or recommended configuration for a production network. The configuration, including IP addresses and all other configuration parameters, is designed only to work on a separate test lab network. Attempting to adapt this test lab configuration to a pilot or production deployment can result in configuration or functionality issues.

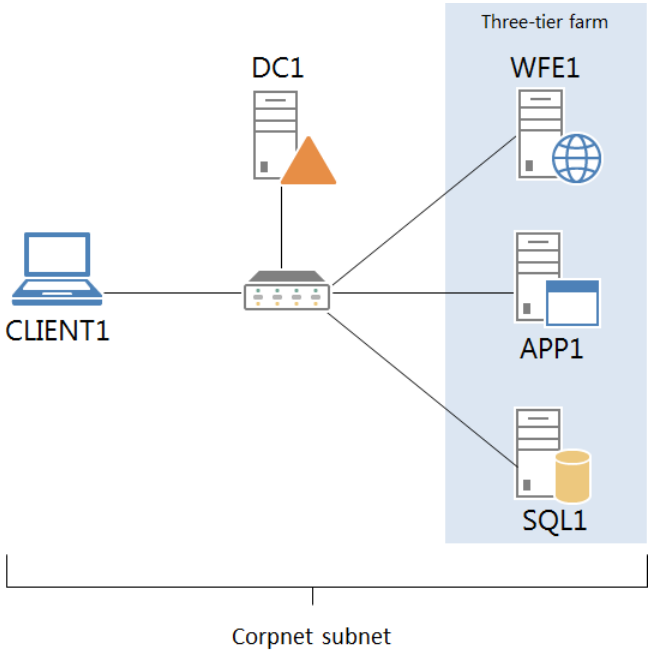
Test lab overview

In this test lab, SharePoint Server 2013 is deployed in a three-tier farm by using the following:

- One computer running Windows® Server® 2008 R2 Enterprise Edition with Service Pack 1 named DC1 that is configured as an intranet domain controller, Domain Name System (DNS) server, DHCP server, and enterprise root certification authority (CA).
- One intranet member server running Windows Server 2008 R2 Enterprise Edition with Service Pack 1 named SQL1 that is configured as a SQL database server.

- One intranet member server running Windows Server 2008 R2 Enterprise Edition with Service Pack 1 named APP1 that is configured as the SharePoint Server 2013 application server.
- One intranet member server running Windows Server 2008 R2 Enterprise Edition with Service Pack 1 named WFE1 that is configured as the SharePoint front-end web server.
- One member client computer running Windows 7 Enterprise or Ultimate named CLIENT1.

The SharePoint Server 2013 test lab consists of a single subnet named Corpnet (10.0.0.0/24) that simulates a private intranet. Computers on the Corpnet subnet connect by using a hub or switch. See the following figure.



Hardware and software requirements

The following are required components of the test lab:

- The product disc or files for Windows Server 2008 R2 with Service Pack 1.
- The product disc or files for Windows 7.
- The product disc or files for Microsoft SQL Server 2012 or Microsoft SQL Server 2008 R2 with Service Pack 1.
- The product disc or files for SharePoint Server 2013.
- Four computers that meet the minimum hardware requirements for Windows Server 2008 R2 Enterprise Edition.

- One computer that meets the minimum hardware requirements for Windows 7 Enterprise or Ultimate.

Steps for Configuring the SharePoint Server 2013 Permissions Test Lab

Use the following steps to set up the SharePoint Server 2013 permissions lab.

1. Set up the intranet and team sites test lab.
2. Prepare groups and accounts and initial permissions.
3. Configure a secured Human Resources subsite.
4. Configure a subsite for vendor use.
5. Configure an archives subsite.

Note

You must be logged on as a member of the Domain Admins group or a member of the Administrators group on each computer to complete the tasks described in this guide. If you cannot complete a task while you are logged on with an account that is a member of the Administrators group, try performing the task while you are logged on with an account that is a member of the Domain Admins group.

The following sections provide details about how to perform these steps.

Step 1: Set up intranet and team sites test lab

Set up intranet and team sites test lab by using the procedures in the Test Lab Guide: Configure Intranet and Team Sites with SharePoint Server 2013.

Step 2: Prepare groups and accounts and initial permissions

In this section, you configure the accounts and groups that enable you to configure and demonstrate the three scenarios: a secured Human Resources subsite, a site for vendor documents, and an archival subsite.

To create the accounts and groups

1. Log in to DC1 with the CORP\User1 account.
2. Click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
3. In the console tree, open the **corp.contoso.com** domain.
4. Right-click **Users**, point to **New**, and then click **User**.
5. Type **User2** in **First name**, type **user2** in **User logon name**, and then click **Next**.
6. Type **P@ssword1** in **Password**, **Confirm password**, clear **User must change password at next logon**, select **Password never expires**, click **Next**, and then click **Finish**.
7. Right-click **Users**, point to **New**, and then click **Group**.

8. Double-click the new **Teams** group, click the **Members** tab, click **Add**, type **user1;user2**, and then click **OK** twice.
9. Right-click **Users**, point to **New**, and then click **Group**.
10. Type **HR** in **Group name**, and then click **OK**.
11. Right-click **Users**, point to **New**, and then click **User**.
12. Type **HRUser1** in First name, type **hruser1** in **User logon name**, and then click **Next**.
13. Type **P@ssword1** in **Password**, **Confirm password**, clear **User must change password at next logon**, select **Password never expires**, click **Next**, and then click **Finish**.
14. In the details pane, right-click the **HRUser1** user account, and then click **Add to a group**.
15. Type **HR**, and then click **OK** twice.
16. Right-click **Users**, point to **New**, and then click **Group**.
17. Type **Vendors** in **Group name**, and then click **OK**.
18. Right-click **Users**, point to **New**, and then click **User**.
19. Type **V-Vendor1** in **First name**, type **v-vendor1** in **User logon name**, and then click **Next**.
20. Type **P@ssword1** in **Password**, **Confirm password**, clear **User must change password at next logon**, select **Password never expires**, click **Next**, and then click **Finish**.
21. In the details pane, double-click the **Vendor1** user account.
22. Click the **Member of** tab, and then click **Add**.
23. Type **vendors**, and then click **OK**.
24. In the list of groups under **Member of**, click **Vendors**, and then click **Set Primary Group**.
25. Click **Domain Users**, click **Remove**, and then click **Yes**.

In the following procedure, you demonstrate the access to the intranet and team sites for the User1 and User2 accounts.

To test the default access the intranet and team sites from CLIENT1

1. On CLIENT1, log on with the CORP\User1 account.
2. Start Internet Explorer.
3. Verify that you can access to the following URLs:
    - http://intranet.corp.contoso.com
    - http://teams.corp.contoso.com/sites/team1
    - http://teams.corp.contoso.com/sites/team2
    - http://teams.corp.contoso.com/sites/team3
4. Log off and log on with the CORP\User2 account (the password is P@ssword1).
5. Start Internet Explorer.
6. Verify that you **cannot** access to the following URLs:
    - http://intranet.corp.contoso.com

- http://teams.corp.contoso.com/sites/team1
- http://teams.corp.contoso.com/sites/team2
- http://teams.corp.contoso.com/sites/team3

Because User2 or user accounts other than User1 have not been granted access to the resources of the Contoso Intranet and teams sites, you cannot access them unless you use the User1 account.

In the following procedure, you configure initial permissions for the Contoso Intranet and teams site collections.

To create the initial permissions for the Contoso Intranet, Team 1, Team 2, and Team 3 site collections

1. Log on to CLIENT1 with the CORP\User1 account.
2. Start Internet Explorer and browse to **http://intranet.corp.contoso.com**.
3. On the Contoso Intranet page, click the **Settings** icon in the upper-right corner (the cogged wheel), and then click **Site Settings**.
4. In the **Users and Permissions** group, click **Site permissions**.
5. In the list, click **Contoso Intranet Members**.
6. On the Contoso Intranet Members page, click **New**.
7. In **Share 'Contoso Intranet'**, type **domain users**, click the resolved name, and then click **Share**.
8. Use Internet Explorer to browse to **http://teams.corp.contoso.com/team1**.
9. On the Team 1 page, click the **Settings** icon in the upper-right corner (the cogged wheel), and then click **Site Settings**.
10. In the **Users and Permissions** group, click **Site permissions**.
11. In the list, click **Team 1 Members**.
12. On the Team 1 Members page, click **New**.
13. In **Share 'Team 1'**, type **teams**, click the resolved name, and then click **Share**.
14. Use Internet Explorer to browse to **http://teams.corp.contoso.com/team2**.
15. On the Team 2 page, click the **Settings** icon in the upper-right corner (the cogged wheel), and then click **Site Settings**.
16. In the **Users and Permissions** group, click **Site permissions**.
17. In the list, click **Team 2 Members**.
18. On the Team 2 Members page, click **New**.
19. In **Share 'Team 2'**, type **teams**, click the resolved name, and then click **Share**.
20. Use Internet Explorer to browse to **http://teams.corp.contoso.com/team3**.
21. On the Team 3 page, click the **Settings** icon in the upper-right corner (the cogged wheel), and then click **Site Settings**.
22. In the **Users and Permissions** group, click **Site permissions**.
23. In the list, click **Team 3 Members**.
24. On the **Team 3 Members** page, click **New**.

25. In **Share 'Team 3'**, type **teams**, click the resolved name, and then click **Share**.
26. Log off, and then log on with the CORP\User2 account.
27. Start Internet Explorer.
28. Verify that you can now access to the following URLs:
    a. http://intranet.corp.contoso.com
    b. http://teams.corp.contoso.com/sites/team1
    c. http://teams.corp.contoso.com/sites/team2
    d. http://teams.corp.contoso.com/sites/team3

This is now successful because User2 has explicit permissions through membership in the following:

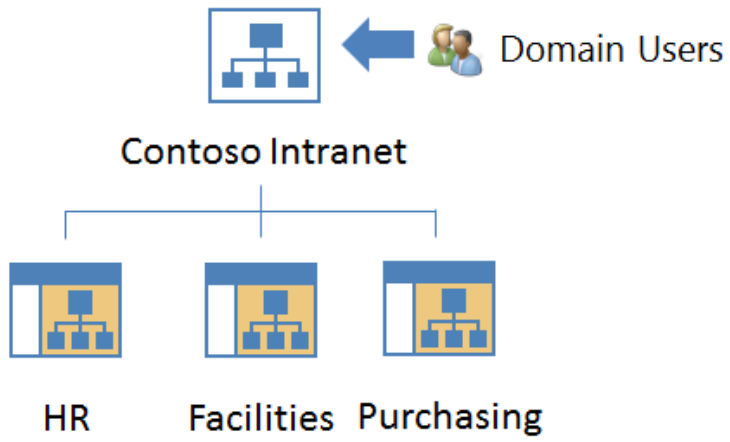
- Contoso Intranet Members group for the Contoso Intranet site collection (by using the Domain Users security group)
- Team 1 Members group for the Team 1 site collection (by using the Teams security group)
- Team 2 Members group for the Team 2 site collection (by using the Teams security group)
- Team 3 Members group for the Team 3 site collection (by using the Teams security group)

Step 3: Configure a secured Human Resources subsite

In this section, you configure permissions on the Human Resources subsite so that it is locked down and accessible only for the HR department.

The starting point is the permissions configured in **Step 2: Prepare groups and accounts and initial permissions** of this guide, in which the Contoso Intranet site collection was configured with the Domain Members security group as a member of the Contoso Intranet Members group. These permissions by default flow down to the HR, Facilities, and Purchasing subsites.

See the following figure.



In this section, you will do the following:

- In the Human Resources subsite (HR in the preceding figure), break permissions inheritance and configure the HR Members group with the HR security group as a member.
- Demonstrate that you can access the Human Resources subsite only when logged on as HRUser1 (or User1, because it is a site collection administrator).

To secure the Human Resources subsite

1. On CLIENT1, log off and then log on with the CORP\User2 account (the password is P@ssword1).
2. Start Internet Explorer and browse to **http://intranet.corp.contoso.com**.
3. On the Contoso Intranet page, click **Human Resources**.

   Note that you can view the Human Resources subsite page.
4. Log off CLIENT1, and then log on with the CORP\User1 account.
5. Start Internet Explorer and browse to **http://intranet.corp.contoso.com**.
6. On the Contoso Intranet page, click **Human Resources**.
7. On the Human Resources page, click the **Settings** icon in the upper-right corner (the cogged wheel), and then click **Site Settings**.
8. In the **Users and Permissions** section, click **Site permissions**.
9. In the ribbon, click **Stop Inheriting Permissions**, and then click **OK**.
10. In **Set up Groups for this Site**, in the **Visitors to this Site** section, click **Create a new group**.
11. In the **Members of this Site** section, click **Create a new group**, and then type **HR Members** for group name.
12. In the box below **Human Resources Members**, delete **User1**, type **HR**, and then click the **Check Names** icon.
13. In the **Owners of this Site** section, click **Create a new group**, and then type **HR Owners** for group name.
14. Click **OK**.
15. On the Human Resources page, click the **Settings** icon in the upper-right corner (the cogged wheel), and then click **Site Settings**.
16. In the **Users and Permissions** group, click **Site permissions**.
17. In the list of groups, select **Contoso Intranet Members**, **Contoso Intranet Owners**, and **Contoso Intranet Visitors**.
18. In the ribbon, click **Remove User Permissions**, and then click **OK**.
19. In the ribbon, click **Check Permissions**.
20. In **Human Resources: Check Permissions**, type **User1** in **User/Group**, and then click **Check Now**.

    You should see that User1 has no permission levels, but there is a list of factors that also affect the level of access. These are permissions that the User1 account has because it is the configured site administrator for the Contoso Intranet site collection.

21. Remove **User1** and type **User2** in **User/Group**, and then click **Check Now**.

    You should see that User2 has no permission levels given.

22. Remove **User2** and type **V-Vendor1** in **User/Group**, and then click **Check Now**.

    You should see that V-Vendor1 has no permission levels.

23. Remove **V-Vendor1** and type **HRUser1** in **User/Group**, and then click **Check Now**.

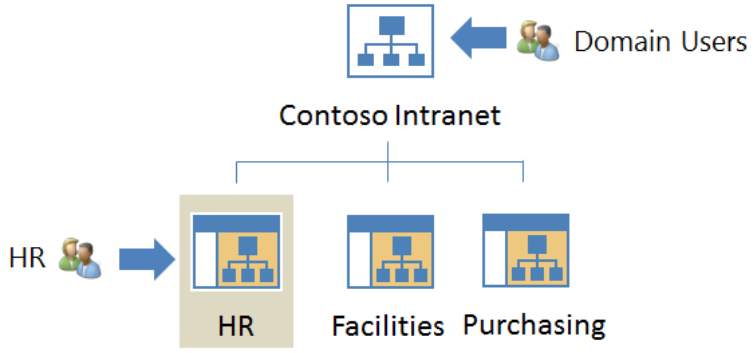
    You should see that HRUser1 has the Edit permissions level, based on its membership in the HR security group, which is a member of the Human Resources Members group.

24. Click **Close**.

The resulting site infrastructure and permissions configuration is the following:

- The Domain Users security group has edit-level permissions for the Contoso Intranet site collection, and those permissions still flow down into the Facilities and Purchasing subsites.
- The HR subsite has custom permissions, with the HR security group having edit-level permissions.

See the following figure.



To demonstrate access to the Human Resources subsite

1. On CLIENT1, log off and then log on with the CORP\User2 account (the password is P@ssword1).
2. Start Internet Explorer and browse to **http://intranet.corp.contoso.com**.
3. On the Contoso Intranet page, note that there is no longer a link for the Human Resources subsite.
4. Use Internet Explorer to browse to **http://intranet.corp.contoso.com/hr**.

   You should see a **Sorry, this site hasn't been shared with you** message.

5. Log off CLIENT1 and then log on with the CORP\HRUser1 account (the password is P@ssword1).
6. Start Internet Explorer and browse to **http://intranet.corp.contoso.com**.
7. On the Contoso Intranet page, click **Human Resources**.

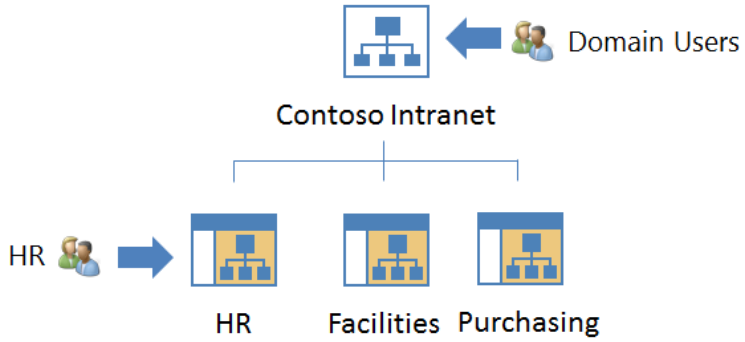
   You should see the Human Resources page.

Step 4: Configure a subsite for vendor use

In this section, you create a Vendors subsite and permissions so that users and vendors can access it, but vendors cannot access any other part of the Published Intranet Content or Teams web applications.

The starting point is the permissions configured in **Step 2: Prepare groups and accounts and initial permissions** of this guide, in which the Contoso Intranet site collection was configured with the Domain Members security group as a member of the Contoso Intranet Members group. These permissions by default flow down to the Facilities and Purchasing subsites.

See the following figure.



In this section, you will do the following:

- Create a new subsite named Vendors in the Facilities subsite.
- In the Vendors subsite, break permissions inheritance and configure the Vendors Members group with the User2 account and the Vendors security group as members.
- Demonstrate that when you are logged on as:
  - HRUser1, you cannot access the Vendors subsite.
  - User2, you can access the Vendors subsite.
  - V-Vendor1, you can access the Vendors subsite, but you cannot access any other subsite or site collection of the Published Intranet Content or Teams web applications.

To configure a Vendors subsite with vendor access permissions

1. On CLIENT1, log off and then log on with the CORP\User1 account.
2. Start Internet Explorer and browse to **http://intranet.corp.contoso.com**.
3. On the Contoso Intranet page, click **Facilities**.
4. Click **Site Contents** in the Quick Launch, and then click **new subsite**.
5. Type **Vendors** in **Title**, type **vendors** in **URL name**, click **Use unique permissions**, and then click **Create**.
6. In **Set up Groups for this Site**, in the **Members of this Site** section, in the box below **Vendors Members**, delete **User1**, type **Vendors**, click the **Check Names** icon, type **User2**, and then click the **Check Names** icon.
7. Click **OK**.

8. On the Vendors page, click the **Settings** icon in the upper-right corner (the cogged wheel), and then click **Site Settings**.
9. In the **Users and Permissions** group, click **Site permissions**.
10. Click **Check Permissions** in the ribbon.
11. In **Vendors: Check Permissions**, type **User1** in **User/Group**, and then click **Check Now**.

    You should see that User1 has the Full Control permission level.

12. Remove **User1**, type **User2** in **User/Group**, and then click **Check Now**.

    You should see that User2 has the Edit permission level given through the Vendors Members group.

13. Remove **User2**, type **HRUser1** in **User/Group**, and then click **Check Now**.

    You should see that HRUser1 has no permission levels.

14. Remove **HRUser1**, type **V-Vendor1** in **User/Group**, and then click **Check Now**.

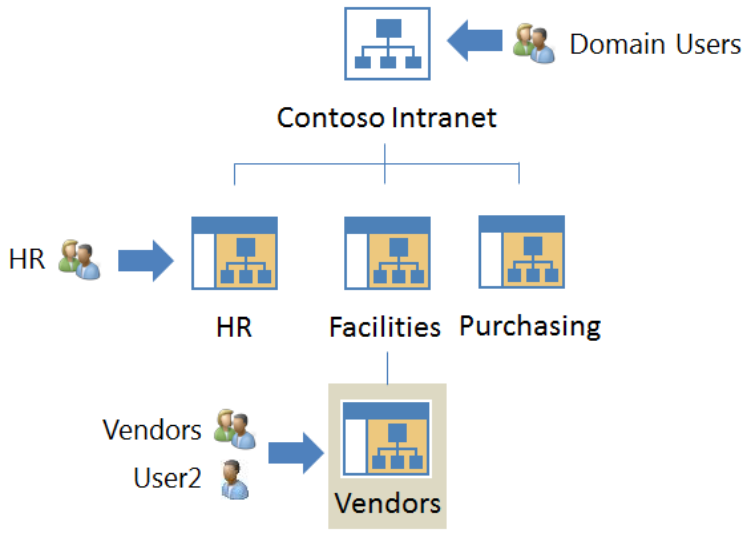
    You should see that V-Vendor1 has the Edit permission level given through the Vendors Members group.

15. Click **Close**.

The resulting site infrastructure and permissions configuration is the following:

- The Domain Users security group has edit-level permissions for the Contoso Intranet site collection, and those permissions still flow down into the Facilities and Purchasing subsites.
- The HR subsite has custom permissions, with the HR security group having edit-level permissions.
- The Vendors subsite has custom permissions, with the Vendors security group and the User2 account having edit-level permissions.

See the following figure.



To demonstrate access to the Vendors subsite

1. On CLIENT1, log off and then log on with the CORP\HRUser1 account (the password is P@ssword1).
2. Start Internet Explorer and browse to **http://intranet.corp.contoso.com/facilities**.
3. On the Facilities page, note that there is no link for the Vendors subsite.
4. Use Internet Explorer to browse to **http://intranet.corp.contoso.com/facilities/vendors**.

   You should see a **Sorry, this site hasn't been shared with you** message.

5. Log off CLIENT1 and then log on with the CORP\User2 account (the password is P@ssword1).
6. Start Internet Explorer and browse to **http://intranet.corp.contoso.com/facilities**.
7. On the Facilities page, click **Vendors**.

   You should see the Vendors page.

8. Log off CLIENT1 and then log on with the CORP\v-vendor1 account (the password is P@ssword1).
9. Start Internet Explorer and browse to the following locations:
   a. http://intranet.corp.contoso.com
   b. http://intranet.corp.contoso.com/facilities
   c. http://teams.corp.contoso.com/team1
10. In each case, you should see a **Sorry, this site hasn't been shared with you** message.
11. Use Internet Explorer to browse to **http://intranet.corp.contoso.com/facilities/vendors**.

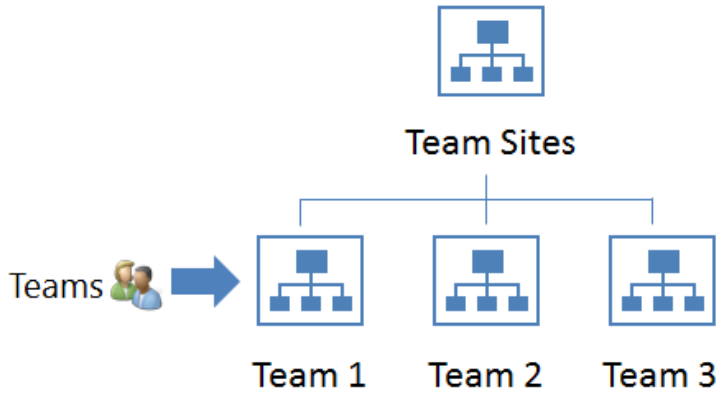
    You should now see the Vendors subsite page.

Step 5: Configure an archives subsite

In this section, you create an Archives subsite in the Team 1 site collection and use a custom permission level so that users who are not site collection administrators can view, add, and change documents, but not delete them.

The starting point is the permissions configured in **Step 2: Prepare groups and accounts and initial permissions** of this guide, in which the Team 1 site collection was configured with the Teams security group as a member of the Team 1 Members group. These permissions by default will flow down to any subsites of the Team 1 site collection.

See the following figure.



In this section, you will do the following:

- Create a new custom permissions level named Archive in the Team 1 site collection.
- Create a new subsite named Archives in the Team 1 site collection.
- In the Archives subsite, break permissions inheritance and configure the Archives Members group with the Teams security group as a member with the Archive permission level.
- Add a document to the Archives subsite (logged on as User1).
- Demonstrate that when logged on as User2, you can add and view documents in the Archives subsite, but not delete them.

To configure an Archives subsite with a custom permission level

1. On CLIENT1, log off and then log on with the CORP\User1 account.
2. Start Internet Explorer and browse to **http://teams.corp.contoso.com/sites/team1**.
3. On the Team 1 page, click the **Settings** icon in the upper-right corner (the cogged wheel), and then click **Site Settings**.
4. In the **Users and Permissions** group, click **Site permissions**.
5. Click **Permission Levels** in the ribbon.
6. In Permission Levels, click **Add a Permission Level**.
7. In **Add Permission Policy Level**, type **Archive** in **Name**, and then type **Add, view, change, but not delete.** in **Description**.

8. In **Permissions**, in the **List Permissions** section, select the following:
    a. Add Items
    b. Edit Items
    c. View Items
    d. Approve Items
    e. Open Items
    f. View Versions
    g. Create Alerts
    h. View Application Pages
9. In **Permissions**, in the **Site Permissions** section, select the following:
    a. Use Self-Service Site Creation
    b. View Pages
    c. Browse User Information
    d. Use Remote Interfaces
    e. Use Client Integration Features
    f. Open
10. Click **Create**, and then click **OK**.
11. Click **Site Contents** in the Quick Launch, and then click **new subsite**.
12. In **New SharePoint Site**, type **Archives** in **Title**, **archives** in **URL name**, and then click **Create**.
13. On the **Archives** page, click the **Settings** icon in the upper-right corner (the cogged wheel), and then click **Site Settings**.
14. In the **Users and Permissions** group, click **Site permissions**.
15. Click **Stop Inheriting Permissions** in the ribbon, and then click **OK**.
16. In **Set Up Groups for this Site**, click **OK**.
17. Click the **Settings** icon in the upper-right corner (the cogged wheel), and then click **Site Settings.**
18. In the **Users and Permissions** group, click **Site permissions.**
19. Click **Create Group** in the ribbon.
20. In **Create Group**, type **Archive Members** in **Name**.
21. In **Give Group Permission to this Site**, select **Archive**, and then click **Create**.
22. In **Archive Members**, click **New**, type **Teams**, type the resolved name, and then click **Share**.
23. On the Archive Members page, click the **Settings** icon in the upper-right corner (the cogged wheel), and then click **Site Settings**.
24. In the **Users and Permissions** group, click **Site permissions**.
25. In the list of groups, select **Team 1 Members**, **Team 1 Owners**, and **Team 1 Visitors**.
26. Click **Remove User Permissions** in the ribbon, and then click **OK**.
27. Click **Check Permissions** in the ribbon.
28. In **Archives: Check Permissions**, type **User1** in **User/Group**, and then click **Check Now**.

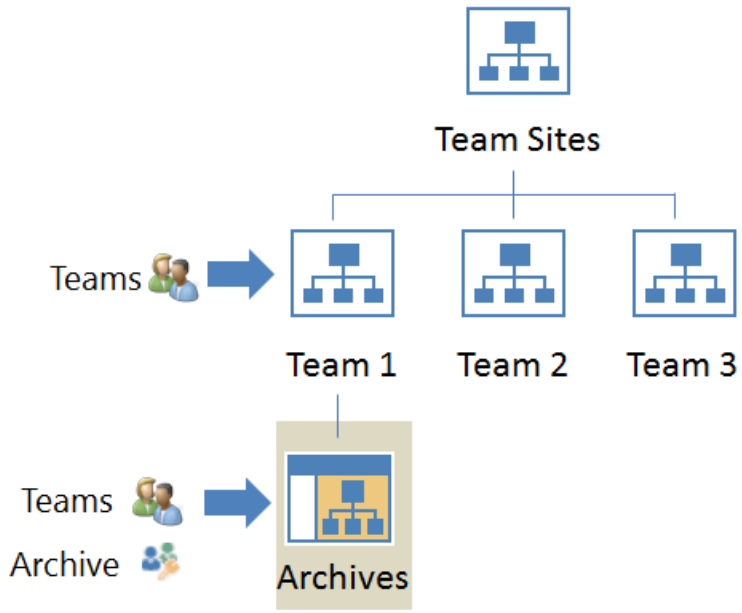
You should see that User1 has the Archive permission level and there is a list of factors that also affect the level of access. These are permissions that the User1 account has because it is the configured site administrator for the Teams site collection.

29. In **User/Group**, remove **User1** and type **User2**, and then click **Check Now**.
    You should see that User2 has the Archive permission level.
30. In **User/Group**, remove **User2** and type **V-Vendor1**, and then click **Check Now**.
    You should see that V-Vendor1 has no permission levels.
31. In **User/Group**, remove **V-Vendor1** and type **HRUser1**, and then click **Check Now**.
    You should see that HRUser1 has no permissions levels.
32. Click **Close**.
33. Click **Home** in the Quick Launch.
34. On the Team 1 site, click **Archives**.
35. Click new document.
36. In the **Add a document** dialog box, click **Browse**.
37. In **Choose File to Upload**, in the tree pane, click **Pictures** under **Libraries**, and then double-click **Sample Pictures** in the contents pane.
38. In the **Pictures library**, double-click **Chrysanthemum**, and then click **OK**.

The resulting site infrastructure and permissions configuration is the following:

- The Teams security group has edit-level permissions for the Team 1 site collection.
- The Archives subsite has custom permissions, with the Teams security group configured to use the new Archive permission level.

See the following figure.



To demonstrate the Archives subsite

1. On CLIENT1, log off and then log on with the CORP\User2 account.
2. Start Internet Explorer and browse to **http://teams.corp.contoso.com/sites/team1**.
3. On the Team 1 page, click **Archives**.
4. On the Archives page, click **new document**.
5. In **Add a document**, click **Browse**.
6. In **Choose a File to Upload**, in the tree pane, click **Pictures** under **Libraries**, and then double-click **Sample Pictures** in the contents pane.
7. In the **Pictures** library, double-click **Koala**, and then click **OK**.

   User2 can add documents to the archive.
8. On the Archives page, click the **Chrysanthemum** document to view the picture, and then click the **Back** button.

   User2 can view documents in the archive.
9. Select the **Chrysanthemum** document, and then click **Files** in the menu bar.

   Notice that the icon to delete the document is unavailable. User2 cannot delete this document from the archive.
10. Select the **Koala** document, and then click **Files** in the menu bar.

    Notice that the icon to delete the document is unavailable. User2 cannot delete this document from the archive.

Snapshot the Configuration

This completes the SharePoint Server 2013 permissions test lab. To save this configuration so that you can quickly return to a working configuration from which you can test other SharePoint TLGs or test lab extensions or for your own experimentation and learning, do the following:

1. On all physical computers or virtual machines in the test lab, close all windows and then perform a graceful shutdown.
2. If your lab is based on virtual machines, save a snapshot of each virtual machine and name the snapshots **SP2013Permissions**. If your lab uses physical computers, create disk images to save the SharePoint Server 2013 permissions test lab configuration.

Additional Resources

For more information about SharePoint Server 2013, see the SharePoint 2013 product information web page and SharePoint 2013 for IT pros.

To provide the authors of this guide with feedback or suggestions for improvement, send an email message to itspdocs@microsoft.com.

To submit your questions about this test lab or SharePoint 2013, see the SharePoint 2013 for IT Professionals Forum.

For a list of TLGs related to this test lab or extensions to demonstrate additional functionality, see SharePoint Server 2013 Test Lab in the TechNet Wiki.

Microsoft strongly encourages you to develop and publish your own TLG content for SharePoint Server 2013. For example, you can publish in the TechNet Wiki (example: Test Lab Guide: Demonstrate Remote Access VPNs) or in your own publishing forum (example: Test Lab Guide (Part 1) - Demonstrate TMG PPTP, L2TP/IPsec and SSTP Remote Access VPN Server). See Wiki: Creating and Publishing Test Lab Guide Content for information about the types of content you can create and for links to guidance, templates, and examples.

For a list of additional Microsoft TLGs, see Test Lab Guides in the TechNet Wiki.