WHITE PAPER – **JUNE 2017**

# SECURING CLOUD PLATFORMS WITH PROJECT LIGHTWAVE

## Multitenant, Multimaster, Geo-Distributed Identity and Access Management for the Cloud

## Table of Contents

## Introduction

The need for security in the cloud is acute. Extending the security frameworks, standards, and policies of your on-premises infrastructure to your resources in the cloud establishes the level of consistency that's required to protect the integrity, availability, and confidentiality of your cloud operations.

To consistently apply your on-premises security controls and policies in the cloud, several requirements for high-quality identity and access management come to the fore:

- Standards
- Flexibility, portability, and cloud-platform independence
- Interoperability
- Scalability
- Administrative control

### Identity and Access Management Requirements in the Cloud

Standards are a key requirement because they let you apply trusted tools and protocols across disparate environments to reduce the risk of security incidents and compliance problems.

Flexibility enables you to port your security policies and controls from one environment to another as you move a server or application. As more workloads migrate to the cloud, the cloud-platform independence of your identity service helps you move from one cloud provider to another without having to redeploy or reconfigure identity management systems.

Interoperability ensures that security mechanisms are compatible with other systems. Scalability addresses the need for cloud-scale as operations expand. And administrative control empowers you to implement the security frameworks and policies that you want while reducing your reliance on cloud providers and third parties.

### Security Problems in Cloud Computing

The multitenant environment of public clouds complicates identity and access management. In the cloud, it is important to securely authenticate system users and administrators, giving them access only to the resources they own or need to do their jobs. But authentication and access control become difficult when assets are spread across both on-premises data centers and cloud services. Porting identities and access policies to the cloud depends on how easily you can integrate your corporate identity directories and policies with the service provider's systems.

Implementing seamless security across both your on-premises environment and multiple public clouds is increasingly becoming a necessity. Project Lightwave™ is a massively scaled, multitenant, open-source identity platform that solves this problem by delivering a standards-based directory service, Active Directory integration, certificate services, and Kerberos authentication.

**USE CASES FOR MULTITENANT SECURITY ACROSS ENVIRONMENTS**

- Identity federation across data centers
- Hybrid data center
- Stand-alone directory service in the cloud
- Directory service managed by a cloud provider
- As a bridge to identity as a service (IDaaS)

## Use Cases

As enterprises move workloads to public clouds, hybrid clouds, or private clouds, security administrators seek security functionality on par with the de facto standard for identity management in place in many data centers: Microsoft Active Directory.

A widely deployed directory service, Active Directory hosts the accounts and credentials of users, machines, and applications. When logging in to a machine that has been joined to an Active Directory domain, a user enters his or her domain credentials. Active Directory authenticates the user and authorizes access to the machine or the resources running on it. For authentication, Active Directory typically uses the highly secure Kerberos protocol. For authorization, Active Directory uses membership in security groups. In addition, certificates play a role as a security mechanism for certain services.

Public cloud services, to a certain extent, have mirrored this approach. AWS, for example, requires you to create a security group and set it to allow SSH, HTTP, and HTTPS connections so that you can be authorized to access a resource through a port. In addition, Amazon uses the pairing of an RSA user-signing certificate and a private key for handshake verification of SSH connections.

To support workloads running on Windows or Linux computers, system administrators who are porting their workloads to the cloud or refactoring applications with container technology often look for solutions to one or more use cases, such as enforcing consistent security across a hybrid data center. The use cases that follow define some of the problems that IT and system administrators are grappling with as they seek to streamline application development and deployment while keeping their systems and applications secure.

### Identity Federation Across Data Centers

A multinational corporation with four geographically distributed data centers in Tokyo, London, New York, and Los Angeles seeks to implement identity federation across the data centers with local domain controllers and Active Directory replication. The local domain controllers keep the latency of authentication and authorizing requests low. A major problem the company faces as it attempts to implement this approach is scalability. The directory service must be highly scalable. At the same time, the company's development teams seek to refactor some of their traditional applications as containerized applications using Docker containers and Kubernetes clusters while authenticating developers as they access Kubernetes.

### Hybrid Data Center

A company with a headquarters in Tokyo runs many remote offices and data centers in the United States. The company wants to deploy local applications closer to a cloud provider, such as GCP or AWS, but authenticating and authorizing users with the Active Directory domain controllers in Tokyo results in too much latency and other performance problems.

**LIGHTWAVE SERVICES**

- Identity management and directory services
- Authentication and authorization
- Certificates

By using a virtual private cloud, the company wants to sync its AD cluster in Tokyo to its projects running in the cloud. If the company can replicate the right Active Directory organizational units to a local directory service running in the cloud in the United States on a nightly basis, it can solve its problems with latency and performance. When a local user accesses cloud applications in the United States, the user can then be authenticated and authorized by using the local copy of the organizational unit data. If the local directory service can be used, there will be little or no latency for application access.

### Stand-Alone Directory Service in the Cloud

Companies want to run a separate forest or organizational unit in the cloud to service cloud-only nodes. Connectivity to an on-premises environment is not required. In this case, the directory service must support LDAP but not Kerberos.

### Directory Managed by Cloud Provider

In this use case, the provider of public cloud services, such as Google or Amazon, runs the directory service. The provider runs the directory service but lets a customer use it as a dedicated cloud-based domain controller running in active-active mode with an on-premises directory service. Alternatively, the customer might use it as a stand-alone, dedicated directory service in the cloud.

### Bridge to Identity as a Service

In this advanced use case, a directory service acts as a bridge to synchronize identities between a company's on-premises directory service and a cloud-provider's stand-alone identity as a service (IDaaS) system in the cloud, such as Microsoft Azure Active Directory (Azure AD). In such a case, a directory service running in the cloud could be an intermediary that synchronizes user principals and other metadata from a company's on-premises directory to a cloud provider's IDaaS tenant.

## Implementing Cloud-Scale Security with Lightwave

Lightwave meets the requirements of these use cases with its directory service, Active Directory interoperability, Kerberos authentication, and certificate services. Lightwave provides the following services:

- Directory services and identity management with LDAP and Active Directory interoperability
- Authentication services with Kerberos, SRP, WS-Trust (SOAP), SAML WebSSO (browser-based SSO), OAuth/OpenID Connect (REST APIs), and other protocols
- Certificate services with a certificate authority and a certificate store

Using these Lightwave security services in the cloud empowers IT security managers to impose the proven security policies and best practices of on-premises computing systems on their cloud computing environment. The Lightwave security services work in the cloud, in an on-premises data center, and in a hybrid cloud. The security frameworks, standards, and policies that come with Lightwave can follow users, applications, and workloads anywhere.

## Directory Services and Identity Management

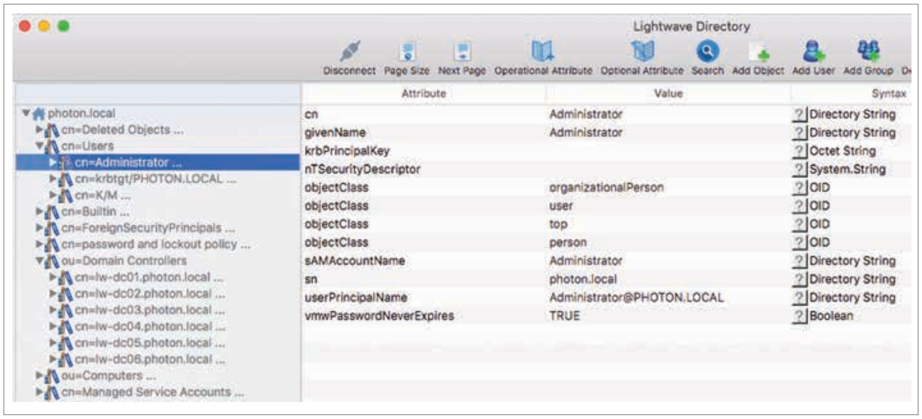
Lightwave is an extensible identity platform that works with multiple identity sources, including Microsoft Active Directory, LDAP, OpenLDAP, and MIT Kerberos with LDAP. The platform includes a REST API for LDAP, integrated DNS, and support for the System for Cross-domain Identity Management (SCIM). SCIM is an open standard that simplifies identity management in the cloud by automatically exchanging user identities with a REST API between domains.

At the core of Lightwave is a standards-based, AD-compatible LDAP 3 directory service with multimaster replication. The LDAP service, which can be managed with LDAP-compliant browsers, supports such operations as bind, add, modify, delete, search, extended operation, and controls. It manages users and groups, including nested groups, and provides policy-based password management.

The directory service uses the following secure data access mechanisms:

- Generic Security Service Application Program Interface (GSSAPI) over the Secure Remote Password protocol (SRP)
- Simple Authentication and Security Layer (SASL) over SRP

Designed for multitenancy, the directory service includes a hierarchical directory store that can accommodate multiple tenants at scale. A directory information tree (DIT) isolates the data of each tenant by placing each tenant in its own subtree. The ACL for a tenant's subtree is for only the tenant's own administrator. Each entry under a tenant gets its own ACL that is based on a security descriptor; each object, that is, receives its own ACL. Lightwave includes a tool for browsing and editing entries in the directory.



- photon.local
  - cn=Deleted Objects ...
  - cn=Users
    - cn=Administrator ...
    - cn=krbtgt/PHOTON.LOCAL ...
    - cn=K/M ...
  - cn=Builtin ...
  - cn=ForeignSecurityPrincipals ...
  - cn=password and lockout policy ...
  - ou=Domain Controllers
    - cn=lw-dc01.photon.local ...
    - cn=lw-dc02.photon.local ...
    - cn=lw-dc03.photon.local ...
    - cn=lw-dc04.photon.local ...
    - cn=lw-dc05.photon.local ...
    - cn=lw-dc06.photon.local ...
  - ou=Computers ...
  - cn=Managed Service Accounts ...

| Attribute | Value | Syntax |
|---|---|---|
| cn | Administrator | ? Directory String |
| givenName | Administrator | ? Directory String |
| krbPrincipalKey | | ? Octet String |
| nTSecurityDescriptor | | ? System.String |
| objectClass | organizationalPerson | ? OID |
| objectClass | user | ? OID |
| objectClass | top | ? OID |
| objectClass | person | ? OID |
| sAMAccountName | Administrator | ? Directory String |
| sn | photon.local | ? Directory String |
| userPrincipalName | Administrator@PHOTON.LOCAL | ? Directory String |
| vmwPasswordNeverExpires | TRUE | ? Boolean |

**Figure 1:** The built-in Lightwave directory management interface.

### REPLICATION FEATURES IN PROJECT LIGHTWAVE

- Performs deterministic conflict resolution
- Pulls changes from partners on a regular basis
- Uses attribute-level replication to replicate content deltas only
- Contains an efficient replication algorithm, which maintains UTDVector to achieve propagation dampening
- Uses the standard LDAP content synchronization protocol (RFC 4533)
- Offers flexible replication topology management
- Can change replication topology on the fly
- Can create one- or two-way replication

## Scalability and Performance

For scalability, the directory service includes an extensible LDAP schema, an active-active multimaster scheme, and dynamic indexing.

For performance, the directory service uses a Lightning Memory-Mapped Database (LMDB). It is an ACID-compliant persistent data store from OpenLDAP that has the following performance-enhancing features:

- B+ tree key-value store
- Single writer plus many readers
- Multi-version concurrency—the readers never block the writer
- Memory-mapped file with copy-on-write
- Write-ahead logging developed by VMware

## Replication

For replication, the directory service uses a state-based scheme for eventually consistent multi-node LDAP replication. Every directory node in a Lightwave domain accepts write requests. On Lightwave, the replication service includes a tool with a user interface and a single command to add or remove a node, which simplifies topology management. In addition, backup and restore is supported on a per-node basis. Overall, this approach to replication simplifies the life-cycle management of a domain.

## Architecture

The following architectural diagram summarizes the main components of the Lightwave directory service.

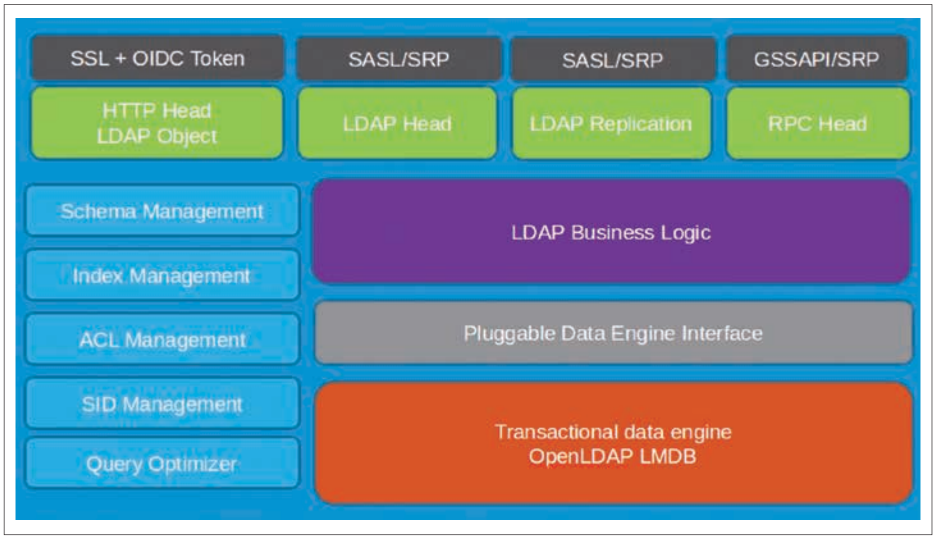


**Figure 2:** The architecture of the Lightwave directory service.

### Authentication Services

The authentication services of Lightwave contain two main components: A server that acts as a Kerberos 5 key distribution center and a secure token service that supports the OIDC, WS-TRUST, and SAML 2.0 (WebSSO) standards for single sign-on.

In Lightwave's converged identity model, Kerberos, OAuth 2.0, and OIDC are integrated with the LDAP directory server process.

The secure token service can issue Security Assertion Markup Language (SAML) 2.0 tokens as well as OIDC tokens. Lightwave can be integrated with Active Directory to issue secure tokens to principals defined in Active Directory forests. With SAML 2.0, Lightwave gives a user SSO access to different services by using the same credentials.

Lightwave works with OAuth 2.0 and OpenID Connect, a protocol for authentication and authorization that lets you set up one SSO service for different cloud services. After users enter their credentials to access one service, they don't need to do it again to access others.

Lightwave also works with the WS-Trust standard to issue and validate security tokens and to broker trust relationships between parties exchanging secure messages.

### Kerberos Key Distribution Center

The Kerberos key distribution center (KDC) handles authentication and authorization for Kerberized applications. LDAP, SASL, DCE/RPC, and GSSAPI applications can all use Kerberos. Security principals are stored in a replicated directory, and Kerberos service tickets are extended to include Lightwave authorization data.

### Features and Capabilities

The secure token service supports the WS-Trust, SAML, OAuth2 and OpenID Connect standards with the following capabilities:

- Browser-based single sign-on (SSO)
- Full multi-tenancy support
- External SAML Federation
- Just-in-time provisioning (JIT)
- IDP discovery and selection
- Multiple identity sources, including the native VMware directory, Microsoft Active Directory, and OpenLDAP
- Full Kerberos support and full AD domain trust support for integrating authentication with Microsoft Windows and Active Directory
- Schema customization for OpenLDAP to support a broad range of OpenLDAP deployments
- Two-factor smart card support with a common access card (CAC) or with an RSA SecurID token
- REST management APIs

### COMPONENTS IN THE LIGHTWAVE ARCHITECTURE

To summarize, the Lightwave security services form an architecture that comprises these components:

- The directory service and its directory store
- A Kerberos key distribution center that is integrated with the directory service
- An integrated DNS server
- A multi-protocol secure token service (STS) for authentication and authorization
- A certificate authority
- A certificate store

## Certificate Services

The Lightwave certificate service includes an X509-compliant certificate authority and a certificate store. The certificate authority issues and revokes certificates, and the certificate store holds certificates and keys. Together they provide a complete certificate management stack that integrates with LDAP and establishes user identities with Kerberos authentication.

### The Lightwave Certificate Authority

The certificate authority issues signed X.509 digital certificates and supports the PKIX standard. It can distribute CA roots and CRLs over HTTP and LDAP in accordance with RFC 4387. It also supports CSR and key generation as well as auto-enrollment and certificate revocation.

Secured and authenticated by Kerberos, the certificate authority validates certificate requests by analyzing key usage, extensions, SAN, and other factors. Server policies can be used to automatically approve or reject certificates.

The certificate authority has a dual mode in which it can act as an enterprise root CA or as a subordinate or intermediate CA. The key lengths are strong, ranging from 1 K to 16 K, and the hashing algorithms use SHA-1 or SHA-2, the latter of which is the default. The key usage is encryption and signing. The certificate file formats are PKCS12, PEM and JKS.

For administration, Lightwave lets you access the certificate authority with a user interface or command-line utilities, including diagnostic tools. It also supports certificate-auditing requirements.

### The Lightwave Certificate Store

The Lightwave endpoint certificate store holds certificates, private keys, and certificate revocation lists (CRLs). Lightwave controls access to the certificate store by using Kerberos. By default, only the user who created the store—that is, the owner—has access. The certificate store typically contains three kinds of entries:

- A private key associated with a certificate or certificate chain
- A certificate of a trusted entity
- A certificate revocation list published by the Lightwave certificate authority

## Addressing the Use Cases

Returning to the use cases described earlier, this section briefly summarizes how the Lightwave security suite supplies a solution to each use case.

| USE CASE | SOLUTION |
|---|---|
| Hybrid Data Center | By implementing Lightwave in a public cloud in the United States and replicating data from its AD cluster in Tokyo to it nightly, the Lightwave directory service can contain the organizational units that the Tokyo company needs to authenticate and authorize users in the United States as they access the applications running in a public cloud in the United States. Implementing Lightwave eliminates the application-access latency that would otherwise occur if the company had to use its AD cluster in Tokyo. |
| Stand-Alone Directory Service in the Cloud | Lightwave fulfills this use case by enabling companies to implement a separate forest or organizational unit in the cloud to provide LDAP support to applications and users in the cloud. |
| Directory Managed by a Cloud Provider | Lightwave can be implemented and run by a cloud provider. The cloud provider's customers can then use it as a cloud-based domain controller running in active-active mode with an on-premises directory service or as a stand-alone directory service. |
| Bridge to Identity as a Service | With its support for a multitude of security protocols, Lightwave can serve as an intermediary between a company's on-premises directory service and a cloud-provider's stand-alone identity as a service (IDaaS) system. The Lightwave directory service can synchronize user principals and other metadata from a company's on-premises directory to a cloud provider's IDaaS tenant. |

### Lightwave in vSphere and vCenter

Lightwave acts as the directory service, authentication engine, secure token service, lookup service, certificate authority, and certificate store in deployments of VMware vCenter® and VMware vSphere® 6. In addition, Lightwave lets system administrators join a vCenter instance to Active Directory. In vSphere 6, the Lightwave components are collectively known as the VMware Platform Services Controller (PSC). It handles such security functions as single sign-on and certificate management.

vCenter provides an example of how Lightwave delivers single sign-on to an enterprise platform. When a user authenticates with the Lightwave identity management service on vCenter, the user receives a SAML token issued by the embedded Lightwave secure token service. With the SAML token, the user can then use any vCenter service (and perform actions the user has privileges for) without having to sign in again. The vCenter single sign-on service signs tokens with a signing certificate and stores the token-signing certificate. The service's certificate is also stored.

### Identity Federation Across Data Centers

The role of Lightwave in Photon Platform illustrates how Lightwave meets the requirements of a use case to establish a system for identify federation across data centers. VMware Photon™ Platform delivers compute, storage, and networking infrastructure that is optimized for running containerized applications. The platform combines VMware Photon Controller with Project Lightwave, VMware NSX®, and VMware vSAN™. Photon Controller manages virtualized infrastructure and supplies Kubernetes as a service to securely run containerized workloads at scale. NSX provides software-defined virtualized networking. vSAN establishes a virtual storage area network.

Photon OS and Harbor also play a role in Photon Platform's architecture. Photon OS is a minimalist Linux host optimized for running containerized applications. Harbor provides an enterprise container registry with role-based access control and a web interface.

Lightwave secures Photon Platform. Lightwave authenticates and authorizes users as they work with the system and manage Kubernetes clusters. System administrators and DevOps can create security groups in Lightwave to control access to Photon Platform within the context of the platform's model of multitenancy. Harbor also uses the Lightwave directory service to control access to the resources stored in Harbor registries.

The following diagram illustrates how the component architecture of Photon Platform delivers infrastructure as a service with identify federation across geo-distributed data centers. Photon Platform gives tenants on-demand, self-service

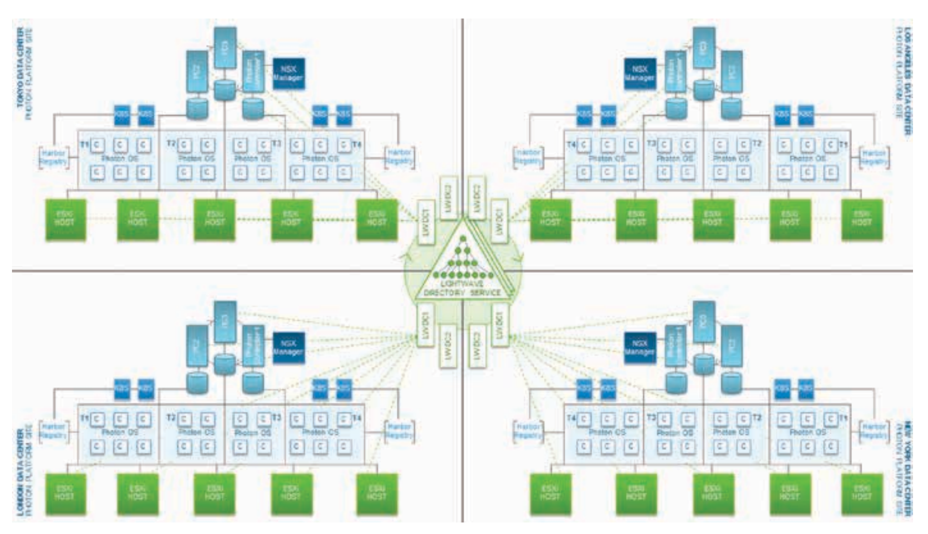


**Figure 3:** Lightwave acting as the identity and access management system for geo-distributed data centers running Photon Platform.

access to such IaaS resources as virtual machines, persistent storage disks, virtualized subnets, and Kubernetes clusters.

In this example, Lightwave secures Photon Platform in geo-distributed data centers with converged identity management. The quadrant showing the London data center, for instance, contains a Photon Platform site. The Photon Controller management machines and the ESXi hypervisors are connected to the redundant Lightwave domain controllers that form a ring around the diagram's centerpiece—the multitenant, multimaster Lightwave directory service. Lightwave also controls access to the Kubernetes clusters running on Photon Platform in the data center by implementing OpenID Connect for authentication. Lightwave helps ensure that only authorized users can connect to Kubernetes clusters.

### Identity Federation Across Data Centers and Public Clouds

Again taking Photon Platform as an example, the following diagram demonstrates how the Lightwave directory service and its domain controllers can act as the security platform for operations that range from an on-premises data center in Tokyo to other geo-distributed data centers that each use a different public cloud service:

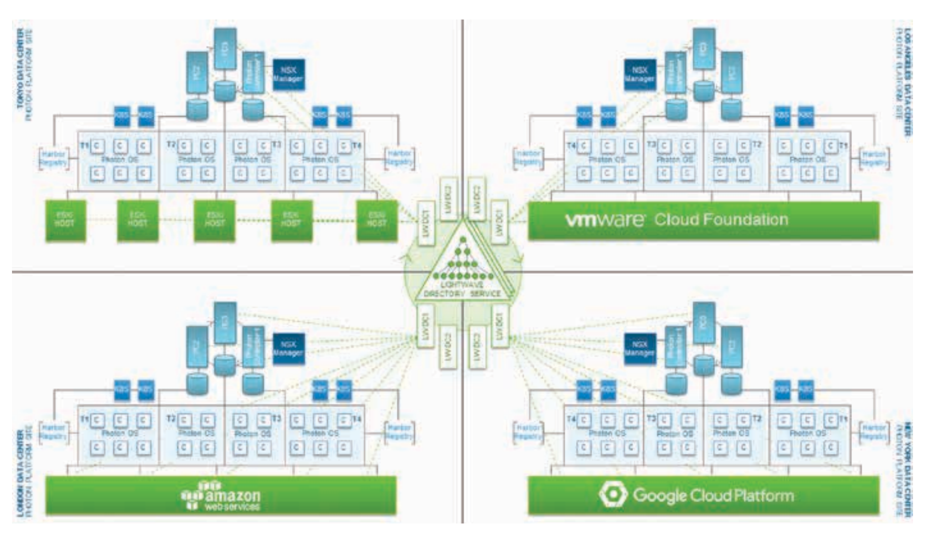


**Figure 4:** Lightwave acting as the identity and access management system for geo-distributed data centers using different cloud platforms.

In this architecture, Photon Platform is merely an example of a platform that uses Lightwave for identity and access management. With its capability to interoperate with other platforms by using standard protocols and tools, Lightwave can serve as the security system for various platforms.

## Plugging into the Cloud

Lightwave is designed for the cloud. As a cloud administrator or DevOps manager, you can implement Lightwave in, for instance, the Amazon and Google clouds to provide identity and security services for your machines, users, and applications in the cloud.

In addition, the pluggable architecture of Lightwave allows you, as an architect at a cloud provider such as a Google or Amazon, to integrate Lightwave into your cloud and extend its capabilities as identity services to your customers.

### Instant Integration with Photon OS

Lightwave provides security services to Photon OS, an open-source minimalist Linux operating system from VMware optimized for running containers. You can use Lightwave to join a Photon OS virtual machine to the Lightwave directory service and then authenticate users with Kerberos.

Because the Photon OS repository includes the Lightwave packages, installing the packages for either Lightwave client or the server is simple. Here's an example of installing the Lightwave server packages on a virtual machine running Photon OS:

```
tdnf install vmware-lightwave-server

Installing:

apache-ant                noarch   1.10.1-1.ph2dev    3.66 M
vmware-dns-client         x86_64   1.2.0-1.ph2dev     614.42 k
apache-tomcat             noarch   8.5.13-2.ph2dev    8.59 M
commons-daemon            x86_64   1.0.15-9.ph2dev    79.41 k
jansson                   x86_64   2.10-1.ph2dev      74.52 k
vmware-sts-client         x86_64   1.2.0-1.ph2dev     41.09 M
vmware-sts                x86_64   1.2.0-1.ph2dev     67.91 M
vmware-afd                x86_64   1.2.0-1.ph2dev     763.81 k
vmware-dns                x86_64   1.2.0-1.ph2dev     344.19 k
vmware-directory          x86_64   1.2.0-1.ph2dev     4.03 M
vmware-ca-client          x86_64   1.2.0-1.ph2dev     501.53 k
vmware-ic-config          x86_64   1.2.0-1.ph2dev     114.89 k
likewise-open             x86_64   6.2.11-1.ph2dev    11.26 M
vmware-afd-client         x86_64   1.2.0-1.ph2dev     931.89 k
vmware-directory-client   x86_64   1.2.0-1.ph2dev     714.02 k
vmware-ca                 x86_64   1.2.0-1.ph2dev     206.27 k
vmware-lightwave-server   x86_64   1.2.0-1.ph2dev     0.00 b
Total installed size:     140.78 M
```

(In the names of the packages, "afd" stands for authentication framework daemon; "ic" stands for infrastructure controller, which is Lightwave's internal name for its domain controller. Several of the packages, such as Jansson and Tomcat, are used by Lightwave for Java services or other tooling.)

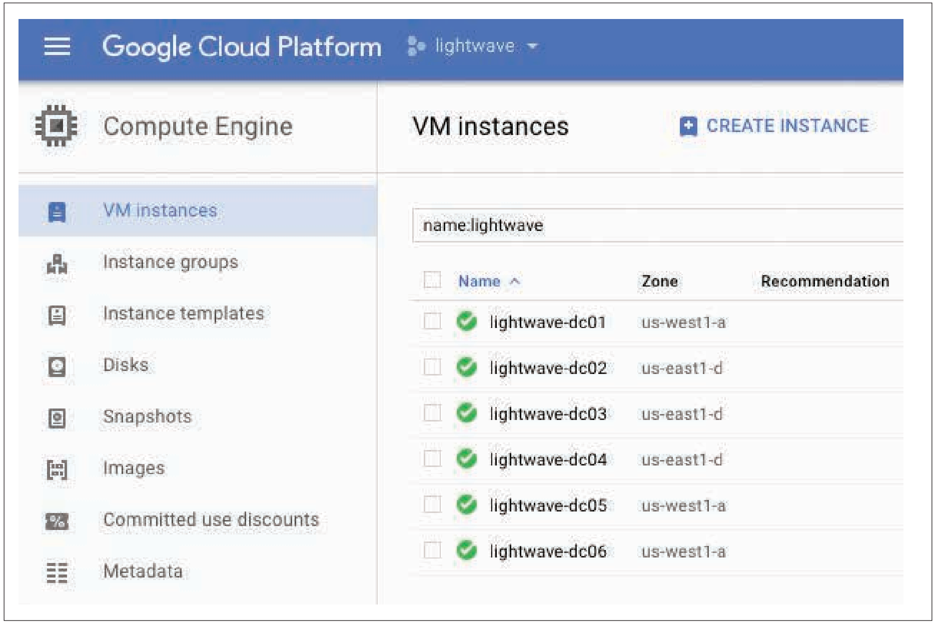
The convenience and expedience of being able to instantly install the Lightwave packages from a secure, signed VMware repository become even more significant when the cloud-ready image of Photon OS runs on Amazon Elastic Cloud Compute or Google Compute Engine. The Amazon machine image of Photon OS and the Google Compute Engine version of Photon OS are available as free downloads on Bintray.

### Deploying Lightwave on Google

Cloud administrators and DevOps personnel can rapidly deploy Lightwave on Google Compute Engine by using Photon OS or another Linux image, such as Ubuntu. The process goes like this:

- Set up firewall rules and open ports for Lightwave DNS, LDAP, STS, and the other Lightwave services.
- Upload the freely available Photon OS image for GCE.
- Create a Photon OS instance, set the hostname for your Lightwave instance, and set the instance to use Lightwave for DNS.
- Install Lightwave from the Photon OS repository.
- Promote the first Lightwave domain controllers and add more of them if you want.

For instructions on how to set up Lightwave on GCE, see Lightwave on GitHub.



name:lightwave

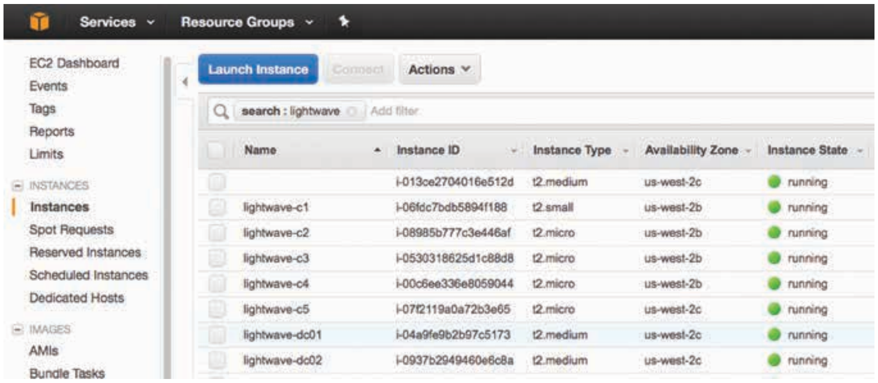
| Name | Zone | Recommendation |
|---|---|---|
| lightwave-dc01 | us-west1-a | |
| lightwave-dc02 | us-east1-d | |
| lightwave-dc03 | us-east1-d | |
| lightwave-dc04 | us-east1-d | |
| lightwave-dc05 | us-west1-a | |
| lightwave-dc06 | us-west1-a | |

**Figure 5:** Lightwave domain controllers running on Google Cloud Platform.

After deploying and promoting the Lightwave domain controllers, you can see them in the GCE web interface:

### Deploying Lightwave on AWS

Lightwave can run on Photon OS on Amazon Elastic Compute Cloud to provide identity services to your machines, users, and applications running in the Amazon cloud. The process of deploying Lightwave on EC2 entails creating a Photon OS instance, setting firewall rules to open several ports, setting a hostname for the machine, installing the Lightwave server components, and promoting a Lightwave domain controller. Once deployed, the Lightwave domain controllers appear in the EC2 Dashboard:



| Name | Instance ID | Instance Type | Availability Zone | Instance State |
|---|---|---|---|---|
| | i-013ce2704016e512d | t2.medium | us-west-2c | ● running |
| lightwave-c1 | i-06fdc7bdb5894f188 | t2.small | us-west-2b | ● running |
| lightwave-c2 | i-08985b777c3e446af | t2.micro | us-west-2b | ● running |
| lightwave-c3 | i-0530318625d1c88d8 | t2.micro | us-west-2b | ● running |
| lightwave-c4 | i-00c6ee336e8059044 | t2.micro | us-west-2b | ● running |
| lightwave-c5 | i-07f2119a0a72b3e65 | t2.micro | us-west-2c | ● running |
| lightwave-dc01 | i-04a9fe9b2b97c5173 | t2.medium | us-west-2c | ● running |
| lightwave-dc02 | i-0937b2949460e6c8a | t2.medium | us-west-2c | ● running |

**Figure 6:** Lightwave domain controllers running on Amazon EC2

For more information, see Lightwave on GitHub.

## Conclusion

Lightwave provides a directory service, Active Directory interoperability, Kerberos authentication, and certificate services to meet the requirements of a range of uses cases.

Using Lightwave security services in the cloud empowers IT administrators and DevOps managers to impose the proven security policies and best practices of on-premises computing systems on their cloud computing environment. The security standards and protocols that come with Lightwave can work across clouds, on-premises data centers, and hybrid clouds.

**VMware, Inc.** 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com