Installing and Configuring VMware Workspace ONE Access

OCT 2020

VMware Workspace ONE Access 20.10

vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

Installing and Configuring VMware Workspace ONE Access

The VMware Workspace ONE® Access™ service (formerly known as VMware Identity Manager™) is available on-premises with Project Photon OS™, a minimal Linux container host. When the on-premises installation is finished, you can use the administration console to manage users and groups, set up and manage authentication and access policies, add resources to the catalog, including web applications, VMware Horizon® applications and desktops, and Citrix-published resources, and manage entitlements to resources in the catalog.

Intended Audience

This information is intended for administrators of Workspace ONE Access. The information is written for experienced Linux and Windows system administrators who are familiar with VMware technologies, particularly vCenter™, ESX™, and vSphere®, networking concepts, Active Directory servers, databases, backup and restore procedures, Simple Mail Transfer Protocol (SMTP), and NTP servers. Knowledge of other technologies, such as VMware ThinApp®, Citrix-published resources, and RSA SecurID, is helpful if you plan to implement those features.

Workspace ONE Access and Other Technologies

You must integrate the Workspace ONE Access service with several other technologies, including the Workspace ONE Access connector, which starting with version 19.03, is available solely on Windows. You must integrate the service with other VMware technologies, such as vCenter™, ESX™, and vSphere®. Knowledge of many other technologies is required, such as of Active Directory, databases, backup and restore procedures, Simple Mail Transfer Protocol (SMTP), and NTP servers. Knowledge of other technologies, such as VMware Horizon and RSA SecurID, is helpful if you plan to implement those features.

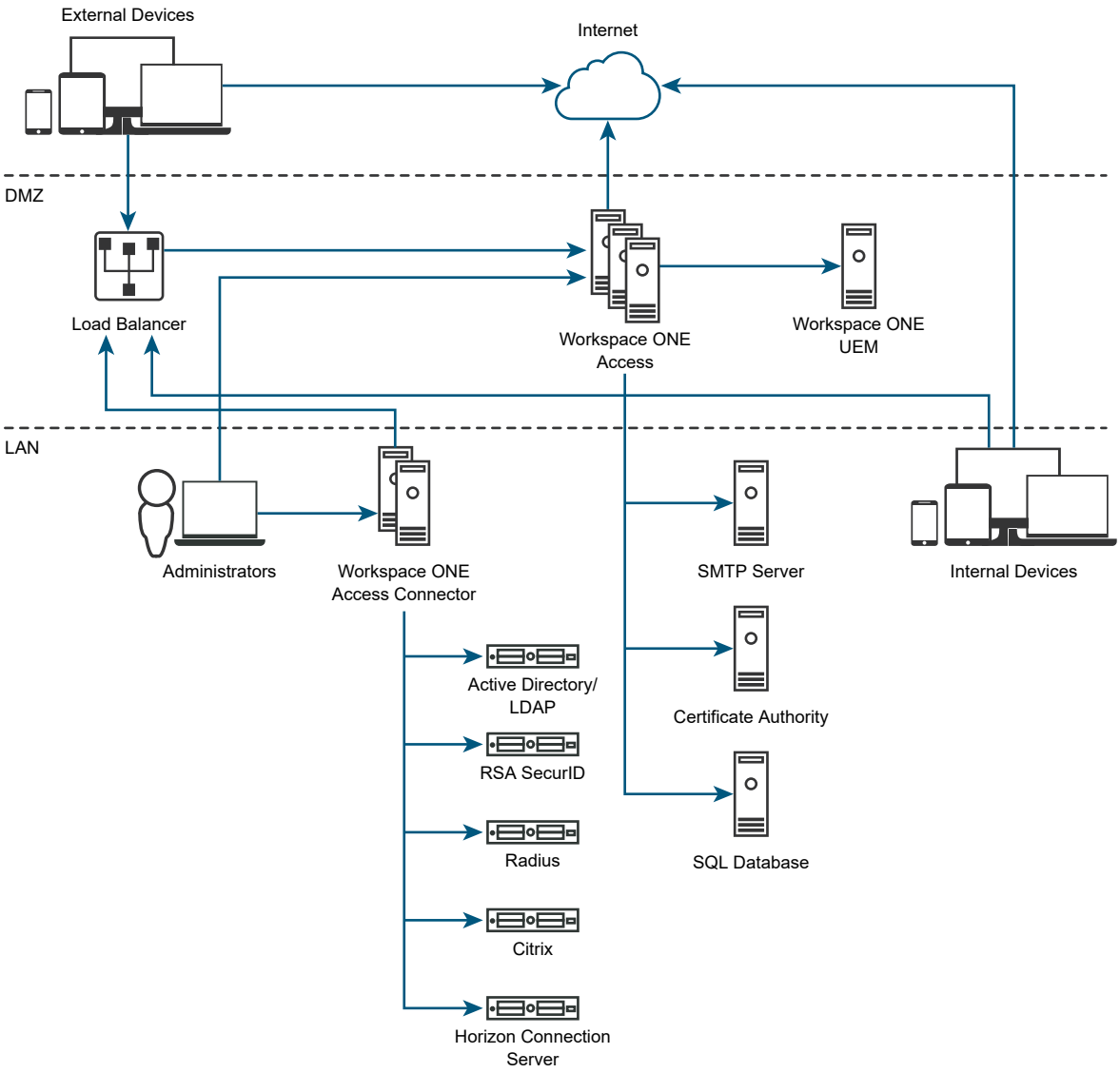
Preparing to Install Workspace ONE Access

1

You can install the Workspace ONE Access service in a new standalone server or in a cluster of three or more nodes.

The tasks to deploy and set up Workspace ONE Access require that you perform the prerequisites, deploy the Workspace ONE Access OVA file, and finish the setup from the Workspace ONE Access Setup wizard.

Figure 1-1. Workspace ONE Access Architecture Diagram for Typical Deployments



Important Citrix, Horizon, Horizon Cloud, and ThinApp integrations are not available with the Workspace ONE Access 20.10 or 20.01 connectors.

- To use ThinApp packaged applications, use VMware Identity Manager connector (Linux) version 2018.8.1.0.
- To use other Virtual Apps, such as Horizon desktops and applications or Citrix published resources, use VMware Identity Manager connector (Windows) version 19.03.0.1.

Note

- If you plan to enable certificate or smart card-based authentication, use the SSL pass-through setting at the load balancer, instead of the terminate SSL setting. This configuration ensures that the SSL handshake is between the Workspace ONE Access connector and the client.
- Depending on the location of the Workspace ONE UEM deployment, the Workspace ONE UEM REST APIs can be in the cloud or on premises.
- For information about configuring and enabling Kerberos authentication in Workspace ONE Access, see *Managing VMware Workspace ONE Access User Authentication Methods*.

This chapter includes the following topics:

Workspace ONE Access System and Network Configuration Requirements

Consider your entire deployment, including how you integrate resources, when you make decisions about hardware, resources, and network requirements.

Supported vSphere and ESX Versions

The following versions of vSphere and ESXi server are supported:

- 6.0 and later

Compatibility Between Workspace ONE Access Service and Connector

With the Workspace ONE Access on premises service, you can use supported connector versions that are either the same or lower than the service version. For example, with the Workspace ONE Access 20.10 service, you can use connector 20.10 and earlier versions. You cannot use a connector version that is higher than the service version. For example, you cannot use the 20.10 connector with the 20.01 service. Using the latest compatible version of the connector is recommended.

For information on supported versions, see https://www.vmware.com/support/policies/lifecycle.html.

Hardware Sizing Requirements

Ensure that you meet the requirements for the number of Workspace ONE Access virtual appliances and the resources allocated to each appliance.

Note For new deployments, the default Workspace ONE Access sizing requirements are as follows:

- 4vCPU
- 8 GB Memory
- 100 GB disk space

Number of Users	Up to 1,000	1,000-10,000	10,000-25,000	25,000-50,000	50,000-100,000
Number of Workspace ONE Access servers	1 server	3 load-balanced servers	3 load-balanced servers	3 load-balanced servers	3 load-balanced servers
CPU (per server)	4 CPU	4 CPU	4 CPU	8 CPU	8 CPU
RAM (per server)	8 GB	8 GB	8 GB	16 GB	32 GB
Disk space (per server)	100 GB	100 GB	100 GB	100 GB	100 GB

Also, Ensure that you meet the requirements for the number of Workspace ONE Access connector instances. See *Installing and Configuring Workspace ONE Access Connector*.

Database Requirements

Set up Workspace ONE Access with the appropriate database to store and organize server data.

You can use the internal PostgreSQL database or an external Microsoft SQL database. An internal Postgres SQL database is embedded in the Workspace ONE Access appliance, but the internal database is not recommended for use with production deployments.

For information about the Microsoft SQL database versions and service pack configurations supported, see the VMware Product Interoperability Matrices at https://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

The following database requirements apply. The exact specifications needed depend on the size and needs of your deployment.

Number of Users	Up to 1,000	1,000-10,000	10,000-25,000	25,000-50,000	50,000-100,000
CPU	2 CPU	2 CPU	4 CPU	8 CPU	8 CPU
RAM	4 GB	4 GB	8 GB	16 GB	32 GB
Disk space	50 GB	50 GB	50 GB	100 GB	100 GB

The SQL Server AlwaysOn capability is a combination of failover clustering and database mirroring combined with log shipping for faster availability. AlwaysON allows for multiple read copies of your database and a single read-write copy for operations. If your deployment environment has the bandwidth to support the traffic generated, the Workspace ONE Access database supports AlwaysON.

Network Configuration Requirements

Component	Minimum Requirement
DNS record and IP address	IP address and DNS record
Firewall port	Ensure that the inbound firewall port 443 is open for users outside the network to the Workspace ONE Access instance or the load balancer.
Reverse Proxy	Deploy a reverse proxy such as F5 Access Policy Manager in the DMZ to allow users to access the Workspace ONE Access user portal remotely and securely. VMware Unified Access Gateway 2.8 and later supports reverse proxy functionality to allow users to access the Workspace ONE Access unified catalog remotely and securely. Unified Access Gateway can be deployed in the DMZ behind the load balancers front-ending the Workspace ONE Access appliance.

Port Requirements

Ports used in the server configuration are described in the following table. For the most up-to-date port information, see https://ports.vmware.com/home/Workspace-ONE-Access.

Your deployment might include only a subset of the listed ports. For example:

- To sync users and groups from Active Directory, Workspace ONE Access must connect to Active Directory.
- To sync with ThinApp, Workspace ONE Access must join the Active Directory domain and connect to the ThinApp Repository share.

Note For information about configuring and enabling Kerberos authentication in Workspace ONE Access, including port information, see *Managing Workspace ONE Access User Authentication Methods*.

Port	Protocol	Source	Target	Description
443	HTTPS	Load Balancer	Workspace ONE Access machine	
443	HTTPS	Workspace ONE Access machine	Load Balancer	Required to validate the load balancer FQDN when it is set.

Port	Protocol	Source	Target	Description
443, 8443	HTTPS/HTTP	Workspace ONE Access machine	Workspace ONE Access machine	For all Workspace ONE Access instances in a cluster, and across clusters in different data centers.
443	HTTPS	Browsers	Workspace ONE Access machine	
443, 80	HTTPS, HTTP	Workspace ONE Access machine	vapp-updates.vmware.com	Access to the upgrade server
443	HTTPS	Workspace ONE Access machine	discovery.awmdm.com	Access for Workspace ONE Intelligent Hub application autodiscovery
443	HTTPS	Workspace ONE Access machine	catalog.vmwareidentity.com	Access to Cloud Catalog
443	HTTPS	Workspace ONE Access machine	signing.awmdm.com	Mandatory to launch Hub Services console and to provision certificates for Workspace ONE Notifications service.
7443	TCP	Browsers	Workspace ONE Access machine	SSL certificate authentication
8443	HTTPS	Browsers	Workspace ONE Access machine	Administrator Port
25	SMTP	Workspace ONE Access machine	SMTP	Port to relay outbound mail.
389 636 3268 3269	LDAP LDAPS MSFT-GC MSFT-GC-SSL	Workspace ONE Access machine	Active Directory	Default values are shown. These ports are configurable.
445	TCP	Workspace ONE Access machine	VMware ThinApp repository	Access to the ThinApp repository.
5500	UDP	Workspace ONE Access machine	RSA SecurID system	Default value is shown. This port is configurable.

Port	Protocol	Source	Target	Description
53	TCP/UDP	Workspace ONE Access machine	DNS server	Every virtual appliance must have access to the DNS server on port 53 and allow incoming SSH traffic on port 22.
88, 464, 135, 445	TCP/UDP	Workspace ONE Access machine	Domain controller	
9300	TCP	Workspace ONE Access machine	Workspace ONE Access machine	Audit needs.
54328	UDP			
5701	TCP	Workspace ONE Access machine	Workspace ONE Access machine	Hazelcast cache.
40002 40003	TCP	Workspace ONE Access machine	Workspace ONE Access machine	Ehcache.
1433	TCP	Workspace ONE Access machine	Database	Microsoft SQL default port is 1433.
443		Workspace ONE Access machine	Horizon Connection Server	Access to Horizon Connection Server.
80, 443	TCP	Workspace ONE Access machine	Integration Broker server	Connection to the Integration Broker. Port option depends on whether a certificate is installed on the Integration Broker server.
443	HTTPS	Workspace ONE Access	Workspace ONE UEM REST API	For device compliance checking and for the AirWatch Cloud Connector password authentication method, if that is used.
88	UDP	Unified Access Gateway	Workspace ONE Access machine	UDP port to open for mobile SSO.
5262	TCP	Android mobile device	Workspace ONE UEM HTTPS proxy service	VMware Tunnel client routes traffic to the HTTPS proxy for Android devices.
88	UDP	iOS mobile device	Workspace ONE Access machine	Port used for Kerberos traffic

Port	Protocol	Source	Target	Description
443	HTTPS/TCP			from iOS devices to the hosted cloud KDC service.
514	UDP	Workspace ONE Access machine	syslog server	UDP For external syslog server, if configured.
88	UDP	Workspace ONE Access machine	Hybrid KDC Server in the cloud. Hostname is kdc.<realm>. For example, kdc.op.vmwareidentity.com	UDP port used to authenticate iOS Mobile SSO auth adapter configuration updates that are saved to the cloud KDC service. This port is only used if the Hybrid KDC iOS Mobile SSO feature is used.

Time Synchronization

Configuring time synchronization on all Workspace ONE Access service and connector instances is required for a Workspace ONE Access deployment to function correctly.

For information on configuring time synchronization for the Workspace ONE Access service, see Configuring Time Synchronization for the Workspace ONE Access Service.

For information on configuring time synchronization for the Workspace ONE Access connector, see *Installing and Configuring Workspace ONE Access Connector*.

Supported Directories

You integrate your enterprise directory with Workspace ONE Access and sync users and groups from your enterprise directory to the service.

- The Active Directory environment can consist of a single Active Directory domain, multiple domains in a single Active Directory forest, or multiple domains across multiple Active Directory forests.

  Workspace ONE Access supports Active Directory on Windows 2012 R2, 2016, and 2019 with a Domain functional level and Forest functional level of Windows 2003 and later.

  Note A higher functional level might be required for some features. For example, to allow users to change Active Directory passwords from Workspace ONE, the Domain functional level must be Windows 2008 or later.

Supported Web Browsers to Access the Workspace ONE Access Console

The Workspace ONE Access console is a web-based application you use to manage the Workspace ONE Access service . You can access the Workspace ONE Access console from the latest versions of Mozilla Firefox, Google Chrome, Safari, Microsoft Edge, and Internet Explorer 11.

Note In Internet Explorer 11, JavaScript must be enabled and cookies allowed to authenticate through Workspace ONE Access.

Supported Browsers to Access the Workspace ONE Portal

End users can access the Workspace ONE portal from the following browsers.

- Mozilla Firefox (latest)
- Google Chrome (latest)
- Safari (latest)
- Internet Explorer 11
- Microsoft Edge browser
- Native browser and Google Chrome on Android devices
- Safari on iOS devices

Note In Internet Explorer 11, JavaScript must be enabled and cookies allowed to authenticate through Workspace ONE Access.

Prerequisites to Deploying Workspace ONE Access

Before you deploy Workspace ONE Access, you must prepare your environment. This preparation includes downloading the Workspace ONE Access OVA file, creating DNS records, and obtaining IP addresses.

Prerequisites

Before you begin to install Workspace ONE Access complete the prerequisite tasks.

- You need one or more ESX servers to deploy the Workspace ONE Access virtual appliance.

  Note For information about supported vSphere and ESX server versions, see the VMware Product Interoperability Matrixes at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

- VMware vSphere Client or vSphere Web Client is required to deploy the OVA file and access the deployed virtual appliance remotely to configure networking.
- Download the Workspace ONE Access OVA file from the VMware Web site.

Create DNS Records and IP Addresses for the Workspace ONE Access Virtual Appliance

A DNS entry and a static IP address must be available for the Workspace ONE Access virtual appliance. Because each company administers their IP addresses and DNS records differently, before you begin your installation, request the DNS record and IP addresses to use.

Configuring reverse lookup is required. When you implement reverse lookup, you must define a PTR record on the DNS server so the virtual appliance uses the correct network configuration.

You can use the following sample list of DNS records when you talk to your network administrator. Replace the sample information with information from your environment. This example shows forward DNS records and IP addresses.

Table 1-1. Examples of Forward DNS Records and IP Addresses

Domain Name	Resource Type	IP Address
myidentitymanager.example.com	A	10.28.128.3

This example shows reverse DNS records and IP addresses.

Table 1-2. Examples of Reverse DNS Records and IP Addresses

IP Address	Resource Type	Host Name
10.28.128.3	PTR	myidentitymanager.example.com

After you complete the DNS configuration, verify that the reverse DNS lookup is properly configured. For example, the virtual appliance command `host IPaddress` must resolve to the DNS name lookup.

Planning for Kerberos Authentication

If you plan to set up Kerberos authentication, note the following conditions:

In a scenario where you use the Workspace ONE Access connector for Kerberos authentication, the connector host name must match the Active Directory domain to which the connector is joined. For example, if the Active Directory domain is sales.example.com, the connector host name must be *connectorhost*.sales.example.com.

If you cannot assign a hostname that matches the Active Directory domain structure, you need to configure the connector and Active Directory manually. See the Knowledge Base for information.

Using a Unix/Linux-based DNS Server

If you are using a Unix or Linux-based DNS server and plan to join Workspace ONE Access to the Active Directory domain, make sure that the appropriate service (SRV) resource records are created for each Active Directory domain controller.

Note If you have a load balancer with a Virtual IP address (VIP) in front of the DNS servers, note that Workspace ONE Access does not support using a VIP. You can specify multiple DNS servers separated by a comma.

Create the Workspace ONE Access Service Database

The Workspace ONE Access service requires a database to store and organize server data.

An internal Postgres SQL database is embedded in the Workspace ONE Access appliance, but the internal database is not recommended for use with production deployments.

To use an external Microsoft SQL database, your database administrator must prepare an empty Microsoft SQL Server database and schema before you install Workspace ONE Access. When you connect to the Microsoft SQL server, you enter the name of the instance you want to connect to and the authentication mode. You can select either Windows Authentication mode and specify the domain\username or SQL Server Authentication mode and specify the local user name and password.

You connect to the external database connection when you run the Workspace ONE Access Setup wizard. You can also go to the **Database Connection Setup** page to configure the connection to the external database. See Change the Workspace ONE Access Appliance Configuration Settings for information about accessing appliance configuration settings pages, including the **Database Connection Setup** page.

Configure the Microsoft SQL Database with Windows Authentication Mode for Workspace ONE Access

To use a Microsoft SQL database for Workspace ONE Access, you must create a new database in the Microsoft SQL server. During setup, you must select an authentication mode for the database. If you select Windows Authentication, when you create the database, you enter the user name and domain. The user name and domain is entered as `domain\username`.

When you run the Microsoft SQL commands, you create a database on the Microsoft SQL server, enter the database name, add the login user credentials, and create the schema. The schema name is **saas**.

See the Microsoft SQL documentation for information about the file naming conventions before you create the database name.

Note The default collation is case-sensitive.

Prerequisites

- Supported version of the Microsoft SQL server installed as an external database server.

  Note Microsoft SQL server 2012 and 2014 must be updated with the Microsoft SQL patch to support TLS 1.2.

- Load balancing implementation configured.
- Windows Authentication selected as the authentication mode.
- Administrator rights to access and create the database components using Microsoft SQL Server Management Studio or from another Microsoft SQL Server CLI client.

Procedure

1. Log in to the Microsoft SQL Server Management Studio session as the sysadmin or a user account with sysadmin privileges.

   The editor window appears.

2. In the toolbar, click **New Query**.
3. To create the database with the default schema named **saas**, enter the following commands in the editor window.

   You can define the `COLLATE` Windows collation name, case sensitivity and accent sensitivity, The default is `Latin1_General_CS_AS`. CS specifies case-sensitive, AS specifies accent-sensitive.

   Important If you change the `COLLATE` value of the Microsoft database from `Latin1_General_CS_AS`, you must update the property `datastore.collation` in the `runtime-config.properties` file with that collation value.

```
/*
Values within angle brackets (< >) are example values. When replacing the example value,
remove the angle brackets. The database name is case sensitive, and the name must be one
word with no spaces.
Make sure you enter the database name the same in all instances.
*/


CREATE DATABASE <saasdb>
COLLATE <Latin1_General_CS_AS>;
ALTER DATABASE <saasdb> SET READ_COMMITTED_SNAPSHOT ON;
GO

IF NOT EXISTS
(SELECT name
FROM master.sys.server_principals
WHERE name=N'<domain\username>')
BEGIN
CREATE LOGIN [<domain\username>] FROM WINDOWS;
END
```

```
GO

USE <saasdb>;
IF EXISTS (SELECT * FROM sys.database_principals WHERE name=N'<domain\username>')
DROP USER [<domain\username>]
GO

CREATE USER [<domain\username>] FOR LOGIN [<domain\username>]
WITH DEFAULT_SCHEMA=saas;
GO

CREATE SCHEMA saas AUTHORIZATION "<domain\username>"
GRANT ALL ON DATABASE::<saasdb> TO "<domain\username>";
GO

ALTER ROLE db_owner ADD MEMBER "<domain\username>";
GO
```

4 On the toolbar, click **!Execute**.

The Microsoft SQL database server is now ready to be connected to the Workspace ONE Access database.

The server role used to grant server-wide security privileges is set to **public**. The database role membership is **db_owner**. Do not set any other roles.

Results

When you install Workspace ONE Access, you select this database server instance to connect to. After the installation, the JDBC URL and the user name and password created for the database are configured in the Database Connection Setup page in the Workspace ONE Access server. See Configure Workspace ONE Access to Use an External Database

Configure Microsoft SQL Database Using Local SQL Server Authentication Mode for Workspace ONE Access

To use a Microsoft SQL database for the Workspace ONE Access, you must create a new database in the Microsoft SQL server. During setup, you must select an authentication mode for the database. If you select SQL Server Authentication, when you create the database, you enter a local user name and password.

When you run the Microsoft SQL commands, you create a database on the Microsoft SQL server, enter the database name, add the login user credentials, and create the schema. The schema is named **saas**.

See the Microsoft SQL documentation for information about the file naming conventions before you create the database name.

Note The default database collation is case-sensitive.

Prerequisites

- Supported version of the Microsoft SQL server installed as an external database server.

  Note Microsoft SQL server 2012 and 2014 must be updated with the Microsoft SQL patch to support TLS 1.2.

- Load balancing implementation configured.
- SQL Server Authentication selected as the authentication mode.
- Administrator rights to access and create the database components using Microsoft SQL Server Management Studio or from another Microsoft SQL Server CLI client.

Procedure

1. Log in to the Microsoft SQL Server Management Studio session as the sysadmin or a user account with sysadmin privileges.

   The editor window appears.

2. In the toolbar, click **New Query**.
3. To create the database with the default schema named **saas**, enter the following commands in the editor window.

   You can define the `COLLATE` Windows collation name, case sensitivity and accent sensitivity, The default is `Latin1_General_CS_AS`. CS specifies case-sensitive, AS specifies accent-sensitive.

   Important If you change the `COLLATE` value of the Microsoft database from `Latin1_General_CS_AS`, you must update the property `datastore.collation` in the `runtime-config.properties` file with that collation value.

```
/*
Values within angle brackets (< >) are example values. When replacing the example value,
remove the angle brackets. The database name is case sensitive, and the name must be one
word with no spaces.
Make sure you enter the database name the same in all instances.
*/


CREATE DATABASE <saasdb>
COLLATE <Latin1_General_CS_AS>;
ALTER DATABASE <saasdb> SET READ_COMMITTED_SNAPSHOT ON;
GO

BEGIN
CREATE LOGIN <loginusername> WITH PASSWORD = N'<password>';
END
GO

USE <saasdb>;
IF EXISTS (SELECT * FROM sys.database_principals WHERE name=N'<loginusername>')
```

```
DROP USER [<loginusername>]
GO

CREATE USER [<loginusername>] FOR LOGIN [<loginusername>]
WITH DEFAULT_SCHEMA=saas;
GO

CREATE SCHEMA saas AUTHORIZATION <loginusername>
GRANT ALL ON DATABASE::<saasdb> TO <loginusername>;
GO

ALTER ROLE [db_owner] ADD MEMBER <loginusername>;
GO
```

4 On the toolbar, click **!Execute**.

The Microsoft SQL database server is now ready to be connected to the Workspace ONE Access database.

The server role used to grant server-wide security privileges is set to **public**. The database role membership is **db_owner**. Do not set any other roles.

Results

When you install Workspace ONE Access, you select this database server instance to connect to. After the installation, the JDBC URL and the user name and password created for the database are configured in the Database Connection Setup page in the Workspace ONE Access server. See Configure Workspace ONE Access to Use an External Database

Confirm Microsoft SQL Database Is Correctly Configured for Workspace ONE Access

To confirm that the Microsoft SQL database is configured correctly to work with Workspace ONE Access, the following verification script runs after the database is configured.

Prerequisites

The Microsoft SQL database is created for the Workspace ONE Access service.

Procedure

1 Log in to the Microsoft SQL Server Management Studio session with the <saasdb> login user name and password that was created in the script you used to create the database.

The editor window appears.

2 In the toolbar, click **New Query**.

3 Run the following commands. Edit the commands as required.

```
 execute as user = 'domain\username'


/* Check if user is db owner. Return true */
```

```
SELECT IS_ROLEMEMBER('db_owner') as isRoleMember

/* Make sure user is not sysadmin. Should return false */
SELECT IS_SRVROLEMEMBER('sysadmin')  as isSysAdmin

/* check if saas schema exists, should be not null */
SELECT SCHEMA_ID('saas') as schemaId

/* check schema owner, should be user provided to installer */
SELECT SCHEMA_OWNER FROM INFORMATION_SCHEMA.SCHEMATA where SCHEMA_NAME='saas'

/* check if saas is user default schema, should return saas */
SELECT SCHEMA_NAME() as SchemaName

/* check db collation, should return Latin1_General_CS_AS */
SELECT DATABASEPROPERTYEX('<saasdb>', 'Collation') AS Collation

/* check if read committed snapshot is on, should return true */
SELECT is_read_committed_snapshot_on FROM sys.databases WHERE name='<saasdb>'
```

4 On the toolbar, click **!Execute**.

If the configuration is not correct, error messages are displayed. Before continuing to configure the Workspace ONE Access service to use the external Microsoft SQL database, correct the problems described in the error messages.

Change Database-Level Roles After Upgrade to Workspace ONE Access

When the database is created in Microsoft SQL database for the Workspace ONE Access service, the database user is granted to the db_owner role. Members of the db_owner fixed database role can perform all configuration and maintenance activities on the database.

After the database is set up and configured in the Workspace ONE Access service, you can revoke access to db_owner and add db_datareader and db_datawriter as the database roles. Members of the db_datareader role can read all data from all user tables. Member of the db_datawriter role can add, delete, or change data in all user tables.

Note If you have previously revoked access to db_owner role, make sure that the db_owner role is granted back before you start an upgrade to a new version of Workspace ONE Access or make any updates to External Database Settings such as changing database user passwords.

Prerequisites

User role for the Microsoft SQL Server Management Studio as sysadmin or as a user account with sysadmin privileges.

Procedure

1 In the Microsoft SQL Server management Studio session as an admin with sysadmin privileges, connect to the database instance <saasdb> for Workspace ONE Access.

2 Revoke the role **db_owner** on the database, enter the following command

Authentication Mode	Command
Windows Authentication (domain\user)	`ALTER ROLE db_owner DROP MEMBER <domain\username>;`
SQL Server Authentication (local user)	`ALTER ROLE db_owner DROP MEMBER <loginusername>;`

3 Add **db_datawriter** and **db_datareader** role membership to the database.

Authentication Mode	Command

Windows Authentication (domain\user)	`ALTER ROLE db_datawriter ADD MEMBER <domain\username>;`
	`GO`
	
	`ALTER ROLE db_datareader ADD MEMBER <domain\username>;`
	`GO`

SQL Server Authentication (local user)	`ALTER ROLE db_datawriter ADD MEMBER <loginusername>;`
	`GO`
	`ALTER ROLE db_datareader ADD MEMBER <loginusername>;`
	`GO`

Administering the Internal Database for Workspace ONE Access

An internal PostgreSQL database is embedded in the Workspace ONE Access appliance and is configured and ready to use by default.

When Workspace ONE Access is installed and powered on, during the initialization process, a random password for the internal database user is generated. This password is unique to each deployment and can be found in the file `/usr/local/horizon/conf/db.pwd`.

The internal database is not recommended for use with production deployments. The recommended database for production deployments is an external Microsoft SQL database. After the Workspace ONE Access appliance is deployed, you connect to the external database connection when you run the Workspace ONE Access Setup wizard. See Configure Workspace ONE Access Settings.

Change SQL Server Database Auto Growth Settings for Workspace ONE Access

When you create the database, the default settings for auto growing is 1 MB for data files. The auto growth setting for the Workspace ONE Access database must be increased to 128 MB.

To see the vIDMDB database file auto growth setting, navigate to **DataBase Properties > Files**. The setting is displayed in the **Autogrowth / Maxsize** column.

Procedure

1 Log in to the Microsoft SL server Management Studio session as the sysadmin or a user account with sysadmin privileges.

2 In the toolbar, click **New Query**.

3 To change the auto growth setting, run the following command.

```
ALTER DATABASE <saasdb>

        MODIFY FILE ( NAME = N'<saasdb>', FILEGROWTH = 128MB )

GO
```

Results

The auto growth setting is changed to 128 MB.

Deployment Checklists

You can use the deployment checklist to gather the necessary information to install the Workspace ONE Access virtual appliance.

Information for Fully Qualified Domain Name

Table 1-3. Fully Qualified Domain Name (FQDN) Information Checklist

Information to Gather	List the Information
Workspace ONE Access Connector FQDN	If you plan to set up Kerberos authentication, note the following conditions. In a scenario where you use the VMware Workspace ONE Access connector for Kerberos authentication, the connector host name must match the Active Directory domain to which the connector is joined. For example, if the Active Directory domain is sales.example.com, the connector host name must be *connectorhost*.sales.example.com. If you cannot assign a hostname that matches the Active Directory domain structure, you need to configure the connector and Active Directory manually. See the Knowledge Base for information.

Network Information for VMware Workspace ONE Access Appliance

Table 1-4. Network Information Checklist

Information to Gather	List the Information
IP address	**Note** You must use a static IP address and it must have a PTR and an A record defined in the DNS.
DNS host name for each node	
Default Gateway address	
Netmask or prefix	

Directory Information

VMware Workspace ONE Access supports integrating with Active Directory or LDAP directory environments.

Table 1-5. Active Directory Domain Controller Information Checklist

Information to Gather	List the Information
Active Directory server name	
Active Directory domain name	
Base DN	
For Active Directory over LDAP, the Bind DN username and password	
For Active Directory with Integrated Windows Authentication, the user name and password of the account that has privileges to join computers to the domain.	

Table 1-6. LDAP Directory Server Information Checklist

Information to Gather	List the Information
LDAP directory server name or IP address	
LDAP directory server port number	
Base DN	
Bind DN username and password	
LDAP search filters for group objects, bind user objects, and user objects	
LDAP attribute names for membership, object UUID, and distinguished name	

SSL Certificates

You can add an SSL certificate after you deploy the Workspace ONE Access service.

Table 1-7. SSL Certificate Information Checklist

Information to Gather	List the Information
SSL certificate	
Private key	

License Key

Table 1-8. Workspace ONE Access License Key Information Checklist

Information to Gather	List the Information
License key	

Note The License key information is entered in the Workspace ONE Access console in the **Appliance Settings > License** page after the installation is complete. Entering a license key is optional.

External Database

Table 1-9. External Database Information Checklist

Information to Gather	List the Information
Database host name	
Port	
Username	
Password	

Customer Experience Improvement Program for Workspace ONE Access

2

VMware's Customer Experience Improvement Program ("CEIP") provides VMware with information that enables VMware to improve its products and services, to fix problems, and to advise you on how best to deploy and use our products. As part of the CEIP, VMware collects technical information about your organization's use of VMware products and services on a regular basis in association with your organization's VMware license key(s). This information does not personally identify any individual.

If you prefer not to participate in VMware's CEIP for this product, uncheck the box when you install Workspace ONE Access.

You can also join or leave the CEIP for this product at any time after installation.

Note If your network is configured to access the Internet through HTTP proxy, to send the data collected through CEIP to VMware, you must adjust the proxy settings in Workspace ONE Access.

Deploying the Workspace ONE Access Machine Behind a Load Balancer

3

In an enterprise environment, the recommended Workspace ONE Access machine configuration is to deploy a three-node cluster of the Workspace ONE Access service for high availability. After the first Workspace ONE Access node is installed, configured, and tested behind the load balancer, the first node is cloned to create the other nodes in the cluster.

The Workspace ONE Access architecture diagram demonstrates how you can deploy the Workspace ONE Access environment.

See Chapter 1 Preparing to Install Workspace ONE Access for a typical deployment.

This chapter includes the following topics:

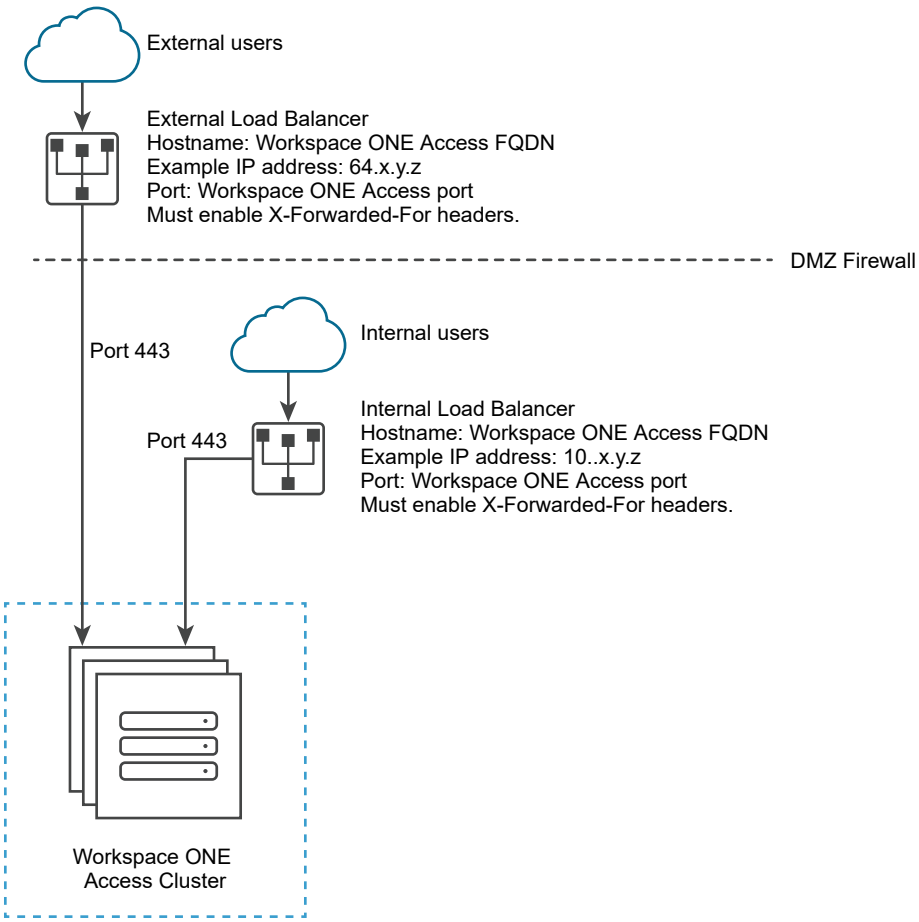
Using a Load Balancer or Reverse Proxy to Enable External Access to Workspace ONE Access

During deployment, the Workspace ONE Access instance is set up inside the internal network. If you want to provide access to the service for users connecting from outside networks, you must install a load balancer or a reverse proxy, such as VMware NSX® Advanced Load Balancer™, Apache, Nginx, or F5, in the DMZ.

If you do not use a load balancer or reverse proxy, you cannot expand the number of Workspace ONE Access instances later. You might need to add more instances to provide redundancy and load balancing. The following diagram shows the basic deployment architecture that you can use to enable external access.

Note The same Workspace ONE Access FQDN is used for both internal and external access in this deployment.

Figure 3-1. External Load Balancer Proxy with Virtual Machines



Specify Workspace ONE Access FQDN during Deployment

During the deployment of the Workspace ONE Access appliance, you enter a single Workspace ONE Access FQDN and the port number. These values must point to the host name that you want end users to access.

The Workspace ONE Access machine always runs on port 443. You can use a different port number for the load balancer. If you use a different port number, you must specify it during deployment. Do not use 8443 as the port number, as this port number is the Workspace ONE Access administrative port and is unique for each machine in a cluster.

Load Balancer Settings to Configure

Load balancer settings to configure include enabling X-Forwarded-For headers, setting the load balancer time-out correctly, and enabling sticky sessions. In addition, SSL trust must be configured between the Workspace ONE Access connector machine and the load balancer.

- X-Forwarded-For Headers

You must enable X-Forwarded-For headers on your load balancer. This determines the authentication method. See the documentation provided by your load balancer vendor for more information.

- Load Balancer Timeout

  For Workspace ONE Access to function correctly, you might need to increase the load balancer request timeout from the default. The value is set in minutes. If the timeout setting is too low, you might see this error, “502 error: The service is unavailable”.

- Enable Sticky Sessions

  You must enable the sticky session setting on the load balancer if your deployment has multiple Workspace ONE Access machines. The load balancer binds a user's session to a specific instance.

- Do not block session cookies

  Do not block session cookies by adding rules to the load balancer. Adding such rules to the load balancer can result in inconsistent behavior and failed requests.

- WebSocket support

  The load balancer must have WebSocket support to enable secure communication channels between connector instances and the Workspace ONE Access nodes.

  For your deployment, if VMware Workspace ONE Hub Services is integrated, WebSocket support is required for Hub Services notifications. Therefore, Web Socket support must be provided for end user browsers and devices.

- Ciphers with forward secrecy

  Apple iOS App Transport Security requirements apply to the Workspace ONE app on iOS. To enable users to use the Workspace ONE app on iOS, the load balancer must have ciphers with forward secrecy. The following ciphers meet this requirement:

  ECDHE_ECDSA_AES and ECDHE_RSA_AES in GCM or CBC mode

  as stated in the iOS 11 *iOS Security* document:

  "App Transport Security provides default connection requirements so that apps adhere to best practices for secure connections when using NSURLConnection, CFURL, or NSURLSession APIs. By default, App Transport Security limits cipher selection to include only suites that provide forward secrecy, specifically ECDHE_ECDSA_AES and ECDHE_RSA_AES in GCM or CBC mode."

Deploying Workspace ONE Access

4

This chapter includes the following topics:

Install the Workspace ONE Access OVA File

You deploy the VMware Workspace ONE Access OVA file using the vSphere Web Client. You can download and deploy the OVA file from a local location that is accessible to the vSphere Web Client, or deploy it from a Web URL.

Note Use either Firefox or Chrome browsers to deploy the OVA file. Do not use Internet Explorer.

Prerequisites

Review Chapter 1 Preparing to Install Workspace ONE Access.

- (Optional) Add IP Pools to the Workspace ONE Access Virtual Appliance

  Network configuration with IP Pools is optional in Workspace ONE Access. You can manually add IP pools to the Workspace ONE Access virtual appliance after it is installed.

- Configure Workspace ONE Access Settings

  After the Workspace ONE Access instance is deployed, you use the Setup wizard to set passwords and select a database.

Procedure

1 Download the VMware Workspace ONE Access OVA file from My VMware.

2 Log in to the vSphere Web Client.

3 Select **File > Deploy OVF Template**.

4 In the Deploy OVF Template wizard, specify the following information.

Page	Description
Source	Browse to the OVA package location, or enter a specific URL.
OVF Template Details	Review the product details, including version and size requirements.
End User License Agreement	Read the End User License Agreement and click **Accept**.
Name and Location	Enter a name for the Workspace ONE Access virtual appliance. The name must be unique within the inventory folder and can contain up to 80 characters. Names are case sensitive. Select a location for the virtual appliance.
Host / Cluster	Select the host or cluster in which to run the virtual appliance.
Resource Pool	Select the resource pool.
Storage	Select the storage for the virtual appliance files. You can also select a VM Storage Profile.
Disk Format	Select the disk format for the files. For production environments, select one of the Thick Provision formats. Use the Thin Provision format for evaluation and testing. In the Thick Provision format, all the space required for the virtual disk is allocated during deployment. In the Thin Provision format, the disk uses only the amount of storage space that it needs for its initial operations.
Network Mapping	Map the networks used in Workspace ONE Access to networks in your inventory.

Page	Description
Properties	■ **Timezone setting** Select the correct time zone. ■ **Join the VMware Customer Experience Improvement Program** This product participates in VMware's Customer Experience Improvement Program ("CEIP"). Details regarding the data collected through CEIP and the purposes for which it is used by VMware are set forth at the Trust & Assurance Center at http://www.vmware.com/trustvmware/ceip.html. If you prefer not to participate in VMware's CEIP for this product, uncheck the box. You can also join or leave the CEIP for this product at any time after installation. **Note** If your network is configured to access the Internet through HTTP proxy, to send the data collected through CEIP to VMware you must adjust the proxy settings in the VMware Workspace ONE Access virtual appliance. See Enabling Proxy Server Settings After Installation of Workspace ONE Access. ■ **Host Name (FQDN)** Enter the host name to use. If this is blank, reverse DNS is used to look up the host name. ■ **Networking Properties** ■ To configure a static IP address for Workspace ONE Access, enter the address for the **Default Gateway**, **DNS**, **IP Address**, and **Netmask** fields. **Note** If you have a load balancer with a Virtual IP address (VIP) in front of the DNS servers, note that Workspace ONE Access does not support using a VIP. You can specify multiple DNS servers separated by a comma. **Important** If any of the four address fields, including **Host Name**, are left blank, DHCP is used. ■ To configure DHCP, leave the address fields blank. **Note** The **Domain Name** and **Domain Search Path** fields are not used. You can leave these blank. (Optional) After Workspace ONE Access is installed, you can configure IP Pools. See (Optional) Add IP Pools to the Workspace ONE Access Virtual Appliance.
Ready to Complete	Review your selections and click **Finish**.

Depending on your network speed, the deployment can take several minutes. You can view the progress in the progress dialog box that appears.

5 When the deployment is complete, click **Close** in the progress dialog box.

6 Select the Workspace ONE Access virtual appliance you deployed, right-click, and select **Power > Power on**.

The virtual appliance is initialized. When the initialization is complete, the console screen displays the Workspace ONE Access version, IP address, and the URLs to log in to the Workspace ONE Access console and to complete the set up.

Note An error message might appear about the network not being detected. You can still access the https://*WS1AccessHostnameFQDN*:8443/cfg/ page to configure the Workspace ONE Access settings. Rebooting the Workspace ONE Access virtual appliance clears the error message.

What to do next

- (Optional) Add IP Pools.
- Configure Workspace ONE Access settings, including connecting to your Active Directory or LDAP directory and selecting users and groups to sync to Workspace ONE Access.

(Optional) Add IP Pools to the Workspace ONE Access Virtual Appliance

Network configuration with IP Pools is optional in Workspace ONE Access. You can manually add IP pools to the Workspace ONE Access virtual appliance after it is installed.

IP Pools act like DHCP servers to assign IP addresses from the pool to the VMware Workspace ONE Access virtual appliance. To use IP Pools, you edit the virtual appliance networking properties to change the properties to dynamic properties and configure the netmask, gateway, and DNS settings.

Prerequisites

The virtual appliance must be powered off.

Procedure

1 In the vSphere Client or the vSphere Web Client, right-click the VMware Workspace ONE Access virtual appliance and select **Edit Settings**.

2 Select the **Options** tab.

3 Under **vApp Options**, click **Advanced**.

4 In the Properties section on the right, click the **Properties** button.

5 In the Advanced Property Configuration dialog box, configure the following keys:

- vami.DNS.IdentityManager
- vami.netmask0.IdentityManager

- vami.gateway.IdentityManager

a Select one of the keys and click **Edit**.

b In the Edit Property Settings dialog box, next to the **Type** field, click **Edit**.

c In the Edit Property Type dialog box, select **Dynamic Property** and select the appropriate value from the drop down menu for **Netmask**, **Gateway Address**, and **DNS Servers** respectively.

d Click **OK**, and click **OK** again.

e Repeat these steps to configure each key.

6 Power on the virtual appliance.

Results

The properties are configured to use IP Pools.

What to do next

Configure Workspace ONE Access settings.

Configure Workspace ONE Access Settings

After the Workspace ONE Access instance is deployed, you use the Setup wizard to set passwords and select a database.

Make sure that your run the Setup wizard using the fully qualified host name. Do not enter the IP address as the name.

Prerequisites

- The Workspace ONE Access machine is powered on.
- The external database is configured and the external database connection information is available. Before you run the Setup wizard, verify that the database configuration is correct. See Create the Workspace ONE Access Service Database for information.
- In the Microsoft SQL server, make sure that the database user is granted the db_owner role. Members of the db_owner database role can perform all configuration and maintenance activities on the database. See

Procedure

1 Go to the Workspace ONE Access URL that was displayed when you finished the installation. Enter the fully qualified domain name (FQDN). For example, `https://WS1AccessHostnameFQDN.example.com`.

2 Accept the certificate, if prompted.

You can update the certificate after the initial set up.

3 In the Get Started page, click **Continue**.

4 In the Set Passwords page, set passwords for the following administrator accounts, which are used to manage the appliance, then click **Continue**.

Account	
Appliance Administrator	Set the password for the **admin** user. This user name cannot be changed. The **admin** user account is used to manage the appliance settings. **Important** The **admin** user password must be at least 6 characters in length.
Appliance Root	Set the **root** user password. The **root** user has full rights to the appliance.
Remote User	Set the **sshuser** password, which is used to log in remotely to the appliance with an SSH connection.

5 In the Select Database page, select the database to use.

See Configure Workspace ONE Access to Use an External Database

- If you are using an external database, select **External Database** and enter the external database connection information, user name, and password. To verify that Workspace ONE Access can connect to the database, click **Test Connection**.

  After you verify the connection, click **Continue**.
- If you are using the internal database, click **Continue**.

  Note The internal database is not recommended for use with production deployments.

  You select the database to use when you first deploy the Workspace ONE Access appliance. You cannot change the database type.

The connection to the database is configured and the database is initialized. When the process is complete, the **Setup is complete** page appears.

What to do next

To set up a directory, you must first install one or more instances of the Workspace ONE Access connector. See the corresponding version of the *Installing Workspace ONE Access Connector* guide. Before setting up the directory, review *Directory Integration with Workspace ONE Access* for requirements and limitations.

Deploying the Workspace ONE Access Machine Behind a Load Balancer

In an enterprise environment, the recommended Workspace ONE Access machine configuration is to deploy a three-node cluster of the Workspace ONE Access service for high availability. After the first Workspace ONE Access node is installed, configured, and tested behind the load balancer, the first node is cloned to create the other nodes in the cluster.

The Workspace ONE Access architecture diagram demonstrates how you can deploy the Workspace ONE Access environment.

See Chapter 1 Preparing to Install Workspace ONE Access for a typical deployment.

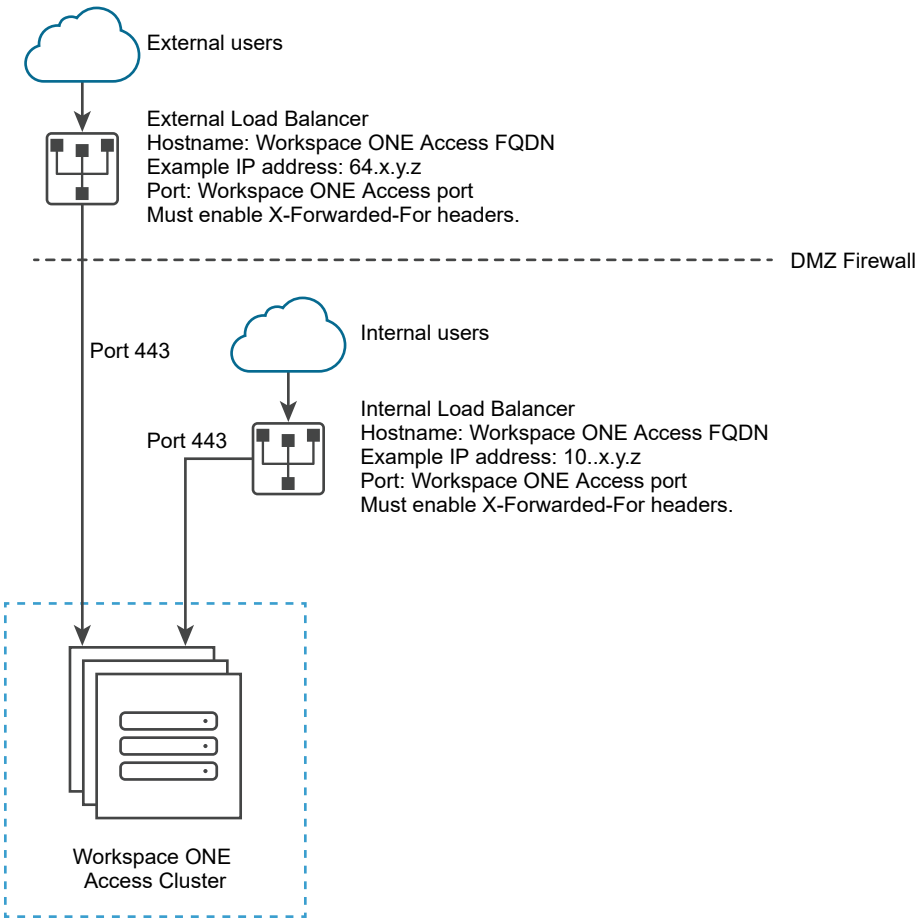
Using a Load Balancer or Reverse Proxy to Enable External Access to Workspace ONE Access

During deployment, the Workspace ONE Access instance is set up inside the internal network. If you want to provide access to the service for users connecting from outside networks, you must install a load balancer or a reverse proxy, such as VMware NSX® Advanced Load Balancer™, Apache, Nginx, or F5, in the DMZ.

If you do not use a load balancer or reverse proxy, you cannot expand the number of Workspace ONE Access instances later. You might need to add more instances to provide redundancy and load balancing. The following diagram shows the basic deployment architecture that you can use to enable external access.

Note The same Workspace ONE Access FQDN is used for both internal and external access in this deployment.

Figure 4-1. External Load Balancer Proxy with Virtual Machines



Specify Workspace ONE Access FQDN during Deployment

During the deployment of the Workspace ONE Access appliance, you enter a single Workspace ONE Access FQDN and the port number. These values must point to the host name that you want end users to access.

The Workspace ONE Access machine always runs on port 443. You can use a different port number for the load balancer. If you use a different port number, you must specify it during deployment. Do not use 8443 as the port number, as this port number is the Workspace ONE Access administrative port and is unique for each machine in a cluster.

Load Balancer Settings to Configure

Load balancer settings to configure include enabling X-Forwarded-For headers, setting the load balancer time-out correctly, and enabling sticky sessions. In addition, SSL trust must be configured between the Workspace ONE Access connector machine and the load balancer.

- X-Forwarded-For Headers

You must enable X-Forwarded-For headers on your load balancer. This determines the authentication method. See the documentation provided by your load balancer vendor for more information.

- Load Balancer Timeout

  For Workspace ONE Access to function correctly, you might need to increase the load balancer request timeout from the default. The value is set in minutes. If the timeout setting is too low, you might see this error, “502 error: The service is unavailable”.

- Enable Sticky Sessions

  You must enable the sticky session setting on the load balancer if your deployment has multiple Workspace ONE Access machines. The load balancer binds a user's session to a specific instance.

- Do not block session cookies

  Do not block session cookies by adding rules to the load balancer. Adding such rules to the load balancer can result in inconsistent behavior and failed requests.

- WebSocket support

  The load balancer must have WebSocket support to enable secure communication channels between connector instances and the Workspace ONE Access nodes.

  For your deployment, if VMware Workspace ONE Hub Services is integrated, WebSocket support is required for Hub Services notifications. Therefore, Web Socket support must be provided for end user browsers and devices.

- Ciphers with forward secrecy

  Apple iOS App Transport Security requirements apply to the Workspace ONE app on iOS. To enable users to use the Workspace ONE app on iOS, the load balancer must have ciphers with forward secrecy. The following ciphers meet this requirement:

  ECDHE_ECDSA_AES and ECDHE_RSA_AES in GCM or CBC mode

  as stated in the iOS 11 *iOS Security* document:

  "App Transport Security provides default connection requirements so that apps adhere to best practices for secure connections when using NSURLConnection, CFURL, or NSURLSession APIs. By default, App Transport Security limits cipher selection to include only suites that provide forward secrecy, specifically ECDHE_ECDSA_AES and ECDHE_RSA_AES in GCM or CBC mode."

Apply Workspace ONE Access Root Certificate to the Load Balancer

When the Workspace ONE Access virtual appliance is configured behind a load balancer, you must establish SSL trust between the load balancer and Workspace ONE Access. The Workspace ONE Access root certificate must be copied to the load balancer.

The Workspace ONE Access root certificate can be downloaded from the **Install SSL Certificates > Server Certificate** page in the Workspace ONE Access administration console. See Change the Workspace ONE Access Appliance Configuration Settings for information about accessing appliance configuration settings pages, including the **Install SSL Certificates** page.

If the Workspace ONE Access FQDN points to a load balancer, the SSL certificate can only be applied to the load balancer.

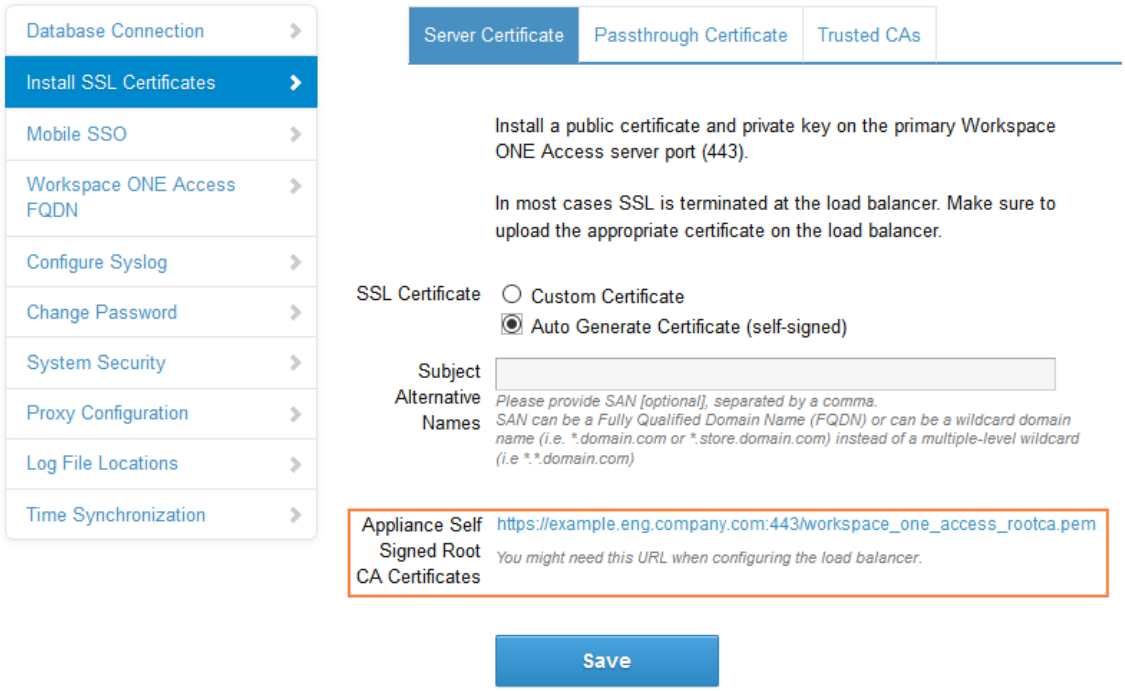
Since the load balancer communicates with the Workspace ONE Access virtual appliance, you must copy the Workspace ONE Access root CA certificate to the load balancer as a trusted root certificate.

Procedure

1. Log in to the Workspace ONE Access console.
2. Select **Dashboard > System Diagnostics Dashboard**.
3. Click **VA Configuration** of the service node you want to configure and log in with the admin user password.
4. Select **Install SSL Certificates > Server Certificate**.
5. Select **Auto Generate Certificate (self-signed)**
6. If applicable, provide the appropriate SAN entries in the **Subject Alternative Names** text box.

   If SSL is not terminated on the load balancer, the SSL certificate used by the service must include Subject Alternative Names (SANs) for each of the fully qualified domain names in the Workspace ONE Access cluster. Including the SAN enables the nodes within the cluster to make requests to each other. Also include a SAN for the FQDN host name that users use to access the Workspace ONE Access service, in addition to using it for the Common Name, because some browsers require it.

7 Click the **Appliance Self Signed Root CA Certificates** link.



The certificate is displayed.

8 Copy everything between and including the lines -----BEGIN CERTIFICATE----- and -----END CERTIFICATE---- and paste the root certificate into the correct location on each of your load balancers. Refer to the documentation provided by your load balancer vendor.

What to do next

Copy and paste the load balancer root certificate to the Workspace ONE Access appliance.

Apply Load Balancer Root Certificate to Workspace ONE Access

When the Workspace ONE Access virtual appliance is configured behind a load balancer, you must establish trust between the load balancer and Workspace ONE Access . In addition to copying the Workspace ONE Access root certificate to the load balancer, you must copy the load balancer root certificate to Workspace ONE Access .

Procedure

1 Obtain the load balancer root certificate.

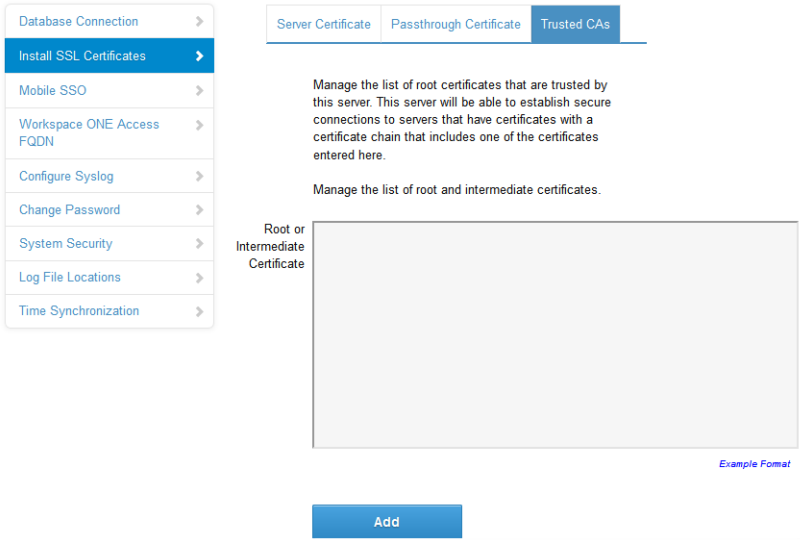
2 Log in to the Workspace ONE Access console.

3 Select **Dashboard > System Diagnostics Dashboard**.

4 Click **VA Configuration** of the service node you want to configure and log in with the admin user password.

5 Select **Install SSL Certificates > Trusted CAs**.

6 Paste the load balancer root certificate into the **Root or Intermediate Certificate** text box.



7 Click **Add**.

Configuring Failover and Redundancy for Workspace ONE Access in a Single Datacenter

To achieve failover and redundancy, you can add multiple Workspace ONE Access virtual appliances in a cluster. If one of the appliances shuts down for any reason, Workspace ONE Access is still available.

To create the cluster, you first install and configure a Workspace ONE Access virtual appliance, then you clone it. Cloning the virtual appliance creates a duplicate of the appliance with the same configuration as the original. You can customize the cloned virtual appliance to change the name, network settings, and other properties as required.

Before you clone the Workspace ONE Access virtual appliance, you must configure it behind a load balancer and change its Fully Qualified Domain Name (FQDN) to match the load balancer FQDN. Also, complete directory configuration in the Workspace ONE Access service before you clone the appliance.

After cloning, you assign the cloned virtual appliance a new IP address before powering it on. The cloned virtual appliance IP address must follow the same guidelines as the IP address of the original virtual appliance. The IP address must resolve to a valid host name using forward and reverse DNS.

All nodes in the Workspace ONE Access cluster are identical and nearly stateless copies of each other. Syncing to Active Directory and to resources that are configured, such as View or ThinApp, is deactivated on the cloned virtual appliances.

Procedure

1 Recommendations for Workspace ONE Access Cluster

Follow these guidelines for setting up a Workspace ONE Access cluster.

2 Change Workspace ONE Access FQDN to Load Balancer FQDN

3 Create Multiple workspace-va Virtual Appliances

For failover, your enterprise can clone the workspace-va virtual appliance to create multiple virtual appliances of the same type to distribute traffic and eliminate potential downtime.

4 Assign a New IP Address to Cloned Workspace ONE Access Virtual Appliance

You must assign a new IP address to each cloned virtual appliance before you power it on. The IP address must be resolvable in DNS. If the address is not in the reverse DNS, you must also assign the host name.

5 Enabling Directory Sync on Another Instance in the Event of a Failure

6 Removing a Workspace ONE Access Node from a Cluster

If a node in the Workspace ONE Access cluster is not functioning correctly and you are unable to recover it, you can remove it from the cluster with the Remove Node command. The command removes the node entries from the Workspace ONE Access database.

Recommendations for Workspace ONE Access Cluster

Follow these guidelines for setting up a Workspace ONE Access cluster.

Recommended Number of Nodes in Workspace ONE Access Cluster

Setting up a Workspace ONE Access cluster with three nodes is recommended.

The Workspace ONE Access appliance includes Elasticsearch, a search and analytics engine. Elasticsearch has a known limitation with clusters of two nodes. For a description of the Elasticsearch "split brain" limitation, see the Elasticsearch documentation. Note that you do not have to configure any Elasticsearch settings.

A Workspace ONE Access cluster with two nodes provides failover capability with a few limitations related to Elasticsearch. If one of the nodes shuts down, the following limitations apply until the node is brought up again:

- The dashboard does not display data.
- Most reports are unavailable.
- Sync log information is not displayed for directories.
- The search field in the top-right corner of the administration console does not return any results.

- Auto-complete is not available for text fields.

There is no data loss during the time the node is down. Audit event and sync log data is stored and will be displayed when the node is restored.

Network Partitions

Creating a network partition between nodes in a Workspace ONE Access cluster is not recommended. If a network partition exists between Workspace ONE Access service nodes such that the nodes cannot communicate with each other, and if all the nodes are still accessible from the load balancer, letting login requests go to any of the partitioned nodes, you might encounter the following problems:

- You might see stale data across requests. For example, changes made to an access policy on one node might not apply to login requests that go to another node if there is a partition between the nodes.
- Login calls that use the outbound connector might fail.

Change Workspace ONE Access FQDN to Load Balancer FQDN

Before you clone the Workspace ONE Access virtual appliance, you must change its Fully Qualified Domain Name (FQDN) to match the load balancer FQDN.

Prerequisites

- The Workspace ONE Access instance is added to a load balancer.
- You have applied the load balancer root CA certificate to Workspace ONE Access.

Procedure

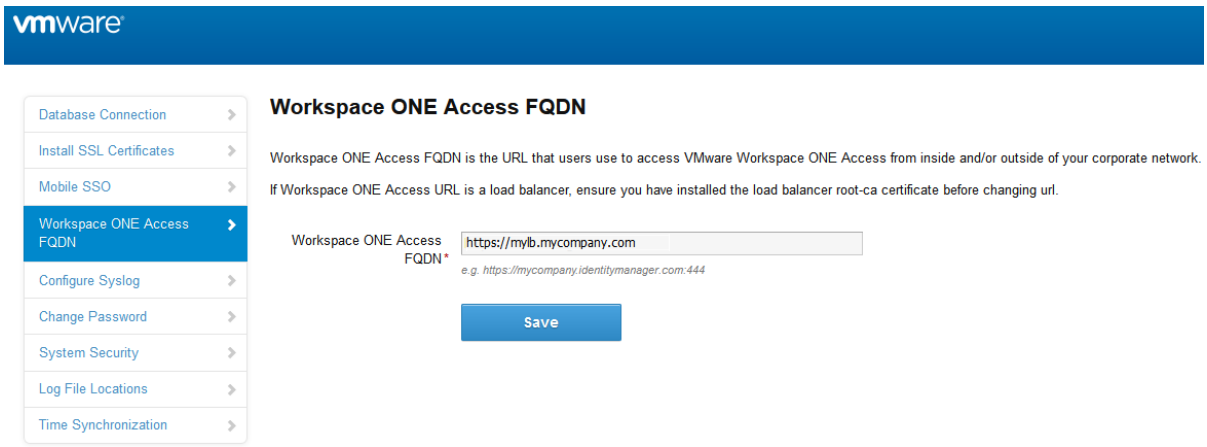
1. Log in to the Workspace ONE Access console.
2. Select **Dashboard > System Diagnostics Dashboard**.
3. Click **VA Configuration** of the service node you want to configure and log in with the admin user password.
4. Click **Workspace ONE Access FQDN** and in the **Workspace ONE Access FQDN** text box change the host name part of the URL from the Workspace ONE Access host name to the load balancer host name.

   For example, if your Workspace ONE Access host name is `myservice` and your load balancer host name is `mylb`, you would change the URL

   `https://myservice.example.com`

   to the following:

   `https://mylb.example.com`



5 Click **Save**.

Results

- The service FQDN is changed to the load balancer FQDN.
- The Identity Provider URL is changed to the load balancer URL.

What to do next

Clone the virtual appliance.

Create Multiple workspace-va Virtual Appliances

For failover, your enterprise can clone the workspace-va virtual appliance to create multiple virtual appliances of the same type to distribute traffic and eliminate potential downtime.

Using multiple workspace-va virtual appliance improves availability, load balances requests to Workspace ONE Access, and decreases response times to the end user.

Prerequisites

- An external database must be set up in order to add additional workspace-va virtual appliances.
- The virtual appliance must be configured behind a load balancer. Make sure that the load balancer port is 443. Do not use 8443 as this port number is the Workspace ONE Access administrative port and is unique to each virtual appliance.
- VMware vSphere Client or vSphere Web Client is required to clone the virtual appliance and to access the cloned virtual appliance to configure networking.

Procedure

1 Power off the workspace-va virtual appliance that is being cloned.

2 Right-click the virtual appliance that is being cloned, and click **Next**.

3 Enter the name you want to use to identify this cloned virtual appliance. The name must be unique within the virtual appliance folder.

4 Select the host or cluster on which to run the cloned virtual appliance.

5 Select the resource pool in which to run the virtual appliance and click **Next**.

6 Select the datastore location where you want to store the virtual appliance files.

7 Select the format for the virtual appliance's disks. This should be the same format as the source. Click **Next**.

8 Select **Do not customize** as the guest operating system option.

9 Review the options you selected. If the information is correct, click **Finish**.

Results

The cloned virtual appliance is deployed. You cannot use or edit the virtual appliance until the cloning is complete.

What to do next

Assign an IP address to the cloned workspace-va before you power up the machine and add the new virtual appliance to the load balancer.

Assign a New IP Address to Cloned Workspace ONE Access Virtual Appliance

You must assign a new IP address to each cloned virtual appliance before you power it on. The IP address must be resolvable in DNS. If the address is not in the reverse DNS, you must also assign the host name.

Procedure

1 In the vSphere Client or the vSphere Web Client, select the cloned virtual appliance.

2 In the **Summary** tab, under **Commands**, click **Edit Settings**.

3 Select **Options** and in the **vApp Options** list, select **Properties**.

4 Change the IP address in the **IP Address** field.

5 If the IP address is not in the reverse DNS, add the host name in the **HostName** text box.

6 Click **OK.**

7 Power on the cloned appliance and wait until the blue login screen appears in the **Console** tab.

> **Important** Before you power on the cloned appliance, ensure that the original appliance is fully powered on.

What to do next

- Wait for a few minutes until the Elasticsearch cluster is created before adding the cloned virtual appliance to the load balancer.

Elasticsearch, a search and analytics engine, is embedded in the virtual appliance.

a Log in to the cloned virtual appliance.

b Check the Elasticsearch cluster:

```
curl -XGET 'http://localhost:9200/_cluster/health?pretty=true'
```

Verify that the result matches the number of nodes.

- Add the cloned virtual appliance to the load balancer and configure the load balancer to distribute traffic. See your load balancer vendor documentation for information.
- If the original service instance was joined to the domain, then you need to join the domain in the cloned service instances.

  a Log in to the Workspace ONE Access console.

  b Select the **Identity & Access Management** tab, then click **Setup**.

  The connector component of each of the cloned service instances is listed on the Connectors page.

  c For each connector instance listed, click **Join Domain** and specify the domain information.

  For more information about Active Directory, see *Directory Integration with Workspace ONE Access*.
- For directories of type Active Directory over Integrated Windows Authentication (IWA), you must do the following:

  a For the cloned service instances, join the domain to which the IWA directory in the original service instance was joined.

  1 Log in to the Workspace ONE Access console.

  2 Select the **Identity & Access Management** tab, then click **Setup**.

  The connector component of each of the cloned service instances is listed in the Connectors page.

  3 For each connector listed, click **Join Domain** and specify the domain information.

  b Save the IWA directory configuration.

  1 Select the **Identity & Access Management** tab.

  2 In the Directories page, click the IWA directory link.

  3 Click **Save** to save the directory configuration.
- Enable the authentication methods configured for the connector on each of the cloned instances. See the *VMware Workspace ONE Access Administration* guide for information.

The Workspace ONE Access service virtual appliance is now highly available. Traffic is distributed to the virtual appliances in your cluster based on the load balancer configuration. Authentication to the service is highly available. For the directory sync feature of the service, however, in the event of a service instance failure, you will need to manually enable directory sync on a cloned service instance. Directory sync is handled by the connector component of the service and can only be enabled on one connector instance at a time. See Enabling Directory Sync on Another Instance in the Event of a Failure.

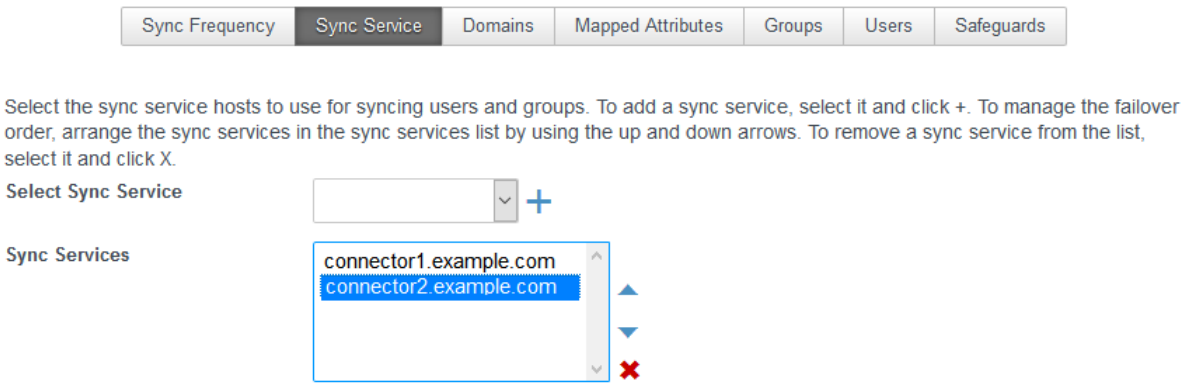
Enabling Directory Sync on Another Instance in the Event of a Failure

Configure multiple instances of Directory Sync for automatic failover in case a node fails to sync.

Perform the steps that follow to configure multiple instances of the Directory Sync service.

Procedure

1. Log in to the Workspace ONE Access console.
2. Click the **Identity & Access Management** tab, then click **Directories**.
3. Click the directory for which you would like to add another Directory Sync service.
4. Click **Sync Settings**.
5. Click **Sync Service**.
6. Use the **Select Sync Service** drop-down menu to select other Directory Sync service instances to add to the **Sync Services** list and use the arrows to manage the failover order.



7. Click **Save**.

Removing a Workspace ONE Access Node from a Cluster

If a node in the Workspace ONE Access cluster is not functioning correctly and you are unable to recover it, you can remove it from the cluster with the Remove Node command. The command removes the node entries from the Workspace ONE Access database.

You can check the health of the nodes in your cluster by viewing their status in the System Diagnostics Dashboard. A `The current node is in a bad state` message indicates that the node is not functioning correctly.

Important Use the Remove Node command sparingly. Only use it when a node is in an unrecoverable state and must be removed completely from the Workspace ONE Access deployment.

Note You cannot use the Remove Node command to remove the last node in a cluster.

Remove the Workspace ONE Access Node from the Cluster

You can remove the node from the cluster.

Note You cannot use the Remove command to remove the last node in a cluster.

Prerequisites

To remove a node, you must log in as a tenant administrator, that is, a local administrator on the Workspace ONE Access service. A domain administrator synced from the enterprise directory does not have the necessary permissions.

Procedure

1. Shut down the node virtual machine.
   a. Log in to the vCenter Server instance.
   b. Right-click the node virtual machine and select **Power > Power Off**.
2. Remove the node from the load balancer.
3. In the Workspace ONE Access console, remove the node.
   a. Log in to the Workspace ONE Access console as a local administrator.
   b. Click the down arrow on the **Dashboard** tab and select **System Diagnostics Dashboard**.
   c. Locate the node you want to remove.

      The node displays the following status:

      ```
      The current node is in a bad state. Do you want to want to remove it?
      ```

   d. Click the **Remove** link that is displayed next to the message.

Results

The node is removed from the cluster. Entries for the node are removed from the Workspace ONE Access database. The node is also removed from the embedded Elasticsearch and Ehcache clusters.

What to do next

Wait 5-15 minutes for the embedded Elasticsearch and Ehcache clusters to stabilize before using any other commands.

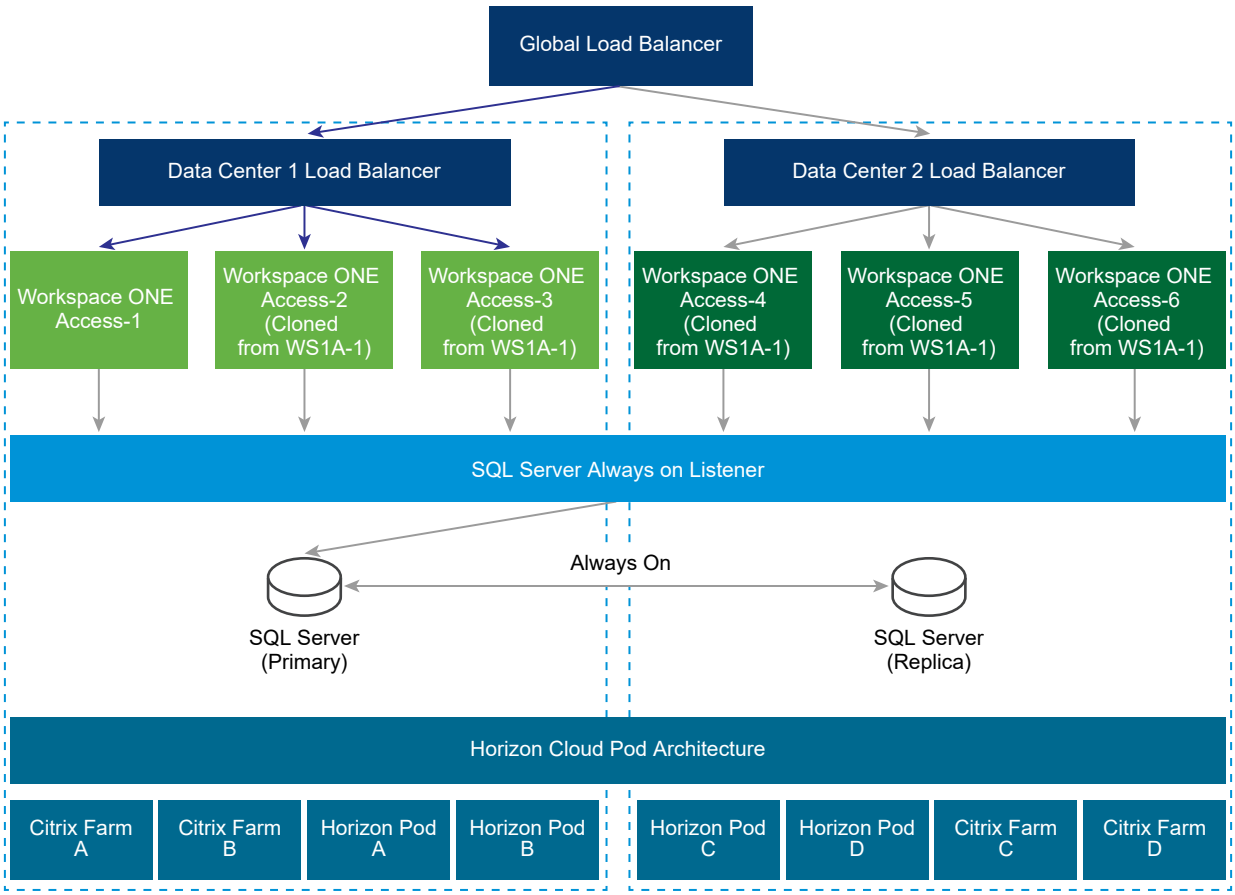
Deploying Workspace ONE Access in a Secondary Data Center for Failover and Redundancy

To provide failover capabilities if the primary Workspace ONE Access data center becomes unavailable, you must deploy Workspace ONE Access in a secondary data center.

For disaster recovery, the recommendation is to use VMware Site Recovery Manager. See Performing Disaster Recovery for Workspace ONE Access Using Site Recovery Manager. If you do not meet the requirements for Site Recovery Manager, implement the following approach.

By using a secondary data center, end users can log in and use applications with minimal downtime. Also, with a secondary data center, you can upgrade Workspace ONE Access to the next version with minimal downtime. See Upgrading Workspace ONE Access with Minimal Downtime.

A typical deployment using a secondary data center is shown here.



For information about the correct version of the connector to use with the ThinApp repository for ThinApp packaged applications, Integration Broker for Citrix published resources, and Horizon Connection Server for Horizon desktops and applications, see the corresponding important note in Chapter 1 Preparing to Install Workspace ONE Access.

Follow these guidelines for a multiple data center deployment.

- Cluster Deployment: You must deploy a set of Workspace ONE Access virtual appliances in two separate data centers.
  - A set of three or more Workspace ONE Access virtual appliances as one cluster in one data center.
  - Another set of three or more Workspace ONE Access virtual appliances as another cluster in a second data center.

  See Setting up a Secondary Data Center for Workspace ONE Access for more information.
- Database: Workspace ONE Access uses the database to store data. For a multiple data center deployment, replication of the database between the two data centers is crucial. Refer to your database documentation about how to set up a database in multiple data centers. For example, with SQL Server, using Always On deployment is preferable. See Overview of Always On Availability Groups (SQL Server) on the Microsoft website for information. Workspace ONE Access functionalities are designed for minimal latency between the database and the Workspace ONE Access appliance. Therefore, appliances in one data center are designed to connect to the database in the same data center.
- Not Active-Active: Workspace ONE Access does not support an Active-Active deployment where users can be served from both data centers at the same time. The secondary data center is a hot stand-by and can be used to provide business continuity for end users. Workspace ONE Access appliances in the secondary data center are in a read-only mode. Therefore, after a failover to that data center, most admin operations, like adding users or applications, or entitling users, will not work.
- Fail-Back to Primary: In most failure scenarios, you can fail back to the primary data center after that data center is back to normal. See Failback to Primary Data Center for Workspace ONE Access for information.
- Promote Secondary to Primary: If an extended data center failure occurs, the secondary data center can be promoted to primary. See Promoting Secondary Data Center to Primary Data Center for Workspace ONE Access for information.
- Fully Qualified Domain Name: The fully qualified domain name to access Workspace ONE Access must be the same in all data centers.
- Audits: Workspace ONE Access uses Elasticsearch embedded in the Workspace ONE Access appliance for auditing, reports, and directory sync logs. Create separate Elasticsearch clusters in each data center. See Setting up a Secondary Data Center for Workspace ONE Access for more information.

- Active Directory: Workspace ONE Access can connect to Active Directory using the LDAP API or using Integrated Windows Authentication. With both of these methods, Workspace ONE Access can use Active Directory SRV records to reach the appropriate domain controller in each data center.
- Windows Apps: Workspace ONE Access supports accessing Windows apps using ThinApp, and Windows Apps and Desktops using Horizon or Citrix technologies. Delivering these resources from a data center that is closer to the user, also called Geo-Affinity, is important.

  Important For information about the correct version of the connector to use with the ThinApp repository for ThinApp packaged applications, Integration Broker for Citrix published resources, and Horizon Connection Server for Horizon desktops and applications, see the corresponding note in Chapter 1 Preparing to Install Workspace ONE Access

  Note the following about Windows resources:

  - ThinApps - Workspace ONE Access supports Windows Distributed File Systems as a ThinApp repository. Use the Windows Distributed File Systems documentation to set up appropriate location-specific policies.
  - Horizon (with Cloud Pod Architecture) - Workspace ONE Access supports Horizon Cloud Pod Architecture. Horizon Cloud Pod Architecture provides Geo-Affinity using global entitlements. See "Integrating Cloud Pod Architecture Deployments" in *Setting up Resources in VMware Workspace ONE Access* for information. No additional changes are required for a Workspace ONE Access multiple data center deployment.
  - Horizon (without Cloud Pod Architecture) - If Horizon Cloud Pod Architecture is not enabled in your environment, you cannot enable Geo-Affinity. After a fail-over event, you can manually switch VMware Workspace ONE Access to run Horizon resources from the Horizon pods configured in the secondary data center. See Configure Failover Order of Horizon and Citrix-published Resources for more information.
  - Citrix Resources - Similar to Horizon (without Cloud Pod Architecture), you cannot enable Geo-Affinity for Citrix resources. After a fail-over event, you can manually switch Workspace ONE Access to run Citrix resources from the XenFarms configured in the secondary data center. See Configure Failover Order of Horizon and Citrix-published Resources for more information.

Setting up a Secondary Data Center for Workspace ONE Access

The secondary data center is typically managed by a different vCenter Server. When you set up the secondary data center, you can configure and implement the following based on your requirements.

- Workspace ONE Access appliances in the secondary data center, created from an OVA file imported from the primary data center
- Load balancer for the secondary data center
- Duplicate Horizon View and Citrix-based resources and entitlements

- Database configuration
- Load balancer or DNS entry across the primary and secondary data centers for failover

Requirements for Deploying Workspace ONE Access in a Secondary Data Center

Ensure that you meet these requirements for deploying Workspace ONE Access in a secondary data center.

- Ensure that the Workspace ONE Access certificate includes the FQDN of the load balancer from the primary data center as well as the FQDN of the load balancer from the secondary data center. Otherwise, the certificate must be a wildcard certificate.
- Ports 443 and 8443 must be open between all Workspace ONE Access instances, both within a cluster and across clusters in different data centers.

Modify the Primary Data Center for Replication

Before you set up the secondary data center, configure the primary data center for Elasticsearch replication across clusters.

Elasticsearch, a search and analytics engine embedded in the Workspace ONE Access virtual appliance, is used for auditing, reports, and directory sync logs.

Make these changes in all the nodes in the primary data center cluster.

Prerequisites

You have set up a Workspace ONE Access cluster in the primary data center.

Procedure

1. Add the load balancer FQDN of the secondary data center cluster to the `/usr/local/horizon/conf/runtime-config.properties` file of each node in the primary data center cluster.
   a. Edit the `/usr/local/horizon/conf/runtime-config.properties` file.

      ```
      vi /usr/local/horizon/conf/runtime-config.properties
      ```

   b. Add this line to the file:

      ```
      analytics.replication.peers=https://LB_FQDN_of_second_cluster
      ```

2. Restart the Workspace ONE Access service on all the nodes.

   ```
   service horizon-workspace restart
   ```

3. Verify that the cluster is set up correctly by running the following command on all the nodes in the cluster.

   ```
   curl 'http://localhost:9200/_cluster/health?pretty'
   ```

The command, which verifies Elasticsearch health, should return a result similar to the following.

```
{
  "cluster_name" : "horizon",
  "status" : "green",
  "timed_out" : false,
  "number_of_nodes" : 3,
  "number_of_data_nodes" : 3,
  "active_primary_shards" : 20,
  "active_shards" : 40,
  "relocating_shards" : 0,
  "initializing_shards" : 0,
  "unassigned_shards" : 0,
  "delayed_unassigned_shards" : 0,
  "number_of_pending_tasks" : 0,
  "number_of_in_flight_fetch" : 0
}
```

What to do next

Verify that the cluster in the primary data center is set up correctly by viewing the Systems Diagnostics dashboard.

Verify Configuration of the Workspace ONE Access Cluster in the Primary Data Center

Before you set up the secondary data center, verify that the cluster in the primary data center is set up correctly. Also verify that the embedded components Elasticsearch and Ehcache are clustered correctly.

Elasticsearch and Ehcache are embedded in the Workspace ONE Access service. Elasticsearch is a search and analytics engine used for auditing, reports, and directory sync logs. Ehcache provides caching capabilities.

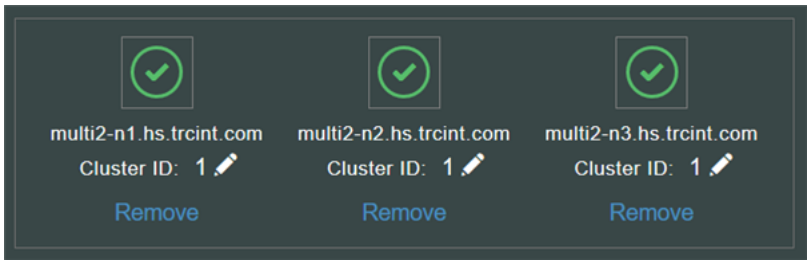
Prerequisites

You set up a Workspace ONE Access cluster in the primary data center and configured the nodes for Elasticsearch replication.

Procedure

1 In the Workspace ONE Access console, select the **Dashboard > System Diagnostics Dashboard** tab.

2 On the top panel, locate the cluster information.



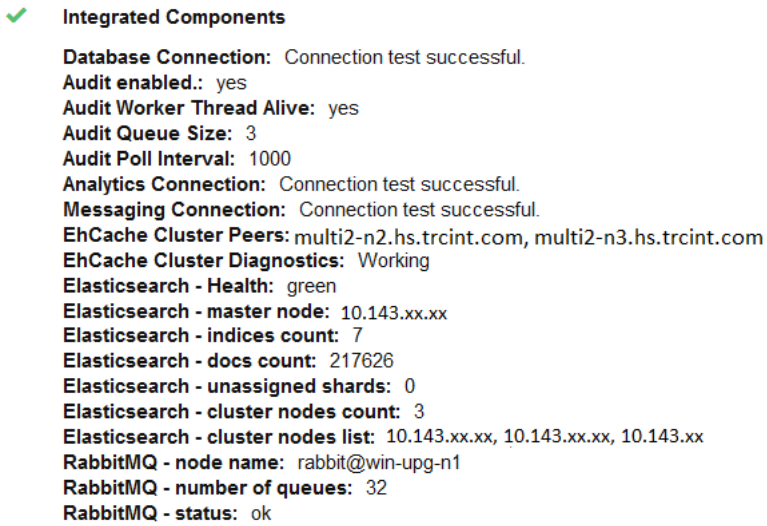
3 Verify that the instances are grouped correctly by checking the Cluster IDs of the instances, and make changes if necessary.

All instances in a cluster must have the same Cluster ID.

- To update the **Cluster ID** of an instance, click the pencil icon next to the number.
- To remove an instance from the cluster, click **Remove**.

4 For each instance listed in the left pane, scroll down to the **Integrated Components** section and verify that the Elasticsearch and Ehcache cluster information is correct.

For example:



What to do next

Create a cluster in the secondary data center. Create the nodes by exporting the OVA file of the first Workspace ONE Access virtual appliance from the primary data center cluster and using it to deploy the new virtual appliances in the secondary data center.

Create Workspace ONE Access Virtual Appliances in Secondary Data Center

To set up a Workspace ONE Access cluster in the secondary data center, you export the OVA file of the original Workspace ONE Access appliance in the primary data center and use it to deploy appliances in the secondary data center.

Prerequisites

- Workspace ONE Access OVA file that was exported from the original Workspace ONE Access appliance in the primary data center
- IP addresses and DNS records for secondary data center

Procedure

1. In the primary data center, export the OVA file of the original Workspace ONE Access appliance.

   See the vSphere documentation for information.

2. In the secondary data center, deploy the Workspace ONE Access OVA file that was exported to create the new nodes.

   See the vSphere documentation for information. Also see Install the Workspace ONE Access OVA File.

3. After the VMware Workspace ONE Access appliances are powered on, update the appliance configuration for each.

   The Workspace ONE Access appliances in the secondary data center are identical copies of the original Workspace ONE Access appliance in the primary data center. Syncing to Active Directory and to resources that are configured in the primary data center is deactivated.

What to do next

Go to the administration console pages and configure the following:

- Enable Join Domain as configured in the original Workspace ONE Access appliance in the primary data center.
- In the Auth Adapters page, add the authentication methods that are configured in the primary data center.
- In the Directory Authentication Method page, enable Windows Authentication, if configured in the primary data center.

Go to the **Install SSL Certificates** page to add Certificate Authority signed certificates, duplicating the certificates in the Workspace ONE Access appliances in the primary data center. See Using SSL Certificates in Workspace ONE Access Service.

Configure Nodes in Secondary Data Center for Workspace ONE Access

After you create nodes in the secondary data center by using the OVA file exported from the primary data center, configure the nodes for Elasticsearch replication.

Follow these steps for each node in the secondary data center.

Procedure

1 Add the load balancer FQDN of the primary data center cluster to the `/usr/local/horizon/conf/runtime-config.properties` file of each node in the secondary data center cluster.

   a Access the `/usr/local/horizon/conf/runtime-config.properties` file for editing.

   ```
   vi /usr/local/horizon/conf/runtime-config.properties
   ```

   b Change the following line in the file:

   ```
   analytics.replication.peers=https://LB_FQDN_of_second_cluster
   ```

   to

   ```
   analytics.replication.peers=https://LB_FQDN_of_primary_cluster
   ```

2 Restart the Workspace ONE Access service on all the nodes.

```
service horizon-workspace restart
```

3 Verify that the cluster is set up correctly by running the following command on all the nodes in the cluster.

```
curl 'http://localhost:9200/_cluster/health?pretty'
```

The command, which verifies Elasticsearch health, should return a result similar to the following.

```
{
  "cluster_name" : "horizon",
  "status" : "green",
  "timed_out" : false,
  "number_of_nodes" : 3,
  "number_of_data_nodes" : 3,
  "active_primary_shards" : 20,
  "active_shards" : 40,
  "relocating_shards" : 0,
  "initializing_shards" : 0,
  "unassigned_shards" : 0,
  "delayed_unassigned_shards" : 0,
  "number_of_pending_tasks" : 0,
  "number_of_in_flight_fetch" : 0
}
```

Set Cluster ID and Verify Cluster in Secondary Data Center for Workspace ONE Access

After you create nodes in the secondary data center and configure Elasticsearch for replication, set the Cluster ID for the secondary data center and verify that the cluster is set up correctly.

Procedure

1 In the Workspace ONE Access console, select the **Dashboard > System Diagnostics Dashboard** tab.

2 On the top panel, change the **Cluster ID** of all the nodes in the secondary data center cluster to a different number than the first data center.

For example:

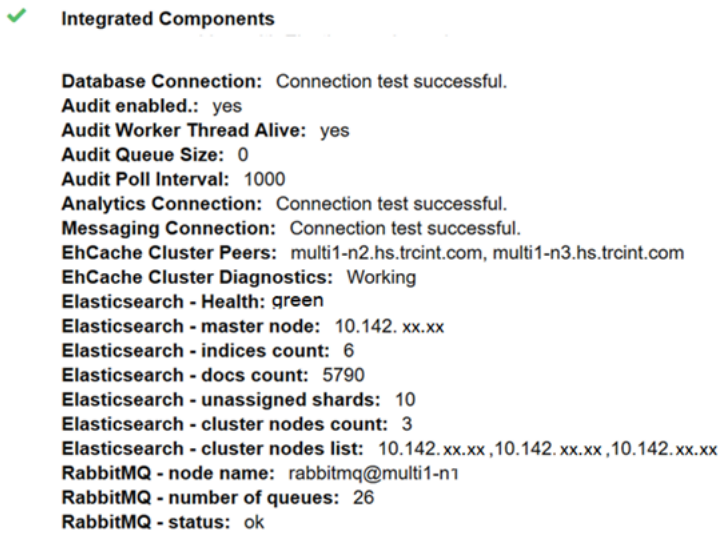
3 Verify that the nodes are grouped correctly by checking the Cluster IDs of the nodes, and make changes if necessary.

All nodes in a cluster must have the same Cluster ID.

- To update the **Cluster ID** of a node, click the pencil icon next to the number.
- To remove a node from the cluster, click **Remove**.

4 For each node listed in the left pane, scroll down to the **Integrated Components** section and verify that the Elasticsearch and Ehcache cluster information is correct.

For example:



Edit runtime-config.properties File for Workspace ONE Access in Secondary Data Center to Set Read-Only Mode

You must edit the `runtime-config.properties` files for the Workspace ONE Access appliances in the secondary data center to configure the appliances for read-only access. Also change the JDBC URL on the secondary data center nodes if you are not using technologies such as SQL Server Always On.

Make these changes in each Workspace ONE Access appliance in the secondary data center.

Procedure

1 Using an SSH client, log in to the Workspace ONE Access appliance as the root user.

2 Open the `/usr/local/horizon/conf/runtime-config.properties` file.

3 Configure the Workspace ONE Access appliance to have read-only access by adding the following line:

```
read.only.service=true
```

4 Also add the following line to the file:

```
cache.service.type=ehcache
```

Note `cache.service.type=ehcache` is required if you set `read.only.service=true`. If `read.only.service=false` or if the `read.only.service` key is not specified, then the default is `cache.service.type=rds`.

5 Set the value of the `ehcache.replication.rmi.servers` entry to the fully qualified domain names (FQDN) of the other nodes in the secondary data center. Use a colon `:` as the separator.

For this example, we have three nodes in the secondary data center (`sva1.example.com`, `sva2.example.com`, and `sva3.example.com`). The current node is `sva1.example.com`. Configure the entry as follows.

```
ehcache.replication.rmi.servers=sva2.example.com:sva3.example.com
```

6 Save the file.

7 Change the JDBC URL on the secondary data center nodes if you are not using technologies such as SQL Server Always On.

See Configure Workspace ONE Access to Use an External Database for information.

8 Restart the Tomcat server on the appliance.

```
service horizon-workspace restart
```

9 Repeat the preceding steps on the remaining nodes in the secondary data center.

For this example, the remaining nodes to configure are `sva2.example.com` and `sva3.example.com`.

Configure Failover Order of Horizon and Citrix-published Resources

When you have Workspace ONE Access deployed in multiple data centers and your deployment includes Horizon and Citrix-published resources, you must configure the failover order of resources in both the primary and secondary data centers to make the appropriate resources available from any data center.

You use the `hznAdminTool` command to create a database table with the failover order for resources in your organization per service instance. The configured failover order is followed when a resource is launched. You run the `hznAdminTool failoverConfiguration` command in both data centers to set up the failover order.

Note This procedure does not apply to environments using Horizon Cloud Pod Architecture (CPA).

Prerequisites

When Workspace ONE Access is deployed in multiple data centers, the same resources are also set up in each data center. Each application or desktop pool in the Horizon pods or Citrix XenFarms is considered as a different resource in the Workspace ONE Access catalog. To prevent duplication of the resource in the catalog, make sure that you enabled **Do not sync duplicate applications** in the Horizon and Citrix configuration pages in the Workspace ONE Access console.

Procedure

1. Using a ssh client, log in to the Workspace ONE Access appliance as the root user.
2. To view a list of the service instances, type:

   ```
   hznAdminTool -j clusterInstances
   ```

   A list of service instances is displayed. The `"id"` value is the service instance ID. For example:

   ```
   {
   "clusterInstances":[{
   "version" : "3.2.0.1 Build 8223322",
   "uuid" : "7451fe26-5b02-32ef-bfe6-6fe0a8710a14",
   "status" : "Active",
   "lastUpdated" : 1523372105701,
   "hostname" : "server.example.com",
   "datacenterId" : 0,
   "id" : 2,
   "ipaddress" : "10.143.xxx.xx"}
   ]}
   ```

3 For each service instance in your organization, configure the failover order for Horizon and Citrix-based resources with the following command:

```
hznAdminTool failoverConfiguration -configType <configType> -configuration
<configuration> -serviceInstanceId <serviceInstanceId>
```

Option	Description
-configType	Type the resource type being configured for failover. Values are either `VIEW` or `XENAPP`.
-configuration	Type the failover order. For VIEW configType, type as a comma separated list of the primary Horizon Connection Server host names that are listed in the Horizon configuration page in the Workspace ONE Access console. For XENAPP configType, type as a comma separated list of XenFarm names.
-serviceInstanceId	Type the ID of the service instance for which the configuration is set. The ID can be found in the list displayed in Step 2, `"id":`

For example:

```
hznAdminTool failoverConfiguration -configType VIEW -configuration
pod1vcs1.domain.com,pod2vcs1.hs.trcint.com -serviceInstanceId 1
```

When you type this command for Workspace ONE Access instances in the secondary data center, reverse the order of the Horizon Connection Servers. In this example, the command would be `hznAdminTool failoverConfiguration -configType VIEW -configuration pod2vcs1.hs.trcint.com, pod1vcs1.domain.com -serviceInstanceId 103`.

Results

The resources failover database table is set up for each data center.

What to do next

To see the existing failover configuration for each of the Horizon and Citrix-published resources, run the command:

```
hznAdminTool failoverConfigurationList -configType <configtype>
```

The value for `<configtype>` is either **`VIEW`** or **`XENAPP`**. The following is an example output of `hznAdminTool failoverConfigurationList` with `<configtype>` **`VIEW`**.

```
{"idOrganization":1,"serviceInstanceId":52,"configType":"VIEW","configuration":"pod1vcs1.domai
n.com,pod2vcs1.domain.com"}
{"idOrganization":1,"serviceInstanceId":103,"configType":"VIEW","configuration":"pod2vcs1.doma
in.com,pod1vcs1.domain.com"}
{"idOrganization":1,"serviceInstanceId":154,"configType":"VIEW","configuration":"pod2vcs1.doma
in.com,pod1vcs1.domain.com"}
```

Clear Cache in Secondary Data Center for Workspace ONE Access

After you finish setting up the primary and secondary data centers, clear the caches in the secondary data center. This is in preparation for a failover. When you fail over to the secondary data center, caches in the secondary data center should be empty.

Use the REST API described here to clear the caches. Another way to clear cache is to reboot the virtual appliances.

Procedure

- Run the following REST API from a REST client such as Postman.

  PATH: /SAAS/jersey/manager/api/removeAllCaches

  Method: POST

  Add Headers:

  ```
  Authorization: HZN <cookie_value>
  Accept: application/vnd.vmware.horizon.manager.cache.removal.response+json
  Content-type: application/vnd.vmware.horizon.manager.cache.removal.request+json
  ```

  Add in Body (raw) section:

  ```
  {}
  ```

  Note

  - You must run the API as the tenant administrator, that is, the administrator created in the System domain when you install Workspace ONE Access. Domain accounts synced from your enterprise directory cannot perform this function.
  - You can obtain the `HZN` cookie by logging into the Workspace ONE Access service as the tenant administrator, then accessing your browser's cookie cache.
  - Empty `cacheNames` indicates remove all caches.

Configure Database for Failover

For Workspace ONE Access, database replication is configured so that data remains consistent across database servers within the primary data center and across to the secondary data center.

You must configure your external database for high availability. Configure a primary and secondary database architecture, where the secondary database is an exact replica of the primary database.

Refer to your external database documentation for information.

If you are using SQL Server Always On, use the hostname or IP address of the SQL Server listener when you configure the database in each Workspace ONE Access appliance. For example:

```
jdbc:jtds:sqlserver://<hostname_or_IP_address:port#>/
<saasdb>;integratedSecurity=true;domain=<domainname>;useNTLMv2=true;multiSubnetFailover=true
```

Failover to Secondary Data Center for Workspace ONE Access

When the primary data center fails, you can fail over to the secondary data center. To fail over, you modify the global load balancer or DNS record to point to the load balancer in the secondary data center.

See Using a DNS Record to Control Which Data Center is Active.

The Workspace ONE Access appliances in the secondary data center are in read-only mode. Therefore, most administrator operations, such as adding users or apps, or entitling users, are not available. See Workspace ONE Access Activities Not Available in Read-Only Mode.

Important After you fail over to the secondary data center, you must clear all caches on the original primary data center. In case you need to fail over to the original primary data center, caches in that data center should be empty.

After the caches are cleared, restart all the connector instances. For 20.01 and later connector instances, restarting the connector instances means restarting all the installed enterprise services, such as VMware User Auth Service, VMware Directory Sync Service, and VMware Kerberos Auth Service, on each connector instance.

You can use a REST API to clear the cache. Run the following REST API from a REST client such as Postman:

PATH: /SAAS/jersey/manager/api/removeAllCaches

Method: POST

Add Headers:

```
Authorization: HZN <cookie_value>
Accept: application/vnd.vmware.horizon.manager.cache.removal.response+json
Content-type: application/vnd.vmware.horizon.manager.cache.removal.request+json'
```

Add in Body (raw) section:

```
{
"cacheNames":[]
}
```

Note

- You must run the API as the tenant administrator, that is, the administrator created in the System domain when you install Workspace ONE Access. Domain accounts synced from your enterprise directory cannot perform this function.
- You can obtain the `HZN` cookie by logging into the Workspace ONE Access service as the tenant administrator, then accessing your browser's cookie cache.
- Empty `cacheNames` indicates remove all caches.

Another way to clear cache is to reboot the virtual appliances.

Using a DNS Record to Control Which Data Center is Active

If you use a Domain Name System (DNS) record to route user traffic in your data centers, the DNS record should point to a load balancer in the primary data center under normal operating situations.

If the primary data center becomes unavailable, the DNS record should be updated to point to the load balancer in the secondary data center.

When the primary data center becomes available again, the DNS record should be updated to point to the load balancer in the primary data center.

Mobile SSO for iOS Authentication

If you are using Mobile SSO for iOS authentication, update both the A and AAAA DNS entries to point to the load balancer in the secondary data center. For example:

```
idm.example.com.   1800 IN  AAAA         ::ffff:1.2.3.4
idm.example.com.   1800 IN  A            1.2.3.4
```

Note If you are using the hybrid KDC feature, this is not required.

Setting Time To Live in DNS Record

The time to live (TTL) setting determines how long before DNS related information is refreshed in the cache. For a seamless failover of Horizon desktops and applications, make sure that the time to live (TTL) setting on the DNS records is short. If the TTL setting is set too long, users might not be able to access their Horizon desktops and applications immediately after failover. To enable quick refresh of the DNS, set the DNS TTL to 30 seconds.

Workspace ONE Access Activities Not Available in Read-Only Mode

Using Workspace ONE Access in read-only mode is designed for high availability to allow end users access to the resources. Some activities in the Workspace ONE Access console and other administration services pages might not be available in read-only mode. Below is a partial list of common activities that are not available.

When Workspace ONE Access is running in read-only mode, activities related to changes in Active Directory or the database cannot be made and syncing to the Workspace ONE Access database does not work.

Administrative functions that require writing to the database are not available during this time. You must wait until Workspace ONE Access returns to read and write mode.

Workspace ONE Access Console Read-Only Mode

The following are some of the limitations in the Workspace ONE Access console in read-only mode.

- Adding, deleting, editing users and groups in the **Users & Groups** tab
- Adding, deleting, editing applications in the **Catalog** tab

- Adding, deleting, editing application entitlements
- Changing branding information
- Directory Sync to add, edit, delete users and groups
- Editing information about resources, including Horizon, XenApp, and other resources
- Editing authentication methods page

Note The connector components of the Workspace ONE Access appliances in the secondary data center appear in the administration console. Make sure that you do not select a connector instance from the secondary data center as the sync connector.

Virtual Appliance Configuration Pages Read-Only Mode

The following are some of the limitations in the Appliance Configuration pages in read-only mode.

- Testing the database connection setup
- Changing the admin password in the Change Password page

End User Apps Portal Read-Only Mode

When Workspace ONE Access is in read-only mode, users can sign in to their portal and access their resources. The following functionality in the end user portal is not available in read-only mode.

- Mark a resource as Favorite or unmark a resource as Favorite
- Add resources from the Catalog page or remove resources from the Bookmarks page
- Change their password from their portal page
- Register a device with Workspace ONE Intelligent Hub when Workspace ONE Access is the source of authentication

Workspace ONE Access Windows Client Read-Only Mode

When Workspace ONE Access is in read-only mode, users cannot set up new Windows clients. Existing Windows clients continue to work.

Failback to Primary Data Center for Workspace ONE Access

In most failure scenarios, you can fail back to the primary data center once that data center is functioning again.

Procedure

1 Modify the global load balancer or the DNS record to point to the load balancer in the primary data center.

  See Using a DNS Record to Control Which Data Center is Active.

2 Clear the cache in the secondary data center.

Run the following REST API from a REST client such as Postman:

PATH: /SAAS/jersey/manager/api/removeAllCaches

Method: POST

Add Headers:

```
Authorization: HZN <cookie_value>
Accept: application/vnd.vmware.horizon.manager.cache.removal.response+json
Content-type: application/vnd.vmware.horizon.manager.cache.removal.request+json'
```

Add in Body (raw) section:

```
{
"cacheNames":[]
}
```

Note

- You must run the API as the tenant administrator, that is, the administrator created in the System domain when you install Workspace ONE Access. Domain accounts synced from your enterprise directory cannot perform this function.
- You can obtain the `HZN` cookie by logging into the Workspace ONE Access service as the tenant administrator, then accessing your browser's cookie cache.
- Empty `cacheNames` indicates remove all caches.

Another way to clear cache is to reboot the virtual appliances.

3 Restart all connector instances to reestablish the communication channel.

For 20.01 and later connector instances, restarting the connector instances means restarting all the installed enterprise services, such as VMware User Auth Service, VMware Directory Sync Service, and VMware Kerberos Auth Service, on each connector instance.

Promoting Secondary Data Center to Primary Data Center for Workspace ONE Access

In case of an extended data center failure, the secondary data center can be promoted to primary.

You need to edit the `runtime-config.properties` file in the Workspace ONE Access appliances in the secondary data center to configure the appliances for read-write mode.

Make these changes in each Workspace ONE Access appliance in the secondary data center.

Procedure

1 Using an SSH client, log in to the Workspace ONE Access appliance as the root user.

2 Open the `/usr/local/horizon/conf/runtime-config.properties` file for editing.

3 Change the `read.only.service=true` line to `read.only.service=false`.

4 Change the `cache.service.type=ehcache` line to `cache.service.type=rds`.

5 Save the `runtime-config.properties` file.

6 Restart the Tomcat server on the appliance.

```
service horizon-workspace restart
```

Upgrading Workspace ONE Access with Minimal Downtime

With a multi-data center deployment, you can upgrade Workspace ONE Access to the next version with minimal downtime. Use this suggested workflow for rolling updates.

Refer to the diagram in Deploying Workspace ONE Access in a Secondary Data Center for Failover and Redundancy as you follow these steps.

Procedure

1 Switch routing on the Global Load Balancer to send the requests to the Data Center 2 Load Balancer.

2 Stop database replication.

3 Update the Workspace ONE Access-1 virtual appliance, then update theWorkspace ONE Access-2 virtual appliance, and then update the Workspace ONE Access-3 virtual appliance.

4 Test updates using Data Center 1 Load Balancer.

5 Once satisfied, switch Global Load Balancer to route requests to Data Center 1 Load Balancer.

6 Update the Workspace ONE Access-4 virtual appliance, then update the Workspace ONE Access-5 virtual appliance, and then update the Workspace ONE Access-6 virtual appliance.

7 Test updates using Data Center 2 Load Balancer.

8 Start database replication.

Performing Disaster Recovery for Workspace ONE Access Using Site Recovery Manager

The information that follows describes how to use VMware Site Recovery Manager™ with other VMware products to configure a disaster-recovery solution for Workspace ONE Access in an on-premises environment.

About Disaster Recovery for Workspace ONE Access

A disaster-recovery deployment requires a protected site and a recovery site. The recommended approach to setting up disaster recovery for Workspace ONE Access is to leverage Site Recovery Manager.

Site Recovery Manager is a disaster-recovery automation software application that provides policy-based management, non-disruptive testing, and automated orchestration.

To protect your Workspace ONE Access deployment, Site Recovery Manager automates every aspect of running a disaster recovery plan to expedite the recovery process and eliminate the risks involved in using a manual process.

The Amount of Downtime to Expect

Site Recovery Manager allows Workspace ONE Access to operate from the recovery site. If a failover occurs, the Recovery Time Objective (RTO) depends on several factors, such as network bandwidth across sites, Site Recovery Manager architecture, and the replication strategy you deploy. To estimate the amount of downtime, consider details such as how long virtual machines and services take to start. These factors combined define the RTO.

See Additional VMware Documentation

Much of the information that follows about using Site Recovery Manager to configure a disaster-recovery solution for Workspace ONE Access points to other VMware documentation, such as the VMware Site Recovery Manager documentation.

For information about how to install and configure Site Recovery Manager and the different technologies, such as the replication technologies, see *VMware Site Recovery Manager Installation and Configuration*, *VMware Site Recovery Manager Administration* and, if you are using VMware vSphere Replication, *VMware vSphere Replication Administration*.

Overview of VMware Site Recovery Manager

VMware Site Recovery Manager is a business continuity and disaster recovery solution that helps you to plan, test, and run the recovery of virtual machines between a protected vCenter Server site and a recovery vCenter Server site.

You can configure Site Recovery Manager to protect virtual machines in different ways.

Datastore groups

Protect the virtual machines in datastore groups by using third-party disk replication mechanisms to configure array-based replication. Array-based replication surfaces replicated datastores to recover virtual machine workloads.

Individual virtual machines

Protect the individual virtual machines on a host by using Site Recovery Manager in combination with VMware vSphere Replication.

Storage policies

Protect virtual machines based on their association with specific storage policies. Protecting virtual machines by using storage policies requires array-based replication.

You can use Site Recovery Manager to implement different types of recovery from the protected site to the recovery site.

Planned migration

The orderly evacuation of virtual machines from the protected site to the recovery site. Planned migration prevents data loss when migrating workloads in an orderly fashion. For planned migration to succeed, both sites must be running and fully functioning.

Disaster recovery

Similar to planned migration except that disaster recovery does not require that both sites be up and running, for example if the protected site goes offline unexpectedly. During a disaster recovery operation, failure of operations on the protected site is reported but is otherwise ignored.

Site Recovery Manager orchestrates the recovery process with the replication mechanisms, to minimize data loss and system down time.

- At the protected site, Site Recovery Manager shuts down virtual machines cleanly and synchronizes storage, if the protected site is still running.
- Site Recovery Manager powers on the replicated virtual machines at the recovery site according to a recovery plan.

A recovery plan specifies the order in which virtual machines start up on the recovery site. A recovery plan specifies network parameters, such as IP addresses, and can contain user-specified scripts that Site Recovery Manager can run to perform custom recovery actions on virtual machines.

Site Recovery Manager lets you test recovery plans. You conduct tests by using a temporary copy of the replicated data in a way that does not disrupt ongoing operations at either site.

Configuring and Using Site Recovery Manager for Workspace ONE Access

You must configure Site Recovery Manager to protect your Workspace ONE Access deployment. Secure this protection by properly installing and configuring Site Recovery Manager.

Prepare the Environment

Before you configure Site Recovery Manager, set up the proper environment.

Confirm that your deployment meets the following prerequisites at each site.

- Configure ESXi 6.7 u2 or later on the protected and recovery sites.
- Update VMware Tools to the latest version.
- Install Site Recovery Manager 8.1 or later on each ESXi host.

  For Site Recovery Manager installation instructions, see the respective version of *Site Recovery Manager Installation and Configuration*.

- Verify that the protected and recovery sites are connected over the same VLAN, Layer 2 over Layer 3, or stretched VLAN.
- For Workspace ONE Access 19.03 only, perform the steps in the following VMware Knowledge Base article, https://kb.vmware.com/s/article/74709, to improve Elasticsearch full cluster restart.
- Verify that you have successfully deployed Workspace ONE Access on the protected site.

Table 4-1. Disaster Recovery Components Per Site

Site A - Protected	Site B - Recovery
vCenter Server 1	vCenter Server 2
vSphere Replication 1 or array-based replication 1	vSphere Replication 2 or array-based replication 2
Site Recovery Manager 1	Site Recovery Manager 2

Configure Workspace ONE Access at Each Site

Install and configure Workspace ONE Access. To provide high availability within the data center, use multiple Workspace ONE Access service nodes. Three service nodes is a common deployment. However, you can configure a single service node for small, non-mission critical deployments. You deploy the components at the protected site and replicate the deployment to the recovery site.

The following example is of a deployment with three-service nodes, two external connector instances, and an external database.

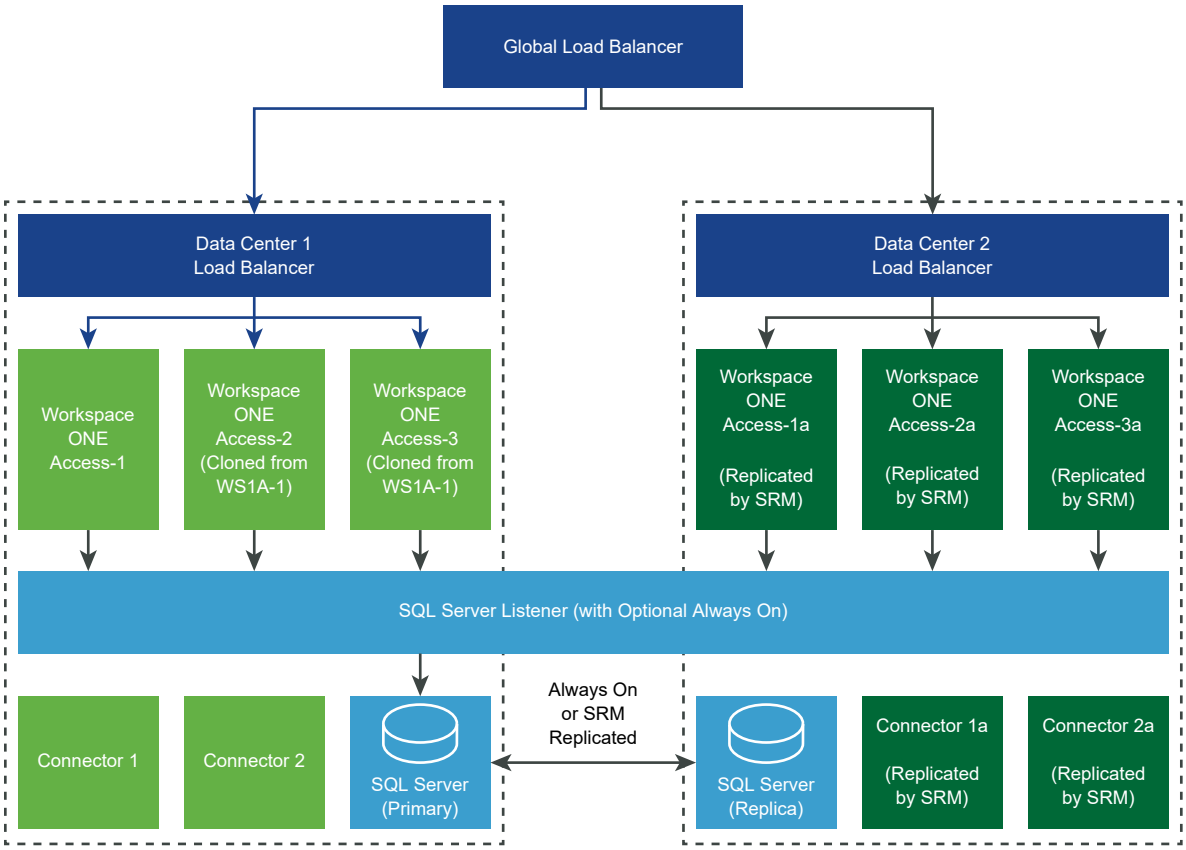


Table 4-2. Typical Workspace ONE Access Cluster Deployment at Protected Site

Site A - Protected Site Workspace ONE Access Deployment
External Database
Service Node 1
Service Node 2
Service Node 3
Connector 1
Connector 2

If you are using the SQL Server Always On capability, you do not need to protect SQL using Site Recovery Manager, which reduces the Site Recovery Manager protection groups to only Workspace ONE Access virtual machines.

Key tasks you must perform to configure and use Site Recovery Manager for Workspace ONE Access include the following.

- Configure a replication-technology type, vSphere Replication or array-based replication. See the appropriate documentation, such as *Site Recovery Manager Administration* and, if you use vSphere Replication, also see *VMware vSphere Replication Administration*.

- Create protection groups. See the appropriate documentation, such as *Site Recovery Manager Administration*, specifically information about creating and managing protection groups based on the replication technology type you use.
- Create and edit a recovery plan. See both the *Site Recovery Manager Administration* guide and the topics that follow in this guide about creating and editing a recovery plan.
- Test and Run a Recovery Plan. See both the Test and Run a Recovery Plan for Your Workspace ONE Access Deployment topic and the *Site Recovery Manager Administration* guide.
- Perform a Failback. See both the Perform a Failback After a Disaster Recovery or Planned Migration of Workspace ONE Access topic and the *Site Recovery Manager Administration* guide.

Adjust the recovery.powerOnDelay Setting for Workspace ONE Access

When you create a recovery plan in Site Recovery Manager, adjust the **recovery.powerOnDelay** setting.

Adjusting the **recovery.powerOnDelay** setting in Site Recovery Manager can improve the Workspace ONE Access disaster-recovery experience. After Site Recovery Manager recovers a virtual machine, a certain amount of time is required for post power-on steps to run and for dependent virtual machines to start. Adding **120** seconds of delay can provide the virtual machine with the amount of process time required.

Perform this specific configuration when you create a recovery plan in Site Recovery Manager. The following instructions are for 8.2, but might also be applicable to other versions. See *Site Recovery Manager Administration*.

Procedure

1. In the vSphere Client or the vSphere Web Client, click **Site Recovery > Open Site Recovery**.
2. On the **Site Recovery** home tab, select a site pair, and click **View Details**.
3. In the left pane, click **Configure > Advanced Settings > Recovery**.
4. Select a site and click **Edit**.
5. In the **recovery.powerOnDelay** text box, enter **120**.
6. Click **OK**.

Specify the Recovery Priority of Each Workspace ONE Access Virtual Machine

When you create a recovery plan in Site Recovery Manager, assign the proper priority to each virtual machine in the Workspace ONE Access deployment.

Perform this specific configuration when you create a recovery plan in Site Recovery Manager. The following instructions are for 8.2, but might also be applicable to other versions. See *Site Recovery Manager Administration*.

The following example illustrates how you can prioritize the virtual machines in a Workspace ONE Access cluster deployment.

Component	Priority Setting
External database	1
All service nodes	2
All connector nodes	3

Procedure

1 In the vSphere Client or the vSphere Web Client, click **Site Recovery > Open Site Recovery**.

2 On the **Site Recovery** home tab, select a site pair, and click **View Details**.

3 Click the **Recovery Plans** tab, click a recovery plan, and click **Virtual Machines**.

4 Right-click a virtual machine and click **Priority Group**.

5 Select a new priority for the virtual machine.

The highest priority is **1**. The lowest priority is **5**.

6 To confirm the change of priority, click **Yes**.

Configure Virtual Machine Dependencies for Workspace ONE Access

Configure a dependency for each Workspace ONE Access service node virtual machine on a respective external database.

for Workspace ONE Access

Perform this specific configuration when you create a recovery plan in Site Recovery Manager. The following instructions are for 8.2, but might also be applicable to other versions. See *Site Recovery Manager Administration*.

When a recovery plan runs, Site Recovery Manager starts the virtual machines that other virtual machines depend on before it starts the virtual machines with the dependencies.

You can configure dependencies for many reasons. A common dependency for Workspace ONE Access is the dependency of a Workspace ONE Access service node on an external database. The following dependencies apply.

Component	Virtual Machine Dependencies
External Database	Not Applicable
All service nodes	External Database
All connector nodes	All Service Nodes

Procedure

1 In the vSphere Client or the vSphere Web Client, click **Site Recovery > Open Site Recovery**.

2 On the **Site Recovery** home tab, select a site pair, and click **View Details**.

3 Click the **Recovery Plans** tab, click a recovery plan, and click **Virtual Machines**

4 Right-click a virtual machine that depends on one or more other virtual machines and click **Configure Recovery**.

5 Expand **VM Dependencies**.

6 From the drop-down menu, select **View all**.

7 Select one or more virtual machines from the list of all virtual machines in the selected recovery plan.

   The selected virtual machines are added to the list of dependencies.

8 Verify that the virtual machines in the **VM Dependencies** list are on and verify that the status of the dependencies is **OK**.

9 (Optional) To remove a dependency, select **View VM Dependencies** from the drop-down menu, select a virtual machine from the list of virtual machines that this virtual machine depends on, and click **Remove**.

10 Click **OK**.

Enable Network Compression for vSphere Replication Data

If you deploy vSphere Replication as your replication-technology type, enable network compression for the vSphere Replication data.

Configure this specific setting when you configure vSphere Replication with Site Recovery Manager. The following instructions are for 8.2, but might also be applicable to other versions. See *Site Recovery Manager Administration* and *VMware vSphere Replication Administration*.

Enabling network compression speeds up the replication process across vCenter Server instances.

Procedure

- To enable network compression, when you configure vSphere Replication, select the **Enable network compression for VR data** check box.

Test and Run a Recovery Plan for Your Workspace ONE Access Deployment

To run a recovery plan or planned migration of your Workspace ONE Access deployment as smoothly as possible, first test the plan to verify that the virtual machines in the Workspace ONE Access deployment recover as expected to the recovery site. After successful tests and requisite cleanup operations, run a recovery plan as necessary for a planned migration or disaster recovery.

You perform a test run of a recovery plan on a test network and on a temporary snapshot of replicated data at the recovery site. The test does not have a permanent effect on the protected or recovery site.

You perform an actual run of a recovery plan on the production deployment of Workspace ONE Access, which significantly affects both sites.

Prerequisites

Configure Site Recovery Manager to protect your Workspace ONE Access deployment. The configuration includes the creation of a recovery plan.

Procedure

- Follow the instructions provided in *Site Recovery Manager Administration* about testing and running recovery plans.

  For example, for Site Recovery Manager 8.2, see Site Recovery Manager Administration 8.2.

What to do next

After you run a recovery plan, either for a planned migration or a disaster recovery, perform a failback. See Perform a Failback After a Disaster Recovery or Planned Migration of Workspace ONE Access.

Perform a Failback After a Disaster Recovery or Planned Migration of Workspace ONE Access

After you run a recovery plan for a planned migration or disaster recovery of Workspace ONE Access, you can restore the pre-recovery site by performing a failback.

Performing a planned migration or a disaster recovery from site A to site B is a two-step process: recovery and reprotect. Recovery results in Recovery Time Objective (RTO) downtime. After the recovery from site A to site B, the recovered virtual machines run on site B without protection until you perform the reprotect operation.

Reprotect runs in parallel with Workspace ONE Access services. Therefore, end users do not experience further downtime during the reprotect operation.

Prerequisites

- You performed a recovery, either as part of a planned migration or as part of a disaster recovery.
- The original protected site, site A, is running.
- You did not run reprotect after the recovery.
- If you performed a disaster recovery, you must perform a planned migration when the hosts and datastores on the original protected site are running again.

Procedure

- Follow the instructions provided in *Site Recovery Manager Administration* about performing a failback.

  For example, for Site Recovery Manager 8.2, see Site Recovery Manager Administration 8.2

Adding Allowlist IP Addresses to Your External Firewall for Workspace ONE Access Services

When you configure Workspace ONE Access with an external firewall, allowlist the IP address ranges or URLs for the following Workspace ONE Access services to provide access to that service.

Use the **nslookup** command or another command-line tool to query the Domain Name System to obtain the IP addresses to add to your external firewall allowlist.

Service	Domain Name System	Description
Workspace ONE Access Catalog	`catalog.vmwareidentity.com`	To make sure that the content of the catalog can be accessed, add the URLs from the list to the allowlist. That content is also delivered through AWS CloudFront CDN, which maintains its own list of public IP addresses. See http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/LocationsOfEdgeServers.html.
VMware Verify	`vmware.authy.com` `api.authy.com`	If VMware Verify is configured as an authentication method, add the URLS from these lists to the allowlist.
Hybrid KDC	`kdc.op.<vmwareidentity.xxx>`	When hybrid KDC is configured for your Workspace ONE Access on-premises operation, select one of the following domains to look up the URLS. ■ vmwareidentity.ca ■ vmwareidentity.com ■ vmwareidentity.eu ■ vmwareidentity.co.uk ■ vmwareidentity.de ■ vmwareidentity.com.au ■ vmwareidentity.asia
Updates from Workspace ONE Access	`vapp-updates.vmware.com`	To receive Workspace ONE Access updates and to download patches from the VMware Update Manager, add the URLs from the list to the allowlist.

Enabling Proxy Server Settings After Installation of Workspace ONE Access

The Workspace ONE Access virtual appliance accesses the cloud application catalog and other Web services on the Internet. If your network configuration provides Internet access through an HTTP proxy, you must adjust your proxy settings on the Workspace ONE Access appliance.

Enable your proxy to handle Internet traffic only. To ensure that the proxy is set up correctly, set the parameter for internal traffic to `no-proxy` within the domain.

Procedure

1. Log in to the Workspace ONE Access console.
2. Select **Dashboard** > **System Diagnostics Dashboard**.
3. Click **VA Configuration** of the service node you want to configure and log in with the admin user password.
4. In the left pane, select **Proxy Configuration**.
5. **Enable** Proxy.
6. In **Proxy host with port** text box, enter the proxy name and port number. For example, proxyhost.example.com:3128
7. If you are using an authenticated proxy, enter the **Proxy username** and **Proxy password**.

   If you are not using an authenticated proxy, leave the text boxes empty.
8. In the **Non-Proxied hosts** text box, enter the non-proxy hosts that are accessed without going through the proxy server. Use a comma to separate a list of host names.
9. Click **Save**.
10. Log in to the Workspace ONE Access appliance as the root user and restart the service. Run `service horizon-workspace restart`.

Enter the Workspace ONE Access License Key

After you deploy the VMware Workspace ONE Access appliance, enter your license key. Entering a license key is optional.

Procedure

1. Log in to the VMware Workspace ONE Access console.
2. Select the **Appliance Settings** tab, then click **License**.
3. In the License Settings page, enter the license key and click **Save**.

Managing Workspace ONE Access Configuration Settings

5

After the initial configuration of Workspace ONE Access is complete, you can go to the Workspace ONE Access console pages to install certificates, manage passwords, and download log files. You can also update the database, change the Workspace ONE Access FQDN, and configure an external syslog server.

The configuration settings pages are available directly at https://*WS1AccessHostnameFQDN*:8443/cfg/ or using the Workspace ONE Access console by selecting **Dashboard > System Diagnostics Dashboard**, clicking **VA Configuration**, and providing the admin user password.

Page Name	Setting Description
Database Connection	The database connection setting, either Internal or External, is enabled. You can change the database type. When you select External Database, you enter the external database URL, user name, and password. To set up an external database, see Create the Workspace ONE Access Service Database.
Install SSL Certificates	On the tabs on this page, you can install an SSL certificate for Workspace ONE Access, download the self-signed Workspace ONE Access root certificate, and install trusted root certificates. For example, if Workspace ONE Access is configured behind a load balancer, you can install the load balancer's root certificate. See Using SSL Certificates in Workspace ONE Access Service.
Mobile SSO	On this page, you can set up cert proxy on Workspace ONE Access to manage Android Mobile SSO requests. See the *Android Mobile Single Sign-On to VMware Workspace ONE Access* guide.
Workspace ONE Access FQDN	On this page, you can view or change the Workspace ONE Access FQDN. The Workspace ONE Access FQDN is the URL that users use to access the service.
Configure Syslog	On this page, you can enable an external syslog server. Workspace ONE Access logs are sent to this external server. See Configure a Syslog Server for Workspace ONE Access.
Change Password	On this page, you can change the Workspace ONE Access admin user password.

Page Name	Setting Description
System Security	On this page, you can change the root password for the Workspace ONE Access appliance and the ssh user password used to log in remotely.
Proxy Configuration	Configure HTTPS proxy settings.
Log File Locations	You can download the logs in a zip file. See Workspace ONE Access Log File Information.
Time Synchronization	On this page, configure time synchronization for the Workspace ONE Access service.

You can also modify the connector URL. See Modifying the Workspace ONE Access Connector URL.

This chapter includes the following topics:

- Change the Workspace ONE Access Appliance Configuration Settings
- Using SSL Certificates in Workspace ONE Access Service
- Configure Workspace ONE Access to Use an External Database
- Modifying the Workspace ONE Access Service URL
- Modifying the Workspace ONE Access Connector URL
- Configure a Syslog Server for Workspace ONE Access
- Workspace ONE Access Log File Information
- Manage Your Workspace ONE Access Appliance Passwords
- Configure SMTP Settings for Workspace ONE Access
- Configuring Time Synchronization for the Workspace ONE Access Service

Change the Workspace ONE Access Appliance Configuration Settings

After you configure Workspace ONE Access, you can go to the appliance configuration settings pages to update the current configuration and monitor system information for the virtual appliance.

Procedure

1. Log in to the Workspace ONE Access console.
2. Select **Dashboard > System Diagnostics Dashboard**.
3. Click **VA Configuration** of the service node you want to configure and log in with the admin user password.
4. In the left pane, select the page to view or edit.

What to do next

Verify that the settings or updates you make are in effect.

Using SSL Certificates in Workspace ONE Access Service

When the Workspace ONE Access appliance is installed, a default SSL server certificate is automatically generated. You can use this self-signed certificate for general testing of your implementation.

A CA is a trusted entity that guarantees the identity of the certificate and its creator. When a certificate is signed by a trusted CA, users no longer receive messages asking them to verify the certificate. Workspace ONE Access supports using PEM formatted certificates that include the private key.

You install a signed CA certificate for an appliance from the System Diagnostics page. Select the appliance and click **VA Configuration** to log in as admin to the appliance configuration pages. Select **Install SSL Certificates**.

If you deploy Workspace ONE Access with the self-signed SSL certificate, the root CA certificate must be available as a trusted CA for any client who accesses the Workspace ONE Access service. The clients can include end-user machines, load balancers, proxies, and so on. You can download the root CA from the **Install SSL Certificates > Server Certificates** page.

Installing an SSL Certificate for the Workspace ONE Access Service (On-Premises Only)

When the Workspace ONE Access service is installed, a default SSL server certificate is generated. You can use this self-signed certificate for testing purposes. However, best practice is to use SSL certificates signed by a public Certificate Authority (CA) for your production environment.

Note If a load balancer in front of Workspace ONE Access terminates SSL, the SSL certificate is applied to the load balancer.

Prerequisites

- Generate a Certificate Signing Request (CSR) and obtain a valid, signed SSL certificate from a CA. The certificate can be either a PEM or PFX file. PEM certificates ae encoded with the private key using the PKCS #1 standard.

  If a PEM file is imported, make sure that the file includes the entire certificate chain in the correct order. Make sure to include these tags -----BEGIN CERTIFICATE----- and -----END CERTIFICATE---- for each certificate. The order is the primary certificate first and then your intermediate certificate, then the ROOT certificate.
- For the Common Name part of the Subject DN, use the fully qualified domain name that users use to access the Workspace ONE Access service. If the Workspace ONE Access appliance is behind a load balancer, this name is the load balancer server name.

- If SSL is not terminated on the load balancer, the SSL certificate used by the service must include Subject Alternative Names (SANs) for each of the fully qualified domain names in the Workspace ONE Access cluster. Including the SAN enables the nodes within the cluster to make requests to each other. Also include a SAN for the FQDN host name that users use to access the Workspace ONE Access service, in addition to using it for the Common Name, because some browsers require it.
- If your deployment includes a secondary data center, ensure that the Workspace ONE Access certificate includes the FQDN of the load balancer from the primary data center as well as the FQDN of the load balancer from the secondary data center. Otherwise, the certificate must be a wildcard certificate.

Procedure

1 Log in to the Workspace ONE Access console.

2 Select **Dashboard > System Diagnostics Dashboard**.

3 Click **VA Configuration** of the service node you want to configure and log in with the admin user password.

4 Select **Install SSL Certificates > Server Certificate**.

5 In the SSL Certificate tab, select **Custom Certificate**.

6 To import the certificate file, click **Choose File** and navigate to the certificate file to import.

If a PEM file is imported, make sure that the file includes the entire certificate chain in the correct order. Make sure to include these tags -----BEGIN CERTIFICATE----- and -----END CERTIFICATE---- for each certificate. The order is the primary certificate first and then your intermediate certificate.

7 If a PEM file is imported, import the private key. Click **Choose File** and navigate to the Private Key file . Everything between ----BEGIN RSA PRIVATE KEY and ---END RSA PRIVATE KEY must be included.

If a PFX file is imported, enter the PFX password.

8 Click **Save.**

Example: PEM Certificate Example

Certificate Chain Example
-----BEGIN CERTIFICATE-----
(Your Primary SSL certificate:your domain_name.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Intermediate certificate: <CA>.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----

Certificate Chain Example
Your Root certificate: TrustedRoot.crt)
-----END CERTIFICATE-----

Private Key Example
-----BEGIN RSA PRIVATE KEY-----
(Your PrivateKey: your_domain_name.key)
-----END RSA PRIVATE KEY-----

Installing Trusted Root Certificates for Workspace ONE Access (On-Premises Only)

Install the root or intermediate certificates that should be trusted by the Workspace ONE Access server. The Workspace ONE Access server will be able to establish secure connections to servers whose certificate chain includes any of these certificates.

If the Workspace ONE Access server is configured behind a load balancer and SSL is terminated on the load balancer, install the load balancer's root certificate.

Procedure

1. Log in to the Workspace ONE Access console.
2. Select **Dashboard > System Diagnostics Dashboard**.
3. Click **VA Configuration** of the service node you want to configure and log in with the admin user password.
4. Click **Install SSL Certificates**, then select the **Trusted CAs** tab.
5. Paste the root or intermediate certificate into the text box.

   Include everything between and including the lines -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----.
6. Click **Add.**

Installing a Passthrough Certificate on Workspace ONE Access (On-Premises Only)

To enable sign in using the certificate authentication method, you configure SSL passthrough on the load balancer for the port defined on the **Install SSL Certificate** > **Passthrough Certificate** tab in the Workspace ONE Access console.

Enabling certificate authentication for a Workspace ONE Access on-premises deployment requires setting SSL pass-through at the load balancer. Upload a root certificate and intermediate certificates and private key to Passthrough Certificate tab. For more information about configuring SSL pass-through with a load balancer, see the Workspace ONE Access installation guide.

You can also upload a certificate to be used for Android SSO device authentication. See the Android Mobile Single Sign-on to VMware Workspace ONE publication.

Configure Workspace ONE Access to Use an External Database

After you create the Microsoft SQL database, if the external database you created is not automatically configured in Workspace ONE Access, you configure Workspace ONE Access to use the database in the Appliance Settings page.

Prerequisites

- The database created in Microsoft SQL server as the external database server. For information about specific versions that Workspace ONE Access supports, see the VMware Product Interoperability Matrixes.
- If you are changing the Microsoft SQL database configuration, make sure that the database user is granted the db_owner role. Members of the db_owner database role can perform all configuration and maintenance activities on the database. See Change Database-Level Roles After Upgrade to Workspace ONE Access.

Procedure

1. Log in to the Workspace ONE Access console.
2. Select **Dashboard > System Diagnostics Dashboard**.
3. Click **VA Configuration** of the service node you want to configure and log in with the admin user password.
4. Click **Database Connection**.
5. Select **External Database** as the database type.

6 Enter information about the database connection.

a Enter the JDBC URL of the Microsoft SQL database server.

Authentication Mode	JDBC URL String
Windows Authentication (domain\user)	`jdbc:jtds:sqlserver://<hostname_or_IP_address:port#>/<saasdb>;integratedSecurity=true;domain=<domainname>;useNTLMv2=true`
SQL Server Authentication (local user)	`jdbc:sqlserver://<hostname_or_IP_address:port#>;DatabaseName=<saasdb>`

To enable **SQL Server Always on** set MultiSubNetFailover to True in the JDBC URL.

```
jdbc:sqlserver://
<hostname_or_IP_address:port#>;DatabaseName=<saasdb>;multiSubnetFailover=true
```

MultiSubnetFailover is not supported when using Windows Authentication.

b Enter the login user name and password configured when you created the database. See Configure Microsoft SQL Database Using Local SQL Server Authentication Mode for Workspace ONE Access

7 Click **Test Connection** to verify access to the database and to save the information.

What to do next

(Optional) Change the db_owner database role membership privileges. See Change Database-Level Roles After Upgrade to Workspace ONE Access.

Modifying the Workspace ONE Access Service URL

You can change the Workspace ONE Access service URL, which is the URL that users use to access the service. For example, you might change the URL to a load balancer URL.

Procedure

1 Log in to the Workspace ONE Access console.

2 Select **Dashboard > System Diagnostics Dashboard**.

3 Click **VA Configuration** of the service node you want to configure and log in with the admin user password.

4 Click **Workspace ONE Access FQDN** and enter the new URL in the **Workspace ONE Access FQDN** text box.

Use the format **`https://`*`WS1AccessHostnameFQDN`*`:`*`port`***. Specifying a port is optional. The default port is 443.

For example, **`https://myservice.example.com`**.

5 Click **Save**.

What to do next

Enable the new portal user interface.

1 Go to https://*WS1AccessHostnameFQDN*/admin to access the administration console.

2 In the administration console, click the arrow on the **Catalog** tab and select **Settings**.

3 Select **New End User Portal UI** in the left pane and click **Enable New Portal UI**.

Modifying the Workspace ONE Access Connector URL

You can change the Workspace ONE Access connector URL by updating the identity provider hostname in the Workspace ONE Access console.

Procedure

1 Log in to the Workspace ONE Access console.

2 Click the **Identity & Access Management** tab, then click the **Identity Providers** tab.

3 In the Identity Providers page, select the identity provider to update.

4 In the **IdP Hostname** field, enter the new hostname.

Use the format ***`hostname:port`***. Specifying a port is optional. The default port is 443.

For example, **`vidm.example.com`**.

5 Click **Save**.

Configure a Syslog Server for Workspace ONE Access

Application-level events from the service can be exported to an external syslog server. Operating system events are not exported.

Since most companies do not have unlimited disk space, Workspace ONE Access does not save the complete logging history. If you want to save more history or create a centralized location for your logging history, you can set up an external syslog server.

If you do not specify a syslog server during the initial configuration, you can configure it later by logging in to the **VA Configuration** page of the service node you want to configure and selecting **Configure Syslog**. For example, select **Dashboard > System Diagnostics Dashboard > VA Configuration > Configure Syslog**.

Prerequisites

- Set up an external syslog server. You can use any of the standard syslog servers available. Several syslog servers include advanced search capabilities.
- Ensure that Workspace ONE Access can reach the syslog server on port 514 (UDP).

Procedure

1 Log in to the Workspace ONE Access console.

2 Select **Dashboard > System Diagnostics Dashboard**.

3 Click **VA Configuration** of the service node you want to configure and log in with the admin user password.

4 Select **Configure Syslog** in the left pane.

5 Click **Enable**.

6 Enter the IP address or the FQDN of the syslog server where you want to store the logs.

7 Click **Save.**

A copy of your logs is sent to the syslog server.

8 If your deployment supports multi-syslog server forwarding and you want to add or remove a syslog server while the syslog service is in use, in the **Manage Syslog servers configuration** section, enter the IP address or the FQDN of the syslog server you want to add or remove and click the corresponding button, **Add Server** or **Remove Server**.

Workspace ONE Access Log File Information

The Workspace ONE Access log files can help you debug and troubleshoot. The log files that follow are a common starting point. Additional Workspace ONE Access service logs can be found in the logs directory. For Workspace ONE Access connector log-file information, see the *Installing Workspace ONE Access Connector* guide.

Table 5-1. Log Files

Component	Location of Log File	Description
Workspace ONE Access Service Logs	`/opt/vmware/horizon/workspace/logs/horizon.log`	Information about activity on the service, such as entitlements, users, and groups.
Configurator Logs	`/opt/vmware/horizon/workspace/logs/configurator.log`	Requests that the Configurator receives from the REST client and the web interface.

Table 5-1. Log Files (continued)

Component	Location of Log File	Description
Update Logs	`/opt/vmware/var/log/update.log` `/opt/vmware/var/log/vami`	A record of output messages related to update requests during an upgrade of Workspace ONE Access. Linux. The files in the `/opt/vmware/var/log/vami` directory are useful for troubleshooting. You can find these files on all virtual machines after an upgrade.
Apache Tomcat Logs	`/opt/vmware/horizon/workspace/logs/catalina.log`	Apache Tomcat records of messages that are not recorded in other log files.

- Collect Workspace ONE Access Log Information

  During testing or troubleshooting, the logs can give feedback about the activity and performance of the virtual appliance, as well as information about any problems that occur.

- Setting the Workspace ONE Access Service Log Level to DEBUG

  You can set the log level to DEBUG to log additional information that can help debug problems.

Collect Workspace ONE Access Log Information

During testing or troubleshooting, the logs can give feedback about the activity and performance of the virtual appliance, as well as information about any problems that occur.

Collect the logs from each appliance in your environment.

Procedure

1. Log in to the Workspace ONE Access console.
2. Select **Dashboard > System Diagnostics Dashboard**.
3. Click **VA Configuration** of the service node you want to configure and log in with the admin user password.
4. Click **Log File Locations** and click **Prepare log bundle**.

   The information is collected into a tar.gz file that can be downloaded.
5. Download the prepared bundle.

What to do next

To collect all logs, do this on each appliance.

Setting the Workspace ONE Access Service Log Level to DEBUG

You can set the log level to DEBUG to log additional information that can help debug problems.

Procedure

1 Log in to the machine.

2 Change to the `/usr/local/horizon/conf/` directory.

3 Update the log level in the `cfg-log4j.properties`, `hc-log4j.properties`, and `saas-log4j.properties` files, which are the most commonly-used `log4j` files for the service.

   a Edit the file.

   b In the lines that have the log level set to `INFO`, replace `INFO` with `DEBUG`.

   For example, change:

   ```
   rootLogger.level=INFO
   ```

   to:

   ```
   rootLogger.level=DEBUG
   ```

   c Save the file.

   A restart of the service or system is not required.

Manage Your Workspace ONE Access Appliance Passwords

When you configured the Workspace ONE Access virtual appliance initially, you created passwords for the admin user, root user, and sshuser. You can change these passwords from the appliance configuration settings in the Workspace ONE Access administration console.

You can also change the admin user password, as well as the Workspace ONE Access admin console password (or operator password), from the command line. See Resetting Workspace ONE Access Console-Related Passwords with the Command Line .

Make sure that you create strong passwords.

Admin passwords must be 8 or more characters long and contain at least one of each of the following.

- Uppercase characters A-Z (Latin alphabet)
- Lowercase characters a-z (Latin alphabet)
- Numeric digits 0-9
- Special characters (!, $, #, %, etc.)

SSH users, including the root user, password must be 14 or more characters long and contain at least one of each of the following.

- Uppercase characters A-Z (Latin alphabet)
- Lowercase characters a-z (Latin alphabet)
- Numeric digits 0-9

- Special characters (!, $, #, %, etc.)

Procedure

1. Log in to the Workspace ONE Access console.
2. Select **Dashboard > System Diagnostics Dashboard**.
3. Click **VA Configuration** of the service node you want to configure and log in with the admin user password.
4. To change the admin password, select **Change Password**. To change the root or sshuser passwords, select **System Security**.

   Important The admin user password must be at least 8 characters in length and include uppercase and lowercase characters and at least one digit and special character.

5. Enter the new password.
6. Click **Save**.

Resetting Workspace ONE Access Console-Related Passwords with the Command Line

You can use the `hznAdminTool` script to change the Workspace ONE Access service admin user password and the Workspace ONE Access admin console password, also known as the operator password.

- The Workspace ONE Access service admin user password is the password for accessing the configuration settings pages: https://*WS1AccessHostnameFQDN*:8443/cfg/
- The Workspace ONE Access admin console password is the password for accessing the Workspace ONE Access admin console: https://*WS1AccessHostnameFQDN*/admin/

You have the option of changing the Workspace ONE Access service admin user password from the following configuration settings page, https://*WS1AccessHostnameFQDN*:8443/cfg/changePassword. See Manage Your Workspace ONE Access Appliance Passwords. However, if you are unable to log in and need to reset the password, you can use the `hznAdminTool` script to reset the password.

For the Workspace ONE Access admin console, the `hznAdminTool`script is the only method for changing the password.

Procedure

1. As root, log in to the Workspace ONE Access virtual appliance host.

2 Run the appropriate command, depending on which password you are resetting.

These console-related passwords must be at least 6 characters in length. However, make sure that you create strong passwords. Strong passwords should be at least eight characters long and include uppercase and lowercase characters and at least one digit or special character.

Option	Description
Workspace ONE Access service admin user password	`/usr/sbin/hznAdminTool setSystemAdminPassword`
Workspace ONE Access admin console password (or operator password)	`/usr/sbin/hznAdminTool setOperatorPassword`

You are prompted for the new password.

3 Provide the new password.

Configure SMTP Settings for Workspace ONE Access

The Workspace ONE Access on-premises appliance supports sending emails to users, for example for password reset. For a more secure connection, Workspace ONE Access can connect to an SMTP server using SSL/TLS. An SMTP server with SSL/TLS passes only encrypted information.

Procedure

1 Log in to the Workspace ONE Access console.

2 Click the **Appliance Settings** tab and click **SMTP**.

3 Enter the SMTP server host name.

For example: `smtp.example.com`

4 Enter the SMTP server port number.

For example: `25`

5 (Optional) If the SMTP server requires authentication, enter the user name and password.

6 (Optional) To customize the sender's address in the email notifications, enter the email address for SMTP email.

If you do not provide an email address, the address defaults to no-reply@vmwareidentity.com.

7 (Optional) If the SMTP server requires encryption of data over the communication, choose the security type, such as **SSL/TLS** or **STARTTLS**.

8 Click **TEST CONNECTION**.

This action checks the connectivity to the SMTP server with the provided configuration.

If the test is successful, the **Save** button is enabled.

9 Click **Save** to save the configuration.

Configuring Time Synchronization for the Workspace ONE Access Service

Configuring time synchronization on all instances of the Workspace ONE Access service and connector is required for a Workspace ONE Access deployment to function correctly. To configure time synchronization for the Workspace ONE Access service, you configure the **Time Synchronization** page in the Workspace ONE Access console.

You can synchronize the Workspace ONE Access service clock either with the ESXi host or with a Network Time Protocol (NTP) server. By default, the Workspace ONE Access service is set to synchronize with the host.

Follow these guidelines:

- As a best practice, synchronize time with an NTP server if the Workspace ONE Access instance can access an NTP server. Otherwise, synchronize time with the ESXi host and configure the ESXi host to synchronize time with an NTP server.
- If your deployment includes Workspace ONE Access service or connector instances on different hosts, the best practice is to synchronize time with an NTP server directly instead of synchronizing with the host to ensure that there is no time drift between the instances.

Procedure

1. Log in to the Workspace ONE Access console.
2. Select **Dashboard > System Diagnostics Dashboard**.
3. Click **VA Configuration** of the service node you want to configure and log in with the admin user password.
4. Click **Time Synchronization**.
5. Select a time synchronization option.

Option	Description
NTP	Synchronizes the Workspace ONE Access computer system clock with an NTP server. The default NTP server is time.nist.gov. To use another NTP server, enter its fully qualified domain name (FQDN) in the **NTP Server** text box. For example: `ntpserver.example.com`
Host Time	Synchronizes the Workspace ONE Access computer system clock with the ESXi host. This is the default setting.

6. Click **Save**.

Using the Built-in KDC for Workspace ONE Access

6

For Mobile SSO for iOS authentication on VMware Workspace ONE™ UEM-managed iOS devices, you can use the built-in KDC. You manually initialize the Key Distribution Center (KDC) in the appliance before you enable the authentication method from the administration console.

Before you initialize KDC in Workspace ONE Access, determine the realm name for the KDC server, whether subdomains are in your deployment, and whether to use the default KDC server certificate or not.

Realm

The realm is the name of an administrative entity that maintains authentication data. Selecting a descriptive name for the Kerberos authentication realm is important. The realm name must be a part of a DNS domain that the enterprise can configure.

The realm name and the fully qualified domain name (FQDN) that is used to access the Workspace ONE Access service are independent. Your enterprise must control the DNS domains for both the realm name and the FQDN. The convention is to make the realm name the same as your Workspace ONE Access DNS domain name, entered in uppercase letters. Sometimes the realm name and domain are different. For example, a realm name is *EXAMPLE.NET*, and *idm.example.com* is the Workspace ONE Access FQDN. In this case, you define DNS entries for both *example.net* and *example.com* domains.

The realm name is used by a Kerberos client to generate DNS names. For example, when the name is EXAMPLE.COM, the Kerberos related name to contact the KDC by TCP is *_kerberos._tcp.EXAMPLE.COM*.

Using Subdomains

The Workspace ONE Access service installed in an on-premises environment can use the Workspace ONE Access FQDN subdomain. If your Workspace ONE Access site accesses multiple DNS domains, configure the domains as location1.example.com; location2.example.com; location3.example.com. The subdomain value in this case is example.com, typed in lowercase. To configure a subdomain in your environment work with your service support team.

Using KDC Server Certificates

When the KDC is initialized, by default a KDC server certificate and a self-signed root certificate are generated. The certificate is used to issue the KDC server certificate. This root certificate is included in the device profile so that the device can trust the KDC.

You can manually generate the KDC server certificate using an enterprise root or intermediate certificate. Contact your service support team for more details about this feature.

Download the KDC server root certificate from the Workspace ONE Access admin console to use in the Workspace ONE UEM configuration of the iOS device management profile.

This chapter includes the following topics:

Initialize the Key Distribution Center in the Appliance

Before you can use the Mobile SSO for iOS authentication method, you must initialize the Key Distribution Center (KDC) in the Workspace ONE Access appliance.

To initialize KDC, you assign your Workspace ONE Access hostname to the Kerberos realms. The realm name is entered in upper-case letters. If you configure subdomains, type the subdomain name in lower-case letters.

Prerequisites

Workspace ONE Access is installed and configured.

Realm name identified. See Chapter 6 Using the Built-in KDC for Workspace ONE Access.

Procedure

1. SSH into the Workspace ONE Access appliance as the root user.
2. Initialize the KDC. Enter `/etc/init.d/vmware-kdc init --realm {REALM.COM} --subdomain {sva-name.subdomain}`.

   For example, `/etc/init.d/vmware-kdc init --realm MY-IDM.EXAMPLE.COM --subdomain my-idm.example.com`

   If you are using a load balancer with multiple Workspace ONE Access appliances, use the name of the load balancer in both cases.
3. Restart the Workspace ONE Access service. Enter `service horizon-workspace restart`.
4. Start the KDC service. Enter `service vmware-kdc restart`.

What to do next

Create public DNS entries. DNS records must be provisioned to allow the clients to find the KDC. See Creating Public DNS Entries for KDC with Built-in Kerberos.

Creating Public DNS Entries for KDC with Built-in Kerberos

After you initialize KDC in Workspace ONE Access, you must create public DNS records to allow the Kerberos clients to find the KDC when the built-in Kerberos authentication feature is enabled.

The KDC realm name is used as part of the DNS name for the Workspace ONE Access appliance entries that are used to discover the KDC service. Two DNS records are required for each Workspace ONE Access site and two address entries.

Note An AAAA record is required for devices running on iOS 9 or are using T-Mobile as the carrier. The AAAA entry value is an IPv6 address that encodes an IPv4 address. If the KDC is not addressable via IPv6 and an IPv4 address is used, the AAAA entry might have to be specified in strict IPv6 notation as `::ffff:175c:e147` on the DNS server. You can use an IPv4 to IPv6 conversion tool, such as one available from Neustar.UltraTools, to convert IPv4 to IPv6 address notation.

Example: DNS Record Entries for KDC

In this example DNS record, the realm is `EXAMPLE.COM`; the Workspace ONE Access fully qualified domain name is `idm.example.com`, and the Workspace ONE Access IP address `1.2.3.4`.

```
kdc.example.com.               1800 IN  A            1.2.3.4

kdc.example.com.               1800 IN  AAAA         ::ffff:1.2.3.4

_kerberos._tcp.idm.EXAMPLE.COM          IN  SRV  10  0   88 kdc.example.com.

_kerberos._udp.idm.EXAMPLE.COM          IN  SRV  10  0   88 kdc.example.com.
```

Replace REALM

To change the realm after the initial configuration, you must add the new realm name and reinitialize the KDC service.

To initialize KDC, you assign your Workspace ONE Access hostname to the Kerberos realms. The domain name is entered in upper-case letters. If you are configuring multiple Kerberos realms, to help identify the realm, use descriptive names that end with your Workspace ONE Access domain name. For example, SALES.MY-WORKSPACEONEACCESS.EXAMPLE.COM. If you configure subdomains, type the subdomain name in lower-case letters.

Procedure

1. SSH into the Workspace ONE Access appliance as the root user.
2. Initialize the KDC. Enter `/etc/init.d/vmware-kdc init --realm {REALM.COM} --subdomain {sva-name.subdomain} --force`.

   For example, `/etc/init.d/vmware-kdc init --realm MY-IDM.EXAMPLE.COM --subdomain my-idm.example.com --force`

   If you are using a load balancer with multiple Workspace ONE Access appliances, use the name of the load balancer in both cases.
3. Restart the Workspace ONE Access service. Enter `service horizon-workspace restart`.
4. Start the KDC service. Enter `service vmware-kdc restart`.

Results

The realm name is updated in the iOS KdcKerberosAuthAdapter authentication method configuration page.

Monitoring Workspace ONE Access 7

Monitoring Workspace ONE Access is an important part of ensuring your Workspace ONE solution works correctly.

You can use third-party tools such as Nagios, Splunk, Symantec Altiris, Spotlight, Ignite, or Montastic. Consult your company's IT department for specific recommendations on monitoring tools if you do not already have a solution in place.

This document provides generic hardware load capacity recommendations and information about log files and URL endpoints. It does not explicitly cover how to configure a monitoring solution.

This chapter includes the following topics:

Hardware Load Capacity Monitoring Recommendations

Use these monitoring standards to ensure server health.

Metrics to Capture

Hardware	Monitors
CPU	Usage
Memory	Usage
Hard Disk	Free space
Network	Usage

Alerts and Thresholds

VMware recommends analyzing each individual use case to determine the correct thresholds for individual environments.

Hardware	Alerts, Samples, Thresholds
CPU	Samples: 5 minute samples Threshold: 90% over 1 hour, 95 over 1 hour Alerts: 90% load is a warning, 95% is critical
Memory	Samples: 5 minute samples Threshold: 90% over 1 hour, 95 over 1 hour Alerts: 90% used is a warning, 95% used is critical
Hard Disk	Samples: 5 minute samples Threshold: 90% over 1 hour, 95 over 1 hour Alerts: 90% used is a warning, 95% used is critical
Network	Samples: 5 minute samples Threshold: 90% over 1 hour, 95 over 1 hour Alerts: 90% load is a warning, 95% is critical

Strategy for Capture

The metrics are captured by the underlying virtual infrastructure utilizing tools such as vSphere or vRealize Operations.

Workspace ONE Access URL Endpoints for Monitoring

Monitor the listed URL endpoints for various Workspace ONE Access components to ensure a functional environment. Certain endpoints can also be used for load balancers to ensure the service is up for traffic.

Health Checks for Load Balancers

Component	Health Check	Expected Return	Notes
Workspace ONE Access Service	`/SAAS/API/1.0/REST/system/health/heartbeat`	String: ok Http: 200	Frequency every 30 seconds
	Android Mobile SSO - Certproxy: `:5262/system/health`	Http: 200	Frequency every 30 seconds
	iOS Mobile SSO - KDC: `TCP half-open to port 88`	Connection	Frequency every 30 seconds
	Certificate adapter: `:7443/SAAS/API/1.0/REST/system/health/heartbeat`	String: ok Http: 200	Frequency every 30 seconds
Workspace ONE Access connector earlier than 20.01	`/hc/API/1.0/REST/system/health/allOk`	String: true Http: 200	Frequency every 30 seconds

Component	Health Check	Expected Return	Notes
Workspace ONE Access connector 20.01 and later	`https://hostname:portnumber/eks/health` **Note** A load balancer is not applicable to the Directory Sync service or User Auth service. If the Kerberos Auth service is configured, it is the only enterprise service you need to configure behind a load balancer. To monitor the Kerberos Auth service, use the preceding end-point, where *portnumber* is a placeholder for the port number of the host. The default port number is 443.	String: true Http: 200	Frequency every 30 seconds
Integration Broker	`/IB/API/RestServiceImpl.svc/ibhealthcheck`	String: All Ok Http: 200	Frequency every 30 seconds
	XenApp 7.x Integration: `/IB/API/RestServiceImpl.svc/hznxenapp/admin/xenfarminfo?computerName=&xenappversion=Version7x`	String: 'SiteName' Http: 200	Frequency every 5 minutes
	XenApp 6.x Integration: `/IB/API/RestServiceImpl.svc/hznxenapp/admin/xenfarminfo?computerName=&xenappversion=Version65orLater`	String: 'FarmName' Http: 200	Frequency every 5 minutes

The health checks for load balancers return simple values for easy parsing by network equipment.

Additional Health Checks for Monitoring

The health checks listed here can be consumed by monitoring solutions that have the ability to parse data and create dashboards. Set the frequency to every 5 minutes.

Workspace ONE Access **Service Monitoring and Health**

URL call: `/SAAS/jersey/manager/api/system/health`

or

/SAAS/API/1.0/REST/system/health

Raw output:


```
{
   "AnalyticsUrl":"unknown",
   "ElasticsearchServiceOk":"true",
   "EhCacheClusterPeers":"unknown",
   "ElasticsearchMasterNode":"unknown",
   "ElasticsearchIndicesCount":"unknown",
   "ElasticsearchDocsCount":"unknown",
   "AuditPollInterval":"0",
   "AnalyticsConnectionOk":"true",
   "EncryptionServiceVerified":"unknown",
   "FederationBrokerStatus":"unknown",
   "ServiceReadOnlyMode":"false",
   "ElasticsearchUnassignedShards":"unknown",
   "AuditWorkerThreadAlive":"true",
   "BuildVersion":"3.3.0.0 Build xxxxxxx",
   "AuditQueueSize":"0",
   "DatabaseStatus":"unknown",
   "HostName":"unknown",
   "ElasticsearchNodesCount":"unknown",
   "EncryptionStatus":"unknown",
   "FederationBrokerOk":"true",
   "EncryptionConnectionOk":"true",
   "EncryptionServiceImpl":"unknown",
   "ClusterId":"22f6e089-45df-41ab-9c8a-77f3e4589230",
   "EhCacheClusterDiagnostics":"unknown",
   "ElasticsearchNodesList":"unknown",
   "DatabaseConnectionOk":"true",
   "ElasticsearchHealth":"unknown",
   "StatusDate":"2018-08-06 19:14:40 UTC",
   "ClockSyncOk":"true",
   "MaintenanceMode":"false",
   "MessagingConnectionOk":"true",
   "fipsModeEnabled":"true",
   "ServiceVersion":"3.3.0",
   "AuditQueueSizeThreshold":"null",
   "IpAddress":"unknown",
   "AuditDisabled":"false",
   "AllOk":"true"
}
```


"AllOk"	"true", "false"	Roll-up health check to monitor overall health of Workspace ONE Access services
"MessagingConnectionOk"	"true", "false"	Verifies that all message producers and consumers are connected to RabbitMQ
"DatabaseConnectionOk"	"true", "false"	Verifies the connection to the database

"EncryptionConnectionOk"	"true", "false"	Verifies that the connection to the encryption service is okay and the primary key store is okay
"AnalyticsConnectionOk"	"true", "false"	Verifies the connection to the analytics service
"FederationBrokerOk"	"true", "false"	Verifies the embedded auth adapters to ensure their subsystems are okay

Note The label "unknown" in the output indicates that the information is restricted. By default, sensitive information such as IP addresses and host names, is hidden. To display this information, see Displaying Additional Information in the Workspace ONE Access Health Check API.

URL call: `/catalog-portal/services/health`

This health check is specific for the user interface part of Workspace ONE Access.

Raw output:


```
{
    "status": "UP",
    "uiService": {
        "status": "UP"
    },
    "apiService": {
        "status": "UP"
    },
    "eucCacheEngine": {
        "status": "UP"
    },
    "cacheEngineClient": {
        "status": "UP"
    },
    "persistenceEngine": {
        "status": "UP",
        "database": "Microsoft SQL Server",
        "hello": 1
    },
    "tenantPersistenceEngine": {
        "status": "UP",
        "database": "Microsoft SQL Server",
        "hello": 1
    },
    "diskSpace": {
        "status": "UP",
        "total": 8460120064,
        "free": 4898279424,
        "threshold": 10485760
    }
}
```

"status"	"UP", "DOWN"	Roll-up health check to monitor overall health of the Workspace ONE Access user interface (UI)
"uiServer.status"	"UP", "DOWN"	UP if the main UI service is running
"apiService.status"	"UP", "DOWN"	UP if the main UI API service is running
"eucCacheEngine.status"	"UP", "DOWN"	UP if the Hazelcast cluster engine is running
"cacheEngineClient.status"	"UP", "DOWN"	UP if the Hazelcast client for the UI is running
"persistenceEngine.status"	"UP", "DOWN"	UP if the main database (SQL) is running
"tenantPersistenceEngine.status"	"UP", "DOWN"	UP if the main database (SQL) is running
"diskSpace.status"	"UP", "DOWN"	UP if the free disk space is greater than the threshold configured, 10 MB
"diskSpace.free"	Bytes	Space free in Bytes on the partition where the Workspace ONE Access UI is installed

Workspace ONE Access **Connector Monitoring and Health**

The following URL call applies to the Workspace ONE Access connector earlier than 20.01.

URL call: **`/hc/API/1.0/REST/system/health`**

Raw output:


```
{
        "HorizonDaaSSyncConfigurationStatus": "",
        "AppManagerServiceOk": "true",
        "DomainJoinEnabled": "false",
        "XenAppEnabled": "true",
        "ViewSyncConfigurationStatus": "",
        "ThinAppServiceOk": "true",
        "ThinAppSyncConfigurationStatus": "unknown",
        "Activated": "true",
        "XenAppServiceOk": "false",
        "DirectoryServiceStatus": "Connection test successful",
         "BuildVersion": "2017.1.1.0 Build 5077496",
        "ThinAppServiceStatus": "unknown",
        "XenAppServiceStatus": "A problem was encountered Sync Integration Broker",
        "HostName": "hostname.company.local",
        "NumberOfWarnAlerts": "0",
        "JoinedDomain": "true",
        "XenAppSyncConfigurationStatus": "Sync configured (manually)",
        "DirectorySyncConfigurationStatus": "Sync configured (manually)",
        "NumberOfErrorAlerts": "0",
        "DirectoryServiceOk": "true",
        "HorizonDaaSTenantOk": "true",
```

```
        "ThinAppDirectoryPath": "",
        "StatusDate": "2017-06-27 10:52:59 EDT",
        "ViewSyncEnabled": "false",
        "ViewServiceOk": "true",
        "HorizonDaaSEnabled": "false",
        "AppManagerUrl": "https://workspaceurl.com/SAAS/t/qwe12312qw/",
        "HorizonDaaSServiceStatus": "unknown",
        "DirectoryConnection": "ldap:///ldapcall",
        "ServiceVersion": "VMware-C2-2017.1.1.0 Build 5077496",
        "IpAddress": "169.118.86.105",
        "DomainJoinStatus": "Domain: customerdomainname",
        "AllOk": "false",
        "ViewServiceStatus": "unknown",
        "ThinAppEnabled": "false",
        "XenAppSyncSsoBroker": "integrationbrokersso:443 / integrationbrokersync:443"
}
```


"AllOk"	"true", "false"	Roll-up health check to monitor overall health of Workspace ONE Access Connector Services.
"ViewServiceOk"	"true", "false"	True, if connection to the View Broker is successful. This attribute will be true if View sync is deactivated.
"HorizonDaaSTenantOk"	"true", "false"	True, if connection to Horizon Cloud is successful. This attribute will be true if Horizon Cloud sync is deactivated.
"DirectoryServiceOk"	"true", "false"	True, if connection to the directory is successful. This attribute will be true if directory sync is deactivated.
"XenAppServiceOk"	"true", "false"	True, if connection to the Citrix server is successful. This attribute will be true if Citrix server is deactivated.
"ThinAppServiceOk"	"true", "false"	True, if connection to the ThinApp packaged applications service is successful. This attribute will be true if packaged applications are deactivated.
"AppManagerServiceOk"	"true", "false"	True, if able to authenticate correctly to the AppManager.

"NumberOfWarnAlerts"	0 - 1000	Number of warning alerts that triggered on this connector instance. These are available on the Connector Sync Log as “Notes.” They can indicate that a resource was synced in that included a user or group that is not in Workspace ONE Access. Depending on the configuration, this may be by design. The counter continues to increment on each sync until Warn and Error alerts equal 1000 and an administrator clears the alerts.
"NumberOfErrorAlerts"	0 - 1000	Number of error alerts that triggered on this connector instance. These are available on the Connector Sync Log as “Error.” They can indicate that a sync failed. The counter continues to increment on each sync until Warn and Error alerts equal 1000 and an administrator clears the alerts.

Workspace ONE Access **Integration Broker Monitoring and Health**

URL call: `/IB/API/RestServiceImpl.svc/ibhealthcheck`

Raw output:

```
“All Ok”
```

This health check verifies that all the software on the Integration Broker is responding properly. It returns a 200 response with the string "All Ok".

Workspace ONE Access **Integration Broker Monitoring and Health with Citrix XenApp 7.x**

URL call: `/IB/API/RestServiceImpl.svc/hznxenapp/admin/xenfarminfo?computerName=&xenappversion=Version7x`

This pulls back information from an API call to Citrix. Monitoring can ensure that the values are consistent.

Raw output:

```
[{
     \ “ConfigurationLoggingServiceGroupUid \ ”:  \ “5e2a5602 - 45a8 - 4b56 - 92e6 -
9fae5a3ff459 \ ”,
     \ “ConfigurationServiceGroupUid \ ”:  \ “620d7c6e - b7c1 - 4ee7 - b192 - d00764f477e7 \
”,         \ “DelegatedAdministrationServiceGroupUid \ ”:  \ “0a59914d - 4b6e - 4cca - bbaa -
a095067092e3 \ ”,
     \ “LicenseServerName \ ”:  \ “xd.hs.trcint.com \ ”,
     \ “LicenseServerPort \ ”:  \ “27000 \ ”,
     \ “LicenseServerUri \ ”:  \ “https:  \  /  \  / xd.hs.domain.com: 8083 \  /  \ ”,
     \ “LicensingBurnIn \ ”:  \ “2014.0815 \ ”,
     \ “LicensingBurnInDate \ ”:  \ “8 \  / 14 \  / 2014 5: 00: 00 PM \ ”,
     \ “LicensingModel \ ”:  \ “UserDevice \ ”,
```

```
    \ "MetadataMap \ ":  \ "System.Collections.Generic.Dictionary
`2[System.String,System.String]\",
    \"PrimaryZoneName\":\"\",
    \"PrimaryZoneUid\":\"00000000-0000-0000-0000-000000000000\",
    \"ProductCode\":\"XDT\",
    \"ProductEdition\":\"PLT\",
    \"ProductVersion\":\"7.6\",
    \"SiteGuid\":\"0c074098-02d2-47cf-aa87-7e3asdsad7c\",
    \"SiteName\":\"customer\"
}]
```

Raw output exception:

```
{"ExceptionType":"System.Management.Automation.CmdletInvocationException","Message":"An
invalid URL was given for the service.  The value given was 'mit-
xen751.hs.trcint.com'.\u000d\u000a    The reason given was: Failed to connect to back-
end server 'mit-xen751.hs.trcint.com' on port 80 using binding WSHttp. The server may
be off-line or may not be running the appropriate service\u000d\u000a\u0009There was
no endpoint listening at http:\/\/mit-xen751.hs.trcint.com\/Citrix\/ConfigurationContract\/v2
that could accept the message. This is often caused by an incorrect address or
SOAP action. See InnerException, if present, for more details.\u000d\u000a\u0009The
remote name could not be resolved: 'mit-xen751.hs.trcint.com'.","StackTrace":"
at System.Management.Automation.Internal.PipelineProcessor.SynchronousExecuteEnumerate(Object
input, Hashtable errorResults, Boolean enumerate)\u000d\u000a
at System.Management.Automation.Internal.PipelineProcessor.SynchronousExecute(Array
input, Hashtable errorResults)\u000d\u000a   at
System.Management.Automation.Runspaces.LocalPipeline.InvokeHelper()\u000d\u000a   at
System.Management.Automation.Runspaces.LocalPipeline.InvokeThreadProc()"}
```

Workspace ONE Access **Integration Broker Monitoring and Health with Citrix XenApp 6.x**

URL call: `/IB/API/RestServiceImpl.svc/hznxenapp/admin/xenfarminfo?computerName=&xenappversion=Version65orLater`

This pulls back information from an API call to Citrix. Monitoring can ensure that the values are consistent.

Raw output:

```
"[{
       \ "FarmName \ ":  \ "NewFarm \ ",
     \ "ServerVersion \ ":  \ "6.5.0 \ ",
     \ "AdministratorType \ ":  \ "Full \ ",
     \ "SessionCount \ ":  \ "0 \ ",
     \ "MachineName \ ":  \ "XENAPPTEST \ "
    }]"
```

Displaying Additional Information in the Workspace ONE Access Health Check API

You can control whether sensitive information, such as IP addresses and host names, is displayed in the output of the health check APIs `https://`*`WS1AccessHostnameFQDN`*`/SAAS/jersey/`

`manager/api/system/health` and `https://WS1AccessHostnameFQDN/SAAS/API/1.0/REST/system/health`. By default, the API output does not include this information.

The `service.health.check.basic` property in the `runtime-config.properties` file controls this setting. When the property is set to **`true`**, only basic information is displayed and sensitive information is hidden. The label `"unknown"` in the output indicates that the information is restricted. For example:

```
AnalyticsUrl:    "unknown"
ElasticsearchServiceOk:    "true"
EhCacheClusterPeers:    "unknown"
ElasticsearchMasterNode:    "unknown"
ElasticsearchIndicesCount    "unknown"
ElasticsearchDocsCount:    "unknown"
AuditPollInterval:    "1000"
AnalyticsConnectionOk:    "true"
...
IpAddress:    "unknown"
AuditDisabled:    "false"
AllOk:    "true"
```

When the property is set to **`false`**, all available information is displayed. For example:

```
AnalyticsUrl: "http://198.51.100.0"
ElasticsearchServiceOk: "true"
EhCacheClusterPeers: ""
ElasticsearchMasterNode: "198.51.100.1"
ElasticsearchIndicesCount: "13"
ElasticsearchDocsCount: "11173"
AuditPollInterval: "1000"
AnalyticsConnectionOk: "true"
...
IpAddress: "198.51.100.2"
AuditDisabled: "false"
AllOk: "true"
```

By default, the property is set to **`true`**.

Note If you have set up a Workspace ONE Access cluster and you change the property, ensure that you make the change in all nodes in the cluster.

Procedure

1 Log in to the Workspace ONE Access virtual appliance as the root user.

2 Edit the `/usr/local/horizon/conf/runtime-config.properties` file and set the value of the `service.health.check.basic` property to **`true`** or **`false`**.

Option	Description
true	Displays only basic information. Sensitive information is hidden and the label `Unknown` appears in its place.
false	Displays all available information

3 Save the file.

4 Restart the service.

```
service horizon-workspace restart
```

5 If you have set up a Workspace ONE Access cluster, make these changes in each node of the cluster.

Workspace ONE Access System Logging

Logging from the Workspace ONE Access service and the Workspace ONE Access connector components are available using syslog. The Integration Broker component logs locally. The logs can be collected and reviewed on the server or through a central logging service such as vRealize Log Insight or Splunk. For Workspace ONE Access connector log-file information, see the *Installing Workspace ONE Access Connector* guide.

To send audit logs and system events to vRealize Log Insight, you can download and install vRealize Log Insight Agent on each Workspace ONE Access node. See Install and Configure the vRealize Log Insight Agent on the Workspace ONE Access Nodes for directions about how to download and install vRealize Log Insight.

Workspace ONE Access Service Logging

Log Locations

Most service logs are located at `/opt/vmware/horizon/workspace/logs/`.

Log	Purpose
`greenbox_web.log`	Log which contains all user interface interactions for web and mobile
`horizon.log`	Workspace ONE Access service log which includes Identity Adapters, RabbitMQ, Elasticsearch, Ehcache, and other subsystems
`connector.log`	Connector log for all authentication methods and integrations with Horizon and Citrix
`cert-proxy.log`	Workspace ONE Access service CertProxy component for Android Mobile SSO
`configurator.log`	Requests that the Configurator receives from the REST client and the Web interface

Log	Purpose
`/opt/vmware/var/log/update.log`	A record of output messages related to update requests during an upgrade of Workspace ONE Access
`/opt/vmware/var/log/vami/`	The files in the `/opt/vmware/var/log/vami` directory are useful for troubleshooting. You can find these files on all virtual machines after an upgrade.
`catalina.log`	Apache Tomcat records of messages that are not recorded in other log files
`/var/log/journal/<logfoldername>`	iOS KDC logs for Mobile SSO To retrieve the logs for iOS KDC, run `journalctl --no-pager --file /var/log/journal/<log folder name, give the latest one>/user-1001.journal`

Syslog Server Setup

To set up a syslog server, see Configure a Syslog Server for Workspace ONE Access.

Integration Broker Logging

Integration Broker logs are located in the following location:

`C:\ProgramData\VMware\HorizonIntegrationBroker`

The logs are captured by day and contain all REST API calls made to and by Integration Broker.

Setting Workspace ONE Access Rate Limits

8

You can set rate limits on the Workspace ONE Access service and the Workspace ONE Access connector.

This chapter includes the following topics:

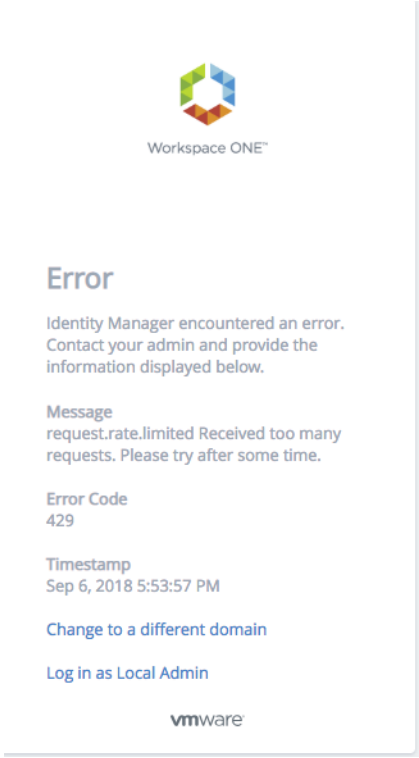
Setting Rate Limits on the Workspace ONE Access Service

You can set limits on the number of login, launch, and WS-Fed requests that can be made per minute to the Workspace ONE Access service. When the limit is reached, subsequent requests are denied. Setting rate limits helps prevent overload of the system.

For example, if you set the rate limit for login requests to 100, the first 100 login requests per minute are accepted but requests 101-n are denied.

For a Workspace ONE Access cluster, the rate limit applies to each node in the cluster. For example, if you set the login request rate limit to 100 for a cluster that has NodeA, NodeB, and NodeC, NodeA can process 100 login requests per minute, NodeB can process 100 login requests per minute, and NodeC can process 100 login requests per minute. You cannot set separate login limits per node.

When the limit is reached and requests are denied, end users see the following error message:



No rate limits are set by default.

You set rate limits using a REST API. Use a REST client such as Postman to make the calls to the Workspace ONE Access service. The changes take effect in a few minutes.

Setting Rate Limits

Use this API to set rate limits for the Workspace ONE Access service.

Endpoint: `https://WS1AccessHostnameFQDN/SAAS/jersey/manager/api/system/tuning/resiliency/tenant/orgResiliencyConfiguration?tenantId=tenantId`

Method: PUT

Description: Sets the maximum number of login, launch, and WS-Fed requests allowed per minute by the Workspace ONE Access service.

Headers:

Content-Type	`application/vnd.vmware.horizon.manager.system.tuning.resiliency.config+json;charset=UTF-8`
Accept	`application/vnd.vmware.horizon.manager.system.tuning.resiliency.config+json`
Authorization	`HZN cookie_value` To get the *cookie_value*, log into the Workspace ONE Access service as the tenant administrator, that is, the admin user that is created when you first install Workspace ONE Access, and obtain the value of the HZN cookie from your browser's cookie cache.

Path Parameters:

`hostname`	The fully-qualified domain name of the Workspace ONE Access service or load balancer.
`tenantId`	The tenantId of the Workspace ONE Access service. The tenant ID is the tenant name that appears in the top-right corner of the Workspace ONE Access console.

Request Body:

```
{
"config": {
          "rateLimitingDisabled": false,
          "rateLimits": {
              "login": {
                  "requestsPerMinute": n
              },
              "launch": {
                  "requestsPerMinute": n
              },
              "ws-fed": {
          "requestsPerMinute": n
          }
      }
  }
  }
```

Request Body Parameters

login requestsPerMinute	Specify the maximum number of login requests allowed per minute. **Note** Take into account that multiple API requests might be needed for a login request to complete and each API call counts towards the rate limits. For example, password authentication involves two API calls, one to render the login page and the second to submit credentials.
launch requestsPerMinute	Specify the maximum number of launch requests allowed per minute.
ws-fed requestsPerMinute	Specify the maximum number of WS-Fed requests allowed per minute. WS-Fed rate limits are for Active Logon configurations only.

Viewing Rate Limits

Use this API to view rate limits that are set for the Workspace ONE Access service.

Endpoint: `https://WS1AccessHostnameFQDN/SAAS/jersey/manager/api/system/tuning/resiliency/tenant/orgResiliencyConfiguration?tenantId=tenantId`

Method: GET

Description: Retrieves the rate limits that are currently set for login, launch, and WS-Fed requests for the Workspace ONE Access service.

Headers:

Authorization	`HZN cookie_value` To get the *cookie_ value*, log into the Workspace ONE Access service as the tenant administrator, that is, the admin user that is created when you first install Workspace ONE Access, and obtain the value of the HZN cookie from your browser's cookie cache.

Path Parameters:

`hostname`	The fully-qualified domain name of the Workspace ONE Access service or load balancer.
`tenantId`	The tenant Id of the Workspace ONE Access service. The tenant ID is the tenant name that appears in the top-right corner of the Workspace ONE Access console.

Sample Output:

```
{
"config": {
          "rateLimitingDisabled": false,
          "rateLimits": {
              "login": {
                  "requestsPerMinute": 100
              },
              "launch": {
                  "requestsPerMinute": 100
              },
              "ws-fed": {
          "requestsPerMinute": 100
          }
      }
  }
  }
```

login requestsPerMinute	The maximum number of login requests allowed per minute.
launch requestsPerMinute	The maximum number of launch requests allowed per minute.
ws-fed requestsPerMinute	The maximum number of WS-Fed requests allowed per minute. WS-Fed rate limits are for Active Logon configurations only.

Setting Rate Limits on the Workspace ONE Access Connector

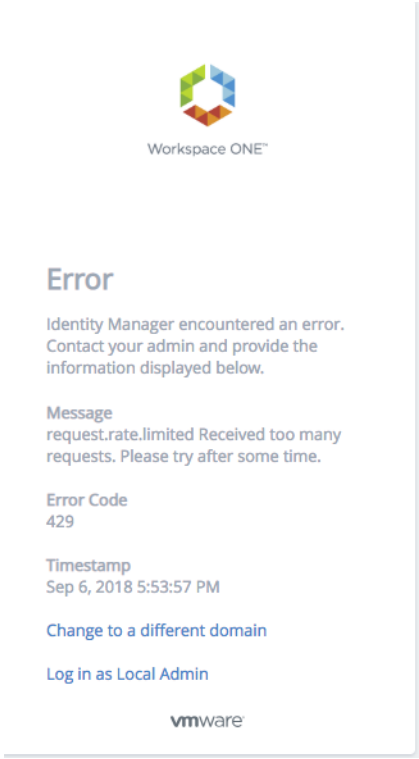
Just as you can set rate limits on the Workspace ONE Access service, you can set rate limits on the Workspace ONE Access connector.

For the connector, you can set a limit on the number of login requests that are allowed per minute. When the limit is reached, subsequent requests are denied. Setting rate limits helps prevent overload of the system.

For example, if you set the rate limit for login requests to 100, the first 100 login requests per minute are accepted but requests 101-n are denied.

For a Workspace ONE Access connector cluster, the limit applies to each node in the cluster. For example, if you set the login request rate limit to 100 for a cluster that has NodeA, NodeB, and NodeC, NodeA can process 100 login requests per minute, NodeB can process 100 login requests per minute, and NodeC can process 100 login requests per minute. You cannot set separate login limits per node.

When the limit is reached and requests are denied, end users see the following error message:



No rate limits are set by default.

You set rate limits using a REST API. Use a REST client such as Postman to make the calls to the Workspace ONE Access service.

Changes take effect after about an hour. If you want the changes to take effect immediately, run the `install_dir\usr\local\horizon\scripts\horizonService.bat restart` script to restart the Windows connector.

Setting Rate Limits

Use this API to set rate limits for the Workspace ONE Access connector .

Endpoint: `https://hostname/SAAS/jersey/manager/api/system/tuning/resiliency/tenant/orgResiliencyConnectorConfiguration?tenantId=tenantId`

Method: PUT

Description: Sets the maximum number of login requests allowed per minute by the Workspace ONE Access connector.

Headers:

Content-Type	`application/vnd.vmware.horizon.manager.system.tuning.resiliency.config+json;charset=UTF-8`
Accept	`application/vnd.vmware.horizon.manager.system.tuning.resiliency.config+json`
Authorization	`HZN cookie_value` To get the *cookie_value*, log into the Workspace ONE Access service as the tenant administrator, that is, the admin user that is created when you first install Workspace ONE Access, and obtain the value of the HZN cookie from your browser's cookie cache.

Path Parameters:

`hostname`	The fully-qualified domain name of the Workspace ONE Access service or load balancer.
`tenantId`	The tenant ID of the Workspace ONE Access service. The tenant ID is the tenant name that appears in the top-right corner of the Workspace ONE Access console.

Request Body:

```
{
"config": {
          "rateLimitingDisabled": false,
          "rateLimits": {
              "login": {
                  "requestsPerMinute": n
              }
      }
  }
  }
```

Request Body Parameters

login requestsPerMinute	Specifiy the maximum number of login requests allowed per minute. **Note** Take into account that multiple API requests might be needed for a login request to complete and each API call counts towards the rate limits. For example, password authentication involves two API calls, one to render the login page and the second to submit credentials.

Viewing Rate Limits

Use this API to view the rate limits that are set currently on the Workspace ONE Access connector.

Endpoint: `https://hostname/SAAS/jersey/manager/api/system/tuning/resiliency/tenant/orgResiliencyConnectorConfiguration?tenantId=tenantId`

Method: GET

Description: Retrieves the rate limits that are currently set for login requests for the Workspace ONE Access connector.

Headers:

Authorization	`HZN cookie_value` To get the *`cookie_value`*, log into the Workspace ONE Access service as the tenant administrator, that is, the admin user that is created when you first install Workspace ONE Access, and obtain the value of the HZN cookie from your browser's cookie cache.

Path Parameters:

`hostname`	The fully-qualified domain name of the Workspace ONE Access service or load balancer.
`tenantId`	The tenant Id of the Workspace ONE Access service. The tenant ID is the tenant name that appears in the top-right corner of the Workspace ONE Access console.

Sample Output:

```
{
"config": {
          "rateLimitingDisabled": false,
          "rateLimits": {
              "login": {
                  "requestsPerMinute": 100
              }
      }
  }
  }
```

login requestsPerMinute	The maximum number of login requests allowed per minute.

Troubleshooting Workspace ONE Access Installation and Configuration

9

The troubleshooting topics describe solutions to potential problems you might encounter when installing or configuring Workspace ONE Access.

This chapter includes the following topics:

Users Unable to Launch Applications or Incorrect Authentication Method Applied in Load-Balanced Environments

Users are unable to launch applications from the Workspace ONE portal or the wrong authentication method is applied in a load-balanced environment.

Problem

In a load-balanced environment, problems such as the following might occur:

- Users are unable to launch applications from the Workspace ONE portal after they log in.
- The wrong authentication method is presented to users for step-up authentication.

Cause

These problems can occur if access policies are determined incorrectly. The client IP address determines which access policy is applied during login and during application launch. In a load-balanced environment, Workspace ONE Access uses the X-Forwarded-For header to determine the client IP address. In some cases, an error might occur.

Solution

Set the `service.numberOfLoadBalancers` property in the `runtime-config.properties` file in each of the nodes in your Workspace ONE Access cluster. The property specifies the number of load balancers fronting the Workspace ONE Access instances.

Note Setting this property is optional.

1 Log in to the Workspace ONE Access appliance.

2 Edit the `/usr/local/horizon/conf/runtime-config.properties` file and add the following property:

```
service.numberOfLoadBalancers numberOfLBs
```

where *numberOfLBs* is the number of load balancers fronting the Workspace ONE Access instances.

3 Restart the workspace appliance.

```
service horizon-workspace restart
```

Users Unable to Launch Applications in Load-balanced Environment

Users are unable to launch applications from the Workspace ONE Intelligent Hub app or portal in a load-balanced Workspace ONE Access deployment.

Problem

Users are unable to launch applications from the Workspace ONE Intelligent Hub portal or app if their client IP address is determined incorrectly. This problem can occur in load-balanced Workspace ONE Access deployments if the X-Forwarded-For (XFF) header contains incorrect IP addresses.

Check the Audit Events launch report in the Dashboard to verify that the client IP address is being resolved correctly. If it is not being resolved correctly, follow this procedure to fix the problem.

Solution

To resolve the issue, first get the list of IP addresses listed in the XFF header by using the `clientipresolutioninfo` REST API and check the response. If it returns the IP address of the load balancer or Workspace ONE Access service node, then set the `service.ipsToIgnoreInXffHeader` property in the `runtime-config.properties` file to filter out the unwanted IP addresses.

To get the list of IP addresses in the XFF header, use a REST client such as Postman to run the following REST API while logged in to the Workspace ONE Access service as the tenant administrator:

Method: `GET`

Path: `/clientipresolutioninfo`

Authorization: `HZN` *`cookie_value`*

Note you can get the `HZN` cookie value by logging into the Workspace ONE Access service as the tenant administrator, then accessing your browser's cookie cache.

Response Media Type: `application/vnd.vmware.horizon.manager.clientipresolutionconfig+json`

Sample JSON response:

```
{
"xffHeaderIpList":["10.112.68.252"], // the IPs part of XFF header
"numberOfLoadBalancers":0, // number of load balancers configured in runtime-config.properties
"configuredIpToIgnoreList":"10.112.68.255", // the list of ips or subnets to ignore as
configured in runtime-config.properties
"clientIpDetermined":"10.112.68.252", // the client IP determined to be used finally for
login/access policy
"_links":{}
}
```

From the output, determine which IP addresses are not needed, then edit the `runtime-config.properties` file to filter them out.

1 Log in to the Workspace ONE Access virtual appliance.

2 Edit the `/usr/local/horizon/conf/runtime-config.properties` file and add the following property:

`service.ipsToIgnoreInXffHeader` *`IPsToIgnore`*

where *`IPsToIgnore`* is a comma-separated list of IP addresses to ignore in the XFF header.

3 Restart the service.

```
service horizon-workspace restart
```

Group Does Not Display Any Members after Directory Sync

Directory sync completes successfully but no users are displayed in synced groups.

Problem

After a directory is synced, either manually or automatically based on the sync schedule, the sync process completes successfully but no users are displayed in synced groups.

Cause

This problem occurs when you have two or more nodes in a cluster and there is a time difference of more than 5 seconds between the nodes.

Solution

1 Ensure that there is no time difference between the nodes. Use the same NTP server across all nodes in the cluster to synchronize the time.

2 Restart the service on all the nodes.

```
service horizon-workspace restart
```

3 (Optional) In the Workspace ONE Access console, delete the group, add it again in the sync settings, and sync the directory again.